ESERCIZI DI ALGEBRA I

ESERCIZI SUI GRUPPI

A) Gruppi, elementi, periodi.

A.1 - Quali fra le seguenti quattro tavole di moltiplicazione sull'insieme $X = \{1,2,3,4\}$ non definiscono un gruppo e perche?

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

sì no

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

sì no

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

sì no

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

sì no

Risposta. La prima tavola non definisce un gruppo perché non ha l'elemento neutro. Infatti, il candidato è 1, che è elemento neutro a sinistra, ma non lo è a destra, dato che $2 \cdot 1 = 3$. La terza e la quarta non soddisfano la legge di cancellazione, poiché in qualche riga o colonna ci sono elementi ripetuti.
La seconda invece potrebbe definire un gruppo. Infatti, 1 è l'elemento neutro, ogni elemento è inverso di se stesso e, si noti, valgono anche le leggi di cancellazione e la proprietà commutativa, ma perché sia un gruppo occorre verificare anche la proprietà associativa: per ogni a, b, c∈X, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

A priori ci sarebbero $4^3 = 64$ terne ordinate da verificare. Si osservi però che se uno dei tre elementi è l'elemento neutro, allora l'uguaglianza è ovvia. Perciò restano $3^3 = 27$ terne senza 1. Ma vale la proprietà commutativa, perciò se una terna (a,b,c) è associativa, lo sono anche quelle ottenute "anagrammandone" gli elementi. Per esempio, la terna (2,2,3) è associativa, dato che $\begin{cases} (2 \cdot 2) \cdot 3 = 1 \cdot 3 = 3 \\ 2 \cdot (2 \cdot 3) = 2 \cdot 4 = 3 \end{cases}$.

Ma allora sono associative anche le altre due terne (2,3,2), (3,2,2) ottenute "anagrammando" la terna (2,2,3). In questo modo la verifica si sveltisce.

A.2 – Sia $\mathbf{R}$ il campo dei numeri reali e sia $\mathbf{R}^*$ l'insieme dei numeri reali non nulli. Nel prodotto cartesiano $G = \mathbf{R}^* \times \mathbf{R} = \left\{ (a,b) \;\middle|\; a \in \mathbf{R}^*,\ b \in \mathbf{R} \right\}$ sia definita la seguente operazione: $(a,b) * (c,d) = (ac, ad + b)$.

a) Si calcoli $\left((1,0) * \left(\frac{1}{2}, -3 \right) \right) * (2,6)$

b) Si dimostri che $(G, *)$ è un gruppo non abeliano. (G è detto *gruppo delle affinità* di $\mathbf{R}$).

Risposta. a) $\left((1,0) * \left(\frac{1}{2}, -3 \right) \right) * (2,6) = \left(\frac{1}{2}, -3 \right) * (2,6) = (1,0)$

b) Si osservi che la definizione di * è corretta perché essendo a, c non nulli anche ac è non nullo. Pertanto, * è una operazione in G. Verifichiamo che possiede le tre proprietà richieste, incominciando con l'associativa. Siano $(a,b),(c,d),(e,f) \in G$. Allora:

$$\begin{cases} \big((a,b) * (c,d)\big) * (e,f) = (ac, ad+b) * (e,f) = \big((ac)e, (ac)f + (ad+b)\big) = (ace, acf + ad + b) \\ (a,b) * \big((c,d) * (e,f)\big) = (a,b) * (ce, cf + d) = \big(a(ce), a(cf+d) + b\big) = (ace, acf + ad + b) \end{cases}$$

e quindi $\big((a,b) * (c,d)\big) * (e,f) = (a,b) * \big((c,d) * (e,f)\big)$.

Chi è l'elemento neutro? Cerchiamolo nella forma (x,y). Deve essere tale che per ogni (a,b)∈G, $(a,b) * (x,y) = (a,b)$. Eseguendo i calcoli e semplificando per a (che sappiamo essere $\neq 0$), otteniamo:

$$(ax, ay + b) = (a,b) \Rightarrow \begin{cases} ax = a \\ ay + b = b \end{cases} \Rightarrow \begin{cases} x = 1 \\ ay = 0 \end{cases} \Rightarrow (x,y) = (1,0)$$

Si verifica subito che $(1,0) * (a,b) = (a,b)$, quindi $1_G = (1,0)$.

Cerchiamo infine l'inverso di (a, b) nella forma (u, v): deve essere tale che $(a,b) * (u,v) = (1,0)$. Eseguendo i calcoli, si ha:

$$(au, av + b) = (1,0) \Rightarrow \begin{cases} au = 1 \\ av + b = 0 \end{cases} \Rightarrow \begin{cases} u = 1/a \\ v = -b/a \end{cases}$$

Si verifica subito che $\left(\frac{1}{a}, \frac{-b}{a} \right) * (a,b) = (1,0)$, quindi $(a,b)^{-1} = \left(\frac{1}{a}, \frac{-b}{a} \right)$. Pertanto, G è un gruppo.

Per verificare che non è abeliano basta esibire due elementi di G che non commutano. Osserviamo intanto che: $\begin{cases}(a,b)*(c,d)=(ac,ad+b)\\(c,d)*(a,b)=(ca,cb+d)\end{cases}$, quindi essendo $ac=ca$, questi due elementi commutano se e solo se $ad+b=cb+d$. Basta prendere per esempio $a=2,\ b=c=d=1$ e si ha $\begin{cases}ad+c=2\cdot1+1=3\\cb+d=1\cdot1+1=2\end{cases}$, quindi gli elementi (2,1) ed (1,1) non commutano.

A.3 – Sia $\mathbf{Z}$ l'anello dei numeri interi e sia $\mathbf{Z}^*=\{1,-1\}$. Nel prodotto cartesiano $G=\mathbf{Z}^*\times\mathbf{Z}=\{(a,b)\mid a\in\mathbf{Z}^*,\ b\in\mathbf{Z}\}$ sia definita la seguente operazione: $(a,b)*(c,d)=(ac,ad+b)$. Si dimostri che $(G,*)$ è un gruppo non abeliano.

Risposta: si veda l'esercizio precedente.

OSSERVAZIONE. La tecnica dei due esercizi precedenti funziona in ogni anello commutativo A con almeno tre elementi. Si consideri il gruppo A^* costituito dagli elementi di A invertibili rispetto alla moltiplicazione, poi nel prodotto cartesiano $G=A^*\times A$ si definisca l'operazione $(a,b)*(c,d)=(ac,ad+b)$, che forma un gruppo non abeliano. In questo modo si fabbricano tanti esempi di gruppi non abeliani.

Se si parte dall'anello $\mathbf{Z}_n$, il gruppo $\mathbf{Z}_n{}^*$ ha $\varphi(n)$ elementi, dove φ denota la funzione di Eulero, perciò il gruppo G ha $\varphi(n)\cdot n$ elementi.

(Per n=2 si ha $\varphi(2)=1$, quindi $G=(\mathbf{Z}_2,+)$). Ecco la tabella per $3\le n\le 12$.

n	3	4	5	6	7	8	9	10	11	12
φ(n)	2	2	4	2	6	4	6	4	10	4
|G|	6	8	20	12	42	32	54	40	120	48

A.5 – Alla luce dell'osservazione precedente, si consideri l'anello $(\mathbf{Z}_4,+,\cdot,1)$, dove per semplicità si è posto $\mathbf{Z}_4=\{0,1,2,3\}$; per la somma ed il prodotto si prendano i resti della divisione per 4 rispettivamente di x+y ed x·y, eseguite in $\mathbf{Z}$.

a) Si scrivano le tavole di addizione e di moltiplicazione di $\mathbf{Z}_4$.

b) Si scriva la tavola di moltiplicazione del gruppo $\mathbf{Z}_4^*$.

c) Si elenchino gli 8 elementi del gruppo G e si calcoli la sua tavola di moltiplicazione (si usino le proprietà gruppali per sveltire il lavoro).

A.4 – Si consideri l'insieme $G = [0, 1[= \{x \in \mathbf{R} \mid 0 \le x < 1\}$. In questo insieme si ponga: $x * y = \begin{cases} x+y & \text{se } x+y < 1 \\ x+y-1 & \text{se } x+y \ge 1 \end{cases}$.

a) Si provi che $(G, *)$ è un gruppo abeliano.

b) Che periodo hanno i seguenti elementi? $\frac{2}{5}$ [ ]; $\frac{\sqrt{2}}{2}$ [ ]

c) Si trovino gli elementi di G di periodo finito.

Risposta. a) L'operazione * produce in ogni caso un numero ∈[0, 1[, perché x+y, se è ≥ 1, è minore di 2, quindi 0 ≤ x+y-1 < 1. Per dimostrare che G è un gruppo con questa operazione occorre dimostrare che l'operazione è associativa, commutativa, ha elemento neutro ed ogni elemento ha l'inverso.

La commutatività è immediata, perché nei due casi ci si riconduce sempre ad x+y che coincide con y+x.

L'elemento neutro è certamente lo zero: per ogni x, 0 ≤ x < 1,

$$0*x = 0+x = x+0 = x*0 = x.$$

Inoltre, x ha l'inverso (o forse è meglio dire l'opposto) 1-x. Infatti, 1-x∈[0, 1[, ed inoltre

$$x+(1-x) = 1 \Rightarrow x*(1-x) = x+(1-x) - 1 = 0.$$

Resta l'associatività, che è più complicata, dato che occorre considerare più casi.

- se x+y+z < 1 allora anche x+y < 1 ed y+z < 1, quindi, in questo primo caso:

$$(x*y)*z = (x+y)+z = x+(y+z) = x*(y*z)$$

- Sia 1 ≤ x+y+z < 2.
  - Se x+y < 1 allora $(x*y)*z = (x+y)*z = x+y+z-1$.
  - Se x+y ≥ 1 allora essendo x+y+z < 2 si ha (x+y-1)+z < 1, quindi nuovamente $(x*y)*z = (x+y-1)+z = x+y+z-1$.

Valutiamo ora x∗(y∗z).

- Se y+z < 1 allora $x*(y*z) = x*(y+z) = x+y+z-1$.
- Se invece y+z ≥ 1, allora essendo x + (y+z) < 2, segue x + (y+z-1) < 1, quindi $x*(y*z) = x*(y+z) = x+y+z-1$.

Riassumendo, in questo secondo caso:

$$\begin{cases}(x*y)*z = x+y+z-1\\ x*(y*z) = x+y+z-1\end{cases} \Rightarrow (x*y)*z = x*(y*z)$$

- Resta il caso x+y+z ≥ 2. Allora necessariamente x+y ≥ 1 e (x+y-1)+z>1; analogamente, y+z ≥ 1 e x+(y+z-1) ≥ 1, quindi, anche in questo terzo caso:

$$\begin{cases}(x*y)*z = (x+y-1)+z-1\\ x*(y*z) = x+(y+z-1)-1\end{cases} \Rightarrow (x*y)*z = x*(y*z)$$

b) Calcoliamo la tabella dei multipli di 2/5. Ricordiamo che se la somma supera 1 occorre togliere 1 = 5/5.

n	1	2	3	4	**5**	6	…
$n\frac{2}{5}$	$\frac{2}{5}$	$\frac{4}{5}$	$\frac{1}{5}$	$\frac{3}{5}$	0	$\frac{2}{5}$	…

In definitiva, al numero $\frac{2n}{5}$ si toglie ogni volta la sua *parte intera* e si prosegue fino ad ottenere 0, il che avviene per n = 5. Dunque, $\frac{2}{5}$ ha periodo 5.

Consideriamo ora $\frac{\sqrt{2}}{2}$. Facendo tesoro dell'esempio precedente, se il suo periodo è un numero finito m, allora $m\frac{\sqrt{2}}{2}$ è uguale alla sua parte intera, ossia è un intero n. Ne segue $m\frac{\sqrt{2}}{2} = n \Rightarrow \sqrt{2} = \frac{2n}{m} \in \mathbf{Q}$, ma sappiamo che non è così. Dunque, $\frac{\sqrt{2}}{2}$ ha periodo infinito.

c) Come sopra, un $x \in G$ ha periodo finito m se mx è un intero n, quindi se x = n/m, ossia è un numero razionale.

OSSERVAZIONE. La parte a) di questo esercizio si può svolgere in modo assai più veloce e senza tutti quei calcoli, mediante i risultati del terzo paragrafo del capitolo sui gruppi. Infatti, il gruppo G è precisamente il gruppo quoziente (**R/Z**, +)

A.5. – Sia dato il gruppo simmetrico $(S_9, \circ)$. Siano:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 4 & 2 & 7 & 9 & 8 & 6 & 5 \end{pmatrix}, \quad \beta = (1324) \circ (2536) \circ (349).$$

a) Si scompongano α e β in cicli disgiunti e si trovino i loro periodi

b) Si calcolino i loro inversi

c) Si determini il periodo di $\alpha^{-1} \circ \beta \circ \alpha$

Risposta. a) Seguendo la procedura indicata negli appunti sui gruppi si ha:

$$\alpha = (1342) \circ (57869), \Rightarrow |\alpha| = 20 = \text{mcm}(4,5).$$

Più complicata è la fattorizzazione di β, che è data come prodotto di cicli, ma non disgiunti. Partendo dalla fine, detti cioè δ, γ, η i tre cicli tali che $\beta = \delta \circ \gamma \circ \eta$ si ha: $1 \xrightarrow{\eta} 1 \xrightarrow{\gamma} 1 \xrightarrow{\eta} 3 \Rightarrow 1 \xrightarrow{\beta} 3$, e così via. Si ottiene:

$$\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 1 & 9 & 2 & 4 & 7 & 8 & 6 \end{pmatrix} = (13) \circ (25) \circ (496) \Rightarrow |\beta| = \text{mcm}(2,2,3) = 6$$

b) Si ha:

$$\alpha^{-1} = \begin{pmatrix} 3 & 1 & 4 & 2 & 7 & 9 & 8 & 6 & 5 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 1 & 3 & 9 & 8 & 5 & 7 & 6 \end{pmatrix} = (1243) \circ (59687)$$

Allo stesso risultato si può pervenire ricordando che i due cicli che fattorizzano α sono disgiunti e quindi commutano. Inoltre, l'inverso di un ciclo è $(i_1 i_2 \ldots i_{m-1} i_m)^{-1} = (i_1 i_m i_{m-1} \ldots i_2)$. Allora:

$$\alpha^{-1} = (1342)^{-1} \circ (57869)^{-1} = (1243) \circ (59687)$$

Analogamente, $\beta^{-1} = (13)^{-1} \circ (25)^{-1} \circ (496)^{-1} = (13) \circ (25) \circ (469)$

d) Si può calcolare esplicitamente il *coniugato* $\alpha^{-1} \circ \beta \circ \alpha$ di β tramite α:

$$\alpha^{-1} \circ \beta \circ \alpha = (1243) \circ (59687) \circ (13) \circ (25) \circ (496) \circ (1342) \circ (57869) =$$
$$= (12) \circ (368) \circ (49)$$

Si ha quindi $|\alpha^{-1} \circ \beta \circ \alpha| = 6 = |\beta|$.

