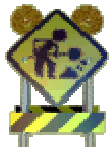
"Come si fa" a svolgere vari tipi di esercizi

2 – gruppi



(algoritmi – avvertenze – casi speciali – esempi) Attenzione… gli argomenti non sono in ordine, poiché sono pensati per essere svolti al termine della teoria. Quindi si usa il metodo migliore per risolverli, anche se nella teoria è presentato più avanti della definizione.

Alcuni degli esercizi presentati erano parte di temi d'esame, e le lettere che compaiono hanno i seguenti significati:
Matricola(**N**) data di nascita (**G**/**M**/**A**)
n:= N mod 1000; g:= (G mod 5) + 4; m:= (M mod 6) + 2; a:= A mod 100

Gruppi di sostituzioni

Per le definizioni, vedi dispense.
Ogni permutazione (o sostituzione) può esser scritta, in modo unico, come prodotto di cicli disgiunti. Il prodotto di permutazioni può essere svolto direttamente, o con le permutazioni scritte come prodotto di cicli disgiunti.
Cicli disgiunti commutano: $p\,q = q\,p$, quindi $(p\,q)^2 = p^2\,q^2$ ecc.
Ogni permutazione può essere scritta in vari modi come prodotto di trasposizioni (o scambi) ma il numero di tali scambi è sempre pari o sempre dispari. Se è un ciclo di lunghezza k, il numero minimo di scambi possibili è $k-1$. Se la permutazione è prodotto di cicli, disgiunti o meno, uno di tali prodotti si ottiene accostando gli scambi con cui vengono ottenuti i vari cicli. Ad esempio il quadrato di una permutazione pari è pari, quello di una permutazione dispari è pari; il prodotto di una permutazione dispari per una pari è dispari ecc.

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

Esempio 2: In S_7 il prodotto di cicli (non disgiunti) $(5\ \ 2\ \ 1\ \ 4)(2\ \ 6\ \ 1\ \ 7)(3\ \ 4\ \ 2\ \ 6)$ è

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

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

Esempio 3: In S_7 il prodotto di cicli (non disgiunti)
$p = (2\ 5\ 3\ 7)(1\ 4\ 3\ 6\ 7)(4\ 2\ 7\ 1)(3\ 5\ 4\ 6)$
$1 \to 1 \to 4 \to 3 \to 7$ si parte dal primo elemento e lo si segue
$7 \to 7 \to 1 \to 4 \to 4$ si riparte dall'elemento a cui si era arrivati
$4 \to 6 \to 6 \to 7 \to 2$ si continua allo stesso modo
$2 \to 2 \to 7 \to 1 \to 1$ il ciclo si è chiuso perché si è ottenuto l'elemento di partenza.
$3 \to 5 \to 5 \to 5 \to 3$ l'elemento sta fermo
$5 \to 4 \to 2 \to 2 \to 5$ l'elemento sta fermo
$6 \to 3 \to 3 \to 6 \to 6$ l'elemento sta fermo ⇨ $p = (1\ 7\ 4\ 2)(3)(5)(6) = (1\ 7\ 4\ 2)$

Esempio 4: Se $f = (1\ 5)\ (2\ 3\ 4)$, calcolare f^2, f^3, f^4 e stabilirne la parità.
$f = (1\ 5)\ (2\ 3\ 4) = (1\ 5)(2\ 4)(2\ 3)$ ⇨ dispari
$f^2 = (2\ \ 4\ \ 3) = (2\ 4)(2\ 3)$, ma anche $(1\ 5)(2\ 4)(2\ 3)(1\ 5)(2\ 4)(2\ 3)$ ⇨ pari
$f^3 = (1\ 5)$ ⇨ dispari
$f^4 = (2\ 3\ 4) = (2\ 4)(2\ 3)$ ⇨ pari

Esempio 5: Se $f = (1\ 5\ 2\ 4\ 3)$, calcolare, f^{-1}
L'inverso di un ciclo si ottiene partendo dal primo elemento (1 in questo caso) e percorrendo il ciclo "dal fondo" cioè f: 1⇨5⇨2⇨4⇨3 f^{-1}: 1⇦5⇦2⇦4⇦3 quindi f^{-1}= (1 3 4 2 5)

Esempio 6: In S_7 consideriamo p= (1 3 7). Trovare alcune permutazioni che commutano con p.
Ci sono sicuramente almeno queste:
Id, che commuta con tutte, (1 7 3) l'inversa (che coincide col quadrato)
(2 4), (2 5), (2 6), (4 5), (4 6) ,(5 6), i cicli disgiunti da p di periodo 2
(2 4 5), (2 4 6), (2 5 6), (4 5 6), (2 5 4), (2 6 4), (2 6 5),(4 6 5) , i cicli disgiunti da p di periodo 3
(2 4 5 6), (2 6 5 4), (2 5 6 4), (2 4 6 5), (2 6 4 5), (2 5 4 6) i cicli disgiunti da p di periodo 4
(2 5)(4 6), (2 6)(4 5), (2 4)(5 6) prodotti possibili di quelli di periodo 2.

Esercizi

- Trasformare in prodotto di cicli disgiunti:
  - $\begin{pmatrix}1&2&3&4&5&6\\5&2&1&3&6&4\end{pmatrix}$ (1 6 5 4 3)
  - $\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&4&1&5&3&8&6&7&9\end{pmatrix}$ (1 2 4 5 3)(6 8 7)
  - $\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$ (1 4)(2 3)
  - $\begin{pmatrix}1&2&3&4&5&6\\2&5&3&6&1&4\end{pmatrix}$ (1 2 5)(4 6)
  - $\begin{pmatrix}1&2&3&4&5\\2&4&5&3&1\end{pmatrix}$ (1 2 4 3 5)
- Eseguire i prodotti seguenti:
  - (1 3 2 4 6)(2 4 3 5 7)(3 1 7 5 4 2) (1 4 6)(2 5)
  - (1 4 2 6 5)(2 5 3 6)(1 6 2 4 3)(2 4 5 6) (1 6 2 5) (3 4)
  - (1 4 2 7 6 5)(2 5 3 6)(1 6 7 4 3)(2 4 5 6) (1 7 2 5 6) (3 4)
  - (2 8 3 6)(1 5 7 2 3)(1 2 4 5 6) (1 6 5 2 4 7 8 3)
- Provare che (1 3)¤(2 4) = (1 4)¤(1 2)¤(4 3)¤(1 4) = (4 2)¤(4 1)¤(4 3)¤(4 1)
- Scrivere come prodotto di cicli disgiunti e stabilire se è pari o dispari:
  - (1 5 2 8)(3 7 2 4 5 8)(1 4 8 3 6) (1 2 4 3 6 5) (8 7) pari
  - (0 5 2 8 1)(4 9 6 1)(2 8 3)(0 2 4 9 3) (0 1 4 6) (3 5 2 9 8) dispari
  - (1 5 3 8 6)(2 8 6)(3 8 6)(1 2 4 9 3) (1 6 8 2 4 9) (3 5) pari
- Sia $f = \begin{pmatrix}1&2&3&4&5\\1&4&3&5&2\end{pmatrix}$. Esiste una sostituzione g (a parte l'identità) tale che $g\,f = f\,g$? In caso affermativo determinare g.

Periodo di un elemento in un gruppo finito

Il periodo di un elemento è il più piccolo esponente a cui si deve elevare l'elemento per avere il neutro.
Nel caso di sostituzioni scritte come prodotto di cicli disgiunti il periodo è uguale al mcm del periodo dei cicli, che coincide con la loro lunghezza.
Alcune proprietà del periodo sono legate ai sottogruppi generati dalle potenze (che nelle dispense si fanno dopo) ad esempio il periodo di un elemento è un divisore dell'ordine del gruppo.

