Risoluzione esercizi di Matematica Discreta

A cura della dott.ssa Maria Santa Santo

Indice

1 Esercizi sulle funzioni **1**

2 Esercizi sulle relazioni d'ordine e di equivalenza **8**

3 Esercizi sul principio di induzione **15**

4 Esercizi sulle strutture algebriche: gruppi, anelli e campi **19**

Capitolo 1

Esercizi sulle funzioni

Di seguito proponiamo lo svolgimento di alcuni esercizi sulle funzioni. Per comprenderli meglio è necessario che si abbiano i seguenti prerequisiti:

1. conoscenza del concetto di funzione,
2. di funzione iniettiva, suriettiva, biiettiva,
3. di funzione inversa,
4. di composizione di funzioni.

Esercizio 1.1 Siano date le seguenti leggi

$$g\colon \mathbb{N} \to \mathbb{R}, \qquad g(n) = \sqrt{n} - 4$$

e

$$h\colon \mathbb{R} \to \mathbb{R}, \qquad h(x) = x^3 + 5.$$

Stabilire se sono funzioni. In caso affermativo, provare se sono iniettive, suriettive o biiettive. Calcolare, ove possibile, le funzioni inverse g^{-1} e h^{-1}, e le composizioni $h \circ g$ e $g \circ h$.

Svolgimento. La legge definita da h è sicuramente una funzione, infatti ad ogni valore x di $\mathbb{R}$ viene associata la sua potenza x^3, che è ancora un numero reale, sommata al numero reale 5. Complessivamente si ottiene un numero reale. Anche la legge definita da g è una funzione, infatti ad ogni numero naturale n viene associata la sua radice quadrata $\sqrt{n}$, che è ancora un numero reale (oltre ad essere ben definita dato che è la radice quadrata di un numero positivo) a cui viene sottratto il numero 4. L'immagine di n non sarà sempre un numero naturale, ma sicuramente un numero reale (ricordiamo che l'insieme dei numeri reali è formato dai numeri naturali, interi, razionali e

irrazionali).
Detto ciò, stabiliamo se g è iniettiva cioè:

$$\forall n_1, n_2 \in \mathbb{N} \quad g(n_1) = g(n_2) \Rightarrow n_1 = n_2.$$

Siano $n_1, n_2 \in \mathbb{N}$ tali che $g(n_1) = g(n_2)$ e proviamo che $n_1 = n_2$. Si ha:

$$g(n_1) = g(n_2) \Leftrightarrow \sqrt{n_1} - 4 = \sqrt{n_2} - 4 \Leftrightarrow \sqrt{n_1} = \sqrt{n_2} \Leftrightarrow n_1 = \pm n_2.$$

Ma l'insieme di partenza di g è $\mathbb{N}$, pertanto $n_1 = \pm n_2$ se e solo se $n_1 = n_2$ (escludiamo il caso $n_1 = -n_2$, infatti, in tal caso, si otterrebbe un numero naturale, n_1, uguale ad un numero negativo $-n_2$, che è sicuramente negativo poiché n_2 è un numero positivo). Quindi g è iniettiva. Ora, vogliamo controllare se g è suriettiva, cioè:

$$\forall x \in \mathbb{R} \quad \exists n \in \mathbb{N} \text{ tale che } g(n) = x.$$

Sia $x \in \mathbb{R}$ e si supponga che esista $n \in \mathbb{N}$ tale che $g(n) = x$, quindi si ha

$$g(n) = x \Leftrightarrow \sqrt{n} - 4 = x \Leftrightarrow \sqrt{n} = x + 4.$$

Sicuramente se $x = -10$ si ottiene $\sqrt{n} = -6$, ma ciò è impossibile poiché la radice quadrata di un numero (positivo) è sempre una quantità positiva. Allora g non è suriettiva. Da ciò risulta che g non è biiettiva e quindi non ammette inversa g^{-1}.
Per quanto riguarda h, stabiliamo se è iniettiva cioè:

$$\forall x_1, x_2 \in \mathbb{R} \quad h(x_1) = h(x_2) \Rightarrow x_1 = x_2.$$

Siano $x_1, x_2 \in \mathbb{R}$ tali che $h(x_1) = h(x_2)$ e proviamo che $x_1 = x_2$. Si ha:

$$h(x_1) = h(x_2) \Leftrightarrow x_1^3 + 5 = x_2^3 + 5 \Leftrightarrow x_1^3 = x_2^3 \Leftrightarrow x_1 = x_2.$$

Quindi h è iniettiva. Ora, controlliamo se h è suriettiva cioè:

$$\forall y \in \mathbb{R} \quad \exists x \in \mathbb{R} \text{ tale che } h(x) = y.$$

Sia $y \in \mathbb{R}$ e si supponga che esista $x \in \mathbb{R}$ tale che $h(x) = y$, quindi si ha

$$h(x) = y \Leftrightarrow x^3 + 5 = y \Leftrightarrow x^3 = y - 5 \Leftrightarrow x = \sqrt[3]{y - 5}. \tag{1.1}$$

Osserviamo che la radice cubica del numero reale $y - 5$ è sicuramente un numero reale per ogni scelta di y in $\mathbb{R}$ (dato che abbiamo una radice di indice dispari non è necessario che sia verificata la condizione che il radicando $(y-5)$

sia maggiore o uguale a 0). Pertanto h è suriettiva. Poiché h è iniettiva e suriettiva allora è biiettiva. Possiamo determinare l'inversa di h data dalla funzione

$$h^{-1}: \mathbb{R} \to \mathbb{R}, \qquad h^{-1}(y) = \sqrt[3]{y-5},$$

la cui espressione è ottenuta sfruttando il calcolo (1.1) fatto per provare la proprietà suriettiva. Infine, ci chiediamo se sono possibili le composizioni $g \circ h$ e $h \circ g$. Ricordiamo che la composizione tra due funzioni $f \circ g$ è possibile se il dominio (insieme di partenza) della funzione f coincide con il codominio (insieme di arrivo) della funzione g. Nel nostro caso, notiamo che il dominio di g è $\mathbb{N}$ e non coincide con il codominio di h che è $\mathbb{R}$. Pertanto non è possibile determinare $g \circ h$. D'altra parte, per quanto riguarda $h \circ g$, si ha che il dominio di h, cioè $\mathbb{R}$, coincide con il codominio di g, cioè $\mathbb{R}$. Quindi possiamo calcolare la composizione di h con g:

$$h \circ g: \mathbb{N} \to \mathbb{R} \to \mathbb{R}, \qquad h(g(n)) = h(\sqrt{n}-4) = (\sqrt{n}-4)^3 + 5.$$

Esercizio 1.2 Siano date le seguenti funzioni

$$h: \mathbb{Z} \to \mathbb{R} - \{1\}, \qquad h(x) = 2 \mid x \mid -\frac{1}{2}$$

e

$$g: \mathbb{R} - \{1\} \to \mathbb{R} - \{0\}, \qquad g(n) = n^3 - 1.$$

Stabilire se sono iniettive, suriettive o biiettive. Calcolare, ove possibile, le funzioni inverse h^{-1} e g^{-1}, e le composizioni $h \circ g$ e $g \circ h$.