OSSERVAZIONE. L'ultima proprietà è vera in ogni gruppo e per ogni coppia di elementi. Si ha infatti $\left(\alpha^{-1}\circ\beta\circ\alpha\right)^2 = \alpha^{-1}\circ\beta\circ\alpha\circ\alpha^{-1}\circ\beta\circ\alpha = \alpha^{-1}\circ\beta^2\circ\alpha$ e, per induzione, $\left(\alpha^{-1}\circ\beta\circ\alpha\right)^n = \alpha^{-1}\circ\beta^n\circ\alpha$, sicché $\left(\alpha^{-1}\circ\beta\circ\alpha\right)^n = \mathrm{id} \Leftrightarrow \beta^n = \mathrm{id}$. Dunque, per ogni gruppo G e per ogni $\alpha,\beta\in G$ si ha $\left|\alpha^{-1}\circ\beta\circ\alpha\right| = |\beta|$.

A6. – a) Si trovi il minimo intero $n \geq 2$ tale che il gruppo $(S_n,\circ)$ contenga un elemento di periodo 100.

b) Si trovi il massimo dei periodi degli elementi di $(S_{12},\circ)$

Risposta. a) Una permutazione ha periodo 100 se 100 è il mcm delle lunghezze dei cicli disgiunti che lo fattorizzano. Pertanto, essendo $100 = 2^2\cdot 5^2 = 4\cdot 25$, occorrono almeno un ciclo di lunghezza 4 ed uno di lunghezza 25. Pertanto, occorrono almeno n = 4+25 = 29 oggetti. In effetti, in $(S_{29},\circ)$ c'è l'elemento $\alpha = (1234)\circ(5\ 6\ 7\ \ldots\ 27\ 28\ 29)$ di periodo 100.

b) Si va per tentativi: ad ogni insieme di addendi che ha per somma 12 (*partizione di 12*) corrisponde una permutazione i cui cicli hanno le lunghezze uguali agli addenti. Si cercano quelle partizioni in cui il mcm sia massimo. Vediamo alcuni esempi:

12 = 12, quindi c'è un ciclo di lunghezza 12, p. es. (1 2 3 ... 12)

12 = 6+4+2, quindi c'è una permutazione di periodo mcm(6,4,2) = 12, per esempio $(123456)\circ(7\ 8\ 9\ 10)\circ(11\ 12)$

12 = 9+2+1, quindi c'è una permutazione di periodo mcm(9,2,1) = 18

12 = 7+5, quindi c'è una permutazione di periodo mcm(7,5) = 35

12 = 7+3+2, quindi c'è una permutazione di periodo mcm(7,3,2) = 42

12 = 5+4+3, quindi c'è una permutazione di periodo mcm(5,4,3) = 60

Nel caso di n = 12, il massimo è effettivamente 60.

OSSERVAZIONE. Il problema precedente è collegato alla ricerca di tutte le *partizioni* di un numero intero positivo n, ossia di tutte le liste (non crescenti) di addendi interi positivi aventi per somma n. Il fatto è è che non c'è un algoritmo per determinare direttamente tutte le partizioni di

n, ma si conoscono solo procedimenti ricorsivi. Il più intuitivo è forse il seguente. Siano note le partizioni di $n-1$. Con i due procedimenti A) e B) costruiamo due liste di partizioni di n.

A) si aggiunge 1 in coda a ciascuna partizione di n-1 e si ha una partizione di n;

B) per ogni partizione di n-1, si somma 1 a turno ad ogni addendo e si riordina in senso non crescente la partizione di n così ottenuta.

C) Si ordinano in ordine lessicografico inverso le partizioni di n così trovate e si eliminano infine i doppioni, un lavoraccio …

Vediamo gli esempi piccoli. Le graffe denotano qui insiemi ordinati, quindi con possibili ripetizioni.

- L'unica partizione di 1 è la banale: {1}
- Per trovare le partizioni di 2,
  - A) aggiungiamo 1 in fondo al'unica lista di 1: {1,1};
  - B) sommiamo 1 all'unico elemento di {1} ottenendo {2};
  - C) le partizioni di 2 sono: {2}, {1,1}.
- Per trovare le partizioni di 3,
  - A) aggiungiamo 1 in fondo alle due liste del 2: {2,1}, {1,1,1};
  - B) sommiamo 1 all'unico elemento di {2} ottenendo {3}, e a ciascuno degli elementi di {1,1} ottenendo {2,1} e {1,2};
  - C) riordiniamo ciascuna lista in senso non crescente, poi elenchiamole in ordine lessicografico inverso e sfoltiamo: {3}, {2,1}, {1,1,1}.
- Troviamo le partizioni di 4, senza commenti
  - A) {3,1}, {2,1,1}, {1,1,1,1}
  - B) {4}, {3,1}, {2,2}, {2,1,1}, {1,2,1}, {1,1,2}
  - C) in definitiva, le partizioni di 4 sono: {4}, {3,1}, {2,2}, {2,1,1}, {1,1,1,1}.
- Concludiamo con le partizioni di 5
  - A) {4,1}, {3,1,1}, {2,2,1}, {2,1,1,1}, {1,1,1,1,1}
  - B) {5}, {4,1}, {3,2}, {3,2}, {2,3}, {3,1,1}, {2,2,1}, {2,1,2}, {2,1,1,1}, …
  - C) in definitiva: {5}, {4,1}, {3,2}, {3,1,1}, {2,2,1}, {2,1,1,1}, {1,1,1,1,1}

La crescita è molto più rapida di quel che sembra. Le partizioni di 6 sono 11:

{6}, {5,1}, {4,2}, {4,1,1}, {3,3}, {3,2,1}, {3,1,1,1}, {2,2,2}, {2,2,1,1}, {2,1,1,1,1}, {1,1,1,1,1,1}

Quelle di 7 sono 15 e quelle di 8 sono 22.

Vediamo la seguente tabella, che nella III riga riporta le differenze.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\lvert\wp_n\rvert$	1	2	3	5	7	11	15	22	30	42	56	77
$\Delta\left(\lvert\wp_n\rvert\right)$		1	1	2	2	4	4	7	8	12	14	21

A7. – Nel gruppo simmetrico $(S_5, \circ)$ definiamo la seguente relazione: $x \sim y$ se x ed y, scomposti in prodotto di cicli disgiunti, determinano la stessa partizione di 5.

a) Si dimostri che $\sim$ è una relazione d'equivalenza in S_5

b) Quanti elementi ha l'insieme quoziente?

c) Quanti elementi ha la classe del ciclo (1 2 3 4 5) ?

d) Compilare la tabella con il numero di elementi per ciascuna classe d'equivalenza.

Risposta. a) La verifica che la relazione è di equivalenza è immediata. C'è però un modo più generale per dimostrarlo: associarle una funzione di cui $\sim$ sia il "nucleo". Sia $\wp_5$ l'insieme delle partizioni di 5. Ogni permutazione $\alpha \in S_5$ determina una ed una sola partizione di 5, mediante la sua fattorizzazione in cicli disgiunti. Possiamo considerare quindi la funzione $\rho : S_5 \to \wp_5$, che ad ogni $\alpha \in S_5$ associa la sua partizione di 5. E' chiaro che la relazione $\sim$ coincide con la relazione $\sim_\rho$, tale che $\alpha \sim_\rho \beta \Leftrightarrow \rho(\alpha) = \rho(\beta)$, perciò è di equivalenza, come noto.

b) Ad ogni partizione di 5 è associata almeno una permutazione $\alpha \in S_5$, quindi le classi sono tante quante le partizioni di 5. Le abbiamo trovate prima, e sono 7.

c) Le permutazioni equivalenti al ciclo dato sono tutte e sole quelle a cui corrisponde la partizione {5}, quindi tutti i cicli di lunghezza 5. Nella loro rappresentazione "canonica" si scrivono tutti nella forma $(1\ i_2\ i_3\ i_4\ i_5)$, dove i 4 elementi successivi sono in un ordine qualunque. Dunque, ce ne sono $24 = 4!$.

d) Le partizioni di 5 sono: {5}, {4,1}, {3,2}, {3,1,1}, {2,2,1}, {2,1,1,1}, {1,1,1,1,1}.

Nel punto c) abbiamo sistemato il primo caso. Vediamo il secondo, ossia quanti elementi ha la classe delle permutazioni corrispondenti alla partizione {4,1}. E' costituita dai cicli di lunghezza 4, perciò ragioniamo così: ognuno di tali cicli fissa uno ed un solo oggetto. Possiamo raggruppare questi cicli in cinque insiemi, a seconda dell'oggetto fissato.

I cicli di lunghezza 4 e che fissano il 5 sono del tipo $(1\ i_2\ i_3\ i_4\ 5)$, dove $i_2, i_3, i_4 \in \{2,3,4\}$ in tutti i modi possibili, ma senza ripetizioni, quindi sono in tutto $3! = 6$.

I cicli che fissano il 4 sono del tipo $(1\ i_2\ i_3\ 4\ i_5)$, dove $i_2,\ i_3,\ i_5 \in \{2,3,5\}$ in tutti i modi possibili, ma senza ripetizioni, quindi sono $3! = 6$.
Analogamente, ci sono 6 cicli che fissano il 3, 6 che fissano il 2 e 6 che fissano 1.
Riassumendo, ci sono $5 \cdot 6 = 30$ cicli di lunghezza 4.

Prima di proseguire, riflettiamo sul fatto che i cicli che coinvolgono gli stessi k oggetti, nella loro scrittura "canonica", cominciano sempre con l'oggetto più piccolo, sicché ciò che distingue un ciclo dall'altro è la disposizione degli altri k–1 oggetti. Ci sono perciò (k–1)! cicli distinti sugli stessi k oggetti.

Inoltre, k oggetti da spostare si scelgono in $\binom{n}{k}$ modi diversi fra n oggetti dati.

Ciò posto, vediamo la partizione {3,2}. Tre oggetti si scelgono in $\binom{5}{3} = 10$ modi diversi. Per ciascuna terna scelta, abbiamo (3-1)! = 2 cicli di lunghezza 3. Sui due oggetti rimenenti c'è un solo ciclo di lunghezza 2, quindi avremo $2 \cdot 1 = 2$ permutazioni distinte per ogni terna scelta. In totale, quindi $10 \cdot 2 = 20$ permutazioni corrispondenti alla partizione {3,2}.
Lo stesso accade per la partizione {3,1,1}, cui corrispondono 20 permutazioni, che sono i cicli di lunghezza 3.
Il caso {2,2,1} è il più difficile, ma possiamo ragionare così: ciascuna di queste permutazioni fissa un oggetto, quindi si può pensare come elemento del gruppo simmetrico su 4 oggetti: in questo gruppo, come noto, ci sono tre doppi scambi. Allora, per ogni oggetto fra i 5, ci sono tre doppi scambi che lo fissano. Allora avremo $5 \cdot 3 = 15$ doppi scambi.
Il caso {2,1,1,1} è immediato: si scelgono 2 oggetti fra i 5, in $\binom{5}{2} = 10$ modi diversi, e per ciascuno c'è un solo ciclo di lunghezza 2, quindi in tutto 10 di questi elementi.
Infine, {1,1,1,1,1} corrisponde solo all'identità.
Riassumendo:

{5}	{4,1}	{3,2}	{3,1,1}	{2,2,1}	{2,1,1,1}	{1,1,1,1,1}	7 classi
24	30	20	20	15	10	1	120

OSSERVAZIONE. Facciamo un piccolo gioco di prestigio. Consideriamo due permutazioni di S_5 dello stesso tipo, per esempio {3,2}, $\alpha = (132)\circ(45)$, $\alpha' = (235)\circ(14)$. Costruiamo una permutazione β scrivendo di seguito nella sua I riga gli elementi di α e nella seconda quelle di α' e poi riordiniamo: $\beta = \begin{pmatrix} 1 & 3 & 2 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} = (1254)$. Allora:

$$\beta\circ\alpha\circ\beta^{-1} = (1254)\circ(132)\circ(45)\circ(1452) = (14)\circ(235) = \alpha'$$

E funziona sempre! Non solo, ma, inversamente, per ogni α, $\beta\in S_n$, la permutazione $\alpha' = \beta\circ\alpha\circ\beta^{-1}$, detta *coniugata di* α *mediante* β, ha la scomposizione in cicli dello stesso tipo di quella di α, ossia produce la stessa partizione di n. Ossia, due permutazioni α, $\alpha'\in S_n$ sono coniugate (cioè esiste $\beta\in S_n$ tale che $\alpha' = \beta\circ\alpha\circ\beta^{-1}$) se e solo se le loro scomposizioni in cicli disgiunti producono la stessa partizione di n.