Esempio 1: Che periodo hanno gli elementi di $(Z^*_{12},\times)=\{1, 5, 7, 11\}$?
Periodo di 1 ⇨1 è così sempre per l'elemento neutro di ogni gruppo, per convenzione sulle potenze.
Periodo di 5 $5^2 = 25 \equiv 1 \bmod 12$ ⇨ 2
Periodo di 7 $7^2 \equiv 1 \bmod 12$ ⇨ 2
Periodo di 11 $11^2 \equiv 1 \bmod 12$ ⇨ 2

Esempio 2: Che periodo hanno gli elementi di $(Z_5,+)$?
Periodo di 0 ⇨1
Periodo di 1 $1^2=2$ $1^3=3$ $1^4=4$ $1^5\equiv0$ ⇨ 5
Periodo di 2 $2^2=4$ $2^3=6\equiv1$ $2^4=3$ $2^5=5\equiv0$ ⇨ 5
Periodo di 3 $3^2=6\equiv1$ $3^3=9\equiv4$ $3^4=7\equiv2$ $3^5=5\equiv0$ ⇨ 5
Periodo di 4 $4^2=8\equiv3$ $4^3=7\equiv2$ $4^4=6\equiv1$ $4^5=5\equiv0$ ⇨ 5

Esempio 3: Che periodo hanno gli elementi di $(Z_6,+)$?
Periodo di 0 ⇨ 1
Periodo di 1 $1^2=2$ $1^3=3$ $1^4=4$ $1^5\equiv5$ $1^6\equiv0$ ⇨6
Periodo di 2 $2^2=4$ $2^3=6\equiv0$ ⇨3
Periodo di 3 $3^2=6\equiv0$ ⇨ 2
Periodo di 4 $4^2=8\equiv2$ $4^3=6\equiv0$ ⇨ 3
Periodo di 5 $5^2= 10 \equiv 4$ $5^3\equiv3$ $5^4\equiv2$ $5^5\equiv1$ $5^6\equiv0$ ⇨ 6

Esempio 4: Che periodo ha il ciclo p = (1 3 6 8 2 5 4)?
ha periodo 7, coincidente col numero dei suoi elementi (lunghezza del ciclo), infatti:
$(1\ 3\ 6\ 8\ 2\ 5\ 4)^2 = (1\ 6\ 2\ 4\ 3\ 8\ 5)$ $(1\ 3\ 6\ 8\ 2\ 5\ 4)^3 = (1\ 8\ 4\ 6\ 5\ 3\ 2)$
$(1\ 3\ 6\ 8\ 2\ 5\ 4)^4 = (1\ 2\ 3\ 5\ 6\ 4\ 8)$ $(1\ 3\ 6\ 8\ 2\ 5\ 4)^5 = (1\ 5\ 8\ 3\ 4\ 2\ 6)$
$(1\ 3\ 6\ 8\ 2\ 5\ 4)^6 = (1\ 4\ 5\ 2\ 8\ 6\ 3)$ p^7=id.
Oss: 1+6=7 2+5=7, 3+4=7 quindi p^6 è l'inversa di p, p^5 è l'inversa di p^2, p^3 è l'inversa di p^4.

Esempio 5: Che periodo ha p = (1 3 5 2) (4 6 7) che è data da un prodotto di cicli disgiunti?
I due cicli hanno rispettivamente lunghezza 4 e 3, p ha come periodo mcm(4, 3)=12, infatti:
$p = (1\ 3\ 5\ 2)(4\ 6\ 7)$ $p^2 = (1\ 5)(3\ 2)(4\ 7\ 6)$ $p^3 = (1\ 2\ 5\ 3)$ $p^4 = (4\ 6\ 7)$
$p^5 = (1\ 3\ 5\ 2)(4\ 7\ 6)$ $p^6 = (1\ 5)(3\ 2)$ $p^7 = (1\ 2\ 5\ 3)(4\ 6\ 7)$ $p^8 = (4\ 7\ 6)$
$p^9 = (1\ 3\ 5\ 2)$ $p^{10} = (1\ 5)(3\ 2)(4\ 6\ 7)$ $p^{11} = (1\ 2\ 5\ 3)(4\ 7\ 6)$ p^{12} = id

---

Esempio 6: Sia p un elemento di periodo 12. Stabilire che periodo hanno p^3, p^5, p^8, p^9, p^{10}.
Sappiamo dall'ipotesi che p^{12} = id. Allora $(p^3)^4$= id, quindi p^3 ha periodo 4, MCD(5,12)=1, quindi p^5 ha periodo 12; MCD(8,12) = 4, allora mcm(8,12)= $\frac{8\cdot12}{4}=24$, quindi p^8 ha periodo 3, che è la più piccola potenza di p^8 che dà id. Risulta 3 = 12/ MCD(8,12). Analogamente p^9 ha periodo 4=12/MCD(9,12) e p^{10} ha periodo 6=12/MCD(10,12).

Esercizi

- Determinare il periodo di p=(1 4 2 6 7 3 8 5), indicandone le potenze.
- Determinare il periodo di p =(1 3 5)(2 4) = $r\,s$, indicandone le potenze.
- Si considerino le permutazioni di S_7 : p = (1253)∘(124)∘(127) e q =(124)∘(126). Scrivere p, q, $q\circ p$ e $p\circ q$ come prodotto di cicli disgiunti e calcolarne il periodo.
- Se g ha periodo 24, che periodo hanno g^4, g^6, g^{18}, g^{21}, g^{46}, g^{412}? Serve sapere qualcosa sul gruppo di cui g è elemento?
- Se g ha periodo 20, che periodo hanno g^4, g^6, g^{18}, g^{12}, g^{15}, g^{14}?

- Si consideri la seguente permutazione p di S_8: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 8 & 4 & 2 & 6 & 1 \end{pmatrix}$.
  - scrivere p come prodotto di cicli disgiunti e stabilire se è pari o dispari
  - determinare il periodo di p, p^3 e p^5
- Nel gruppo simmetrico S_{10} sia k la permutazione così ottenuta:
  - si accostino g, m, a ed N (ad es. 9 11 77 440155) ;
  - si suddividano le cifre in tre gruppi di 2, 2, 3 cifre e le restanti [es. (9 1)(1 7)(7 4 4)(0 1 5 5)]
  - se in un gruppo ci sono cifre ripetute si eliminino quelle più a destra [es. (9 1)(1 7)(7 4)(0 1 5)]
  - si esegua il prodotto dei cicli ottenuti.
  - si scomponga k in cicli disgiunti e in prodotto di trasposizioni stabilendo se k è pari o dispari
  - si determini il periodo di k.
  - Si determini, senza eseguire i conti delle potenze, il periodo di k^g, di k^m, di k^a

Sottogruppi

Un sottoinsieme è sottogruppo se è a sua volta gruppo, ma la definizione è scomoda per le verifiche. C'è una condizione necessaria (il sottoinsieme deve contenere il neutro) che serve a eliminare vari casi, ma per la verifica serve il criterio: se g e h sono generici elementi dell'insieme, anche $g\ h^{-1}$ deve appartenere all'insieme.
Proprietà:

- L'ordine di un sottogruppo è un divisore dell'ordine del gruppo, ma non è detto che ci sia un sottogruppo che abbia come ordine ogni divisore dell'ordine del gruppo, né che ce ne sia uno solo per ogni ordine. Esistenza e unicità sono garantite solo per i gruppi ciclici.
- Tra i vari sottogruppi di un gruppo ci sono quelli *generati* dagli elementi del gruppo, attraverso le loro potenze. Sono i soli esistenti nel caso il gruppo di partenza sia ciclico.
- Laterale di un sottogruppo è l'insieme di tutti gli elementi ottenuti eseguendo l'operazione del gruppo tra un elemento, detto rappresentante, e tutti gli elementi del sottogruppo. I laterali di un sottogruppo non sono sottogruppi, a meno che il rappresentante non appartenga al sottogruppo (nel qual caso il laterale coincide col sottogruppo). I laterali di un sottogruppo di un gruppo finito, hanno lo stesso numero di elementi del sottogruppo stesso.
- I laterali di un sottogruppo costituiscono una partizione del gruppo.

Esempio 1: Si consideri il gruppo S_6

- Scrivere la permutazione α =(2 6 3 5)(4 6 5)(3 4 6)(1 5 3) come prodotto di cicli disgiunti
- stabilire se α è pari o dispari
- determinare l'ordine del sottogruppo H di S_6 generato da α e indicarne gli elementi
- determinare gli elementi del laterale destro di A individuato da (1 2 3).

Risulta α = (1 4 2 6 5 3)
È α = (1 3)(1 5)(1 6)(1 2)(1 4) quindi è dispari
Il sottogruppo H ha ordine 6, uguale al periodo di α. Risulta: H ={α, α^2, α^3, α^4, α^5, α^6=id}=
{α=(1 4 2 6 5 3), α^2=(1 2 5)(3 4 6), α^3=(1 6)(2 3)(4 5), α^4=(1 5 2)(3 6 4), α^5=(1 3 5 6 2 4), id}
Il laterale richiesto è costituito dagli elementi: {(1 4 2 6 5 3)(1 2 3), (1 2 5)(3 4 6)(1 2 3),
(1 6)(2 3)(4 5)(1 2 3), (1 5 2)(3 6 4)(1 2 3), (1 3 5 6 2 4)(1 2 3), (1 2 3)} =
{(1 6 5 3 4 2), (1 5)(2 4 6 3), (1 3 6)(4 5), (2 6 4 3 5), (1 4)(2 5 6), (1 2 3)}

Esempio 2: determinare i sottogruppi di (Z^*_{12},×) = {1, 5, 7, 11}.
Sappiamo che periodo hanno gli elementi di (Z^*_{12},×)

Periodo di 5 $5^2 \equiv 1 \bmod 12$ ⇨ è 2 quindi $\{1, 5\}$ è sottogruppo di $(Z^*_{12},\times)$
Periodo di 7 $7^2 \equiv 1 \bmod 12$ ⇨ è 2 quindi $\{1, 7\}$ è sottogruppo di $(Z^*_{12},\times)$
Periodo di 11 $11^2 \equiv 1 \bmod 12$ ⇨ è 2 quindi $\{1, 11\}$ è sottogruppo di $(Z^*_{12},\times)$
Ne esistono altri? Sicuramente NO: gli ordini possibili dei sottogruppi sono solo 1, 2, 4; i sottogruppi di ordine 1 o 4 sono impropri e di ordine 2 non ne possono esistere altri: devono contenere solo l'identità e un elemento, e quindi sono solo quelli.