Svolgimento. Osserviamo che l'esercizio non ci chiede di verificare che le leggi assegnate siano funzioni, pertanto procediamo direttamente nella verifica delle loro proprietà. Consideriamo inizialmente la funzione h e stabiliamo se è iniettiva. Siano $x_1, x_2 \in \mathbb{Z}$ tali che $h(x_1) = h(x_2)$, si ha

$$h(x_1) = h(x_2) \Leftrightarrow 2 \mid x_1 \mid -\frac{1}{2} = 2 \mid x_2 \mid -\frac{1}{2} \Leftrightarrow 2 \mid x_1 \mid = 2 \mid x_2 \mid \Leftrightarrow \mid x_1 \mid = \mid x_2 \mid.$$

Ma

$$\mid x_1 \mid = \mid x_2 \mid \Leftrightarrow x_1 = \pm x_2,$$

quindi, dato che x_1 e x_2 sono due numeri interi, non è possibile escludere nessun caso (diversamente da quanto fatto nell'esercizio precedente): x_1 può essere uguale a x_2, ma può anche essere uguale a $-x_2$. Quest'ultima possibilità (cioè $x_1 = -x_2$) ci dice che h non è iniettiva.
Inoltre h non è suriettiva. Infatti, sia $y \in \mathbb{R} - \{1\}$ e si supponga che esista $x \in \mathbb{Z}$ tale che $h(x) = y$, quindi

$$h(x) = y \Leftrightarrow y = 2 \mid x \mid -\frac{1}{2} \Leftrightarrow 2 \mid x \mid = y + \frac{1}{2} \Leftrightarrow \mid x \mid = \frac{y}{2} + \frac{1}{4}.$$

Se $y = 4$ allora

$$| x |= \frac{4}{2} + \frac{1}{4} \Leftrightarrow | x |= 2 + \frac{1}{4} \Leftrightarrow | x |= \frac{9}{4} \Leftrightarrow x = \pm\frac{9}{4} \notin \mathbb{Z}.$$

Ciò contraddice la definizione di suriettività (in corrispondenza dell'y fissato, abbiamo determinato x che non è un numero intero). Possiamo dedurre che h non è suriettiva e quindi neanche biiettiva. In realtà, potevamo già dedurlo dopo aver verificato che h non è iniettiva. Pertanto non è possibile calcolare h^{-1}.
Ora, stabiliamo se g è iniettiva. Siano $n_1, n_2 \in \mathbb{R}-\{1\}$ tali che $g(n_1) = g(n_2)$, quindi si ha

$$g(n_1) = g(n_2) \Leftrightarrow n_1^3 - 1 = n_2^3 - 1 \Leftrightarrow n_1^3 = n_2^3 \Leftrightarrow n_1 = n_2.$$

Ciò prova che g è iniettiva. Vediamo se g è anche suriettiva. Sia $x \in \mathbb{R} - \{0\}$ e si supponga che esista $n \in \mathbb{R} - \{1\}$ tale che $g(n) = x$, quindi

$$g(n) = x \Leftrightarrow n^3 - 1 = x \Leftrightarrow n^3 = x + 1 \Leftrightarrow n = \sqrt[3]{x+1}.$$

Poiché x è un numero reale diverso da 0, allora il radicando $x + 1$ è sempre diverso da 1, e quindi $n = \sqrt[3]{x+1}$ è sicuramente un elemento di $\mathbb{R} - \{1\}$. Pertanto g è suriettiva, e quindi biiettiva. La sua inversa è data dalla funzione

$$g^{-1} \colon \mathbb{R} - \{0\} \to \mathbb{R} - \{1\}, \qquad g^{-1}(x) = \sqrt[3]{x+1}.$$

Osserviamo che l'unica composizione possibile è $g \circ h$, infatti solo in questo caso risulta che il dominio della prima funzione (g) coincide con il codominio della seconda funzione (h). Quindi, si ha

$$g \circ h \colon \mathbb{Z} \to \mathbb{R} - \{1\} \to \mathbb{R} - \{0\},$$

$$g(h(x)) = g\biggl(2 \mid x \mid - \frac{1}{2}\biggr) = \biggl(2 \mid x \mid - \frac{1}{2}\biggr)^3 - 1.$$

Esercizio 1.3 Siano date le seguenti leggi

$$h \colon \mathbb{R} \to \mathbb{R}, \qquad h(a) = a^5 - 2$$

e

$$g \colon \mathbb{Q} \to \mathbb{R}, \qquad g(n) = 2 - n^2.$$

Stabilire se sono funzioni, ed in tal caso se sono iniettive, suriettive o biiettive.Calcolare, ove possibile, le funzioni inverse h^{-1} e g^{-1}, e le composizioni $h \circ g$ e $g \circ h$.

Svolgimento. Innanzitutto osserviamo che entrambe le leggi sono due funzioni; infatti h ad ogni valore a di $\mathbb{R}$ associa la sua quinta potenza a^5, che è ancora un numero reale, e ad essa sottrae 2. Sicuramente la quantità che si ottiene è un numero reale. Con un ragionamento analogo, considerata la legge definita da g, osserviamo che ad ogni n, numero razionale, viene associato n^2 che è un numero razionale, e quindi reale, che viene sottratto da 2, ottenendo ancora un numero reale. Pertanto possiamo procedere verificando se g ed h sono funzioni iniettive, suriettive e biiettive. Consideriamo la funzione h e stabiliamo se è iniettiva. Siano $a_1, a_2 \in \mathbb{R}$ tali che $h(a_1) = h(a_2)$, quindi

$$h(a_1) = h(a_2) \Leftrightarrow a_1^5 - 2 = a_2^5 - 2 \Leftrightarrow a_1^5 = a_2^5 \Leftrightarrow a_1 = a_2,$$

da cui risulta che h è iniettiva.
Proviamo la suriettività: sia $y \in \mathbb{R}$ e si supponga che esista $a \in \mathbb{R}$ tale che $h(a) = y$, quindi

$$h(a) = y \Leftrightarrow a^5 - 2 = y \Leftrightarrow a^5 = y + 2 \Leftrightarrow a = \sqrt[5]{y+2} \in \mathbb{R}.$$

Allora h è suriettiva, quindi biiettiva, e pertanto possiamo determinare la sua inversa

$$h^{-1}\colon \mathbb{R} \to \mathbb{R}, \qquad h^{-1}(y) = \sqrt[5]{y+2}.$$

Procediamo analogamente per g. Dapprima, stabiliamo se è iniettiva. Siano $n_1, n_2 \in \mathbb{Q}$ tali che $g(n_1) = g(n_2)$, quindi si ha

$$g(n_1) = g(n_2) \Leftrightarrow 2 - n_1^2 = 2 - n_2^2 \Leftrightarrow n_1^2 = n_2^2 \Leftrightarrow n_1 = \pm n_2,$$

cioè la funzione g non è iniettiva (non è possibile escludere il caso $n_1 = -n_2$ poiché n_1 e n_2 sono due numeri razionali e pertanto potrebbero essere negativi). Ciò esclude il caso che g possa essere biiettiva. Inoltre g non è suriettiva, infatti fissato $y \in \mathbb{R}$, si supponga che esista $n \in \mathbb{Q}$ tale che $g(n) = y$, si ha

$$g(n) = y \Leftrightarrow 2 - n^2 = y \Leftrightarrow n^2 = y + 2 \Leftrightarrow n = \pm\sqrt{y+2}.$$

Ma $\sqrt{y+2} \notin \mathbb{Q}$, infatti se $y = 3$ si avrebbe $\sqrt{y+2} = \sqrt{5}$ che non è un numero razionale. Quindi g non è suriettiva e pertanto non è possibile determinare la sua inversa. Per quanto riguarda le composizioni $g \circ h$ e $h \circ g$, osserviamo che l'unica ammissibile è la seconda dato che solo in questo caso il dominio di h coincide con il codominio di g. Pertanto si ha

$$h \circ g\colon \mathbb{Q} \to \mathbb{R} \to \mathbb{R}, \qquad h(g(n)) = h(2 - n^2) = (2 - n^2)^5 - 2.$$

Esercizio 1.4 Siano date le seguenti leggi

$$h\colon \mathbb{N} \to \mathbb{R}, \qquad h(x) = \frac{1+x}{x+5}$$

e

$$f\colon \mathbb{R} \to \mathbb{R}, \qquad f(z) = \frac{1}{4}z^3 + 7.$$

Stabilire se sono funzioni, ed in tal caso se sono iniettive, suriettive o biiettive. Calcolare, ove possibile, le funzioni inverse h^{-1} e f^{-1}, e le composizioni $h \circ f$ e $f \circ h$.

