Foglio 2

11/10/2023

Esercizio 1. Sia $(G, \bullet)$ un gruppo.
1.1. Verificate l'unicità dell'elemento neutro e (esercizio già fatto in classe, rifatelo senza guardare gli appunti !).
1.2 Verificate l'unicità dell'inverso di un elemento $g \in G$. Questo unico elemento si denota g^{-1}.
1.3 Verificate che $(g \bullet h)^{-1} = h^{-1} \bullet g^{-1}$.

1.1) Supponiamo che esiste un altro elemento neutro $\tilde{e}$, allora sarà vero che: $s \cdot \tilde{e} = s = \tilde{e} \cdot s$ perché $\tilde{e}$ è l'elemento neutro del gruppo $(G, \cdot)$.
Sappiamo che: $s \cdot e = s = e \cdot s$.
Possiamo dire che: $e \cdot \tilde{e} = e = \tilde{e} \cdot e$
e possiamo anche affermare che: $\tilde{e} \cdot e = \tilde{e} = e \cdot \tilde{e}$
quindi, dato che: $\tilde{e} \cdot e = e = \tilde{e} \cdot e = \tilde{e}$
$\tilde{e}$ ed e sono lo stesso elemento pertanto, l'elemento neutro in un gruppo è uno e uno solo.

1.2) Possiamo dire che per assurdo esiste un ulteriore elemento inverso di g, chiamato $\tilde{g}' \mid g \cdot \tilde{g}' = e = \tilde{g}' \cdot g$
Sappiamo che $g \cdot g' = e = g' \cdot g$
Posso scrivere:

$$g' \cdot \underbrace{(g \cdot g')}_{e} = g' \cdot \underbrace{(g \cdot \tilde{g}')}_{e} \Rightarrow \text{per le proprietà associativa}$$

$$g' = (g' \cdot g) \cdot \tilde{g}' \Rightarrow g' = \tilde{g}'$$

1.3) $(g \cdot h)'$ è l'inverso di $(g \cdot h)$
Posso affermare che: $(g \cdot h) \cdot (g \cdot h)' = e$
$(g \cdot h) \cdot (h' \cdot g') = g \cdot (h \cdot h') \cdot g'$ per le proprietà associativa

quindi $(g \circ h)'$ è l'inverso di $(g \circ h)$.
$h' \circ g'$ è l'inverso di $(g \circ h)$ dato che l'inverso di un elemento $g \in G$ è unico $\Rightarrow (g \circ h)' = h' \circ g'$

Esercizio 2. Sia $f : A \to B$ una bigezione, o applicazione biunivoca, e sia $f^{-1} : B \to A$ l'inversa di f.^1 Verificare che

$$1)\ f \circ f^{-1} = \mathrm{id}_B\,, \qquad f^{-1} \circ f = \mathrm{id}_A$$

2.1) $f \circ f^{-1}(b) = f(f^{-1}(b)) =$ PER ^1 $f(a) = b$

2.2) $f^{-1} \circ f(a) = f^{-1}(f(a)) =$ PER ^1 $f^{-1}(b) = a$

^1 Vi ricordo che $f^{-1} : B \to A$ è definita come segue: preso $b \in B$ sappiamo che esiste $a \in A$ tale che $f(a) = b$ (perché f è suriettiva); inoltre a è unico dato che f è iniettiva; riassumendo esiste unico a tale che $f(a) = b$ e si pone $f^{-1}(b) = a$.

Esercizio 3. Sia A un insieme e $G = \{f : A \to A \mid f \text{ bigezione}\}$. Sia $\circ$ la composizione fra applicazioni. Verificare in dettaglio che $(G, \circ)$ è un gruppo (visto rapidamente a lezione).

Se è un gruppo vale la proprietà associativa rispetto a $\circ$, c'è un elemento neutro e ogni elemento f avrà un inverso f'

1) $\circ$ gode della proprietà associativa
2) elemento neutro $= ID_X$
3) ogni f ha il suo inverso f^{-1} dato che f è biettiva

DIMOSTRO:

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

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

$f(g(h(a))) = f(g(h(a)))$

2) ID_X è la funzione che mappa ogni elemento in sé stesso quindi $f \circ ID_X = f$

3) Dato che si parla di funzioni biunivoche $\exists!\ a \mid f(a) = b$, chiamiamo inversa $f^{-1}(b) = a$

$$f \circ f^{-1} = ID_X = f^{-1} \circ f$$

DIMOSTRO:

$$f \circ f^{-1}(b) = f(f^{-1}(b)) = f(a) = b \qquad \bullet\ ID_X(b) = f \circ f^{-1}(b)$$

$$f^{-1} \circ f\ (a) = f^{-1}(f(a)) = f^{-1}(b) = a \qquad \bullet\ ID_X(a) = f^{-1} \circ f(a)$$

Esercizio 4. Sia ora $A = \{1, 2, \ldots, n\}$.
Il gruppo G definito nell'esercizio precedente possiede allora una notazione specifica, che è $\mathcal{S}_n$, ed un nome specifico che è il *gruppo simmetrico di n oggetti.*
Scrivere tutti gli elementi del gruppo $\mathcal{S}_3$ (sono 6). Verificare che S_3 non è un gruppo commutativo.
Suggerimento: per scrivere, ad esempio, l'elemento di $\mathcal{S}_3$ che manda 1 in 3, 2 in 2 e 3 in 1 potete scrivere

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

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

VERIFICO CHE: $g \circ f \neq f \circ g$

$g = 4$, $f = 5$

$$f \circ g = \{(2,2), (3,3), (1,1) \neq g \circ f = \{(1,1), (2,3), (3,2)\}$$

Esercizio 5. Abbiamo visto la definizione rigorosa di $\mathbb{Q}$. Verificare che le operazioni definite in classe sono ben poste e che rendono $\mathbb{Q}$ un campo.