A.8. – Sia dato il gruppo $G = GL_2(3)$ costituito dalle matrici quadrate d'ordine 2 e invertibili ad elementi nel campo $\mathbf{Z}_3 = \{0,1,2\}$. I suoi elementi sono le matrici a determinante $\neq 0$ e l'operazione è il prodotto righe per colonne.

a) Quanti elementi ha G?

b) Che periodo hanno le matrici seguenti?

$$U = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix},\ A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix},\ B = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix},\ C = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix}$$

c) Che cos'hanno di particolare le due matrici $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$?

Risposta. a) Si può rispondere nel modo seguente: sia $M = \begin{bmatrix} x & y \\ z & t \end{bmatrix} \in G$. Allora deve essere det(M) = xt-yz $\neq 0$. Le matrici d'ordine 2 ad elementi in $\mathbf{Z}_3 = \{0,1,2\}$ sono $81 = 3^4$: non sono troppe, si potrebbero verificare una per una, ma forse c'è un modo più furbo. La prima riga deve essere non nulla, altrimenti $\det(M) = 0$, quindi tra le 9 possibili ci sono solo 8 coppie (x,y) accettabili. Per ciascuna di esse, la seconda riga non deve essere direttamente proporzionale alla prima, ossia non deve essere uguale a k(x,y), k = 0, 1 o 2. Ciò esclude tre delle nove coppie (z,t). Allora per ciascuna delle 8 coppie (x,y) abbiamo 6 coppie (z,y) tali che det(M) sia $\neq 0$. Pertanto, abbiamo $8\cdot 6 = 48$ matrici invertibili: $|G| = 48$.

b) $U = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \Rightarrow U^2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \times \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow |U| = 2$ (calcoli in $\mathbf{Z}_3$, ricordiamo).

$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \Rightarrow A^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$, $A^3 = A^2 \times A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow |A| = 3$

$B = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \Rightarrow B^2 = \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix}$, $B^3 = B^2 \times B = \begin{bmatrix} 0 & 2 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix}$

$B^4 = B^3 \times B = \begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \Rightarrow B^8 = \left(B^4\right)^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow |B| = 8$

$C = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \Rightarrow C^2 = \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} \times \begin{bmatrix} 2 & 1 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = A \Rightarrow C^6 = \left(C^2\right)^3 = A^3 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \Rightarrow |C| = 6$

c) Sono due matrici che commutano con tutte le altre matrici $M \in G$. Infatti, la prima è l'elemento neutro I_2, l'altra è $2I_2$. E sono le sole. Infatti, sia $M = \begin{bmatrix} x & y \\ z & t \end{bmatrix} \in G$ una matrice che commuti con tutte le altre. Allora, in particolare, deve commutare per esempio con la matrice $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Ossia:

$$A \times M = \begin{bmatrix} x+z & t+y \\ z & t \end{bmatrix} = \begin{bmatrix} x & x+y \\ z & t+z \end{bmatrix} = M \times A \Rightarrow \begin{cases} x+z = x \\ t+y = x+y \\ z = z \\ t = t+z \end{cases} \Rightarrow \begin{cases} z = 0 \\ t = x \\ 0 = 0 \\ z = 0 \end{cases} \Rightarrow M = \begin{bmatrix} x & y \\ 0 & x \end{bmatrix}$$

Deve commutare anche con la trasposta di A, ossia con $A^T = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$, quindi:

$$A^T \times M = \begin{bmatrix} x+y & y \\ x & x \end{bmatrix} = \begin{bmatrix} x & y \\ x & x+y \end{bmatrix} = M \times A^T \Rightarrow \begin{cases} x+y = x \\ y = y \\ x = x \\ x = x+y \end{cases} \Rightarrow \begin{cases} y = 0 \\ 0 = 0 \\ x = x \\ y = 0 \end{cases} \Rightarrow M = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$$

con $x = 1, 2$, ossia $M = I_2$ oppure $M = 2I_2$.

OSSERVAZIONE. Per ogni campo K e per ogni $n \geq 2$ le sole matrici $\in GL_n(K)$ che commutino con tutte le altre sono le "matrici scalari" $kI_n = \begin{bmatrix} k & 0 & \dots & 0 \\ 0 & k & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & k \end{bmatrix}$, $k \neq 0$.

Se K è finito con q elementi, ce ne sono q-1.

A.9. – Siano $(G,\cdot)$ un gruppo ed $m > 1$ un numero non primo.

a) E' possibile che tutti gli $x \in G,\ x \neq 1_G$, abbiano periodo infinito?

b) E' possibile che tutti gli $x \in G,\ x \neq 1_G$, abbiano periodo m?

c) Esistono gruppi abeliani finiti in cui tutti gli $x \in G,\ x \neq 1_G$ hanno periodo p, con p primo?

d) Esistono gruppi non abeliani in cui tutti gli $x \in G,\ x \neq 1_G$ hanno periodo 2?

Risposta. a) Sì, un esempio è il gruppo $(\mathbf{Z}, +)$.

b) No, infatti siano $m = p \cdot q$ ed $x \in G$, $|x| = m$. Allora $\left|x^q\right| = p < m$. Infatti,

$\forall t \in \mathbf{Z},\ 0 < t < p \Rightarrow qt < m \Rightarrow \left(x^q\right)^t = x^{qt} \neq 1_G$, mentre $\left(x^q\right)^p = x^{qp} = x^m = 1_G$.

c) Sì. Sono i p-gruppi abeliani elementari, prodotti diretti del gruppo ciclico $\left(\mathbf{Z}_p, +\right)$ per se stesso $n \geq 1$ volte.

d) No: se tutti gli elementi $x \in G,\ x \neq 1_G$, hanno periodo 2, allora G è abeliano. Infatti, in tal caso ogni elemento coincide con l'inverso, perciò per ogni $x,y \in G$ si ha: $x \cdot y = \left(x \cdot y\right)^{-1} = y^{-1} \cdot x^{-1} = y \cdot x$.

B) Sottogruppi, sottogruppi normali.

B.1. - Siano $\mathbf{R}$ il campo reale ed $\left(\mathbf{R}^{\mathbf{R}},+\right)$ l'insieme delle funzioni da $\mathbf{R}$ ad $\mathbf{R}$, con l'addizione punto per punto, che come noto è un gruppo abeliano in cui l'elemento neutro è la funzione costante nulla.

a) Una funzione $f:\mathbf{R}\to\mathbf{R}$ si dice *pari* se per ogni $x\in\mathbf{R}$ si ha $f(-x) = f(x)$. Si provi che l'insieme P delle funzioni pari costituisce un sottogruppo di $\left(\mathbf{R}^{\mathbf{R}},+\right)$. E' finito o infinito? Si diano esempi di funzioni pari.

b) Una funzione $f:\mathbf{R}\to\mathbf{R}$ si dice *dispari* se per ogni $x\in\mathbf{R}$ si ha $f(-x) = -f(x)$. Si provi che l'insieme D delle funzioni dispari costituisce un sottogruppo di $\left(\mathbf{R}^{\mathbf{R}},+\right)$. E' finito o infinito? Si diano esempi di funzioni dispari.

c) Si determini $P\cap D$.

d) Si dimostri che l'insieme $P+D=\left\{f\in\mathbf{R}^{\mathbf{R}}\;\middle|\;\exists g\in P,\ h\in D,\ f=g+h\right\}$ costituisce un sottogruppo di $\left(\mathbf{R}^{\mathbf{R}},+\right)$ e che

$$\forall g_1,g_2\in P,\ \forall h_1,h_2\in D,\ g_1+h_1=g_2+h_2\Rightarrow\begin{cases}g_1=g_2\\h_1=h_2\end{cases}$$

e) Si dimostri che ogni *funzione polinomiale* f, definita da $f(x)=\sum_{i=0}^{n}a_i x^i$, appartiene a P+D.

Risposta. a) La funzione costante nulla è ovviamente pari. Se f, g sono funzioni pari, allora per ogni x, (f+g)(-x) = f(-x)+g(-x) = f(x)+g(x) = (f+g)(x), quindi f+g è pari. Infine, (-f)(-x) = -f(-x) = -f(x) = (-f)(x), quindi –f è pari. Dunque, P è un sottogruppo.

Esempi di funzioni pari: le costanti (e sono tante quanti i numeri reali), i monomi di grado pari $a\cdot x^{2n}$, il coseno, il valore assoluto.

b) La funzione costante nulla è dispari, perché -0 = 0. Se f, g sono funzioni dispari, allora per ogni x, (f+g)(-x) = f(-x)+g(-x) = -f(x)-g(x) = (-f-g)(x) = -(f+g)(x), quindi f+g è dispari. Infine, (-f)(-x) = -f(-x) = f(x) = -(-f(x)) = -(-f)(x), quindi –f è dispari. Dunque, anche D è un sottogruppo.

Esempi di funzioni dispari: i monomi di grado dispari $a \cdot x^{2n+1}$ (e sono tanti quanti i numeri reali), il seno.

c) Sia $f \in P \cap D$. Allora, per ogni x∈**R**,

$$\begin{cases} f(-x) = f(x) \\ f(-x) = -f(x) \end{cases} \Rightarrow f(x) = -f(x) \Rightarrow 2f(x) = 0 \Rightarrow f(x) = 0$$

ossia f è la costante nulla.

d) Usiamo le proprietà associativa e commutativa dell'addizione. Si ha:

$$\forall g_1, g_2 \in P,\ \forall h_1, h_2 \in D,\ (g_1 + h_1) + (g_2 + h_2) = (g_1 + g_2) + (h_1 + h_2) \in P + D,$$

quindi P+D è chiuso rispetto a +. Inoltre, 0 = 0+0∈P+D.

Infine, -(g+h)=(-g)+(-h) ∈P+D. Perciò, P+D è un sottogruppo.

Supponiamo ora che uno stesso elemento f di P+D si possa scrivere in due modi:

$$f = g_1 + h_1 = g_2 + h_2.$$

Allora, si ricava $\underbrace{g_1 - g_2}_{\in P} = \underbrace{h_2 - h_1}_{\in D}$. Poiché sono uguali, devono coincidere entrambi col solo elemento comune ai due sottogruppi, cioè con la costante nulla. Ne segue $g_1 = g_2,\ h_1 = h_2$.

e) Se f è il polinomio nullo, allora appartiene a P+D. Altrimenti, $f(x) = \sum_{i=0}^{n} a_i x^i$ è somma di monomi. Riuniamo insieme i monomi di grado pari e quelli di grado dispari: allora $f = \underbrace{(a_0 + a_2x^2 + a_4x^4 + \ldots)}_{\in P} + \underbrace{(a_1x^1 + a_3x^3 + \ldots)}_{\in D} \in P + D$.

OSSERVAZIONE. Il punto d) di questo esercizio è un caso particolare di un fatto generale, che si dimostra allo stesso modo: in un gruppo abeliano (G ,+) la somma H+K di due sottogruppi H, K è sempre un sottogruppo. Inoltre, se H∩K = 0 allora ogni elemento di H+K si esprime in un solo modo nella forma h+k, con h∈H, k∈K.

B.2. - Sia dato il gruppo simmetrico $(S_9, \circ)$ su X = {1,2,...,9} e sia Y= {1,3,4,7}.

a) Sia $H = \{\alpha \in S_9 \mid \forall y \in Y,\ \alpha(y) = y\}$. Si dimostri che è un sottogruppo di S_9. Quanti elementi ha?

b) Sia $K = \{\alpha \in S_9 \mid \forall y \in Y,\ \alpha(y) \in Y\}$. Si dimostri che è un sottogruppo di S_9. Che relazione c'è con H? Quanti elementi ha?

Risposta. a) L'identità fissa tutti i 9 oggetti, dunque fissa anche i 4 appartenenti ad Y ed appartiene perciò ad H. Siano $\alpha,\beta\in H$. Allora per ogni $y\in Y$ si ha:

$$\alpha\circ\beta(y)=\alpha(\beta(y))=\alpha(y)=y,\Rightarrow\alpha\circ\beta\in H$$

$$y=\alpha(y)\Rightarrow\alpha^{-1}(y)=\alpha^{-1}(\alpha(y))=y\Rightarrow\alpha^{-1}\in H$$

Quindi, H è un sottogruppo. I suoi elementi agiscono come permutazioni sull'insieme $X\backslash Y=\{2,5,6,8,9\}$, che ha 5 elementi, in tutti i modi possibili, quindi $|H|=5!=120$.

b) L'identità ovviamente appartiene a K. Siano $\alpha,\beta\in K$. Allora per ogni $y\in Y$, posto $y_1=\beta(y)\in Y$, si ha: $\alpha\circ\beta(y)=\alpha(\beta(y))=\alpha(y_1)\in Y,\Rightarrow\alpha\circ\beta\in K$.

Poiché per ogni $y\in Y$, $y'=\alpha(y)\in Y$ ed inoltre α è biiettiva ed Y è finito, segue che la restrizione di α ad Y è suriettiva e quindi per ogni $y'\in Y$ esiste $y\in Y$ tale che $\alpha(y)=y'$. Ma allora $\alpha^{-1}(y')=y\in Y\Rightarrow\alpha^{-1}\in K$.