Svolgimento. Inizialmente stabiliamo se h e g sono due funzioni. Osserviamo che h, ad ogni numero naturale x, associa sempre un numero razionale e quindi un numero reale (x assume valori maggiori o uguali a 0 quindi il denominatore $x+5$ è sempre strettamente maggiore di 0). La legge definita da g ad ogni numero reale z associa la sua terza potenza z^3 moltiplicata per $\frac{1}{4}$ ottenendo ancora un numero reale, che, sommato a 7, appartiene all'insieme di arrivo.
Ora, possiamo stabilire se h è una funzione iniettiva. Siano $x_1, x_2 \in \mathbb{N}$ tali che $h(x_1) = h(x_2)$, allora si ha

$$\begin{aligned} h(x_1) = h(x_2) &\Leftrightarrow \frac{1+x_1}{x_1+5} = \frac{1+x_2}{x_2+5} \\ &\Leftrightarrow (1+x_1)(x_2+5) = (1+x_2)(x_1+5) \\ &\Leftrightarrow x_2 + 5 + x_1x_2 + 5x_1 = x_1 + 5 + x_1x_2 + 5x_2 \\ &\Leftrightarrow x_2 + 5x_1 = x_1 + 5x_2 \\ &\Leftrightarrow 4x_1 = 4x_2 \\ &\Leftrightarrow x_1 = x_2. \end{aligned}$$

Allora h è iniettiva. Controlliamo se è anche suriettiva. Sia $y \in \mathbb{R}$ e si supponga che esiste $x \in \mathbb{N}$ tale che $h(x) = y$, allora

$$\begin{aligned} h(x) = y &\Leftrightarrow \frac{1+x}{x+5} = y \\ &\Leftrightarrow 1 + x = y(x+5) \\ &\Leftrightarrow 1 + x = yx + 5y \\ &\Leftrightarrow x - yx = 5y - 1 \\ &\Leftrightarrow x(1-y) = 5y - 1 \\ &\Leftrightarrow x = \frac{5y-1}{1-y}. \end{aligned}$$

Se $y = 2$ si ottiene $x = -9 \notin \mathbb{N}$. Quindi h non è suriettiva. Perciò non è biiettiva e non possiamo determinare la sua inversa. Ora, vediamo che f è iniettiva. Infatti, siano $z_1, z_2 \in \mathbb{R}$ tali che $f(z_1) = f(z_2)$, allora

$$f(z_1) = f(z_2) \Leftrightarrow \frac{1}{4}z_1^3 + 7 = \frac{1}{4}z_2^3 + 7 \Leftrightarrow \frac{1}{4}z_1^3 = \frac{1}{4}z_2^3 \Leftrightarrow z_1^3 = z_2^3 \Leftrightarrow z_1 = z_2.$$

Ora, verifichiamo la suriettività: sia $y \in \mathbb{R}$ e si supponga che esista $z \in \mathbb{R}$ tale che $f(z) = y$, allora

$$f(z) = y \Leftrightarrow \frac{1}{4}z^3 + 7 = y \Leftrightarrow \frac{1}{4}z^3 = y - 7 \Leftrightarrow z^3 = 4y - 28 \Leftrightarrow z = \sqrt[3]{4y - 28}.$$

Sicuramente z è un numero reale, perciò f è anche suriettiva e quindi biiettiva. Determiniamo la funzione inversa di f, cioè

$$f^{-1}\colon \mathbb{R} \to \mathbb{R}, \qquad f^{-1}(y) = \sqrt[3]{4y - 28}.$$

Determiniamo le composizioni $h \circ f$ e $f \circ h$. L'unica possibile è $f \circ h$, poiché è l'unico caso in cui il dominio della prima funzione coincide con il codominio della seconda. Quindi si ha

$$f \circ h\colon \mathbb{N} \to \mathbb{R} \to \mathbb{R}, \qquad f(h(x)) = f\left(\frac{1+x}{x+5}\right) = \frac{1}{4}\left(\frac{1+x}{x+5}\right)^3 + 7.$$

Capitolo 2

Esercizi sulle relazioni d'ordine e di equivalenza

Ora proponiamo lo svolgimento di alcuni esercizi sulle relazioni. Per comprenderli meglio è necessario che si abbiano i seguenti prerequisiti:

1. conoscenza del concetto di relazione,
2. di relazione d'ordine,
3. di relazione di equivalenza.

Esercizio 2.1 Sia $A = \{a, b, c, d, e\}$ e sia $\mathcal{R} \subseteq A \times A$ la relazione su A definita da

$$\mathcal{R} = \{(a, a), (b, b), (c, c), (d, d), (e, e), (b, d), (a, c), (d, b)\}.$$

1. Dire se $\mathcal{R}$ è riflessiva, simmetrica, antisimmetrica, transitiva su A.
2. Verificare che $\mathcal{R}$ non è una relazione di equivalenza su A.
3. Verificare che si può ottenere una relazione di equivalenza su A aggiungendo un unico elemento (cioè una coppia) ad $\mathcal{R}$.

Svolgimento.

1. Innanzitutto stabiliamo se $\mathcal{R}$ è una relazione riflessiva, cioè:

   $$\forall x \in A \quad x\mathcal{R}x.$$

   Ricordiamo che la notazione $x\mathcal{R}x$ indica che la coppia (x, x) è un elemento di $\mathcal{R}$. Quindi, osservato che A è costituito da a ,b ,c ,d ,e, ci chiediamo se le coppie (a, a), (b, b), (c, c), (d, d), (e, e) appartengono ad $\mathcal{R}$. La risposta al nostro quesito è affermativa e pertanto possiamo affermare che $\mathcal{R}$ gode della proprietà riflessiva. Ora, verificare che $\mathcal{R}$ è una relazione simmetrica vuol dire che

$$\forall x, y \in A \quad x\mathcal{R}y \Rightarrow y\mathcal{R}x,$$

cioè, considerati due qualunque elementi x, y di A, se la coppia (x, y) è un elemento di $\mathcal{R}$ allora lo è anche la coppia (y, x). Ovviamente le coppie formate da due elementi uguali (ovvero (a, a), (b, b), (c, c), (d, d), (e, e)) verificano banalmente questa proprietà, dato che equivale ad uno scambio di due componenti uguali, pertanto la proveremo per le restanti coppie di R (cioè (b, d), (a, c), (d, b)). Stabiliamo, quindi, se sono verificate le seguenti implicazioni:

$$(b, d) \in \mathcal{R} \Rightarrow (d, b) \in \mathcal{R}$$
$$(d, b) \in \mathcal{R} \Rightarrow (b, d) \in \mathcal{R}$$
$$(a, c) \in \mathcal{R} \Rightarrow (c, a) \in \mathcal{R}.$$