Esempio 3: determinare i sottogruppi di $(Z^*_{16},\times) = \{1, 3, 5, 7, 9, 11, 13, 15\}$.
Z^*_{16} ha ordine 8. I divisori di 8 sono 1, 2, 4, 8 ma 1 e 8 danno i sottogruppi impropri. Cerchiamo dapprima i sottogruppi ciclici:
1 {1}
3 {3, 9, 11, 1}
5 {5, 9, 13, 1}
7 {7, 1}
9 {9, 1}
11 {11, 9, 3, 1}
13 {13, 9, 5, 1}
15 {15, 1} questi sono TUTTI i sottogruppi generati dagli elementi.
Ce ne sono altri? Potrebbero: ci sono elementi di periodo 2 che potrebbero essere contenuti in sottogruppi propri di ordine 4: proviamo a costruire il sottogruppo che contiene 7 e 9… deve contenere anche 7^2, 9^2 e 7×9, quindi si trova $\{7, 9, 1, 15\}$ non generato da nessun elemento o con due generatori, 7 e 9; si verifica con pochi conti che anche i prodotti degli altri elementi stanno nel sottoinsieme.

Esercizi

- Stabilire quali dei seguenti sottoinsiemi sono sottogruppi dei gruppi assegnati:
  - L'insieme dei numeri pari o dei numeri dispari in $(Z,+)$
  - I quadrati perfetti in $(Z,+)$
  - Il sottoinsieme di $(Q_0,\times)$ o $(Q_0,+)$ formato da tutte le frazioni egiziane (con numeratore 1) $\{1, 1/2, 1/3, 1/4, 1/5, ...\}$
  - L'insieme $(\{1,-1\},\times)$ in Q o in R.
  - Se $n < m$, $(Z_n,+)$ in $(Z_m,+)$
  - Le potenze di 2 in $(Z,+)$
- Si consideri il gruppo S_6
  - Scrivere la permutazione $\alpha = (1\ 6\ 3\ 5)(4\ 2\ 6\ 5)(3\ 5\ 4\ 6)(1\ 5\ 4)$ come prodotto di cicli disgiunti
  - stabilire se α è pari o dispari
  - determinare l'ordine del sottogruppo X di S_6 generato da α e indicarne gli elementi
  - determinare gli elementi del laterale destro di A individuato da (1 2 3).
  - Determinarne tutti i sottogruppi.
- Si consideri un gruppo $(G,\circ)$ di a elementi. Quali delle seguenti affermazioni sono vere?
  - G può ammettere un sottogruppo di ordine m e un sottogruppo di ordine g.
  - Se $z \in G$, $z^{2a} = u$ (ove u è l'unità del gruppo).

Gruppi ciclici

I gruppi ciclici sono un particolare tipo di gruppi, i cui elementi sono tutte potenze di uno stesso elemento detto generatore. Sono quindi tutti abeliani.
Abbiamo già detto più sopra le caratteristiche dei sottogruppi di un gruppo ciclico: sono tutti gruppi ciclici e ne esiste uno e uno solo per ogni divisore dell'ordine del gruppo.

Abbiamo già visto che gruppi non ciclici, e addirittura non abeliani, hanno sottogruppi ciclici: quelli generati dai vari elementi.
I gruppi $(Z_n,+)$ sono tutti ciclici, poiché 1 è un loro generatore.
I gruppi $(Z^*_p, \times)$ sono ciclici se p è primo, ma il generatore non è così evidente.
I gruppi $(Z^*_n, \times)$, con n non primo, non è detto che siano ciclici.
Tutte le potenze di un eventuale generatore con esponente primo col periodo del generatore sono a loro volta generatori.

Esempio 1: Trovare un generatore diverso da 1 nel gruppo $(Z_8,+)=\{0, 1, 2, 3, 4, 5, 6, 7\}$.
È notoriamente inutile provare il neutro, che genera sempre solo sé stesso.

2 4 6 0	NO
3 6 1 4 7 2 5 0	Sì
4 0	NO
5 2 7 4 1 6 3 0	Sì
6 4 2 0	NO
7 6 5 4 3 2 1 0	Sì …… sono generatori gli elementi primi con 8.

Questa proprietà è comune a tutti gli $(Z_n, +)$: i generatori sono i numeri primi con n.

Esempio 2: Si stabilisca se il gruppo $(Z^*_{15},\times)$ è ciclico. Se ne determinino tutti i possibili sottogruppi.
$(Z^*_{15},\times) = \{1, 2, 4, 7, 8, 11, 13, 14\}$ ordine 8
Costruiamo i sottogruppi generati dagli elementi.
{2, 4, 8, 1} {4, 1} {7, 4, 13, 1} {8, 4, 2, 1} {11, 1} {13, 4, 7, 1} {14, 1} non è ciclico perché nessun elemento ha periodo 8.
Si noti che 2 e $8=2^3$ generano lo stesso sottogruppo di ordine 4 (come pure 7 e $13=7^3$) poiché MCD(1,4) = MCD(3,4)=1.
Oss. Abbiamo detto che tutte le potenze di un eventuale generatore con esponente primo col periodo del generatore sono a loro volta generatori. Quindi se fosse stato ciclico generato da un elemento a, essendo di ordine 8 anche a^3, a^5, a^7 sarebbero stati generatori, e non potevano esserci due sottogruppi diversi di ordine 4, ma solo quello costituito da a^2, a^4, a^6, a^8 e uno solo di ordine 2, costituito da a^4, a^8.
Ammette altri sottogruppi?
È possibile, dal momento che esistono elementi di periodo 2 e il massimo ordine possibile per i sottogruppi propri (per il teorema di Lagrange) è 4. Se esistono altri sottogruppi, non possono contenere gli elementi di periodo 4, perché altrimenti conterrebbero tutto il sottogruppo da essi generato, e quindi coinciderebbero col gruppo.
Un eventuale sottogruppo non ciclico può contenere ad esempio, 11 e 14, ma allora contiene anche 4 che è il loro prodotto e 1 che è il loro quadrato.
Si trova quindi il sottogruppo non ciclico {11, 14, 1, 4}

Esempio 3: $(Z^*_n, \times)$ Proviamo a vedere alcuni valori di n non primo:

gruppo	Elementi	ord	Ciclico?	generatori	Sottogruppi non banali
$Z^*_4, \times$	{1, 3}	2	Sì	3⇨ 3,1	
$Z^*_6, \times$	{1, 5}	2	Sì	5⇨ 5,1	
$Z^*_8, \times$	{1, 3, 5, 7}	4	No		{3, 1}, {5,1}, {7, 1}
$Z^*_9, \times$	{1, 2, 4, 5, 7, 8}	6	Sì	2 ⇨ 2, 4, 8, 7, 5, 1 5 ⇨ 5, 7, 8, 4, 2, 1	{8, 1} {4, 7, 1}

$Z^*_{10}, \times$	{1, 3, 7, 9}	4	Sì	3 ⇨ 3,9,7,1 7 ⇨ 7,9,3,1	{9, 1}
$Z^*_{12}, \times$	{1, 5, 7, 11}	4	No		{5, 1}, {7, 1}, {11, 1}
$Z^*_{14}, \times$	{1, 3, 5, 9, 11, 13}	6	Sì	3 ⇨3,9,13,11,5,1 5 ⇨5,11,13,9,3,1	{1, 13} {1, 9, 11},
$Z^*_{15}, \times$	{1,2,4,7,8,11,13,14}	8	No		{2,4,8,1},{7,4,13,1}, {4,1},{11,1},{14,1}, {11,14,4,1} non ciclico
$Z^*_{16}, \times$	{1,3,5,7,9,11,13,15}	8	No		{3,9,11,1},{5,9,13,1}, {7,1},{9,1},{15,1}, {7,15,9,1} non ciclico
$Z^*_{18}, \times$	{1,5,7,11,13,17}	6	Sì	5 ⇨ 5,7,17,13,11,1 11⇨11,13,17,7,5,1	{17,1} {7,13,1},
$Z^*_{20}, \times$	{1,3,7,9,11,13,17,19}	8	No		{3,9,7,1},{13,9,17,1}, {11,1},{9,1},{19,1}, {11,9,19,1} non ciclico
$Z^*_{22}, \times$	{1, 3, 5, 7, 9, 13, 15, 17, 19, 21}	10	Sì	7⇨7,5,13,3,21,15,17,9,19,1	{3,9,5,15,1} {21,1}

Esercizi

- Si consideri la seguente permutazione p di S_9: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 1 & 9 & 6 & 8 & 5 & 2 & 3 \end{pmatrix}$.
  a) Scrivere p e p^{-1} come prodotto di cicli disgiunti.
  b) Determinare l'ordine e gli elementi del sottogruppo X di S_9 generato da p.
  c) Individuare quali potenze di p **non** sono generatori per X.