Ne segue che anche K è un sottogruppo. Inoltre, $H\subseteq K$, perché per ogni $y\in Y$, $\alpha(y)=y\in Y$. Calcoliamo infine $|K|$. I suoi elementi sono biiezioni che portano Y su se stesso, ma allora portano anche $X\backslash Y$ su se stesso, senza mischiarli. Essi agiscono su Y e su $X\backslash Y$ come permutazioni in tutti i modi possibili. In definitiva, per ogni $\alpha\in K$ esistono una permutazione β che agisce solo su Y ed una, γ, che agisce solo su $X\backslash Y$, tali che $\alpha=\beta\circ\gamma$. Per β ci sono 4! scelte, per γ ce ne sono 5!. Pertanto, $|K|=4!\cdot5!=24\cdot120=2880$.

OSSERVAZIONE. In un gruppo finito $(G,\cdot)$, per mostrare che un sottoinsieme H contenente 1_G è un sottogruppo basta la sua chiusura rispetto al prodotto. Infatti, ogni $h\in H$ ha periodo finito, diciamo m, quindi, essendo H chiuso rispetto al prodotto, $h^{-1}=h^{m-1}=\underbrace{h\cdot h\cdots h}_{m-1}\in H$.

Addirittura, se H è chiuso rispetto al prodotto, per essere un sottogruppo al posto della condizione $1_G\in H$ basta la condizione $H\neq\varnothing$. Infatti, $H\neq\varnothing\Rightarrow\exists h\in H$ e se $|h|=m$ allora $1_G=h^m=\underbrace{h\cdot h\cdots h}_{m}\in H$.

B.3. – Sia dato il gruppo simmetrico $(S_4, \circ)$.

a) E' "lagrangiano"?.

b) Per quali divisori di 24 ci sono sottogruppi ciclici e quanti sono?

Risposta. a) Ricordiamo che il teorema di Lagrange dice che l'ordine di ogni sottogruppo di un gruppo finito G è divisore dell'ordine del gruppo. In alcuni gruppi G, per ogni divisore m dell'ordine di G c'è un sottogruppo di ordine m, e questi gruppi sono detti "lagrangiani".
Nel nostro caso, il gruppo S_4 ha ordine 24. I divisori di 24 sono: 1, 2, 3, 4, 6, 8, 12, 24. Cerchiamo un sottogruppo per ciascuno di questi divisori.

I primi quattro sono immediati, perché S_4 ha cicli di quelle lunghezze.

Per il 6 = 3!, tenendo presente l'esercizio precedente B2 a), basta prendere il sottogruppo formato dalle permutazioni che fissano un elemento, p. es. il 4. Esso agisce sui restanti tre oggetti, quindi è sostanzialmente S_3, che ha 6 elementi.

Per l'8 occorre fantasia: un quadrato ha 4 vertici ed il gruppo D_4, che ha otto elementi, li permuta in 8 modi diversi. Se numeriamo i vertici da 1 a 4, abbiamo 8 permutazioni appartenenti ad S_4 e che formano un sottogruppo d'ordine 8.

D'ordine 12 c'è il sottogruppo alterno A_4, costituito dalle permutazioni pari. D'ordine 24 c'è S_4 stesso. Riassumendo:

ordine	1	2	3	4	6	8	12	24
sottogruppo	$\{id\}$	$\langle(12)\rangle$	$\langle(123)\rangle$	$\langle(1234)\rangle$	S_3	D_4	A_4	S_4

b) Di sottogruppi di ordine 1 ce n'è uno, il banale.
I sottogruppi di ordine primo sono tutti ciclici. Di ordine 2 ce ne sono di due tipi: quelli come $\langle(12)\rangle$, che sono $\binom{4}{2} = 6$, e quelli del tipo $\langle(12)\circ(34)\rangle$, che sono 3 in tutto.

Poiché ci sono $\binom{4}{3}\cdot 2 = 8$ cicli di lunghezza 3, ma ogni sottogruppo ciclico d'ordine 3 ne contiene 2 (il generatore e l'inverso), allora ci sono 8:2 = 4 sottogruppi d'ordine 3.

Ci sono poi 3! = 6 cicli d'ordine 4. Poiché ogni sottogruppo ciclico d'ordine 4 ne contiene 2, ci sono tre sottogruppi ciclici d'ordine 4.
Non ci sono sottogruppi ciclici d'ordine superiore a 4.
Non ci sono sottogruppi ciclici d'ordine 6, perché le due fattorizzazioni di 6, ossia $6 = 6$ e $6 = 2\cdot 3$ richiedono permutazioni rispettivamente su 6 e $2+3 = 5$ oggetti. Ciò esclude anche sottogruppi ciclici di ordine multiplo di 6.
D'altra parte, 8 non è mcm di divisori propri, ed una permutazione di periodo 8 richiede almeno 8 oggetti. Pertanto, S_4 non ha sottogruppi ciclici di ordine 8.

OSSERVAZIONE. Sappiamo che i sottogruppi di **Z** sono tutti ciclici. Sia $(G,\cdot)$ un gruppo ciclico: sarà sempre vero che i suoi sottogruppi sono tutti ciclici?
Sia g un suo generatore, ossia $\langle g\rangle = \{g^n \mid n\in \mathbf{Z}\} = G$ e sia $H \le G$. Anche ogni suo elemento è una potenza di g, ma dobbiamo trovarne una che generi H.
$H = \{1_G\} \Rightarrow H = \langle 1_G\rangle$ ciclico. Sia $H \neq \{1_G\}$, allora esiste in H qualche potenza g^n di g ad esponente non nullo, ma anche $g^{-n} = (g^n)^{-1} \in H$ e tra n e –n uno dei due è positivo.
Perciò in H ci sono potenze di g ad esponente positivo. Sia m il minimo di questi esponenti: allora $H = \langle g^m\rangle$. Infatti, per ogni $x\in H$ esiste $n\in Z$ tale che $x = g^n$. Dividiamo n per m: $n = mq+r$, $0 \le r \le m-1$. Allora

$$g^r = g^{n-mq} = \underbrace{g^n}_{\in H}\cdot \underbrace{(g^m)^{-q}}_{\in H} \in H$$

e per la minimalità di m deve essere r = 0. Allora $x = g^n = (g^m)^q$ e $H = \langle g^m\rangle$.
Pertanto, i sottogruppi di un gruppo ciclico sono tutti ciclici.
Inoltre, un gruppo ciclico finito è lagrangiano. Sia $(G,\cdot)$ ciclico di ordine n, $G = \langle g\rangle$ e sia k un divisore di n. Allora $|\langle g^{n/k}\rangle| = k$. Infatti, $(g^{n/k})^k = g^n = 1$, mentre per ogni $k' < k$ si ha $(n/k)k' < n \Rightarrow (g^{n/k})^{k'} \neq 1$. Allora $|g^{n/k}| = k \Rightarrow |\langle g^{n/k}\rangle| = k$.

B.4. – Sia $G = \left(GL_3(3), \times\right)$ il gruppo delle matrici quadrate di ordine 3 invertibili sul campo $\mathbf{Z}_3 = \{0,1,2\}$, con la moltiplicazione righe per colonne. Denotiamo con m_{ij} gli elementi di una matrice M. Ciò posto:

a) Quanti elementi ha G?

b) Sia $T_3(3) = \{A \in G \mid a_{ij} = 0 \ \forall i, j, \ i > j\}$. Si dimostri che è un sottogruppo di G (sottogruppo *triangolare superiore*). Quanti elementi ha?

c) Sia $D_3(3) = \{A \in G \mid a_{ij} = 0 \ \forall i, j, \ i \neq j\}$. Si dimostri che è un sottogruppo di $T_3(3)$ (sottogruppo *diagonale*). Quanti elementi ha? Che periodo hanno i suoi elementi?

d) Sia $UT_3(3) = \{A \in T_3(3) \mid a_{ii} = 1 \ \forall i\}$. Si dimostri che è un sottogruppo di $T_3(3)$ (sottogruppo *unitriangolare superiore*). Quanti elementi ha? Che periodo hanno i suoi elementi?

e) Si dimostri che ogni elemento di $T_3(3)$ è prodotto di un elemento di $D_3(3)$ per uno di $UT_3(3)$.

Risposta. a) Si può ripetere il ragionamento già visto per $GL_2(3)$. Sia $M = \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & k \end{bmatrix}$. Affinché sia det(M)≠ 0 occorre che la I riga (a, b, c) sia non nulla.

Ci sono $3^3 = 27$ terne (a, b, c), e solo la terna (0,0,0) va esclusa, quindi 27-1 = 26 possibili prime righe. Per ciascuna di esse, la seconda riga non deve essere del tipo k(a, b, c), con k = 0, 1, 2, perciò delle 27 terne (d, e, f) dobbiamo scartarne 3. Ne restano così 27-3 = 24. Abbiamo allora 26·24 = 624 scelte per le prime due righe. Per ciascuna scelta $\begin{bmatrix} a & b & c \\ d & e & f \end{bmatrix}$ delle prime due righe, affinché det(M) sia non nullo occorre che la riga (g,h,k) non sia combinazione lineare delle prime due, ossia non sia del tipo r(a,b,c)+s(d,e,f), con r, s = 0, 1, 2. Al variare di r ed s, ci sono 9 righe "proibite" (g,h,k) = r(a,b,c)+s(d,e,f), quindi restano 27-9 = 18 righe (g,h,k) accettabili. Dunque, abbiamo 624·18 = 11.232 matrici di questo

tipo. Come insegna la geometria, esse hanno *rango* 3 e quindi sono tutte invertibili. Pertanto, $|G| = 11232 = 2^5 \cdot 3^3 \cdot 13$.

b) Trattandosi di un sottoinsieme del gruppo finito G, e che contiene anche la matrice unità $I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, basta provare che $T_3(3)$ è chiuso rispetto al prodotto righe per colonne. I suoi elementi sono del tipo $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{bmatrix}$, con $\det(A) = a_{11} \cdot a_{22} \cdot a_{33} \neq 0$, il che implica che i tre elementi sulla diagonale siano tutti non nulli. Sia anche $B = \begin{bmatrix} b_{11} & b_{12} & b_{13} \\ 0 & b_{22} & b_{23} \\ 0 & 0 & b_{33} \end{bmatrix} \in T_3(3)$. Allora:

$$A \times B = \begin{bmatrix} a_{11} \cdot b_{11} & a_{11} \cdot b_{12} + a_{12} \cdot b_{22} & a_{11} \cdot b_{13} + a_{12} \cdot b_{23} + a_{13} \cdot b_{33} \\ 0 & a_{22} \cdot b_{22} & a_{22} \cdot b_{23} + a_{23} \cdot b_{33} \\ 0 & 0 & a_{33} \cdot b_{33} \end{bmatrix}$$

Questa matrice è triangolare superiore e i tre elementi della diagonale sono non nulli, perché prodotto di elementi a_{ii}, b_{ii} non nulli per ogni i = 1, 2, 3. Pertanto, $T_3(3)$ è un sottogruppo di G. Per calcolarne gli elementi, osserviamo che i tre elementi della diagonale sono non nulli, quindi ciascuno vale 1 o 2. Invece, ciascuno degli altri tre sopra la diagonale può essere indifferentemente 0, 1, 2. Allora ci sono $2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 = 216$ matrici di questo tipo.

c) Le matrici appartenenti a $D_3(3)$ elementi sono del tipo $A = \begin{bmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{bmatrix}$, con $\det(A) = a_{11} \cdot a_{22} \cdot a_{33} \neq 0$, il che implica come sopra che i tre elementi sulla diagonale siano tutti non nulli. Ci sono perciò $2 \cdot 2 \cdot 2 = 8$ matrici di questo tipo, tra le quali c'è l'identità. Sia anche $B = \begin{bmatrix} b_{11} & 0 & 0 \\ 0 & b_{22} & 0 \\ 0 & 0 & b_{33} \end{bmatrix} \in D_3(3)$, allora:

$A \times B = \begin{bmatrix} a_{11} \cdot b_{11} & 0 & 0 \\ 0 & a_{22} \cdot b_{22} & 0 \\ 0 & 0 & a_{33} \cdot b_{33} \end{bmatrix}$, che è diagonale e con determinante non

nullo, quindi è in $D_3(3)$. Ne segue che $D_3(3)$ è un sottogruppo di G, incluso in $T_3(3)$. Si noti che è abeliano e che, essendo in $\mathbf{Z}_3 = \{0,1,2\}$, $\begin{cases} 1^2 = 1 \\ 2^2 = 2 \end{cases}$, allora

$$A^2 = \begin{bmatrix} a_{11}{}^2 & 0 & 0 \\ 0 & a_{22}{}^2 & 0 \\ 0 & 0 & a_{33}{}^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3 \text{ e quindi } \forall A \in D_3(3),\ A \neq I_3 \Rightarrow |A| = 2.$$

d) Gli elementi di $UT_3(3)$ sono del tipo $A = \begin{bmatrix} 1 & a_{12} & a_{13} \\ 0 & 1 & a_{23} \\ 0 & 0 & 1 \end{bmatrix}$ ed I_3 è fra questi.