Osservando l'insieme $\mathcal{R}$, notiamo che le prime due affermazioni sono vere, invece l'ultima è falsa. Quindi $\mathcal{R}$ non è simmetrica. Stabiliamo se $\mathcal{R}$ è antisimmetrica, cioè

$$\forall x, y \in A \quad x\mathcal{R}y \wedge y\mathcal{R}x \Rightarrow x = y.$$

Questa proprietà è verificata sicuramente per le coppie formate da due elementi uguali (ovvero (a, a), (b, b), (c, c), (d, d), (e, e)). D'altra parte, considerate le coppie (b, d) e (d, b), si ha che le seguenti implicazioni

$$b\mathcal{R}d \wedge d\mathcal{R}b \Rightarrow b = d$$

e

$$d\mathcal{R}b \wedge b\mathcal{R}d \Rightarrow d = b$$

non sono verificate. Infatti se fossero vere si avrebbe che $b = d$, ma ciò non è possibile poiché un insieme è costituito da elementi tutti distinti. Inoltre non abbiamo considerato la coppia (a, c) dato che la coppia (c, a) non è un elemento di $\mathcal{R}$ (per poter verificare l'antisimmetria è necessario che due coppie del tipo (x, y) e (y, x) appartengano ad $\mathcal{R}$). Infine decidiamo se $\mathcal{R}$ è transitiva, cioè

$$\forall x, y, z \in A \quad x\mathcal{R}y \wedge y\mathcal{R}z \Rightarrow x\mathcal{R}z.$$

Così come per le altre proprietà, la transitività è verificata per le coppie (a,a), (b,b), (c,c), (d,d), (e,e). Pertanto restano solo da verificare

$$a\mathcal{R}a \wedge a\mathcal{R}c \Rightarrow a\mathcal{R}c$$

$$a\mathcal{R}c \wedge c\mathcal{R}c \Rightarrow a\mathcal{R}c$$

$$b\mathcal{R}b \wedge b\mathcal{R}d \Rightarrow b\mathcal{R}d$$

$$d\mathcal{R}d \wedge d\mathcal{R}b \Rightarrow d\mathcal{R}b$$

$$b\mathcal{R}d \wedge d\mathcal{R}d \Rightarrow b\mathcal{R}d.$$

$$b\mathcal{R}d \wedge d\mathcal{R}b \Rightarrow b\mathcal{R}b.$$

$$d\mathcal{R}b \wedge b\mathcal{R}b \Rightarrow d\mathcal{R}b.$$

$$d\mathcal{R}b \wedge b\mathcal{R}d \Rightarrow d\mathcal{R}d.$$

E' sufficiente osservare gli elementi di $\mathcal{R}$ per poter dire che sono tutte vere.

2. Da quanto provato nel punto 1. si ha che $\mathcal{R}$ non è una relazione d'equivalenza dato che non è simmetrica.

3. Abbiamo osservato che $\mathcal{R}$ non è una relazione di equivalenza poiché non è simmetrica. Infatti quest'ultima proprietà non è verificata dato che la coppia (c,a) non appartiene ad $\mathcal{R}$. Pertanto si può ottenere una relazione di equivalenza su A aggiungendo solo la coppia (c,a) all'insieme $\mathcal{R}$.

Esercizio 2.2 E' assegnata su $\mathbb{Q}$ la relazione

$$\mathcal{R} = \{\, (p,q) \in \mathbb{Q} \times \mathbb{Q} \mid \exists h \in \mathbb{Z} \text{ tale che } p - q = h \,\}.$$

1. Provare che $\mathcal{R}$ è di equivalenza.

2. Verificare che $(\frac{1}{2}, -\frac{5}{3}) \notin \mathcal{R}$.

3. Individuare due elementi di $\mathbb{Q}$ in relazione tra loro.

4. Determinare la classe di equivalenza di 0.

Svolgimento.

1. Stabiliamo se $\mathcal{R}$ è riflessiva. Sia $p \in \mathbb{Q}$, allora

$$p\mathcal{R}p \Leftrightarrow \exists h \in \mathbb{Z} \text{ tale che } p-p=h \Leftrightarrow \exists h \in \mathbb{Z} \text{ tale che } 0=p-p=h.$$

Da cui

$$p\mathcal{R}p \Leftrightarrow \exists h=0 \in \mathbb{Z} \text{ tale che } p-p=0.$$

Quindi è possibile trovare $h=0$ che ci permette di affermare che p è in relazione $\mathcal{R}$ con sè stesso, cioè $\mathcal{R}$ è riflessiva. Ora, stabiliamo se $\mathcal{R}$ è simmetrica. Consideriamo $p, q \in \mathbb{Q}$ tali che $p\mathcal{R}q$, cioè

$$\exists h \in \mathbb{Z} \text{ tale che } p-q=h.$$

Verifichiamo se $q\mathcal{R}p$, cioè

$$\exists k \in \mathbb{Z} \text{ tale che } q-p=k.$$

Per ipotesi, si ha

$$\exists h \in \mathbb{Z} \text{ tale che } p-q=h$$

che equivale a dire che

$$\exists h \in \mathbb{Z} \text{ tale che } q-p=-h \Leftrightarrow \exists k=-h \in \mathbb{Z} \text{ tale che } q-p=k.$$

Quindi $\mathcal{R}$ è anche simmetrica. Resta ancora da stabilire se $\mathcal{R}$ è transitiva. Siano $p, q, r \in \mathbb{Q}$ tali che

$$p\mathcal{R}q \wedge q\mathcal{R}r.$$

Ma

$$p\mathcal{R}q \Leftrightarrow \exists h \in \mathbb{Z} \text{ tale che } p-q=h$$

e

$$q\mathcal{R}r \Leftrightarrow \exists k \in \mathbb{Z} \text{ tale che } q-r=k$$

quindi

$$\begin{aligned}
&\exists h, k \in \mathbb{Z} \text{ tale che } p-q=h \wedge q-r=k \\
&\Rightarrow \exists h, k \in \mathbb{Z} \text{ tale che } p-q+q-r=h+k \\
&\Rightarrow \exists l=h+k \in \mathbb{Z} \text{ tale che } p-r=l.
\end{aligned}$$

Pertanto $p\mathcal{R}r$, cioè $\mathcal{R}$ è transitiva. Allora $\mathcal{R}$ è una relazione di equivalenza.

2. Osserviamo che $\left(\frac{1}{2}, -\frac{5}{3}\right) \notin \mathcal{R}$. Infatti, se per assurdo fosse un elemento di $\mathcal{R}$, si avrebbe

$$\begin{aligned}\left(\frac{1}{2}, -\frac{5}{3}\right) \in \mathcal{R} &\Leftrightarrow \exists h \in \mathbb{Z} \text{ tale che } \frac{1}{2} - \left(-\frac{5}{3}\right) = h \\ &\Leftrightarrow \exists h \in \mathbb{Z} \text{ tale che } \frac{13}{6} = h.\end{aligned}$$

   Ma questa equivalenza non è vera poiché $\frac{13}{6}$ non è un numero intero.

3. Per determinare due elementi di $\mathbb{Q}$ in relazione tra loro (ovvero $p, q \in \mathbb{Q}$ tali che $(p, q) \in \mathcal{R}$) è sufficiente considerare due razionali tali che, sottraendo uno dall'altro, diano un numero intero. Ad esempio, possiamo pensare di prendere la coppia $(1, 2) \in \mathbb{Z} \times \mathbb{Z}$, cioè due numeri interi (e quindi razionali), la cui differenza è -1 cioè un numero intero. Inoltre, se consideriamo la coppia $(\frac{1}{2}, \frac{3}{2}) \in \mathbb{Q} \times \mathbb{Q}$ si ha che la loro differenza è -1 che è un numero intero.