Omomorfismi di gruppi

Si dice omomorfismo tra due gruppi $(H, \circ)$ e $(K, \square)$ una corrispondenza $f: H \to K$ tra gli elementi che associ ad ogni elemento del dominio H un elemento del codominio K in modo tale che soddisfi la condizione $f(x \circ y) = f(x) \square f(y)$ per ogni coppia di elementi

- L'insieme degli elementi che sono trasformati nel neutro del codominio è un sottogruppo del dominio chiamato nucleo.
- L'insieme degli elementi che sono i trasformati negli elementi del dominio è un sottogruppo del codominio chiamato immagine
- Se il dominio è finito, l'ordine del nucleo moltiplicato per l'ordine dell'immagine è l'ordine del codominio.
- Tutti gli elementi di uno stesso laterale del nucleo vengono trasformati nello stesso elemento.

Le ultime due proprietà consentono di calcolare tutti i possibili omomorfismi di un gruppo in un altro, utilizzando sempre la stessa struttura:

- nucleo ⇨ neutro,
- laterali del nucleo ⇨ elementi immagine

Attenzione:

- deve conservare le operazioni, cioè essere un omomorfismo!
- Se un elemento x del dominio ha periodo h, e quindi $x^k = u$ (neutro), il suo trasformato $y = f(x)$ ha periodo o k o un divisore di k, infatti deve essere $y^k = f(x)^k = f(u) = u'$

Due gruppi ciclici dello stesso ordine sono **sempre** isomorfi. La corrispondenza biunivoca tra due gruppi ciclici dello stesso ordine si ottiene mettendo in corrispondenza i generatori. Questo però non vuole affatto dire che ogni omomorfismo tra gruppi ciclici dello stesso ordine sia un isomorfismo, ma solo che ne esiste almeno uno.
Questa affermazione si può adattare anche al caso in cui il codominio sia un gruppo qualsiasi.
Se **il dominio è ciclico** si può costruire una "tavola pitagorica" degli omomorfismi, mettendo

- nella prima colonna un **generatore**, seguito dalle sue potenze, in ordine crescente di esponente
- nella prima riga gli elementi del codominio, in un ordine qualsiasi.
- Nella seconda riga, cioè la effettiva prima riga della tavola, si copiano gli elementi della prima riga, intendendo così dire che il generatore del dominio viene trasformato in quel elemento del codominio.
- Si riempiono le colonne costruendo le successive potenze (nell'operazione del codominio, ovviamente) del primo elemento.
- Se g che è il generatore e ha periodo k e se è $f(g)=y$ se risulta che y^k non è l'unità, non si è ottenuto un omomorfismo.

Esempio 1: stabilire se i seguenti sono omomorfismi.

$f : (Z,+) \to (Q,+)$

$f(z) = z + \frac{1}{2}$ C.N. $f(0)=\frac{1}{2}$ non verificata. No

$f(z) = 2z^3$ C.N. $f(0)=0$ verificata $f(a+b)=2(a+b)^3=2a^3+6a^2b+6ab^2+2b^3$
$f(a) \square f(b)=2a^3+2b^3$

$f : (Q,+) \to (Z,+)$ definita da:

$f\left(\frac{a}{b}\right) = a$ C.N. $f(0)=0$ verificata. $f\left(\frac{a}{b}+\frac{c}{d}\right) = f\left(\frac{ad+bc}{bd}\right) = ad+bc \neq a+c$ No

---

Esempio 2: Si consideri il gruppo S_6 delle permutazioni sugli elementi 1, 2, ... ,6

a) Scrivere la permutazione p =(2 3 5)(4 1)(3 4 6)(1 5 2 3) come prodotto di cicli disgiunti e stabilire se è pari o dispari.
b) determinare l'ordine del sottogruppo $\mathbf{X}$ di S_7 generato da p^{-1} e indicarne gli elementi.
c) indicare tutti i sottogruppi di $\mathbf{X}$ e tutti i sottogruppi di $(Z^*_7,\times)$ e di $(Z^*_8,\times)$, esplicitandone gli elementi
d) Stabilire quanti e quali omomorfismi $f: \mathbf{X} \to (Z^*_7,\times)$ e $g: (Z^*_8,\times) \to \mathbf{X}$, si possono costruire.

Soluzione:

a. p =(1 2)(3 4 6 5) = (1 2)(3 5)(3 6)(3 4) quindi è pari
b. sappiamo che il gruppo generato da p e quello generato da p^{-1}=(1 2)(3 5 6 4) = q sono lo stesso sottogruppo, comunque è indifferente calcolare uno o l'altro.
   mcm(2, 4)=4 ordine di $\mathbf{X}$
   $\mathbf{X}$ ={q = (1 2)(3 5 6 4), q^2 = (3 6)(5 4), q^3 = (1 2)(3 4 6 5) =p, id }
c. cerchiamo i sottogruppi dei vari gruppi.
   - l'unico sottogruppo proprio di $\mathbf{X}$ è {q^2, id} ordine sottogruppi 1 2 4
   - $(Z^*_7,\times)$ = {1, 2, 3, 4, 5, 6} ha ordine 7-1=6 ordine sottogruppi 1 2 3 6
     {1} {2, 4, 1} {6, 1} Z^*_7 {3, 2, 6, 4, 5, 1} {5, 4, 6, 2, 3, 1}
   - $(Z^*_8,\times)$ = {1, 3, 5, 7} ordine sottogruppi 1 2 4 {1} {3, 1} {5, 1} {7, 1} Z^*_8
     nessun elemento ha periodo 4 ⇨ $(Z^*_8,\times)$ non è ciclico

d. Per f: senza utilizzare il fatto che $(Z^*_7,\times)$ è ciclico, ma usando il teorema dell'ordine, poiché il dominio ha ordine 4, abbiamo le possibilità:
   - $4 = 1 \times 4$ no, perché non c'e una possibile immagine di ordine 4
   - $4 = 4 \times 1$ è l'omomorfismo banale
   - $4 = 2 \times 2$ nucleo $\{q^2, \mathrm{id}\}$ immagine $\{6, 1\}$

Gli elementi del dominio	q	q^2	q^3	id
sono trasformati in	6	1	6	1

Ma poiché so che il dominio è ciclico, posso anche ragionare così:

f	1	2	3	4	5	6
q	1	2	3	4	5	6
q^2	1	4	2	2	4	1
q^3	1	1	6	1	6	6
q^4=i	1	2	4	4	2	1
Ker$f$	X	NO	NO	NO	NO	$\{q^2, \mathrm{i}\}$
Im f	{1}					{1, 6}

Per g:
Il dominio non è ciclico, quindi devo ragionare sugli ordini di nucleo e immagine:
$4 = 1 \times 4$ se esiste è un isomorfismo ma non esiste perché uno è ciclico e l'altro no
$4 = 4 \times 1$ è l'omomorfismo banale
$4 = 2 \times 2$ ho 3 possibili nuclei {3, 1} {5, 1} {7, 1} una sola immagine $\{q^2, \mathrm{id}\}$

Gli elementi del dominio	1	3	5	7	
sono trasformati in	id	id	q^2	q^2	primo
oppure in	id	q^2	id	q^2	Secondo
oppure in	id	q^2	q^2	id	Terzo
oppure in	id	id	id	id	quarto

Esempio 3: Determinare tutti i possibili omomorfismi di $(Z^*_7,\times)$ in un qualsiasi gruppo ciclico X di ordine 12, generato da p.
Soluzione:
$(Z^*_7,\times) = \{1, 2, 3, 4, 5, 6\}$ ha ordine 6
So che è ciclico, ma devo trovare un generatore cioè un elemento di periodo 6
2⇨4⇨1 ha periodo 3
3⇨2⇨6⇨4⇨5⇨1 ha periodo 6 quindi è generatore.
Non interessa nessuna informazione ulteriore sul gruppo X, se non che è ciclico e generato da p
$X = \{ p, p^2, p^3, p^4, p^5, p^6, p^7, p^8, p^9, p^{10}, p^{11}, n\}$

Anche se non serve, visto che il dominio è ciclico, troviamo i sottogruppi del codominio X che sono le possibili immagini: $A=\{ p^2, p^4, p^6, p^8, p^{10}, p^{12} = n \}$ $B=\{ p^3, p^6, p^9, p^{12} = n \}$
$C=\{ p^4, p^8, p^{12} = n \}$ $D= \{ p^6, p^{12} = n \}$ $\{p^{12} = n\}$ X

Analogamente, troviamo i sottogruppi di Z^*_7 che sono i possibili nuclei: {1}, {1,6}, {2,4,1}, Z^*_7.
Conviene usare il metodo della tavola pitagorica per costruire gli omomorfismi.