Sia anche $B = \begin{bmatrix} 1 & b_{12} & b_{13} \\ 0 & 1 & b_{23} \\ 0 & 0 & 1 \end{bmatrix} \in UT_3(3)$. Allora:

$$A \times B = \begin{bmatrix} 1 & a_{12} + b_{12} & a_{12} \cdot b_{23} + a_{13} + b_{13} \\ 0 & 1 & a_{23} + b_{23} \\ 0 & 0 & 1 \end{bmatrix} \in UT_3(3)$$

Pertanto, $UT_3(3)$ è un sottogruppo di G. Per calcolarne gli elementi, osserviamo che ciascuno dei tre elementi sopra la diagonale può essere indifferentemente 0, 1, 2. Allora ci sono $3 \cdot 3 \cdot 3 = 27$ matrici di questo tipo.
Calcoliamo il periodo dei suoi elementi non banali, ricordando che in $\mathbf{Z}_3$ si ha sempre $3x = 0$ per ogni x:

$$A = \begin{bmatrix} 1 & a_{12} & a_{13} \\ 0 & 1 & a_{23} \\ 0 & 0 & 1 \end{bmatrix} \Rightarrow A^2 = \begin{bmatrix} 1 & 2a_{12} & a_{12} \cdot a_{23} + 2a_{13} \\ 0 & 1 & 2a_{23} \\ 0 & 0 & 1 \end{bmatrix},$$

$$A^3 = \begin{bmatrix} 1 & 3a_{12} & 3a_{12} \cdot a_{23} + 3a_{13} \\ 0 & 1 & 3a_{23} \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = I_3 \Rightarrow |A| = 3$$

Questo sottogruppo non è abeliano, infatti

$$B \times A = \begin{bmatrix} 1 & b_{12} + a_{12} & b_{12} \cdot a_{23} + b_{13} + a_{13} \\ 0 & 1 & b_{23} + a_{23} \\ 0 & 0 & 1 \end{bmatrix} = A \times B \Leftrightarrow a_{12} \cdot b_{23} = b_{12} \cdot a_{23}$$

e basta prendere per esempio $a_{12} = 0,\ b_{23} = b_{12} = a_{23} = 1$ perché le due matrici non commutino.

e) Si ha: $\underbrace{\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33} \end{bmatrix}}_{\in T_3(3)} = \underbrace{\begin{bmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33} \end{bmatrix}}_{\in D_3(3)} \times \underbrace{\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}}_{\in UT_3(3)} = \begin{bmatrix} a_{11} & a_{11}\cdot x & a_{11}\cdot y \\ 0 & a_{22} & a_{22}\cdot z \\ 0 & 0 & a_{33} \end{bmatrix} \Leftrightarrow$

$\Leftrightarrow \begin{cases} a_{11}\cdot x = a_{12} \\ a_{11}\cdot y = a_{13} \\ a_{22}\cdot z = a_{13} \end{cases} \Rightarrow \begin{cases} x = a_{12}/a_{11} \\ y = a_{13}/a_{11} \\ z = a_{23}/a_{22} \end{cases}$ (ricordiamo che i tre elementi a_{ii} sono non nulli). Pertanto, effettivamente ogni elemento di $T_3(3)$ è prodotto di un elemento di $D_3(3)$ per uno di $UT_3(3)$. Per esempio: $\begin{bmatrix} 2 & 2 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

OSSERVAZIONE. Per ogni m ≥ 3 esistono gruppi non abeliani G tali che $|G| = p^m$ ed ogni elemento $\neq 1_G$ ha periodo p. Non è difficile infatti dimostrare che il gruppo non abeliano $UT_3(p)$ costituito dalle matrici unitriangolari d'ordine 3 sul campo $\mathbf{Z}_p$ e che ha ordine p^3, ha gli elementi diversi dalla matrice unità I_3 tutti di periodo p. Per induzione, si dimostra innnanzi tutto che per ogni n ≥ 1 si ha $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & na & nb+\binom{n}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{bmatrix}$.

Infatti, $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}^{n+1} = \begin{bmatrix} 1 & na & nb+\binom{n}{2}ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} =$

$$= \begin{bmatrix} 1 & na+a & nb+\binom{n}{2}ac+nac+b \\ 0 & 1 & nc+c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & (n+1)a & (n+1)b+\binom{n+1}{2}ac \\ 0 & 1 & (n+1)c \\ 0 & 0 & 1 \end{bmatrix}$$

Pertanto, per n = p si ottiene la matrice I_3, in quanto, essendo dispari, p divide anche $\binom{p}{2} = p\cdot\frac{p-1}{2}$. Infine, per m ≥ 4, il gruppo $G = UT_3(p) \times \underbrace{\mathbf{Z}_p \times \ldots \mathbf{Z}_p}_{m-3}$ è non abeliano di ordine p^m, con gli elementi $\neq 1_G$ di ordine p. Per m ≤ 2, invece, si può dimostrare che se $|G| = p^m$ allora G è abeliano.

B.5. – Sia $G = UT_3(3)$ il gruppo di matrici già visto nell'esercizio precedente. Si considerino le matrici $A \in UT_3(3)$, $A = \begin{bmatrix} 1 & 0 & a_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $a_{13} \in \mathbf{Z}_3$

a) Formano un sottogruppo di G?

b) Che cos'hanno di particolare?

Risposta. a) L'insieme H di queste tre matrici contiene l'identità. Il prodotto di due di esse è: $A \times B = \begin{bmatrix} 1 & 0 & a_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & b_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & a_{13}+b_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in H$, quindi H è un sottogruppo di G.

b) H sembra uno qualunque dei sottogruppi ciclici d'ordine 3 di G, ma non è così. Infatti, i suoi elementi commutano con tutti gli altri di G:

$$\begin{bmatrix} 1 & m_{12} & m_{13} \\ 0 & 1 & m_{23} \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & a_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & m_{12} & m_{13}+a_{13} \\ 0 & 1 & m_{23} \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & a_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & m_{12} & m_{13} \\ 0 & 1 & m_{23} \\ 0 & 0 & 1 \end{bmatrix}$$

Sono i soli. Infatti, affinché una matrice $M \in G$ commuti con ogni altra $B \in G$, come visto nell'esercizio precedente (con M al posto di A) si deve avere:

$$m_{12} \cdot b_{23} = b_{12} \cdot m_{23} \ \forall b_{12}, b_{23} \in \mathbf{Z}_3,$$

ma allora: $\begin{cases} b_{23} = 0 \\ b_{12} = 1 \end{cases} \Rightarrow m_{23} = 0$, $\begin{cases} b_{23} = 1 \\ b_{12} = 0 \end{cases} \Rightarrow m_{12} = 0$, quindi $M \in H$.

OSSERVAZIONE. In ogni gruppo $(G, \cdot)$ l'insieme degli elementi che commutano con ogni altro è denotato con Z(G) e detto *centro* di G. E' un sottogruppo di G. Infatti, esso contiene ovviamente 1_G. Inoltre, per ogni x, y∈Z(G) si ha:

$$\forall g \in G,\ g \cdot (x \cdot y) = (g \cdot x) \cdot y = (x \cdot g) \cdot y = x \cdot (g \cdot y) = x \cdot (y \cdot g) = (x \cdot y) \cdot g \Rightarrow x \cdot y \in Z(G),$$

$$x \cdot g = g \cdot x \Rightarrow x^{-1} \cdot (x \cdot g) \cdot x^{-1} = x^{-1} \cdot (g \cdot x) \cdot x^{-1} \Rightarrow x^{-1} \cdot g = g \cdot x^{-1} \Rightarrow x^{-1} \in Z(G)$$

ed allora Z(G) è un sottogruppo di G. Inoltre, è normale in G, in quanto per ogni g∈G si ha: gZ(G) = {gx | x∈Z(G)} = {xg | x∈Z(G)} = Z(G)g.

Nel caso di un gruppo finito G, nella tavola di moltiplicazione ogni elemento x∈Z(G) si riconosce perché essendo xg = gx per ogni g∈G, allora la riga e la colonna di x sono

uguali. Se osserviamo la tavola del gruppo S_3, notiamo che solo l'identità ha questa proprietà, quindi $Z(S_3) = \{id\}$.

Al contrario, se G è un gruppo abeliano allora Z(G) = G, e viceversa.

Negli esercizi precedenti abbiamo visto che $Z\left(GL_2(3)\right) = \left\{I_2, 2I_2\right\}$ e che $Z\left(UT_3(3)\right) = \left\{A \in UT_3(3) \mid a_{12} = a_{23} = 0\right\}$. In questi due casi il centro è un sottogruppo proprio e non banale.

B.6. – Sia $(G,\cdot)$ un gruppo abeliano.

a) Sia S l'insieme degli elementi di periodo infinito di G. E' un sottogruppo?

b) Sia T l'insieme degli elementi di periodo finito di G. E' un sottogruppo?

Risposta. a) ovviamente no, dato che l'elemento neutro 1_G 1ha periodo finito 1.

b) Come detto, $1_G \in T$. Inoltre, per ogni x, y∈T, siano h e k i loro periodi ed $m = mcm(h,k)$. Allora $(x\cdot y)^m = x^m \cdot y^m = 1_G \cdot 1_G = 1_G$, dunque x·y ha periodo divisore di m, ossia finito, ed x·y∈T. Infine, $x^h = 1_G \Rightarrow \left(x^{-1}\right)^h = 1_G \Rightarrow x^{-1} \in T$. Pertanto, T è un sottogruppo di G.

OSSERVAZIONE. Il sottoinsieme T degli elementi di periodo finito del gruppo abeliano G è detto *sottogruppo di torsione* di G Se T è il sottogruppo banale, G è detto "privo di torsione". Se G non è abeliano, T non è in generale un sottogruppo.

B.7. – Nel gruppo additivo (**Q**, +) si considerino i due sottogruppi

$$A = \left\langle \frac{5}{12} \right\rangle,\ B = \left\langle \frac{25}{18} \right\rangle.$$

a) Si descrivano gli elementi del sottogruppo M = A+B.

b) Si descrivano gli elementi del sottogruppo L = A∩B

c) Si trovi [M:L].

Risposta. a) Si ha $A = \left\langle \frac{5}{12} \right\rangle = \left\{ h \cdot \frac{5}{12} \mid h \in \mathbf{Z} \right\}$, $B = \left\langle \frac{25}{18} \right\rangle = \left\{ k \cdot \frac{25}{18} \mid k \in \mathbf{Z} \right\}$.

Allora $M = A+B = \left\{ h \cdot \frac{5}{12} + k \cdot \frac{25}{18} \;\middle|\; h,k \in \mathbf{Z} \right\}$. Miglioriamo la rappresentazione degli elementi di M: $h \cdot \frac{5}{12} + k \cdot \frac{25}{18} = \frac{15h+50k}{36} = \frac{5(3h+10k)}{36}$. Ora, il numeratore è multiplo di 5 e l'espressione tra parentesi, essendo MCD(3, 10) = 1, descrive tutto **Z**. Ne segue $M = \left\langle \frac{5}{36} \right\rangle$.

b) Si ha $x \in L \Leftrightarrow$ esistono h, k∈**Z**, tali che $x = h \cdot \frac{5}{12} = k \cdot \frac{25}{18}$. Allora abbiamo l'equazione lineare omogenea $h \cdot \frac{5}{12} = k \cdot \frac{25}{18}$, che diventa l'equazione diofantea $3h = 10k$. Allora $\begin{cases} h = 10t \\ k = 3t \end{cases}$, t∈**Z**, ossia $x \in L \Leftrightarrow x = h \cdot \frac{5}{12} = \frac{50t}{12} = \frac{25}{6}t$.

Pertanto, $L = \left\langle \frac{25}{6} \right\rangle$.

c) L è un sottogruppo di M, che è generato da $\frac{5}{36}$, quindi cerchiamo il minimo intero positivo n tale che $n\frac{5}{36} \in L$. Come sopra, $n\frac{5}{36} = k\frac{25}{6} \Leftrightarrow n = 30k$. Il minimo valore positivo di n è perciò m = 30. Questo è l'indice di L in M.

Infatti, i laterali di L sono tutti del tipo $L + \frac{5r}{36}$, $0 \le r < 30$. Dimostriamolo. Ogni elemento x di M è della forma $\frac{5n}{36}$. Dividiamo n per 30, ottenendo n = 30q+r, 0 ≤ r < 30. Allora

$$x = \frac{5n}{36} = \frac{5}{36}(30q + r) = \underbrace{q\left(\frac{5}{36} \cdot 30\right)}_{\in L} + \frac{5r}{36} \in L + \frac{5r}{36}$$

Per completare la risposta, occorre osservare che per 0 ≤ r < s < 30 i laterali $L + \frac{5r}{36}$, $L + \frac{5s}{36}$, sono diversi. Se fossero uguali, allora $\frac{5s}{36} - \frac{5r}{36} = \frac{5(s-r)}{36} \in L$, con 0 < s–r < 30, contro la minimalità di 30. Dunque, [M:L] = 30.

OSSERVAZIONI. A) E' sempre vero che in un gruppo ciclico $(G,\cdot)$, generato da un elemento g, ogni sottogruppo H ha per indice il minimo esponente positivo m tale che $g^m \in H$, e la dimostrazione generale è la stessa seguita nell'esercizio: si divide ogni intero n per m ottenendo $n = mq+r$, $0 \le r < m$, quindi $g^n = \underbrace{\left(g^m\right)^q}_{\in H} \cdot g^r \in Hg^r$. La minimalità di m assicura che gli m laterali Hg^r di H in G, al variare di r, $0 \le r < m$, sono tutti distinti.
Il fatto che in **Z** il sottogruppo m**Z** abbia indice m è un caso particolare di questo fatto generale sui gruppi ciclici.

B) Un gruppo $(G,\cdot)$, nel quale ogni sottogruppo generato da due elementi è ciclico è detto *localmente ciclico*. E' necessariamente abeliano, perché per ogni $a,b \in G$ il sottogruppo $\langle\{a,b\}\rangle$ è ciclico, quindi abeliano e dunque $a\cdot b = b\cdot a$. Il gruppo $(Q,+)$ è localmente ciclico, perché il discorso fatto con le due frazioni 5/12 e 25/18 del problema precedente si può ripetere in generale per ogni coppia di frazioni. L'esempio dimostra anche che un gruppo localmente ciclico non è necessariamente ciclico.