4. Ricordiamo che la classe di equivalenza di un elemento p, appartenente a $\mathbb{Q}$, rispetto alla relazione $\mathcal{R}$ è definita come segue

$$[\,p\,]_{\mathcal{R}} = \{\, q \in \mathbb{Q} \mid p\mathcal{R}q \,\} = \{\, q \in \mathbb{Q} \mid \exists h \in \mathbb{Z} \text{ tale che } p - q = h \,\}.$$

   Allora

$$\begin{aligned}[\,0\,]_{\mathcal{R}} &= \{\, q \in \mathbb{Q} \mid 0\mathcal{R}q \,\} \\ &= \{\, q \in \mathbb{Q} \mid \exists h \in \mathbb{Z} \text{ tale che } \ -q = h \,\} \\ &= \{\, q \in \mathbb{Q} \mid \exists h \in \mathbb{Z} \text{ tale che } q = -h \,\} \\ &= \{\, q \in \mathbb{Q} \mid \exists k \in \mathbb{Z} \text{ tale che } q = k \,\} \\ &= \{\, q \in \mathbb{Z} \,\} = \mathbb{Z}.\end{aligned}$$

   Quindi la classe di equivalenza di 0 coincide con l'insieme dei numeri interi.

Esercizio 2.3 Assegnata su $\mathbb{Z}$ la relazione

$$\mathcal{R} = \{\, (a, b) \in \mathbb{Z} \times \mathbb{Z} \mid 12 \,|\, 7b + 5a \,\},$$

(ovvero $a\mathcal{R}b \Leftrightarrow 12 \,|\, 7b + 5a$).

1. Verificare che $\mathcal{R}$ definisce una relazione di equivalenza su $\mathbb{Z}$.

2. Scrivere la classe di equivalenza di 0.

Svolgimento.

1. Innanzitutto stabiliamo se $\mathcal{R}$ è riflessiva. Sia $a \in \mathbb{Z}$, si ha

$$a\mathcal{R}a \Leftrightarrow 12 \,|\, 7a + 5a \Leftrightarrow 12 \,|\, 12a.$$

Questa equivalenza è vera dato che $12a$ è un multiplo di 12 e quindi sicuramente $12 \,|\, 12a$. Vediamo, ora, se $\mathcal{R}$ è simmetrica ossia, considerati $a, b \in \mathbb{Z}$ deve risultare che

$$a\mathcal{R}b \Rightarrow b\mathcal{R}a.$$

Ma

$$a\mathcal{R}b \Leftrightarrow 12 \,|\, 7b + 5a.$$

D'altra parte, $12 \,|\, 12a + 12b$ ($12a + 12b$ è un multiplo di 12 pertanto 12 sarà un suo divisore). Ricordando che, in generale

$$\forall x, y, z \in \mathbb{Z} \quad (z \,|\, x) \wedge (z \,|\, y) \Rightarrow z \,|\, (x \pm y) \tag{2.1}$$

si ha che

$$(12 \,|\, 12a + 12b) \wedge (12 \,|\, 7b + 5a) \Rightarrow 12 \,|\, 12a + 12b - 7b - 5a,$$

da cui

$$12 \,|\, 7a + 5b$$

cioè $b\mathcal{R}a$. Quindi $\mathcal{R}$ è simmetrica. Infine stabiliamo se $\mathcal{R}$ è transitiva. Siano $a, b, c \in \mathbb{Z}$ tali che

$$a\mathcal{R}b \wedge b\mathcal{R}c.$$

Da ciò, si ha

$$(12 \,|\, 7b + 5a) \wedge (12 \,|\, 7c + 5b).$$

Quindi, per la proprietà (2.1), otteniamo che

$$(12 \,|\, 7b + 5a + 7c + 5b) \Rightarrow 12 \,|\, 12b + 5a + 7c.$$

Affinchè $a\mathcal{R}c$ (e quindi dire che $\mathcal{R}$ è transitiva) è necessario che, dalla relazione precedente, si cancelli la quantità $12b$. Ma sicuramente $12 \,|\, 12b$, pertanto applicando nuovamente la proprietà vista prima, si ha

$$(12 \,|\, 12b+5a+7c) \wedge (12 \,|\, 12b) \Rightarrow 12 \,|\, 12b + 5a + 7c - 12b \Rightarrow 12 \,|\, 5a + 7c.$$

Pertanto $a\mathcal{R}c$, cioè $\mathcal{R}$ è transitiva e quindi $\mathcal{R}$ è una relazione di equivalenza.

2. Determiniamo la classe di equivalenza di 0. Si ha

$$\begin{aligned}[0]_{\mathcal{R}} &= \{\, a \in \mathbb{Z} \mid 0\mathcal{R}a \,\} = \{\, a \in \mathbb{Z} \mid 12 \,|\, 7a \,\} \\ &= \{\, a \in \mathbb{Z} \mid \exists h \in \mathbb{Z} \text{ tale che } 7a = 12h \,\} \\ &= \{\, a \in \mathbb{Z} \mid \text{a e}' \text{ un multiplo di } 12 \,\}\,.\end{aligned}$$

Esercizio 2.4 Provare che la relazione $|$ su $\mathbb{N}^*$ tale che per ogni $a, b \in \mathbb{N}^*$,

$$a|b \Leftrightarrow \exists n \in \mathbb{N}^* \text{ tale che } b = na$$

è una relazione d'ordine su $\mathbb{N}^*$.

Svolgimento. Innanzitutto stabiliamo se la relazione $|$ è riflessiva. Sia $a \in \mathbb{N}^*$, allora

$$\begin{aligned} a|a &\Leftrightarrow \exists n \in \mathbb{N}^* \text{ tale che } a = na \\ &\Leftrightarrow \exists n = 1 \in \mathbb{N}^* \text{ tale che } a = 1 \cdot a.\end{aligned}$$

Quindi $a|a$ dato che esiste $n = 1 \in \mathbb{N}^*$ tale che $a = 1 \cdot a$. Ciò significa che la relazione $|$ è riflessiva. Ora, verifichiamo la proprietà antisimmetrica. Siano $a, b \in \mathbb{N}^*$ tali che

$$(a|b) \wedge (b|a),$$

e vediamo se $a = b$. Poiché

$$a|b \Leftrightarrow \exists n \in \mathbb{N}^* \text{ tale che } b = na$$

$$b|a \Leftrightarrow \exists m \in \mathbb{N}^* \text{ tale che } a = mb,$$

allora

$$b = na = n(mb) = (nm)b,$$

ove abbiamo sostituito l'espressione di a in b. Ma l'ultima relazione è vera se e solo se $nm = 1$ cioè $n = m = 1$ (questa è l'unica possibilità dato che n, m e b sono numeri naturali). Pertanto, sostituendo il valore $n = 1$ in $b = na$ (o rispettivamente il valore $m = 1$ in $a = mb$) si ottiene $b = a$. Infine stabiliamo se tale relazione è anche transitiva. Siano $a, b, c \in \mathbb{N}^*$ tali che

$$(a|b) \wedge (b|c),$$

e vediamo se $a|c$. Poiché

$$a|b \Leftrightarrow \exists n \in \mathbb{N}^* \text{ tale che } b = na$$

$$b|c \Leftrightarrow \exists m \in \mathbb{N}^* \text{ tale che } c = mb,$$

allora

$$c = mb = m(na) = (mn)a.$$

Quindi, ponendo $r = mn \in \mathbb{N}^*$, si ha che $c = ra$ cioè $a|c$. Pertanto la relazione $|$ è transitiva e quindi è una relazione d'ordine.