	p	p^2	p^3	p^4	p^5	p^6	p^7	p^8	p^9	p^{10}	p^{11}	n
3	p	p^2	p^3	p^4	p^5	p^6	p^7	p^8	p^9	p^{10}	p^{11}	n
$3^2=2$	p^2	p^4	p^6	p^8	p^{10}	n	p^2	p^4	p^6	p^8	p^{10}	n
$3^3=6$	p^3	p^6	p^9	n	p^3	p^6	p^9	n	p^3	p^6	p^9	n
$3^4=4$	p^4	p^8	n	p^4	p^8	n	p^4	p^8	n	p^4	p^8	n
$3^5=5$	p^5	p^{10}	p^3	p^8	p	p^6	p^{11}	p^4	p^9	p^2	p^7	n
$3^6=1$	p^6	n	p^6	n	p^6	n	p^6	n	p^6	n	p^6	n
	no	sì	no	sì	no	sì	no	sì	no	sì	no	Sì
ker		{1}		{1,6}		{2,4,1}		{6,1}		{1}		Z^*_7
im		A		C		D		C		A		{n}

Se non avessimo visto che Z^*_7 è ciclico, come si procede?
Prodotti che danno 6 = ordine dominio 6 = 1 × 6 6=2×3 6= 3×2 6=6×1
Si può costruire la tabella delle corrispondenze senza usare i laterali…? proviamo

	1	2	4	3	5	6
6 = 1 × 6 no	n	p^2	p^4	p^6 no		
6 = 1 × 6 no	n	p^2	p^4	p^8 no		
6 = 1 × 6 no	n	p^2	p^4	p^{10} no		
6 = 1 × 6 si	n	p^4	p^8	p^2	p^{10}	p^6
6 = 1 × 6 no	n	p^8	p^4	p^2	p^6	p^{10}
6 = 1 × 6 si	n	p^8	p^4	p^{10}	p^2	p^6

Procedere a caso è troppo faticoso…. Ragioniamo:
1 ha come trasformato solo n, e questa è la prima condizione.
6 ha periodo 2 quindi 6 può avere come trasformato solo p^6 o n.
2 non può avere come trasformato p^2 perché 2 ha periodo 3, mentre p^2 ha periodo 6
2 può avere come trasformato solo p^4 o p^8 o n come pure 4
3 non può essere a caso, perché $3^2=2$
Riproviamo a costruire la tabella mettendo dentro le condizioni.

	1	2	3	4	5	6
6 =1×6 sì	n	p^4	p^2	p^8	p^{10}	p^6
6 =1×6 sì	n	p^8	p^{10}	p^4	p^2	p^6
6 =2×3 sì	n	p^4	p^8	p^8	p^4	n
6 =2×3 sì	n	p^8	p^4	p^4	p^8	n
6 =3×2 sì	n	n	p^6	n	p^6	p^6
6 =6×1 sì	n	n	n	n	n	n

Esempio 4: Si consideri $(Z^*_{15},\times)$. Dopo averne indicato gli elementi, stabilire se è ciclico determinandone un eventuale generatore e indicarne tutti i sottogruppi.
Determinare gli eventuali omomorfismi $f:(Z^*_{15},\times)\to G$, gruppo ciclico di ordine 6 con generatore s.
$(Z^*_{15},\times)$= {1, 2, 4, 7, 8, 11, 13, 14} ordine 8
Per il teorema di Lagrange l'ordine dei possibili sottogruppi è 1, 2, 4, 8

È ciclico? Cerco generatore ⇨ elemento di periodo 8

2, 4, 8, 1 no ; 4, 1 no ; 7 , 4, 13, 1 no ; 8 ha lo stesso periodo di 2 perché è 2^{-1} no 11, 1 no ; 13 $=7^{-1}$ no ; 14, 1 no ⇨ non è ciclico

{1}, {2, 4, 8, 1}, {4, 1}, {7 , 4, 13, 1}, {11, 1} {14, 1} sono i sottogruppi ciclici

non ciclici? Se c'è deve avere ordine 4. Non può contenere elementi di periodo 4.

L'unico tentativo è che contenga 4 e 11 {4, 11, 14, 1} ECCOLO!!!!

Non funziona l'algoritmo che prevede il dominio ciclico

Teorema: ord nucleo * ord immagine = ordine dominio =8

Candidati nuclei ordine 1, 2, 4, 8 sottogruppi dominio 1 no 2 no 4 sì 8 banale

Candidati immagini ordine 1, 2, 3, 6 sottogruppi codominio 2 1

nucleo	1	2	4	7	8	11	13	14
{2, 4, 8, 1}	n	n	n	s^3	n	s^3	s^3	s^3
{7 , 4, 13, 1}	n	s^3	n	n	s^3	s^3	n	s^3
{4, 11, 14, 1}	n	s^3	n	s^3	s^3	n	s^3	n

Esempio 5: Determinare tutti i possibili omomorfismi del gruppo del triangolo: $\mathcal{G}=\{I,R_1,R_2,S_A,S_B,S_C\}$ in $(Z_6,+)$ e viceversa. (La tabella moltiplicativa di $\mathcal{G}$ è sotto)

$\mathcal{G}$ ha come sottogruppi

{I} di ordine 1, $\{I,R_1,R_2\}$ di ordine 3, $\{I,S_A\}$, $\{I,S_B\}$, $\{I,S_C\}$ di ordine 2, $\mathcal{G}$ di ordine 6.

$(Z_6,+)$ ha come sottogruppi

{0} di ordine 1, {0,3} di ordine 2, {0,2,4} di ordine 3, e Z_6 di ordine 6.

Omomorfismi f: $(\mathcal{G},\lozenge)\to(Z_6,+)$ Prodotti possibili: 6= 6×1, 6=3×2, 6=2×3, 6=1×6

Ker*f*	**Im*f***	**Possibili omomorfismi**	I	R_1	R_2	S_A	S_B	S_C
{I}	Z_6	Isomorfismo. Non esiste: le due strutture sono diverse (una abeliana e l'altra no), quindi è inutile cercarlo.	-	-	-	-	-	-
$\{I,R_1,R_2\}$	{0,3}	$f(I)=f(R_1)=f(R_2)=0$, $f(S_A)=f(S_B)=f(S_C)=3$	0	0	0	3	3	3
$\{I,S_A\}$	{0,2,4}	$f(I)=f(S_A)=0$ $f(R_1)=f(R_1\lozenge S_A)=f(S_C)=2$ $f(R_2)=f(R_2\lozenge S_A)=f(S_B)=4$	0	2	4	0	4	2
$\{I,S_A\}$	{0,2,4}	$f(I)=f(S_A)=0$ $f(R_1)=f(R_1\lozenge S_A)=f(S_C)=4$ $f(R_2)=f(R_2\lozenge S_A)=f(S_B)=2$	0	4	2	0	2	4
$\{I,S_B\}$	{0,2,4}	$f(I)=f(S_B)=0$ $f(R_1)=f(R_1\lozenge S_B)=f(S_A)=2$ $f(R_2)=f(R_2\lozenge S_B)=f(S_C)=4$	0	2	4	2	0	4
$\{I,S_B\}$	{0,2,4}	$f(I)=f(S_B)=0$ $f(R_1)=f(R_1\lozenge S_B)=f(S_A)=4$ $f(R_2)=f(R_2\lozenge S_B)=f(S_C)=2$	0	4	2	4	0	2
$\{I,S_C\}$	{0,2,4}	$f(I)=f(S_C)=0$ $f(R_1)=f(R_1\lozenge S_C)=f(S_B)=2$ $f(R_2)=f(R_2\lozenge S_C)=f(S_A)=4$	0	2	4	4	2	0
$\{I,S_C\}$	{0,2,4}	$f(I)=f(S_C)=0$ $f(R_1)=f(R_1\lozenge S_C)=f(S_B)=4$ $f(R_2)=f(R_2\lozenge S_C)=f(S_A)=2$	0	4	2	2	4	0
$\mathcal{G}$	{0}	Omomorfismo banale $f(a)=0$ per ogni a (che esiste sempre).	0	0	0	0	0	0

Vediamo gli omomorfismi f: $(Z_6,+)\to(\mathcal{G},\lozenge)$

Ker$f$	Imf	Possibili omomorfismi	0	1	2	3	4	5
{0}	G	Isomorfismo. Non esiste: le due strutture sono diverse (una abeliana e l'altra no), quindi è inutile cercarlo.						
{0,3}	{I,R_1,R_2}	$f(0)=f(3)=$ I, $f(1)=f(4)=R_1$, $f(2)=f(5)=R_2$	I	R_1	R_2	I	R_1	R_2
{0,3}	{I,R_1,R_2}	$f(0)=f(3)=$I, $f(1)=f(4)=R_2$, $f(2)=f(5)=R_1$	I	R_2	R_1	I	R_2	R_1
{0,2,4}	{I,S_A}	$f(0)=f(2)=f(4)=$ I, $f(1)=f(3)=f(5)=S_A$	I	S_A	I	S_A	I	S_A
{0,2,4}	{I,S_B}	$f(0)=f(2)=f(4)=$ I, $f(1)=f(3)=f(5)=S_B$	I	S_B	I	S_B	I	S_B
{0,2,4}	{I,S_C}	$f(0)=f(2)=f(4)=$ I, $f(1)=f(3)=f(5)=S_C$	I	S_C	I	S_C	I	S_C
Z_6	{I}	Omomorfismo banale $f(z)$=I per ogni z	I	I	I	I	I	I