B.8. - Siano dati il gruppo moltiplicativo $\left(\mathbf{C}^*,\cdot\right)$ dei numeri complessi non nulli ed un numero primo p. Sia $H = \left\{ z \in \mathbf{C}^* \;\middle|\; \exists n \in \mathbf{N},\ z^{p^n} = 1 \right\}$.

a) Si dimostri che H costituisce un sottogruppo di $\left(\mathbf{C}^*,\cdot\right)$.

b) H è finito o infinito? [ ]

c) H è ciclico? [Sì] [No]

Risposta. a) Poiché $1 = 1^{p^0}$, allora $1 \in H$. Siano ora $x, y \in H$. Esistono $m,n \in \mathbf{N}$ tali che $x^{p^m} = y^{p^n} = 1$. Sia s il massimo tra m ed n, allora $p^s = \mathrm{mcm}\left(p^m, p^n\right)$. Pertanto,

$$\left(x\cdot y\right)^{p^s} = x^{p^s}\cdot y^{p^s} = 1 \Rightarrow x\cdot y \in H.$$

Infine, $\left(x^{-1}\right)^{p^m} = \left(x^{p^m}\right)^{-1} = 1^{-1} = 1 \Rightarrow x^{-1} \in H$.

Perciò H è un sottogruppo di $\left(\mathbf{C}^*,\cdot\right)$.

b) Per ogni $n\in\mathbf{N}$ consideriamo $z_n = \cos\left(\frac{2\pi}{p^n}\right) + i\cdot\sin\left(\frac{2\pi}{p^n}\right)$, che è la radice p^n –esima di 1 di argomento minimo ed appartiene ad H. Dalla formula di De Moivre sappiamo che ogni radice dell'equazione $z^{p^n} = 1$ è potenza di questa radice. Pertanto, z_n non è radice p^k –esima di 1 per $k < n$. Allora la successione:

$$\left\{1 = z_0, z_1, z_2, \ldots, z_n, \ldots\right\} \subseteq H$$

ha gli elementi tutti distinti, quindi ha infiniti elementi ed H è infinito.

c) Se H fosse ciclico, sarebbe generato da un elemento di periodo infinito, ma tutti gli elementi di H hanno periodo finito. Infatti, $\forall z\in H\ \exists n\in\mathbf{N}$, $z^{p^n} = 1$, quindi z ha periodo divisore di p^n.

B.9. - Siano $\alpha = (1234)\circ(34567)$ e $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 7 & 5 & 6 & 4 \end{pmatrix}$ due elementi del gruppo simmetrico S_7.

a) $|\alpha| =$ [ ], $|\beta| =$ [ ].

b) Qualcuna delle due appartiene ad A_7? [Sì] [No]. Quale? [ ]

c) Esiste in S_7 una permutazione di periodo 8? [Sì] [No].

Risposta. a) Il calcolo del periodo di α richiede di scriverla come prodotto di cicli disgiunti. Si ha $\alpha = (123)\circ(4567) \Rightarrow |\alpha| = \mathrm{mcm}(3,4) = 12$.

Analogamente, $\beta = (13)\circ(47) \Rightarrow |\beta| = 2$.

b) Poiché $N(\alpha) = (3-1)+(5-1) = 7$, allora α è dispari. Invece, essendo $N(\beta) = 2$, allora β è pari, quindi appartiene al sottogruppo alterno A_7.

c) Una permutazione γ ha periodo 8 se 8 è il mcm dei cicli disgiunti in cui si fattorizza. Ma 8 non è il mcm di numeri minori di 8, quindi nella fattorizzazione di γ c'è almeno un ciclo di lunghezza 8. Ne segue che in S_7 una tal permutazione non esiste.

B.10. - Siano $\alpha = (2345)\circ(12468)$ e $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 4 & 5 & 8 & 7 & 6 \end{pmatrix}$ due elementi del gruppo simmetrico S_8.

a) Si calcolino i prodotti $\alpha\circ\beta$ e $\beta\circ\alpha$

b) Si trovi una permutazione $x \in S_8$ tale che $\alpha\circ\beta = (\beta\circ\alpha)\circ x$

c) $H = \{\tau \in S_8 \mid \tau(7) = 7\}$ costituisce un sottogruppo di S_8? Sì No. Quanti elementi ha?

Risposta. a) Conviene scrivere le due permutazioni nella stessa forma, o nella scrittura su due righe o come prodotti di cicli. Perciò calcoliamo $\beta = (123)\circ(68)$ e poi $\begin{cases} \alpha\circ\beta = (2345)\circ(12468)\circ(123)\circ(68) = (15246) \\ \beta\circ\alpha = (123)\circ(68)\circ(2345)\circ(12468) = (25348) \end{cases}$.

b) Risolviamo l'equazione rispetto ad x:

$$x = (\beta\circ\alpha)^{-1}\circ(\alpha\circ\beta) = (15246)^{-1}\circ(25348) = (16425)\circ(25348) = (1648532)$$

c) L'identità appartiene ad H, poiché porta tra gli altri anche il 7 in sé. Siano $\alpha, \beta \in H$, ossia $\begin{cases} \alpha(7) = 7 \\ \beta(7) = 7 \end{cases}$. Allora, $\alpha\circ\beta(7) = \alpha(\beta(7)) = \alpha(7) = 7$, quindi $\alpha\circ\beta \in H$. Poiché siamo in un gruppo finito, allora questo basta per dimostrare che H è un sottogruppo (in quanto l'inverso α^{-1} di un elemento $\alpha \in H$ è prodotto di un numero finito di fattori $= \alpha$, quindi $\alpha^{-1} \in H$). Infine, H fissa il 7 e agisce come insieme di permutazioni sugli altri 7 oggetti, in tutti i modi possibili, quindi ha 7! = 5040 elementi.

C) Omomorfismi, congruenze, quozienti.

C.1. – Sia I un intervallo di $\mathbf{R}$, siano $\left(\mathbf{R}^I,+\right)$ il gruppo delle funzioni f:I→$\mathbf{R}$, con l'addizione punto per punto, ed il suo sottoinsieme D_I costituito dalle funzioni derivabili su I.

a) Si dimostri che D_I costituisce un sottogruppo di $\mathbf{R}^I$.

b) Si dimostri che la derivata $\frac{d}{dx}: D_I \to \mathbf{R}^I$, che associa ad ogni funzione f derivabile su I la sua derivata f', è un omomorfismo di gruppi.

c) Si trovi il nucleo K dell'omomorfismo $\frac{d}{dx}$.

Risposta. a) Dall'Analisi Matematica sappiamo che la somma e l'opposta di funzioni derivabili su I sono derivabili su I. La funzione nulla è derivabile, quindi D_I costituisce un sottogruppo di $\mathbf{R}^I$.

b) Dall'Analisi Matematica sappiamo che la derivata di una somma di funzioni è la somma delle derivate. Ciò significa che per ogni $f,g \in D_I$ si ha $\frac{d(f+g)}{dx} = \frac{df}{dx} + \frac{dg}{dx}$, quindi $\frac{d}{dx}: D_I \to \mathbf{R}^I$ è in particolare un omomorfismo di gruppi.

c) Come corollario del teorema del valor medio, sappiamo che una funzione che su un intervallo I ha derivata nulla è costante su I. Pertanto, il nucleo K dell'omomorfismo "derivata" $\frac{d}{dx}: D_I \to \mathbf{R}^I$ è costituito dall'insieme delle funzioni costanti su I. Ne segue che due funzioni f, g con la stessa derivata su I appartengono allo stesso laterale di K, ossia g∈f+K. Pertanto, esiste k costante tale che g = f+k.

C.2. – Sia sempre $\mathbf{R}$ il campo reale. Si consideri l'insieme P_1 delle funzioni polinomiali di primo grado f:$\mathbf{R}$→$\mathbf{R}$, f(x) = ax+b, con a ≠ 0.

a) Si dimostri che rispetto all'operazione di composizione, P_1 è un gruppo.

b) Si dimostri che il gruppo $(P_1, \circ)$ è isomorfo al gruppo costruito sull'insieme $G = \mathbf{R}^* \times \mathbf{R} = \{(a,b) \mid a \in \mathbf{R}^*,\ b \in \mathbf{R}\}$ con l'operazione: $(a,b) * (c,d) = (ac, ad+b)$, come nell'esercizio A.2.

Risposta. a) Sappiamo che la composizione di funzioni è associativa. L'elemento neutro è l'identità f(x) = x = 1x+0, che appartiene a P_1. Sia anche g(x) = cx+d, con c ≠ 0. Allora f(g(x)) = a(cx+d)+b = (ac)x+(ad+b)∈ P_1. Infine, posto y = ax+b, ricavando la x si ha $x = \frac{1}{a}y + \frac{-b}{a}$, da cui segue $f^{-1}(x) = \frac{1}{a}x + \frac{-b}{a} \in P_1$. Pertanto, $(P_1, \circ)$ è un gruppo.

b) Per provare che $(P_1, \circ)$ e $(G, *)$ sono isomorfi occorre trovare una biiezione tra di essi che sia un omomorfismo. Sia F: $P_1 \to G$, F(ax+b) = (a,b). Allora, intanto F è una funzione, perché sappiamo che ogni polinomio di I grado si scrive in modo unico nella forma ax+b, a ≠ 0. Per la stessa ragione, F è iniettiva. Inoltre,

$$F(f \circ g(x)) = F((ac)x + (ad+b)) = (ac, ad+b) = (a,b) * (c,d) = F(f(x)) * F(g(x))$$

quindi F è un omomorfismo. Infine, è suriettiva, poiché per ogni (a,b)∈G si ha $(a,b) = F(ax+b)$.

C.3. - Un omomorfismo tra due gruppi G ed H si dice banale se ha per immagine $\{1_H\}$ e quindi ha per nucleo tutto G. Si dica se può esistere un omomorfismo non banale e non iniettivo né suriettivo, un monomorfismo o un epimorfismo tra i gruppi seguenti:

gruppi	Omom. non ban.	monomorfismo	epimorfismo
$(\mathbf{Z}, +)$ e $(S_5, \circ)$			
$(\mathbf{Z}_5, +)$ e $(S_5, \circ)$			
$(\mathbf{Z}_5, +)$ e $(\mathbf{Z}_6, +)$			
$(S_5, \circ)$ e $(\mathbf{Z}, +)$			
$(\mathbf{Z}_6, +)$ e $(S_5, \circ)$			
$(S_5, \circ)$ e $(\mathbf{Z}_2, +)$			

Risposta. Ricordiamo che se fra due insiemi X ed Y c'è un'applicazione iniettiva f, allora $|X| = |\mathrm{im}(f)| \le |Y|$. Se invece c'è un'applicazione f suriettiva, allora $|X| \ge |Y|$. Ciò posto, vediamo i vari casi:

gruppi	Omom. non ban.	monomorfismo	epimorfismo
$(\mathbf{Z},+)$ ed $(S_5,\circ)$	sì	no	no

Infatti, tra $(\mathbf{Z},+)$ e un gruppo qualsiasi G, preso un elemento $a \in G$, la funzione $f:\mathbf{Z}\to G$, $f(n) = a^n$, è sempre un omomorfismo di gruppi. Se $a \ne 1_G$, è non banale. E' iniettiva se e solo se a ha periodo infinito, ed è suriettiva se e solo se $\langle a \rangle = G$. Dato che $(S_5,\circ)$ è finito e non ciclico, allora non ci sono né mono né epimorfismi tra $(\mathbf{Z},+)$ e $(S_5,\circ)$, mentre ci sono $120 = 5!$ omomorfismi distinti, 119 dei quali non banali.

gruppi	Omom. non ban.	monomorfismo	epimorfismo
$(\mathbf{Z}_5,+)$ ed $(S_5,\circ)$	no	sì	no

Infatti, $(S_5,\circ)$ contiene un elemento di periodo 5, per esempio $\alpha = (12345)$, quindi l'applicazione $F : \mathbf{Z}_5 \to S_5$, $F([n]_5) = \alpha^n$ è un monomorfismo. Secondo il teorema fondamentale di omomorfismo, si tratta del monomorfismo indotto da $f : \mathbf{Z} \to S_5$, $f(n) = \alpha^n$ tra il gruppo quoziente $\mathbf{Z}_5 = \mathbf{Z}/5\mathbf{Z}$ e il codominio S_5.