Capitolo 3

Esercizi sul principio di induzione

Ora proponiamo lo svolgimento di alcuni esercizi sul principio di induzione. Per comprenderli meglio è necessario che si conoscano gli enunciati dei teoremi ad esso relativi.

Esercizio 3.1 Mediante il principio di induzione si provi la seguente proprietà:

$$P(n) : \sum_{i=0}^{n+1}(2i+1) = n^2 + 4n + 4, \quad n \in \mathbb{N}.$$

Svolgimento. Usiamo il principio di induzione per provare che $P(n)$ è vera per ogni $n \in \mathbb{N}$.

1. PASSO BASE: Verifichiamo innanzitutto che

   $$P(0) : \sum_{i=0}^{0+1}(2i+1) = 0^2 + 4 \cdot 0 + 4$$

   è vera. Si ha:

   $$\sum_{i=0}^{0+1}(2i+1) = \sum_{i=0}^{1}(2i+1) = (1) + (2+1) = 4,$$

   d'altra parte

   $$0^2 + 4 \cdot 0 + 4 = 4.$$

   Quindi, data l'uguaglianza tra i due membri, $P(0)$ è vera.

2. PASSO INDUTTIVO: Ora proviamo che per ogni $n \in \mathbb{N}$, supponendo vera $P(n)$, è vera $P(n+1)$, ovvero

   $$\forall n \in \mathbb{N} \quad P(n) \text{ vera} \Rightarrow P(n+1) \text{ vera}.$$

Esplicitando la tesi si ha:

$$P(n+1): \sum_{i=0}^{(n+1)+1} (2i+1) = (n+1)^2 + 4(n+1) + 4,$$

cioè

$$P(n+1): \sum_{i=0}^{n+2} (2i+1) = (n+1)^2 + 4(n+1) + 4. \qquad (3.1)$$

Tenendo presente l'ipotesi di induzione, si ha:

$$\sum_{i=0}^{n+2}(2i+1) = \sum_{i=0}^{n+1}(2i+1) + (2(n+2)+1) = n^2+4n+4+2n+4+1 = \\ = n^2+6n+9.$$

D'altra parte:

$$(n+1)^2 + 4(n+1) + 4 = n^2+1+2n+4n+4+4 = n^2+6n+9.$$

Data l'uguaglianza tra i due membri di (3.1), $P(n+1)$ è vera. Pertanto la proprietà è completamente verificata.

Esercizio 3.2 Verificare per induzione completa che $\forall n \in \mathbb{N}$, $n \geq 2$ è vera

$$3^n > 1 + 2n.$$

Svolgimento. Usiamo il principio di induzione per provare che $P(n)$ è vera per ogni $n \in \mathbb{N}$.

1. PASSO BASE: Verifichiamo innanzitutto che

   $$P(2): 3^2 > 1 + 2 \cdot 2,$$

   è vera. Ma sicuramente $9 > 5$, quindi $P(2)$ è vera.

2. PASSO INDUTTIVO: Ora proviamo che per ogni $n \in \mathbb{N}$, supponendo vera $P(n)$, è vera $P(n+1)$, ovvero

   $$\forall n \in \mathbb{N} \quad P(n) \text{ vera} \Rightarrow P(n+1) \text{ vera}.$$

   Esplicitando la tesi si ha:

   $$P(n+1): 3^{n+1} > 1 + 2(n+1) = 2n+3.$$

   Tenendo presente l'ipotesi di induzione ed il fatto ovvio che $3^n > 1$ (dato che $n \geq 2$), si ha:

   $$3^{n+1} = 3^n \cdot 3 = 3^n + 3^n + 3^n > 1 + 2n + 1 + 1 = 2n + 3.$$

   In conclusione, $3^{n+1} > 2n+3$, cioè $P(n+1)$ è vera.

Esercizio 3.3 Mediante il principio di induzione si provi la formula

$$3|\, 2n - 5n^3, \quad n \in \mathbb{N}.$$

Svolgimento. Usiamo il principio di induzione per provare che $P(n)$ è vera per ogni $n \in \mathbb{N}$.

1. PASSO BASE: Verifichiamo innanzitutto che

$$P(0) : 3|\, 2 \cdot 0 - 5 \cdot 0^3$$

   è vera. Deve risultare che $3|\, 0$, ma ciò è sempre vero.

2. PASSO INDUTTIVO: Ora proviamo che per ogni $n \in \mathbb{N}$, supponendo vera $P(n)$, è vera $P(n+1)$, ovvero

$$\forall n \in \mathbb{N} \quad P(n) \text{ vera} \Rightarrow P(n+1) \text{ vera}.$$

   Si ha

$$P(n+1) : 3|\, 2(n+1) - 5(n+1)^3,$$

   ove, a conti fatti, $2(n+1) - 5(n+1)^3 = (2n - 5n^3) - 3 - 15n^3 - 15n$. Allora, usando l'ipotesi di induzione e sapendo che $-3 - 15n^3 - 15n$ è un multiplo di 3, cioè

$$3| - 3 - 15n^3 - 15n,$$

   si ha

$$((3|\, 2n - 5n^3) \wedge (3| - 3 - 15n^3 - 15n)) \Rightarrow 3|\, (2n - 5n^3) - 3 - 15n^3 - 15n.$$

   Quindi $P(n+1)$ è verificata.

Esercizio 3.4 Verificare che la seguente successione definita per ricorrenza

$$\{b_n\}_n = \begin{cases} b_0 = 0, & n = 0 \\ b_n = b_{n-1} + 6n, & n \geq 1 \end{cases}$$

ammette come formula chiusa la successione $\{a_n\}_n$ con $a_n = 3n(n+1)$, per ogni $n \geq 0$.

Svolgimento. Usiamo il principio di induzione per provare che $P(n) : a_n = b_n$ è vera per ogni $n \in \mathbb{N}$.

1. PASSO BASE: Verifichiamo innanzitutto che
$$P(0) : a_0 = b_0,$$
è vera. Ma $a_0 = 3 \cdot 0 \cdot (0+1) = 0$ e $b_0 = 0$. Quindi, essendo entrambi nulli, il passo base è verificato.

2. PASSO INDUTTIVO: Ora proviamo che per ogni $n \in \mathbb{N}$, supponendo vera $P(n)$, è vera $P(n+1)$, ovvero
$$\forall n \in \mathbb{N} \quad P(n) : a_n = b_n \Rightarrow P(n+1) : a_{n+1} = b_{n+1}.$$
Quindi si ha:
$$\begin{aligned} b_{n+1} = b_{n+1-1} + 6(n+1) &= b_n + 6(n+1) = a_n + 6(n+1) = \\ &= 3n(n+1) + 6(n+1) \\ &= (3n+6)(n+1) = 3(n+2)(n+1). \end{aligned}$$
Ma $a_{n+1} = 3(n+1)(n+1+1) = 3(n+1)(n+2)$. Pertanto, poiché a_{n+1} coincide con b_{n+1}, si ha che $P(n+1)$ è verificata.

Capitolo 4

Esercizi sulle strutture algebriche: gruppi, anelli e campi

Ora proponiamo lo svolgimento di alcuni esercizi riguardanti i gruppi, gli anelli e i campi. Per comprenderli meglio è necessario che si conoscano le loro definizioni e le relative proprietà.