Tavola moltiplicativa di (G,°)

◊	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_I	R_2	I

Esempio 5: **Un tema d'esame:**

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

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

Soluzione

1. Gli elementi di $P_1[x]$ sono i polinomi della forma $ax+b$, con a,b in Z_3, quindi sono 9:
   $$\{0,\ 1,\ 2,\ x,\ 2x,\ x+1,\ x+2,\ 2x+1,\ 2x+2\}$$
2. Cerchiamo i periodi degli elementi non nulli (lo 0 non può essere un generatore):
   - $1 \to 2 \to 0$ quindi 1 e 2 hanno periodo 3 e {0, 1, 2} è un sottogruppo;
   - $x \to 2x \to 0$ quindi x e $2x$ hanno periodo 3 e $\{0, x, 2x\}$ è un sottogruppo;
   - $x+1 \to 2x+2 \to 0$ quindi $x+1$ e $2x+2$ hanno periodo 3 e $\{0, x+1, 2x+2\}$ è un sottogruppo;
   - $2x+1 \to x+2 \to 0$ quindi $2x+1$ e $x+2$ hanno periodo 3 e $\{0, 2x+1, x+2\}$ è un sottogruppo;

   Sono stati elencati tutti i sottogruppi di ordine 3, poiché 3 è l'unico divisore di 9, non esistono altri sottogruppi propri.
3. nessun elemento ha periodo 9, quindi il gruppo non è ciclico.
4. Il gruppo (Z_9,+) è ciclico e quindi non può essere isomorfo a $P_1[x]$; 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}.

- N={0, 1, 2} Nucleo; ⇨ i laterali sono $N+x=\{x, x+1, x+2\}$ e $N+2x=\{2x, 2x+1, 2x+2\}$
- M={0, x, $2x$} Nucleo; ⇨ i laterali sono $M+1=(1, x+1, 2x+1\}$ e $M+2=\{2, x+2, 2x+2\}$
- P={0, $x+1$, $2x+2$} Nucleo; ⇨ i laterali sono $P+1=\{1, x+2, 2x\}$ e $P+2=\{2, x, 2x+1\}$

- $Q=\{0, 2x+1, x+2\}$ Nucleo; ⇨ i laterali sono $Q+1=\{1, 2x+2, x\}$ e $Q+2=\{2, 2x, x+1\}$

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

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

Esempio 6: Altro tema d'esame

Si consideri la seguente permutazione p di S_8: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 7 & 5 & 8 & 4 & 2 & 6 & 1 \end{pmatrix}$.

1. scrivere p come prodotto di cicli disgiunti e stabilire se è pari o dispari
2. determinare il periodo di p, p^3 e p^5
3. determinare l'ordine del sottogruppo X di S_8 generato da p^3 e indicarne gli elementi.
4. stabilire quanti laterali ha X in S_8 e scrivere gli elementi del laterale di X individuato dal ciclo (1 2) (cioè il laterale (1 2) X).

Soluzione:

1. Risulta p = (1 3 5 4 8)(2 7 6) = (1 8)(1 4)(1 5)(1 3)(2 6)(2 7), quindi p è pari.
2. Posto c = (1 3 5 4 8) e d = (2 7 6), risulta c^5=Id e quindi c ha periodo 5; d^3=Id e dunque d ha periodo 3, quindi p ha periodo mcm(5,3)=15.
   Risulta inoltre $p^3 = c^3 d^3 = c^3$ = (1 4 3 8 5), quindi p^3 ha periodo 5, mentre $p^5 = c^5 d^5 = d^5 = d^2$ = (2 6 7), quindi p^5 ha periodo 3.
3. Ricordando che l'ordine del sottogruppo di un gruppo generato da un elemento coincide col periodo dell'elemento stesso, l'ordine di X è 5 e
   $X = \{p^3 = (1\ 4\ 3\ 8\ 5), (p^3)^2 = (1\ 3\ 5\ 4\ 8), (p^3)^3 = (1\ 8\ 4\ 5\ 3), (p^3)^4 = (1\ 5\ 8\ 3\ 4), (p^3)^5 = \mathrm{Id}\}$.
4. Gli elementi di S_8 sono 8!; gli elementi di X sono 5. Poiché ogni laterale di X è costituito da tanti elementi quanti quelli di X e i laterali di un sottogruppo costituiscono una partizione, i laterali di X sono 8!/5. Gli elementi di (1 2)X sono:
   (1 2)(1 4 3 8 5) = (1 4 3 8 5 2), (1 2)(1 3 5 4 8) = (1 3 5 4 8 2),
   (1 2)(1 8 4 5 3) = (1 8 4 5 3 2), (1 2)(1 5 8 3 4) = (1 5 8 3 4 2), (1 2) Id = (1 2).

Esempio 7: Cerchiamo tutti i possibili omomorfismi f: $(\mathbb{Z}^*_{15}, \times) \to (\mathbb{Z}^*_{16}, \times)$ molto DIFFICILE

Candidato nucleo	ordine		ordine	Candidata immagine
{1}	1		1	{1}
{4, 1}	2		2	{7, 1}
{11, 1}	2		2	{9, 1}
{14, 1}	2		2	{15, 1}
{2, 4, 8, 1}	4		4	{3, 9, 11, 1}
{7, 4, 13, 1}	4		4	{5, 9, 13, 1}
{11, 14, 1, 4}	4		4	{7, 9, 15, 1}
$(Z^*_{15}, \times)$	8		8	$(Z^*_{16}, \times)$

C'è, come sempre, l'omomorfismo banale. Costruiamo gli altri:
Per semplificare la comprensione di quello che segue, scriviamo le tavole pitagoriche dei due gruppi:

Z^*_{15}	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Z^*_{16}	1	3	5	7	9	11	13	15
1	1	3	5	7	9	11	13	15
3	3	9	15	5	11	1	7	13
5	5	15	9	3	13	7	1	11
7	7	5	3	1	15	13	11	9
9	9	11	13	15	1	3	5	7
11	11	1	7	13	3	9	15	5
13	13	7	1	11	5	15	9	3
15	15	13	11	9	7	5	3	1

Ricordiamo che ogni omomorfismo deve soddisfare la condizione $f(a\times b)=f(a)\times f(b)$

Per gli ordini: ordineNucleo × ordineImmagine = 8 ⇨ 1×8, 4×2, 2×4 8×1
I caso: Nucleo {4, 1} Laterali del nucleo {2, 8} {7,13} {11, 14}
Immagine {3, 9, 11, 1} o {5, 9, 13, 1} o {7, 9, 15, 1} che è quello non ciclico.

1	2	4	7	8	11	13	14
1	3 o 11 no	1					
1	9	1	3	9	11	3	11
1	9	1	11	9	3	11	3
1	5 o 13 no	1					
1	9	1	5	9	13	5	13
1	9	1	13	9	5	13	5

Per i primi due casi, ragioniamo, ad esempio, in questo modo:

- $f(1)=f(4)=1$ perché {1, 4} è il nucleo
- i due elementi di ogni laterale del nucleo vanno nello stesso elemento.
- Proviamo a mandare 2 nei vari elementi, controllando di avere un omomorfismo.
- 3 e 11 nel primo caso e 5 e 13 nel secondo non danno luogo ad omomorfismi perché hanno periodo 4, mentre $f(2^2)=1$, poiché 4 appartiene al nucleo.
- Sistemato 2 (e quindi 8) nell'unico modo possibile cioè con $f(2)=9$, mandiamo 7 (e quindi 13) in un altro elemento dell'immagine, e di conseguenza 11 e 14 nell'ultimo elemento. Controlliamo che l'operazione si conservi guardando se $f(7\times 11)=f(7)\times f(11)$, $f(7\times 7)=f(7)\times f(7)$ e $f(11\times 11)=f(11)\times f(11)$. Gli altri prodotti vengono di conseguenza.

Si trovano quindi 4 omomorfismi.

Il terzo sottogruppo candidato immagine si comporta in modo diverso perché tutti i suoi elementi hanno periodo 2. La condizione $f(2^2)=1$ è quindi soddisfatta da tutti e tre gli elementi.
Dunque 2, e quindi 8, può essere trasformato sia in 7 che in 9 che in 15.
Poniamo per prima cosa $f(2)=7$.
Supponiamo ora che sia $f(7)=f(13)=9$. Poiché $7^3=13$, $f(7^3)=f(7)^3=9^3=9=f(13)$, quindi l'ipotesi

fatta non contrasta col fatto che si cerca un omomorfismo.
Risulta di conseguenza che $f(11)= f(14)=15$ e poiché 11 e 14 nel dominio e 15 nel codominio hanno periodo 2 anche per questi sembra non ci siano problemi.
Resta da verificare che $f(7\times11) = f(7) \times f(11)$ e infatti è $f(7\times11)= f(2)=7$ e $f(7) \times f(11) = 9 \times 15 =7$; gli altri vengono di conseguenza.
Discorso esattamente identico se $f(7)= f(13)=15$ e $f(11)= f(14)=9$ e negli altri casi come nella tabella sotto.