Non ci può essere un epimorfismo, perché il codominio S_5 ha più elementi del dominio $\mathbf{Z}_5$ (o anche perché non è ciclico). Poiché 5 è primo, il dominio $\mathbf{Z}_5$ non ha sottogruppi propri, quindi il nucleo di ogni omomorfismo f uscente da $\mathbf{Z}_5$ è o $\{[0]_5\}$ (ed allora f è iniettivo) oppure è tutto $\mathbf{Z}_5$, quindi f è banale.

gruppi	Omom. non ban.	monomorfismo	epimorfismo
$(\mathbf{Z}_5,+)$ e $(\mathbf{Z}_6,+)$	no	no	no

Infatti, $(\mathbf{Z}_6,+)$ non ha elementi di periodo 5, perciò, tenuto conto di quanto precede, non ci sono omomorfismi non banali.

gruppi	Omom. non ban.	monomorfismo	epimorfismo
$(S_5,\circ)$ e $(\mathbf{Z},+)$	no	no	no

Infatti, gli elementi di S_5 hanno tutti periodo finito, mentre in $\mathbf{Z}$ solo 0 ha periodo finito. Ora, se f:G→H è un omomorfismo, per ogni a∈G si ha: $a^n = 1_G \Rightarrow 1_H = f(1_G) = f(a^n) = (f(a))^n$, quindi $|f(a)|$ è un divisore di $|a|$. In particolare, un elemento di periodo finito non può essere portato in uno di periodo infinito. Ne segue che tra S_5 e $\mathbf{Z}$ non ci sono omomorfismi non banali.

gruppi	Omom. non ban.	monomorfismo	epimorfismo
$(\mathbf{Z}_6,+)$ e $(S_5,\circ)$	sì	sì	no

Infatti, in $(S_5,\circ)$ ci sono elementi di periodo 6, per esempio $\alpha = (123)\circ(45)$. Allora l'applicazione $f:\mathbf{Z}_6 \to S_5$, $f([n]_6) = \alpha^n$, è un monomorfismo tra i due gruppi. Tuttavia, ci sono anche omomorfismi non banali e non iniettivi: posto per esempio $\beta = (123)$, l'applicazione $g:\mathbf{Z}_6 \to S_5$, $f([n]_6) = \beta^n$ è un omomorfismo che ha $\langle\beta\rangle$ come immagine e $\{[0]_6,[3]_6\}$ come nucleo. Non ci sono epimorfismi, perché $(S_5,\circ)$ ha più elementi del dominio (oppure perché non è ciclico).

gruppi	Omom. non ban.	monomorfismo	epimorfismo
$(S_5,\circ)$ e $(\mathbf{Z}_2,+)$	no	no	sì

Infatti, in $(S_5,\circ)$ ci sono più elementi che in $(\mathbf{Z}_2,+)$, il che esclude il monomorfismo. Inoltre, un omomorfismo f non banale tra $(S_5,\circ)$ e $(\mathbf{Z}_2,+)$ ha per immagine più di un elemento, quindi tutti e due ed è necessariamente un epimorfismo; quindi, il suo nucleo deve essere un sottogruppo normale di indice 2 in $(S_5,\circ)$. E un tal sottogruppo esiste: è il sottogruppo alterno A_5. Pertanto, agli elementi del nucleo A_5 è associato l'elemento neutro $[0]_2$, mentre agli altri, ossia alle permutazioni dispari, è associato $[1]_2$. Questa funzione suriettiva è anche un omomorfismo, come si vede esaminando per due permutazioni α,β le quattro possibilità di essere pari o dispari, riassunte dallo specchietto seguente:

$\circ$	pari	dispari
pari	pari	dispari
dispari	dispari	pari

$\xrightarrow{f}$

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

OSSERVAZIONE. Se A e B sono gruppi finiti e G = A×B è il loro prodotto diretto, il periodo di un elemento $g=(a,b)$ è il minimo comune multiplo dei periodi dei due elementi. Infatti, per ogni intero n si ha $g^n=(a^n,b^n)$, quindi n è multiplo di $|g| \Leftrightarrow g^n=1_G=(1_A,1_B) \Leftrightarrow \begin{cases} a^n=1_A \\ b^n=1_B \end{cases} \Leftrightarrow$n è multiplo sia di $|a|$ sia di $|b| \Leftrightarrow$n è multiplo di mcm($|a|,|b|$). Ne segue n = mcm($|a|,|b|$).

Chiamiamo *esponente* exp(G) di un gruppo G il minimo comune multiplo dei periodi dei suoi elementi. Se G è finito, poiché tutti i periodi sono divisori dell'ordine di G, anche exp(G) divide l'ordine di G.

Se A e B sono gruppi ciclici di ordini h e k rispettivamente, e G = A×B allora exp(G)=mcm(h,k). Dunque, G è ciclico se e solo se h e k sono coprimi.

C.4. - Si dimostri che il gruppo simmetrico S_4 ha il centro banale.

Risposta. Una permutazione $\alpha \in S_4$ è nel centro di S_4 se per ogni altra permutazione $\beta \in S_4$ si ha $\alpha \circ \beta = \beta \circ \alpha$. Sia $\alpha \neq$ id. Scomponiamo α in cicli disgiunti ed esaminiamo i vari casi:

- $\alpha=(i_1i_2i_3i_4)$. Posto $\beta=(i_1i_2)$, si ha $\begin{cases} i_1 \xrightarrow{\alpha} i_2 \xrightarrow{\beta} i_1 \\ i_1 \xrightarrow{\beta} i_2 \xrightarrow{\alpha} i_3 \end{cases} \Rightarrow \alpha\circ\beta \neq \beta\circ\alpha$
- $\alpha=(i_1i_2i_3)$. Posto $\beta=(i_1i_2)$, tutto va come sopra.
- $\alpha=(i_1i_2)\circ(i_3i_4)$. Posto $\beta=(i_1i_3)$, si ha $\begin{cases} i_1 \xrightarrow{\alpha} i_2 \xrightarrow{\beta} i_2 \\ i_1 \xrightarrow{\beta} i_3 \xrightarrow{\alpha} i_4 \end{cases} \Rightarrow \alpha\circ\beta \neq \beta\circ\alpha$
- $\alpha=(i_1i_2)$. Posto $\beta=(i_1i_3)$, $i_3 \neq i_2$, tutto va come sopra.

Allora una tale $\alpha \neq$ id nel centro di S_4 non esiste.

C.5. - Si costruiscano gruppi di ordine 24.

Risposta. Incominciamo dai gruppi abeliani. Esprimiamo 24 come prodotto di suoi divisori, per ciascun divisore consideriamo il gruppo ciclico di quell'ordine e applichiamo il risultato contenuto nell'osservazione e nel cap. I degli appunti.
Innanzi tutto, 24 = 12·2 = 8·3 = 6·4 = 6·2·2 = 4·3·2 = 3·2·2·2.
In alcuni di questi casi si hanno fattori coprimi, che si possono sostituire con il loro prodotto: 8·3 = 24, 4·6 = 4·3·2 = 12·2 , 3·2·2·2 = 6·2·2. Allora restano tre prodotti "indipendenti", ossia con mcm distinti, che ci danno gruppi non isomorfi a causa del diverso esponente:

24	mcm(12,2) = 12	mcm(6,2,2) = 6
$\mathbf{Z}_{24}$	$\mathbf{Z}_{12}\times\mathbf{Z}_2$	$\mathbf{Z}_6\times\mathbf{Z}_2\times\mathbf{Z}_2$

Conosciamo poi alcuni gruppi non abeliani di ordine 24: il gruppo simmetrico $(S_4,\circ)$ ed il diedrale $(D_{12},\circ)$. Proviamo a costruirne altri.
Per cominciare, se G = H×K, con almeno uno dei due fattori non abeliano, allora G stesso non è abeliano. Ma allora sono gruppi non abeliani di ordine 24 i gruppi seguenti:

$$A_4\times\mathbf{Z}_2,\ D_6\times\mathbf{Z}_2,\ S_3\times\mathbf{Z}_4,\ S_3\times\mathbf{Z}_2\times\mathbf{Z}_2,\ D_4\times\mathbf{Z}_3,\ Q_8\times\mathbf{Z}_3,\ldots$$

Sappiamo poi che il gruppo $GL_2(3)$ delle matrici invertibili d'ordine 3 sul campo $\mathbf{Z}_3$ ha 48 elementi (cfr. Esercizio A.8.a). Il determinante di una di queste matrici è sempre $\neq 0$, quindi appartiene al gruppo $\mathbf{Z}_3^* = \{1,2\}$ degli elementi invertibili di $\mathbf{Z}_3$. Inoltre, il determinante di un prodotto è il prodotto dei determinanti, quindi $\det: GL_2(3)\to \mathbf{Z}_3^*$ è un omomorfismo di gruppi ed è banalmente suriettivo: $\forall k\in\{1,2\},\ \det\left(\begin{bmatrix} k & 0\\ 0 & 1\end{bmatrix}\right) = k$. Allora è un epimorfismo. Il suo nucleo ha quindi $\frac{|GL_2(3)|}{|\mathbf{Z}_3^*|} = \frac{48}{2} = 24$ elementi, ed è costituito dalle matrici a determinante 1. Tale gruppo si denota con $SL_2(3)$ e si chiama *gruppo speciale lineare* di dimensione 2 sul campo $\mathbf{Z}_3$.

Abbiamo costruito così ben 9 gruppi non abeliani di ordine 24.

Ci saranno tutti? Saranno a due a due non isomorfi?

Il primo quesito è molto difficile e al di fuori della portata di un corso di Algebra. Il secondo è un poco più accessibile. Se si trova una proprietà che è posseduta da alcuni e non dagli altri, si può fare una partizione di questo insieme di 9 gruppi in blocchi disgiunti e forse isolare qualcuno di essi. Per esempio, abbiamo visto che cos'è il centro di un gruppo: è un sottogruppo normale, costituito dagli elementi che commutano con tutti gli altri. Ebbene, se in un prodotto diretto un fattore è abeliano, allora è incluso nel centro. Inoltre, se n ≥ 3 è pari, il gruppo diedrale D_n contiene la *simmetria centrale,* che scambia ogni vertice col vertice opposto ed ogni lato col lato opposto, e la simmetria centrale commuta con ogni altro elemento di D_n. Nel nostro caso, 12 è pari quindi D_{12} ha il centro non banale. Poiché poi in $\mathbf{Z}_3$ si ha 2·2 = 1, allora nel gruppo $SL_2(3)$ c'è la matrice $2I_2 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$, che commuta con tutte le altre, quindi anche $SL_2(3)$ ha il centro non banale. Dall'esercizio C.4. sappiamo che S_4 ha invece il centro banale.

Nessuno degli altri otto gruppi ha il centro banale, quindi nessuno di essi è isomorfo ad S_4.

Gli altri confronti sono assai più difficili e su questi naturalmente soprassediamo.

C.6. - Sia X un insieme e sia $\wp(X)$ l'insieme dei suoi sottoinsiemi. Si definisca in $\wp(X)$ l'operazione seguente: per ogni $A,B\in\wp(X)$, $A\Delta B = (A\setminus B)\cup(B\setminus A)$. Questa operazione è detta *differenza simmetrica.* Si dimostri che $(\wp(X), \Delta)$ è un gruppo.

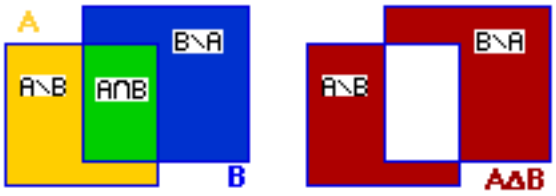
Risposta. E' immediato dimostrare che $A\Delta B = B\Delta A$, $A\Delta\varnothing = \varnothing\Delta A = A$. Inoltre, $A\Delta A = \varnothing$. Una volta dimostrata la proprietà associativa, allora $(\wp(X), \Delta)$ risulterà essere un gruppo abeliano in cui l'elemento neutro è ø ed in cui ogni elemento è inverso di se stesso. La dimostrazione della proprietà associativa si può fare con le tavole di verità. Innanzi tutto, si ha

x∈A	x∈B	x∈AΔB
v	v	f
v	f	v
f	v	v
f	f	f

. Ciò posto:

x∈A	x∈B	x∈C	x∈AΔB	**x∈(AΔB)ΔC**	x∈BΔC	**x∈AΔ(BΔC)**
v	v	v	f	**v**	f	**v**
v	v	f	f	**f**	v	**f**
v	f	v	v	**f**	v	**f**
v	f	f	v	**v**	f	**v**
f	v	v	v	**f**	f	**f**
f	v	f	v	**v**	v	**v**
f	f	v	f	**v**	v	**v**
f	f	f	f	**f**	f	**f**

Pertanto, per ogni $x \in X$ si ha $x \in (A \Delta B) \Delta C \Leftrightarrow x \in A \Delta (B \Delta C)$, ossia $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.



C.7. - Sia $G = \left\{ 2n + \sqrt{2}m \mid m, n \in \mathbf{Z} \right\} \subseteq \mathbf{R}$.

a) Si dimostri che è un sottogruppo di $(\mathbf{R}, +)$.

b) G è ciclico?

Risposta. a) Si ha $0 = 2 \cdot 0 + \sqrt{2} \cdot 0 \in G$. Inoltre, per ogni $2n + \sqrt{2}m$, $2n' + \sqrt{2}m' \in G$,

$$\left(2n + \sqrt{2}m\right) + \left(2n' + \sqrt{2}m'\right) = 2\left(n + n'\right) + \sqrt{2}\left(m + m'\right) \in G,$$

$$-\left(2n + \sqrt{2}m\right) = 2\left(-n\right) + \sqrt{2}\left(-m\right) \in G$$

e quindi G è un sottogruppo.

b) Se G è ciclico esiste un elemento $g = 2n + \sqrt{2}m$ di G tale che ogni altro elemento di G è della forma $kg = k \cdot \left(2n + \sqrt{2}m\right) = 2nk + \sqrt{2}mk$. Tra gli elementi di G ci sono anche 2 e $\sqrt{2}$, ed allora $2nk + \sqrt{2}mk = 2 \Rightarrow \begin{cases} nk = 1 \\ mk = 0 \end{cases} \Rightarrow \begin{cases} k \neq 0 \\ m = 0 \end{cases} \Rightarrow g = 2n$.

Tuttavia, $\sqrt{2}$ non è della forma 2nk per nessun n e k, perciò un tal g non esiste, e G non è ciclico.

C.8. - Sia $\mathbf{N}^+$ l'insieme dei numeri naturali ≥ 1. Per ogni $x, y \in \mathbf{N}^+$ poniamo $x \sim y$ se esistono $m, n \in \mathbf{N}^+$ tali che $x \cdot m^5 = y \cdot n^5$.

a) Si provi che $\sim$ è una relazione d'equivalenza in $\mathbf{N}^+$.

b) Si provi che $\sim$ è compatibile con la moltiplicazione di $\mathbf{N}^+$.

c) $\left[1\right]_{\sim} =$ ____.

d) $\left(\left[3\right]_{\sim}\right)^{-1} =$ ____.

e) Si dimostri che $G = \mathbf{N}^+ / \sim$ è un gruppo.

f) Si trovi una forma canonica per i rappresentanti delle classi e si concluda che $\mathbf{N}^+ / \sim$ è infinito.