Esercizio 4.1 Si consideri la seguente struttura algebrica $(\mathbb{Z}, *)$, dove la legge di composizione interna $*$ è definita come segue:

$$\forall x, y \in \mathbb{Z}, \quad x * y = x + y + 1.$$

1. Stabilire se $*$ è una legge associativa e/o commutativa.
2. Determinare l'eventuale elemento neutro della struttura algebrica $(\mathbb{Z}, *)$.
3. Se la struttura algebrica $(\mathbb{Z}, *)$ ammette elemento neutro, determinare gli (eventuali) elementi di $\mathbb{Z}$ che hanno inverso rispetto ad $*$.
4. Concludere se la struttura algebrica $(\mathbb{Z}, *)$ è un monoide o un gruppo (abeliano).

Svolgimento.

1. Verifichiamo innanzitutto se $*$ è associativa, cioè

$$\forall x, y, z \in \mathbb{Z} \quad (x * y) * z = x * (y * z). \tag{4.1}$$

Siano $x, y, z \in \mathbb{Z}$, e calcoliamo separatamente i due membri della (4.1). Si ha:

$$(x * y) * z = (x + y + 1) * z = (x + y + 1) + z + 1 = x + y + z + 2,$$

$$x * (y * z) = x * (y + z + 1) = x + (y + z + 1) + 1 = x + y + z + 2.$$

Quindi si ottiene l'uguaglianza richiesta. Ora, verifichiamo se $*$ è commutativa, cioè

$$\forall x, y \in \mathbb{Z} \quad x * y = y * x.$$

Siano $x, y \in \mathbb{Z}$, e calcoliamo

$$x * y = x + y + 1,$$

$$y * x = y + x + 1.$$

Ma, per la proprietà commutativa della somma tra numeri interi, si ha

$$x + y + 1 = y + x + 1,$$

cioè l'uguaglianza voluta.

2. Determiniamo l'elemento neutro dell'operazione $*$, verificando che

$$\exists u \in \mathbb{Z} \quad t.c \quad \forall x \in \mathbb{Z} \quad x * u = x = u * x.$$

Poiché abbiamo osservato che $*$ è commutativa, basta dimostrare che è verificata solo la prima parte dell'uguaglianza della definizione, cioè

$$\exists u \in \mathbb{Z} \quad t.c \quad \forall x \in \mathbb{Z} \quad x * u = x.$$

Sia $x \in \mathbb{Z}$ e determiniamo u dalla relazione seguente:

$$x * u = x + u + 1 = x \Rightarrow x + u + 1 = x \Rightarrow u + 1 = 0 \Rightarrow u = -1.$$

Quindi $u = -1$ è l'elemento neutro dell'operazione $*$.

3. Dato che abbiamo determinato l'elemento neutro, affinchè ogni numero intero ammetta inverso rispetto a $*$ verifichiamo se

$$\forall x \in \mathbb{Z} \quad \exists x' \in \mathbb{Z} \quad t.c. \quad x * x' = x' * x = u.$$

Anche qui, come prima, è sufficiente provare solo la prima parte dell'uguaglianza, poiché la seconda parte è garantita dalla commutatività di $*$. Sia $x \in \mathbb{Z}$. Si ha

$$\begin{aligned} x * x' = x + x' + 1 = u \Rightarrow x + x' + 1 = u = -1 \Rightarrow x + x' + 1 &= -1 \\ \Rightarrow x' &= -2 - x. \end{aligned}$$

Quindi x ammette $x' = -2 - x$ come inverso rispetto all'operazione $*$.

4. Concludiamo che la struttura algebrica $(\mathbb{Z}, *)$ è un gruppo abeliano dato che $*$ è associativa, ammette elemento neutro, ogni elemento ammette inverso ed è commutativa.

Esercizio 4.2 Si consideri il gruppo $(\mathbb{Z}_{12}, +)$.

1. Determinare tutti i generatori di $(\mathbb{Z}_{12}, +)$;
2. Determinare l'ordine di $[10]_{12}$, di $[8]_{12}$ e $[6]_{12}$ in $(\mathbb{Z}_{12}, +)$;
3. Determinare il sottogruppo ciclico di $(\mathbb{Z}_{12}, +)$ generato da $[8]_{12}$;
4. Stabilire se $H = \{[0]_{12}, [4]_{12}, [8]_{12}\}$, $K = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}, [11]_{12}\}$ sono sottogruppi di $(\mathbb{Z}_{12}, +)$ ed in caso affermativo determinare un generatore.

Svolgimento.

1. Determiniamo i generatori di $(\mathbb{Z}_{12}, +)$, cioè le classi di congruenza $[a]_{12}$ tali che $MCD(a, 12) = 1$. A tal fine, per determinarli più facilmente, esplicitiamo tutti gli elementi di $\mathbb{Z}_{12}$:

   $\mathbb{Z}_{12} = \{[0]_{12}, [1]_{12}, [2]_{12}, [3]_{12}, [4]_{12}, [5]_{12}, [6]_{12}, [7]_{12}, [8]_{12}, [9]_{12}, [10]_{12}, [11]_{12}\}$.

   Quindi, dato che

   $MCD(1, 12) = 1$, $MCD(5, 12) = 1$, $MCD(7, 12) = 1$, $MCD(11, 12) = 1$,

   si ha che $[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}$ sono tutti e soli i generatori di $(\mathbb{Z}_{12}, +)$.

2. Poiché abbiamo osservato che $[1]_{12}$ è un generatore per il gruppo $(\mathbb{Z}_{12}, +)$, possiamo determinare gli ordini degli elementi mediante la seguente formula
$$o([a]_{12}) = o([1]_{12} \cdot [a]_{12}) = \frac{|\mathbb{Z}_{12}|}{MCD(a, 12)},$$
   ove $|\mathbb{Z}_{12}|$ è la cardinalità di $\mathbb{Z}_{12}$, e $[a]_{12}$ è un suo generico elemento, con $a \in \mathbb{Z}$. Quindi
$$o([10]_{12}) = \frac{|\mathbb{Z}_{12}|}{MCD(10, 12)} = \frac{12}{2} = 6,$$
$$o([8]_{12}) = \frac{|\mathbb{Z}_{12}|}{MCD(8, 12)} = \frac{12}{4} = 3,$$
$$o([6]_{12}) = \frac{|\mathbb{Z}_{12}|}{MCD(6, 12)} = \frac{12}{6} = 2.$$

3. Osserviamo che, poiché $o([8]_{12}) = 3$, il sottogruppo ciclico generato da $[8]_{12}$ avrà 3 elementi. Pertanto
$$< [8]_{12} >= \{h[8]_{12}|\, h \in \mathbb{Z}\} = \{[0]_{12}, [8]_{12}, [16]_{12} = [4]_{12}\}.$$

4. Per poter stabilire se H e K sono sottogruppi di $(\mathbb{Z}_{12}, +)$, applichiamo il Teorema di Lagrange. Quindi, poiché la cardinalità di K è 5, e quella di H è 3, l'unico possibile sottogruppo di $(\mathbb{Z}_{12}, +)$ è H (3 divide $12 = |\mathbb{Z}_{12}|$). Resta solo da verificare che H è effettivamente un sottogruppo di $(\mathbb{Z}_{12}, +)$. Verichiamo se sono soddisfatte le tre proprietà che caratterizzano la definizione di sottogruppo di un gruppo. Innanzitutto possiamo affermare prontamente che H contiene l'elemento neutro di $(\mathbb{Z}_{12}, +)$, cioè $[0]_{12}$. Inoltre ogni elemento ha opposto che è ancora un elemento di H. Infine H è chiuso rispetto alla somma, poichè comunque considero due elementi di H, la loro somma è ancora un elemento di H. Pertanto H è un sottogruppo di $(\mathbb{Z}_{12}, +)$. In realtà, dal punto 3., si osserva che il sottogruppo generato da $[8]_{12}$ è proprio H, pertanto si può subito concludere che H è un sottogruppo di $(\mathbb{Z}_{12}, +)$.