1	2	4	7	8	11	13	14
1	7	1	9	7	15	9	15
1	7	1	15	7	9	15	9
1	9	1	7	9	15	7	15
1	9	1	15	9	7	15	7
1	15	1	7	15	9	7	9
1	15	1	9	15	7	9	7

Si trovano quindi 6 omomorfismi; in tutto, con nucleo {1, 4} 10 omomorfismi.
Allo stesso modo si trovano 10 omomorfismi con nucleo {1, 11} e 10 con nucleo {1, 14}.

Se invece il nucleo ha ordine 4 il discorso è molto più semplice perché c'è un solo laterale per il nucleo, quindi gli elementi del nucleo vanno in 1, quelli del laterale nell'altro elemento dell'immagine, che ha ordine 2. Quindi:

Nucleo {2, 4, 8, 1} →1 Immagine {7, 1} Laterale del nucleo {14, 13, 11, 7} →7
Nucleo {2, 4, 8, 1} →1 Immagine {9, 1} Laterale del nucleo {14, 13, 11, 7} →9
Nucleo {2, 4, 8, 1} →1 Immagine {15, 1} Laterale del nucleo {14, 13, 11, 7} →15
Nucleo {7, 4, 13, 1} →1 Immagine {7, 1} Laterale del nucleo {14, 8, 9, 2} →7
Nucleo {7, 4, 13, 1} →1 Immagine {9, 1} Laterale del nucleo {14, 8, 9, 2} →9
Nucleo {7, 4, 13, 1} →1 Immagine {15, 1} Laterale del nucleo {14, 8, 9, 2} →15
Nucleo {11, 4, 14, 1} →1 Immagine {7, 1} Laterale del nucleo {7, 8, 13, 2} →7
Nucleo {11, 4, 14, 1} →1 Immagine {9, 1} Laterale del nucleo {7, 8, 13, 2} →9
Nucleo {11, 4, 14, 1} →1 Immagine {15, 1} Laterale del nucleo {7, 8, 13, 2} →15

Quindi altri 9 omomorfismi
Poiché i due gruppi hanno lo stesso numero di elementi, ci possono essere isomorfismi.

- Gli elementi di periodo 2 del dominio (4, 11, 14) devono essere trasformati in elementi di periodo 2 del codominio (7, 9, 15), ma poiché $4\times11=14$ deve essere $f(4\times11)= f(4)\times f(11)= f(14)$ e questo risulta vero in tutti i sei casi possibili.
- Chi può essere $f(2)$? Sappiamo che $f(2^2)=7$ o $f(2^2)=9$ o $f(2^2)=15$. Ma guardando la tavola pitagorica di $(Z^*_{16},\times)$ scopriamo che solo 9 è un quadrato, quindi è obbligatorio che sia $f(4)=9$.
- Peraltro 9 è il quadrato sia di 3 che di 5 che di 11 e 13, quindi $f(2)$ è uno di questi valori.
- $2\times4=8$ → $f(2\times4) = f(2) \times f(4) = f(2) \times 9 = f(8)$
- $2\times8=1$ → $f(2\times8) = f(2) \times f(8) = f(1) = 1$ quindi
- $2\times7=14$ → $f(2\times7) = f(2) \times f(7) = f(14) = 15$ oppure 7 ; a seconda di quanto vale $f(2)$ troviamo $f(7)$ nei due casi:
  - se $f(2)=3$ e $f(14) = 15$ → $f(7) = 5$ se $f(14) = 7$ → $f(7) =13$
  - se $f(2)=5$ e $f(14) = 15$ → $f(7) = 3$ se $f(14) = 7$ → $f(7) =11$
  - se $f(2)=11$ e $f(14) = 15$ → $f(7) = 13$ se $f(14) = 7$ → $f(7) =5$
  - se $f(2)=13$ e $f(14) = 15$ → $f(7) = 11$ se $f(14) = 7$ → $f(7) =3$
- $2\times11=7$ → $f(2\times11)= f(2) \times f(11) = f(7)$ questo risulta un controllo perché i valori sono già

fissati:

- $3 \times 7 = 5$ sì, $5 \times 7 = 3$ sì, $11 \times 7 = 13$ sì, $13 \times 7 = 11$ sì,
- $3 \times 15 = 13$ sì, $5 \times 15 = 11$ sì, $11 \times 15 = 5$ sì, $13 \times 15 = 3$ sì

➢ $2 \times 13 = 11 \rightarrow f(2 \times 13) = f(2) \times f(13) = f(11) = 7$ oppure 15 di qui si ricava $f(13)$, che è l'ultimo che manca:

- se $f(2)=3$ e $f(11) = 15 \rightarrow f(13) = 13$ se $f(11) = 7 \rightarrow f(13) = 5$
- se $f(2)=5$ e $f(11) = 15 \rightarrow f(13) = 11$ se $f(11) = 7 \rightarrow f(13) = 3$
- se $f(2)=11$ e $f(11) = 15 \rightarrow f(13) = 5$ se $f(11) = 7 \rightarrow f(13) = 13$
- se $f(2)=13$ e $f(11) = 15 \rightarrow f(13) = 3$ se $f(11) = 7 \rightarrow f(13) = 11$

➢ $2 \times 14 = 13 \rightarrow f(2 \times 14) = f(2) \times f(14) = f(13)$. Anche questo è un controllo, sempre soddisfatto.

Gli isomorfismi trovati sono quindi 8 e sono i seguenti:

1	2	4	7	8	11	13	14
1	3	9	5	11	7	13	15
1	5	9	3	13	7	11	15
1	11	9	13	3	7	5	15
1	13	9	11	5	7	3	15
1	3	9	13	11	15	5	7
1	5	9	11	13	15	3	7
1	11	9	5	3	15	13	7
1	13	9	3	5	15	11	7

Esercizi

1. Verificare che $(\mathbb{Z},+)$ e $(M_k,+) = \{$insieme dei multipli di $k\}$ sono isomorfi.

2. $(\mathbb{Z},+)$ è isomorfo al gruppo $(\{k^2, k \in \mathbb{Z}\},+)$?

3. $(\mathbb{Z}_4,+)$ e $(\mathbb{Z}^*_5,\times)$ sono isomorfi? .

4. Mostrare che non sono isomorfi i gruppo del rettangolo e $(\mathbb{Z}_4, +)$.

5. Mostrare che se tra due gruppi dello stesso ordine esiste un omomorfismo iniettivo, questo è un isomorfismo.

6. Mostrare che se un omomorfismo è iniettivo, $\ker(f) = \{u\}$

7. In un gruppo $(G,\circ)$ si consideri la seguente relazione $\approx$: dati $x, y \in G$, $x \approx y$ se esiste $z \in G$ tale che $y = z \circ x \circ z^{-1}$
   a. mostrare che $\approx$ è una relazione di equivalenza.
   b. Se G è il gruppo di sostituzioni su 3 elementi determinare le classi di equivalenza dell'identità e del ciclo (1 3 2).

8. Si consideri il gruppo S_7 delle permutazioni sugli elementi 1, 2, ... ,7
   a. Scrivere la permutazione α come prodotto di cicli disgiunti e stabilire se è pari o dispari
      i) $\alpha = (2\ 3\ 5\ 7)(4\ 1)(3\ 4\ 6)(1\ 5\ 2\ 7\ 3)$
   b. Determinare l'ordine e gli elementi del sottogruppo di S_7 generato da α

9. Si consideri il gruppo S_7 delle permutazioni sugli elementi 1, 2, ... ,7
   a. Scrivere la permutazione α =(1 3 6 2)(4 3 6)(3 5 7)(1 5 7 2) come prodotto di cicli disgiunti e stabilire se α è pari o dispari
   b. determinare l'ordine del sottogruppo X di S_7 generato da α e indicarne gli elementi.
   c. determinare tutti i possibili omomorfismi di $(Z_6,+)$ in X.
   d. determinare tutti i possibili omomorfismi di $(Z_8,+)$ in X.