Risposta. a) Per cominciare, $x \sim x$ perché $x \cdot 1^5 = x \cdot 1^5$. Poi, sia $x \sim y$, ossia esistono $m,n \in \mathbf{N}^+$ tali che $x \cdot m^5 = y \cdot n^5$. Allora la stessa uguaglianza, letta da destra a sinistra, dice che $y \sim x$.

Oltre a $x \sim y$, sia poi $y \sim z$, ossia esistono $h,k \in \mathbf{N}^+$ tali che $y \cdot h^5 = z \cdot k^5$. Ne segue: $\left(x \cdot m^5\right) \cdot \left(y \cdot h^5\right) = \left(y \cdot n^5\right) \cdot \left(z \cdot k^5\right)$. Si può semplificare per y, che è > 0, ed accorpare potenze con lo stesso esponente, ottenendo: $x \cdot \left(mh\right)^5 = z \cdot \left(nk\right)^5$, quindi $x \sim z$.

b) Si ha: $\begin{cases} x \sim x' \\ y \sim y' \end{cases} \Rightarrow \exists h,k,m,n \in \mathbf{N}^+ \;\middle|\; \begin{cases} x \cdot h^5 = x' \cdot k^5 \\ y \cdot m^5 = y' \cdot n^5 \end{cases} \Rightarrow \left(x \cdot y\right)\left(h \cdot m\right)^5 = \left(x' \cdot y'\right)\left(k \cdot n\right)^5$,

quindi $x \cdot y \sim x' \cdot y'$

c) Si ha $x \sim 1$ se e solo se esistono $m,n \geq 1$ tali che $x \cdot m^5 = n^5$. Ciò significa che m^5 divide n^5 e quindi il quoziente $x = \dfrac{n^5}{m^5} = \left(\dfrac{n}{m}\right)^5$ è un intero ed è una quinta potenza. Inversamente, se $x = k^5$, con k intero, allora $x \cdot 1^5 = 1 \cdot k^5 \Rightarrow x \sim 1$. Pertanto, $\left[1\right]_\sim = \left\{k^5 \;\middle|\; k \in \mathbf{N}^+\right\}$, e questo è l'elemento neutro del monoide quoziente.

d) $\left(\left[3\right]_\sim\right)^{-1} = \left[3^4\right]_\sim$, infatti $\left[3\right]_\sim \cdot \left[3^4\right]_\sim = \left[3^5\right]_\sim = \left[1\right]_\sim$.

e) Il quoziente è un monoide commutativo, perché la proprietà associativa, la commutativa e l'elemento neutro "passano" al quoziente. Basta dimostrare che ogni elemento ha l'inverso. Prendendo spunto dalla risposta precedente, appare chiaro che per ogni x si ha $\left(\left[x\right]_\sim\right)^{-1} = \left[x^4\right]_\sim$. Abbiamo quindi un gruppo in cui ogni elemento diverso dall'unità ha periodo 5.

f) Sia $x \in \mathbf{N}^+$. Scomponiamo x in fattori primi: $x = p_1^{\xi_1} \cdot p_2^{\xi_2} \cdots p_m^{\xi_m}$. Dividiamo per 5 ogni esponente: $\xi_i = 5q_i + r_i$, $1 \leq i \leq m$. Poniamo $\begin{cases} q = p_1^{q_1} \cdot p_2^{q_2} \cdots p_m^{q_m} \\ r = p_1^{r_1} \cdot p_2^{r_2} \cdots p_m^{r_m} \end{cases}$. Allora $x \cdot 1^5 = x = r \cdot q^5 \Rightarrow x \sim r$, con r "libero da quinte potenze".

Per esempio, $\left[192\right]_\sim = \left[2^6 \cdot 3\right]_\sim = \left[2 \cdot 3\right]_\sim = \left[6\right]_\sim$.

Dunque, i rappresentanti "canonici" sono i numeri non multipli di quinte potenze, che a due a due sono non equivalenti. Tra questi ci sono gli infiniti numeri primi: le loro classi sono tutte distinte, quindi ci sono infinite classi.

C.10. - Sia $(\mathbf{Q},+)$ il gruppo additivo del campo razionale e sia $H=\langle 2/3\rangle$ il sottogruppo ciclico generato da $2/3$.

a) $H\cap\mathbf{Z}=$ [ ].

b) Si trovi un elemento $p/q\in\mathbf{Q}$ tale che $H\subset K=\langle p/q\rangle$.

c) Per ogni $x, y\in\mathbf{Q}$ poniamo $x\sim y$ se $x-y\in H$. Si provi che $\sim$ è una relazione d'equivalenza in $\mathbf{Q}$.

d) Si dimostri che la relazione $\sim$ è compatibile con l'addizione di $\mathbf{Q}$.

e) Si trovino gli elementi di periodo finito nel gruppo quoziente $\mathbf{Q}/\sim$.

Risposta. a) Gli elementi di H hanno la forma $\frac{2k}{3}$, $k\in\mathbf{Z}$. Questo elemento appartiene a $\mathbf{Z}$ se e solo se k è multiplo di 3, ossia $k = 3k'$, quindi $\frac{2k}{3}=\frac{2\cdot 3\cdot k'}{3}=2k'\in 2\mathbf{Z}$. Ne segue $H\cap\mathbf{Z}=2\mathbf{Z}$.

b) Un elemento di cui $\frac{2}{3}$ sia un multiplo è per esempio $\frac{p}{q}=\frac{1}{3}$: si ha $\frac{2}{3}=2\cdot\frac{1}{3}$. Invece, quest'ultimo non è multiplo di $\frac{2}{3}$. In definitiva, $H\subset K=\langle 1/3\rangle$.

c) Sappiamo che H è un sottogruppo. La relazione $\sim$ è proprio quella a lui associata nel teorema di Lagrange, $\sim_H$, e che è una relazione d'equivalenza. Le sue classi sono i laterali H+x.

d) Trattandosi di un sottogruppo del gruppo abeliano $(\mathbf{Q}, +)$, allora H è un sottogruppo normale e dunque la relazione $\sim = \sim_H$ è una congruenza.

e) Sia $G = \mathbf{Q}/\sim = \mathbf{Q}/H$. Sia $\frac{p}{q}+H$ un elemento di periodo finito n, con $MDC(p,q) = 1$. Allora $n\left(\frac{p}{q}+H\right)=0_G=0+H\Rightarrow\frac{np}{q}\in H$, cioè esiste $k\in\mathbf{Z}$, tale che $\frac{np}{q}=\frac{2k}{3}$. Di qui segue che 3 divide q, ossia $q = 3q'$. Allora preso $n = 2q'$, si ha

$\frac{2q'p}{3q'} = \frac{2p}{3} \in H$. Hanno periodo finito perciò tutti e soli gli elementi $\frac{p}{q} + H$ il cui denominatore q è multiplo di 3.

C.11. a) Esiste un monomorfismo dal gruppo $(\mathbf{Z}_{10},+)$ al gruppo $(\mathbf{Z}_{15},+)$?

b) Esiste un monomorfismo dal gruppo $(\mathbf{Z},+)$ al gruppo $(\mathbf{C},+)$?

c) Esiste un monomorfismo dal gruppo $(\mathbf{Z}_8,+)$ al gruppo $\left(\mathbf{Z}_{24},+\right)$?

d) Esiste un monomorfismo dal gruppo $(\mathbf{Z}_{15},+)$ al gruppo $\left(\mathbf{C}^*,\cdot\right)$?

Risposta. a) no, perché altrimenti in $(\mathbf{Z}_{15},+)$ ci dovrebbe essere un sottogruppo con 10 elementi.

b) Sì. Per esempio l'immersione, che ad n associa n+0i.

c) Sì. In $\left(\mathbf{Z}_{24},+\right)$ esiste un elemento di periodo 8, ed è $[3]_{24}$. La funzione f che ad ogni $n\in\mathbf{Z}$ associa $n[3]_{24}=[3n]_{24}$ è un omomorfismo, che ha per immagine $\langle[3]_{24}\rangle$, ciclico di ordine 8. Il nucleo è quindi $8\mathbf{Z}$ ed il teorema di omomorfismo assicura l'esistenza di un monomorfismo dal quoziente $\mathbf{Z}_8 = \mathbf{Z}/8\mathbf{Z}$ a $\mathbf{Z}_{24}$.

d) In modo simile, si prenda un elemento di $\left(\mathbf{C}^*,\cdot\right)$ di periodo 15, se esiste, ed allora si ha un monomorfismo tra $\mathbf{Z}_{15} = \mathbf{Z}/15\mathbf{Z}$ e $\left(\mathbf{C}^*,\cdot\right)$. Si consideri una radice quindicesima primitiva di 1, per esempio $\varepsilon = \cos\left(\frac{2\pi}{15}\right) + i\cdot\sin\left(\frac{2\pi}{15}\right)$, che ha proprio periodo 15, essendo radice del polinomio $z^{15}-1$ e non di polinomi z^k-1, $k<15$.

C.12. a) Esiste un epimorfismo dal gruppo $\left(\mathbf{C}^*,\cdot\right)$ al gruppo $\left(\mathbf{R}^+,\cdot\right)$?

b) Esiste un epimorfismo dal gruppo $\left(\mathbf{Z}_{15},+\right)$ al gruppo $\left(\mathbf{Z}_{12},+\right)$?

c) Esiste un epimorfismo dal gruppo $\left(\mathbf{Z}_{24},+\right)$ al gruppo $\left(\mathbf{Z}_6,+\right)$?

Risposta. a) sì, è il modulo: $|a+ib| = \sqrt{a^2+b^2} \in \mathbf{R}^+$. È suriettivo perché per ogni numero reale positivo a si ha $|a+i0| = \sqrt{a^2+0^2} = \sqrt{a^2} = a$. È un omomorfismo, perché il modulo di un prodotto è il prodotto dei moduli. Il suo nucleo è

costituito dai numeri complessi di modulo 1, ossia, geometricamente, dalla circonferenza di centro O = (0, 0) e raggio 1.

b) No. Se ci fosse, il suo nucleo avrebbe indice 12, che non divide 15.

c) Sì, è la funzione f che associa ad ogni $[k]_{24}$ l'elemento $[k]_6$. È una funzione, perché se $[k]_{24} = [k']_{24}$ allora $k \equiv k' \pmod{24}$, ossia

$$k' = k + 24q = k + 6(4q) \Rightarrow k \equiv k' \pmod 6 \Rightarrow [k]_6 = [k']_6.$$

Inoltre, è banalmente un omomorfismo, ed è suriettiva. Il nucleo di f è $\langle [6]_{24} \rangle$.

C.13. a) Si descriva il gruppo $((\mathbf{Z}_{20})^*, \cdot)$.

b) Si descriva il gruppo $((\mathbf{Z}_{24})^*, \cdot)$.

Risposta. a) Si ha $\varphi(20) = (2^2 - 2)\cdot(5-1) = 8$. Gli elementi primi con 20 sono 1, 3, 7, 9, 11, 13, 17, 19. L'11 ha periodo 2, così come il 9 ed il 19. Si ha $3^{-1} = 3^3 = 7$, $13^{-1} = 13^3 = 17$ ed il 3, il 7, il 13 ed il 17 hanno ordine 4. Si ha $\langle 3 \rangle \cap \langle 11 \rangle = \{1\}$, $\langle 3 \rangle \cdot \langle 11 \rangle = (\mathbf{Z}_{20})^*$. Pertanto, si ha $(\mathbf{Z}_{20})^* \cong \mathbf{Z}_4 \times \mathbf{Z}_2$.

b) Si ha $\varphi(24) = (2^3 - 2^2)\cdot(3-1) = 8$. Gli elementi primi con 24 sono 1, 5, 7, 11, 13, 17, 19, 23. Ogni elemento $\neq 1$ ha periodo 2, pertanto, si ha $(\mathbf{Z}_{24})^* \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, perché non ci sono elementi di periodo maggiore di 2.

OSSERVAZIONE. Ci sono tre tipi di gruppi abeliani con 8 elementi: $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$, $\mathbf{Z}_4 \times \mathbf{Z}_2$, $\mathbf{Z}_8$. Tra questi, il gruppo ciclico $\mathbf{Z}_8$ non è isomorfo ad un gruppo $((\mathbf{Z}_m)^*, \cdot)$. Infatti, 8 si ottiene solo nei seguenti casi:

$8 = 2^4 - 2^3 = \varphi(16)$	$8 = 2\cdot 4 = (3-1)\cdot(5-1) = \varphi(15)$	$8 = (2-1)\cdot(3-1)\cdot(5-1) = \varphi(30)$
$8 = (2^3 - 2^2)\cdot(3-1) = \varphi(24)$	$8 = (2^2 - 2)\cdot(5-1) = \varphi(20)$	

In nessuno di questi casi si ottengono elementi di periodo 8.

C.14. Si dimostri il **teorema di Eulero**: per ogni a, m∈**Z**, non nulli,

$$\mathrm{MCD}(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod m.$$

Risposta. Un tale elemento a è invertibile modulo m, quindi $[a]_m \in (\mathbf{Z}_m)^*$. Quest'ultimo gruppo ha ordine $\varphi(m)$. Per il teorema di Lagrange si ha allora $[a]_m^{\varphi(m)} = [1]_m \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m}$.

OSSERVAZIONE. In particolare, per ogni p primo e per ogni a non multiplo di p si ha $a^{p-1} \equiv 1 \pmod{p}$. Perciò per ogni $a \in \mathbf{Z}$ si ha $a^p \equiv a \pmod{p}$ (**Teorema di Fermàt**).