Esercizio 4.3 Sia $f\colon \mathbb{Z} \to \mathbb{Z}_3$ l'applicazione tale che per ogni $h \in \mathbb{Z}$ $f(h) = [h]_3$. Verificare che f è un omomorfismo di gruppi e calcolare $Ker(f)$.

Svolgimento. Proviamo che f è un omomorfismo del gruppo $(\mathbb{Z}, +)$ in $(\mathbb{Z}_3, +)$, cioè
$$\forall n, m \in \mathbb{Z} \quad f(n + m) = f(n) + f(m).$$
Siano $n, m \in \mathbb{Z}$ e calcoliamo
$$f(n + m) = [n + m]_3 = [n]_3 + [m]_3 = f(n) + f(m),$$
ove nel secondo passaggio abbiamo utilizzato la definizione di somma tra elementi di $\mathbb{Z}_3$. Pertanto f è un omomorfismo. Ora, determiniamo $Ker(f)$, cioè
$$Ker(f) = \{n \in \mathbb{Z}|\, f(n) = [0]_3\} = \{n \in \mathbb{Z}|\, [n]_3 = [0]_3\} = \{n = 3k|\, k \in \mathbb{Z}\}.$$
Quindi il $Ker(f)$ è formato dai multipli di 3.

Esercizio 4.4 Determinare gli elementi invertibili e i divisori dello zero dell'anello $(\mathbb{Z}_{18}, +, \cdot)$. Per ogni elemento invertibile determinarne l'inverso.

Svolgimento. Prima di procedere nel calcolo degli elementi invertibili e dei divisori dello zero di $(\mathbb{Z}_{18}, +, \cdot)$, ricordiamo che se $(A, +, \cdot)$ è un anello commutativo unitario e se $a \in A$ è un elemento invertibile, allora a non è divisore dello zero. E il viceversa è vero solo negli anelli finiti. Pertanto, dato che $(\mathbb{Z}_{18}, +, \cdot)$ è un anello commutativo unitario finito, determineremo prima gli elementi invertibili e i restanti saranno divisori dello zero. Un elemento $[a]_{18}$ di $(\mathbb{Z}_{18}, +, \cdot)$ è invertibile se il $MCD(a, 18) = 1$. Pertanto, si ha

$$MCD(a, 18) = 1 \Leftrightarrow a = 1, 5, 7, 11, 13, 17.$$

Quindi gli elementi invertibili di $(\mathbb{Z}_{18}, +, \cdot)$ sono:

$$[1]_{18},\ [5]_{18},\ [7]_{18},\ [11]_{18},\ [13]_{18},\ [17]_{18}.$$

Ora, ad esempio, determiniamo l'inverso di $[5]_{18}$, cioè un elemento $[a]_{18}$ di $\mathbb{Z}_{18}$ tale che

$$[5]_{18}[a]_{18} = [1]_{18},$$

cioè

$$5a \equiv 1 \pmod{18}.$$

La soluzione di questa congruenza è $a = 11$. Quindi $[11]_{18}$ è l'inverso di $[5]_{18}$. Analogamente si procede per tutti gli altri elementi invertibili. Infine, come già accennato, i divisori dello zero di $(\mathbb{Z}_{18}, +, \cdot)$ sono tutti gli elementi che non sono invertibili, cioè

$$[2]_{18}, [3]_{18}, [4]_{18}, [6]_{18}, [8]_{18}, [9]_{18}, [10]_{18}, [12]_{18}, [14]_{18}, [15]_{18}, [16]_{18}.$$

Esercizio 4.5 Si consideri in S_9 la seguente permutazione

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

1. Scrivere f come prodotto di cicli disgiunti.

2. Stabilire se f è pari o dispari.

3. Calcolare f^{-1} e l'ordine di f in S_9.

4. Calcolare l'ordine del sottogruppo H generato da f e scriverne esplicitamente tutti gli elementi.

5. Calcolare l'ordine degli elementi del sottogruppo H.

Svolgimento.

1. Decomponiamo f in cicli disgiunti, cioè in modo che gli elementi che compaiono nei cicli sono distinti. A tal fine, osserviamo che l'immagine tramite f di 1 è 9, quella di 9 è 7 e di 7 è 1. Quindi il primo ciclo, di lunghezza 3, è dato da (197). Procedendo analogamente per tutti gli altri elementi, si ottiene

$$f = (197)(2)(34)(58)(6) = (197)(34)(58).$$

2. Per stabilire se f è pari o dispari è necessario scrivere f nel prodotto di trasposizioni, cioè cicli di lunghezza 2. Pertanto, osservando che il ciclo $(197) = (17)(19)$, si ha

$$f = (17)(19)(34)(58).$$

Quindi f è il prodotto di 4 cicli di lunghezza 2, cioè f è pari (poiché 4 è un numero pari).

3. Calcoliamo f^{-1} invertendo la seconda riga di f con la prima, e riordinando le colonne in modo da sistemare in modo crescente i numeri della prima riga:

$$f^{-1} = \begin{pmatrix} 9 & 2 & 4 & 3 & 8 & 6 & 1 & 5 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 4 & 3 & 8 & 6 & 9 & 5 & 1 \end{pmatrix}.$$

Ora, ricordiamo che in generale un ciclo di lunghezza k ha ordine k. Quindi l'ordine di f è il minimo comune multiplo delle lunghezze dei cicli disgiunti:

$$|f| = m.c.m(3, 2, 2) = m.c.m(3, 2) = 6.$$

4. Osserviamo che, poiché f ha ordine 6, il sottogruppo H generato da f ha 6 elementi. Essi sono le potenze di f, compresa la permutazione identica. Quindi

$$H =< f >= \{f^0, f^1, f^2, f^3, f^4, f^5\}$$

Ovviamente f^0 è la permutazione identica, f^1 è f stessa. Calcoliamo f^2. Componiamo f con se stessa due volte, cioè:

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

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 2 & 3 & 4 & 5 & 6 & 9 & 8 & 1 \end{pmatrix} = (179),$$

Considerando la permutazione più a destra, si osserva che l'immagine tramite f di 1 è 9. Quest'ultimo, mediante la prima permutazione (quella a sinistra, che è sempre f) ha immagine 7. Pertanto la permutazione f^2 trasformerà 1 in 7 (la prima "colonna" della permutazione f^2). Procedendo così anche per le altre potenze, si ha

$$H = \{Id, f = (17)(19)(34)(58), f^2 = (179), f^3 = (34)(58),$$

$$f^4 = (197), f^5 = (179)(34)(58)\}$$

5. Determiniamo gli ordini degli elementi di H osservando la loro decomposizione in cicli disgiunti. Quindi si ha

$$o(Id) = 1$$

$$o(f) = 6$$
$$o(f^2) = 3$$
$$o(f^3) = m.c.m(2, 2) = 2$$
$$o(f^4) = 3$$
$$o(f^5) = m.c.m(3, 2) = 6.$$