10. Si consideri la seguente permutazione p di S_7: (1 2 6 7) (1 3 5 2).
   a. Scrivere p come prodotto di cicli disgiunti e stabilire se è pari o dispari
   b. Determinare il periodo di p, p^{-1} e p^5
   c. Determinare il più piccolo sottogruppo X di S_7 tale che il suo laterale $X(3\ 7)$ individuato dal ciclo (3 7) contenga p.
   d. determinare tutti i possibili omomorfismi di $(Z^*_8,\times) \to X$ e di $X \to (Z^*_8,\times)$

11. Si consideri la permutazione s = (1 2 5)$\circ$ (3 8 4)$\circ$ (3 4 7)$\circ$ (1 2 6) di S_8.
   a. Scrivere s come prodotto di cicli disgiunti e calcolare se è pari o dispari.
   b. Scrivere gli elementi del sottogruppo G di S_8 generato da s indicandone gli elementi.
   c. Determinare tutti i sottogruppi di G.
   d. Si consideri $(Z^*_9,\times)$. Dopo averne indicato gli elementi, stabilire se è ciclico determinandone un eventuale generatore e indicarne tutti i sottogruppi.
   e. Determinare gli eventuali omomorfismi $f: (Z^*_9,\times) \to G$.
   f. Determinare gli eventuali omomorfismi $f: (Z^*_{15},\times) \to (Z_8,+)$

12. Si consideri la seguente permutazione p di S_7: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 5 & 4 & 7 & 6 & 2 & 1 \end{pmatrix}$.
   a. Scrivere p come prodotto di cicli disgiunti e stabilire se è pari o dispari
   b. Determinare l'ordine del sottogruppo X di S_7 generato da p^3 e elencarne gli elementi
   c. Si consideri il sottogruppo W di S_7 generato da (1 3 2 4). Determinare tutti i possibili omomorfismi di W in X

13. Nel gruppo S_5 sia k=(1 4)(2 3 5).
   a. si scrivano k^4 e k^{-1} come prodotto di cicli disgiunti, si stabilisca se sono pari o dispari e se ne individui il periodo.
   b. Determinare tutti gli elementi del sottogruppo X generato da k
   c. Stabilire quanti e quali omomorfismi esistono tra $(Z_6,+)$ e $(X,\cdot)$

14. Si consideri la seguente permutazione p di S_5: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$.
   a. Determinare l'ordine del sottogruppo X di S_5 generato da p ed elencarne gli elementi. Dato il ciclo q = (1 2 4 3) di S_5 determinare gli elementi del sottogruppo Y di S_5 generato da q.
   b. Stabilire quali e quanti omomorfismi esistono di dominio X e codominio Y

15. Si consideri il gruppo S_7 delle permutazioni sugli elementi 1, 2, ... ,7.
    a. Scrivere la permutazione p=(2 4 3 5)(4 1 7)(3 4 6 5)(1 5 7 3) come prodotto di cicli disgiunti
    b. Determinare l'ordine del sottogruppo X di S_7 generato da p e scriverne gli elementi.
    c. Determinare tutti i sottogruppi di X.
    d. Determinare tutti i possibili omomorfismi di in $(Z_6,+)$.

16. Si consideri il gruppo S_7 delle permutazioni sugli elementi 1, 2, ... ,7
    a. Scrivere la permutazione α =(2 3 5)(4 3 7)(3 4 6)(1 5 2) come prodotto di cicli disgiunti e stabilire se α è pari o dispari
    b. determinare l'ordine e gli elementi del sottogruppo X di di S_7 generato da α
    c. Determinare tutti i possibili omomorfismo di X in $(Z_6,+)$ e di $(Z_9,+)$ in X .

17. Si consideri la seguente permutazione p di S_8 : (1 3 4 7)(1 6 2)(1 5)(5 8 6)(1 2).
    a. Scrivere p come prodotto di cicli disgiunti e stabilire se è pari o dispari
    b. Determinare l'ordine del sottogruppo X di S_8 generato da p indicandone gli elementi.
    c. Indicare i sottogruppi di X
    d. Indicare i sottogruppi di $(Z^*_9, \times)$ e stabilire se è ciclico.
    e. Indicare tutti i possibili omomorfismi f: $X \to (Z^*_9,\times)$ e gli omomorfismi g: $(Z^*_9,\times) \to X$.

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

19. Nel gruppo simmetrico S_6 sia p=(1 2 4 3 6)(1 2 6)(2 5 3 4)(1 4 5).
    a. si scriva p come prodotto di cicli disgiunti, si stabilisca se è pari o dispari.
    b. Si individui il periodo di p, si determinino tutti gli elementi del sottogruppo $(X,\bullet)$ generato da p e se ne indichino i sottogruppi.
    c. Si consideri $(Z^*_8,\times)$. Se ne indichino gli elementi. Si stabilisca se è ciclico e se ne indichino i sottogruppi.
    d. Stabilire quanti e quali omomorfismi esistono tra $(Z^*_8,\times)$ e $(X,\bullet)$ e tra $(X,\bullet)$ e $(Z^*_8,\times)$

20. Nel gruppo simmetrico S_{10} si considerino i due cicli h e k così ottenuti:
    i) si determini il più piccolo numero $p \geq A$ le cui quattro cifre siano distinte tra loro e tali cifre determinino k [es. (1 9 8 0)]
    ii) si determini il più piccolo numero $n' \geq n$ le cui tre cifre siano distinte tra loro e da quelle di p e le tre cifre determinino h [es. (3 2 7)]
    b. Determinare tutti gli elementi dei due sottogruppi H e K generati rispettivamente da h e k.
    c. Determinare tutti gli elementi del "più piccolo" sottogruppo X di S_{10} che contiene sia h che k (per "più piccolo" si intende che deve contenere h, k e tutti gli elementi che di S_{10} sono necessari perché sia un gruppo, senza altri elementi) e verificare che X ha ordine 12
    d. Determinare tutti i sottogruppi di X.
    e. Stabilire se X è ciclico e in caso affermativo indicarne un generatore.
    f. Stabilire quanti e quali omomorfismi $(Z_{12},+) \to (X,.)$ esistono.

21. Sia $h = m$ se m è composto altrimenti sia $h = m + 1$. Si considerino il gruppo $(Z_h,+)$ e $(Z^*_{10},\times)$. (si ricorda che con Z^*_{10} si indica l'insieme degli elementi di Z_{10} primi con 10).
    a. Stabilire se i due gruppi sono isomorfi;

b. Determinare, se esiste, un omomorfismo $(\mathbb{Z}_h,+) \to (\mathbb{Z}^*_{10},\times)$ diverso da quello banale.
c. Determinare, se esiste, un omomorfismo $(\mathbb{Z}^*_{10},\times) \to (\mathbb{Z}_h,+)$ diverso da quello banale.

22. Nel gruppo simmetrico S_{10} sia k la permutazione così ottenuta:
    i) si accosti N con le quattro cifre di A (ad es. 430135 1977) ;
    ii) si suddividano le cifre in tre gruppi di 3, 4, 3 cifre [es. (4 3 0)(1 3 5 1)(9 7 7)]
    iii) se in un gruppo ci sono cifre ripetute si eliminino quelle più a destra [es. (4 3 0)(1 3 5)(9 7)]
    iv) si esegua il prodotto dei cicli ottenuti.
    b. si scomponga k in cicli disgiunti e in prodotto di trasposizioni.
    c. si stabilisca se k e k^2 sono pari o dispari.
    d. Si determini il gruppo X generato da k, indicandone l'ordine e gli elementi
    e. Determinare un intero h tale che il gruppo $(\mathbb{Z}_h,+)$ sia isomorfo ad X. Perché esiste di sicuro? Determinare inoltre tutti i possibili omomorfismi tra $(\mathbb{Z}_h,+)$ ed X e viceversa.

23. In Q si consideri la seguente operazione: $x \square y = x + y + mxy$
    a. mostrare che $\square$ è associativa
    b. determinare l'elemento neutro
    c. determinare per quali elementi di Q esiste l'elemento inverso e quale è.

24. Nel gruppo simmetrico S_{10} sia k la permutazione così ottenuta:
    a. si accosti N con le quattro cifre di A (ad es. 530133 1980) ;
    b. si suddividano le cifre in due gruppi di 4 e 3 cifre tutte distinte tra loro (se non esistono, si aggiungano a destra, in ordine crescente, le cifre mancanti [es. (5 3 0 1)(9 8 2)]
    c. Scrivere gli elementi del gruppo ciclico X generato da k.
    d. Individuare tutti i possibili generatori per tale gruppo.
    e. Determinare tutti i sottogruppi di X.
    f. Scrivere k come prodotto di trasposizioni in due modi diversi (con un numero diverso di trasposizioni)
    g. Stabilire quanti e quali omomorfismi $(\mathbb{Z}_8,+) \to (X,\cdot)$ esistono.
    h. Stabilire quanti e quali omomorfismi $(\mathbb{Z}^*_8,\times) \to (X,\cdot)$ esistono.

25. Nel gruppo simmetrico S_{10} sia k la permutazione così ottenuta:
    i) si accosti la data di nascita con n (ad es. 03 08 1978 732) ;
    ii) si determinino le prime 5 cifre distinte divise in un gruppi di 2 e 3 cifre [es. (0 3) (8 1 9)]
    b. si scrivano k^4 e k^{-1} come prodotto di cicli disgiunti, si stabilisca se sono pari o dispari e se ne individui il periodo.
    c. Determinare tutti gli elementi del sottogruppo X generato da k
    d. Scrivere gli elementi del laterale di X generato da (1 2).
    e. Stabilire quanti e quali omomorfismi esistono tra $(\mathbb{Z}_6,+)$ e $(X,\cdot)$
    f. Stabilire quanti e quali omomorfismi esistono tra $(X,\cdot)$ e $(\mathbb{Z}_6,+)$