- Un operazione ben posta lavora bene anche a meno delle scelte dei rappresentanti delle classi

DIMOSTRO: (SOMMA)

prendo un valore (x, y) rappresentante di una classe. $(x', y') \mathcal{P} (x, y)$, prendo poi un altro valore (a, b) rappresentante di un'altra classe. $(a', b') \mathcal{P} (a, b)$
posso dire: $(x', y') = (x, y)$ perché $(x', y') \mathcal{P} (x, y)$ e che $(a, b) = (a', b')$ per lo stesso motivo
la somma tra (x, y) e (a, b) deve risultato $(xb + ay, by)$

$(x,y)+(a,b)=((xb+ay),by)$, dato che:

$(x',y')=(x,y)$ e

$(a',b')=(a,b)$

allora: $(x',y')+(a',b')=(x,y)+(a,b)$. la somma è ben definita perché non sommando rappresentanti ottengo lo stesso risultato anche sommando i rappresentanti

DIMOSTRO: (PRODOTTO)

Prendo (a,b) rappresentante della classe di equivalenza $[(a,b)]$ e (x,y) rappresentante della classe di equivalenza $[(x,y)]$, $(x',y')\,P\,(x,y) \Rightarrow (x,y)=(x',y')$, $(a',b')\,P\,(a,b) \Rightarrow (a,b)=(a',b')$

il prodotto tra (x,y) e (a,b) darà risultato (xa,yb) dato che:

$(x,y)=(x',y')$ e

$(a,b)=(a',b')$ allora:

$(a',b')\cdot(x',y')=(a,b)\cdot(x,y)$ il prodotto è ben posto dato che ottengo lo stesso risultato moltiplicando rappresentanti delle classi e non rappresentanti delle classi

GIUSTO ???

ESERCIZIO 5) (altra soluzione) (SOMMA)

Sappiamo che: $(a,b)P(a',b')$ e $(c,d)P(c',d')$

$$\Rightarrow ab' = ba' \quad e \quad cd' = dc'$$

dove (a,b) e (c,d) sono i rappresentanti delle classi $[(a,b)]$ e $[(c,d)]$

la somma tra (a,b) e $(c,d) = ((ad+bc), bd)$
la somma tra (a',b') e $(c',d') = ((a'd'+b'c'), b'd')$

$(ad+b\cdot c)\cdot b'd' = (a'd'+b'\cdot c')bd$

$a\cdot d\cdot b'\cdot d' + b\cdot c\cdot b'\cdot d' = a'\cdot d'\cdot b\cdot d + b'\cdot c'\cdot b\cdot d$

$d(ab')d' + b(cd')b' = a'\cdot d'\cdot b\cdot d + b'\cdot c'\cdot b\cdot d \leftarrow$ dato che $a\cdot b = b\cdot a$ perché $\mathbb{Z}$ è un gruppo commutativo $ab=ba$

$d(a'b)d' + b(c'd)b' =$ ''

$da'bd' + bc'db' =$ ''

$d(a'd')b + b(c'b')d =$ ''

$a'd'bd + b'c'bd =$ ''

DATO CHE: i due prodotti sono uguali, posso ottenere gli stessi risultati sommando i rappresentanti delle classi e i non rappresentanti delle classi. Quindi la somma risulta BEN POSTA.

(PRODOTTO)

Sappiamo che: $(a,b)P(a',b')$ e $(c,d)P(c',d')$

$$\Rightarrow ab' = ba' \quad e \quad cd' = dc'$$

dove (a,b) e (c,d) sono i rappresentanti delle classi $[(a,b)]$ e $[(c,d)]$

il prodotto tra (a,b) e $(c,d) = (ac, db)$
'' (a',b') e $(c',d') = (a'c', d'b')$

dobbiamo dimostrare che $(ac, db) = (a'c', d'b')$

se questo è vero deve risultare $(ac)(d'b') = (db)(a'c')$

per le proprietà commutativa in Z posso dire che:

$d'b'ac = acd'b'$ SOSTITUENDO:

$d'a'b'c = acd'b'$

$a'd'cb' = acd'b'$

$a'dc'b = acd'b'$

$(a'c')(db) = acd'b'$

$(db)(a'c') = acd'b'$

quindi: $acd'b' = dba'c'$ perché $acd'b' = db(a'c')$

il prodotto dei rappresentanti delle classi e il prodotto dei non rappresentanti è uguale quindi il prodotto è ben posto.

- Queste operazioni rendono $\mathbb{Q}$ un campo dato che ammettono entrambe un proprio elemento neutro e ogni elemento, escluso lo zero della prima operazione ammette un inverso. $\forall (a,b) \in \mathbb{Q} \; \exists (b,a) \in \mathbb{Q} \mid (a,b) \cdot (b,a) = 1$ (UNITÀ)

facile da dimostrare: Dato (a,b) e (b,a) il suo inverso, il prodotto tra i due sarà uguale a (ab, ba) dato che in $\mathbb{Z}$ vale la proprietà commutativa posso scrivere $b \cdot a = a \cdot b$ quindi $(a,b) \cdot (b,a) = (ab, ab)$ e questo valore è in relazione P con $(1,1)$ dato che: $ab \cdot 1 = ab \cdot 1$

$\Rightarrow (ab, ab) P (1,1) \Rightarrow (ab, ab) = (1,1)$