

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) - Sia e l'elemento neutro, vale che $\forall x \in G, x \cdot e = x = e \cdot x$. Si consideri un altro elemento \tilde{e} tale che $\forall x \in G, x \cdot \tilde{e} = x = \tilde{e} \cdot x$

$$\begin{cases} e \cdot \tilde{e} = e = \tilde{e} \cdot e \\ \tilde{e} \cdot e = \tilde{e} = e \cdot \tilde{e} \end{cases} \Rightarrow \begin{cases} e \cdot \tilde{e} = e \\ e \cdot \tilde{e} = \tilde{e} \end{cases} \Rightarrow e = \tilde{e}$$

(1.2) - Sia x un generico elemento di G , l'inverso di x è $\bar{x}^{-1} \Rightarrow x \cdot \bar{x}^{-1} = e = \bar{x}^{-1} \cdot x$

Suppongo esista $y \in G \mid x \cdot y = e = y \cdot x$

$$\begin{cases} x \cdot y = e = y \cdot x \\ x \cdot \bar{x}^{-1} = e = \bar{x}^{-1} \cdot x \end{cases} \Rightarrow \begin{cases} x \cdot y = e \\ x \cdot \bar{x}^{-1} = e \end{cases} \Rightarrow x \cdot y = x \cdot \bar{x}^{-1} \Rightarrow y = \bar{x}^{-1}$$

(1.3) - $(g \cdot h)^{-1} \cdot (g \cdot h) = e$, poniamo $(g \cdot h)^{-1} = x \cdot y \Rightarrow x \cdot y \cdot g \cdot h = e = g \cdot h \cdot x \cdot y$
 $\Leftrightarrow y \cdot g = e = g \cdot y \wedge x \cdot h = e = h \cdot x \Leftrightarrow y = g^{-1} \wedge x = h^{-1} \Rightarrow (g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$

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

$$f \circ f^{-1} = \text{id}_B, \quad f^{-1} \circ f = \text{id}_A$$

dove per ogni insieme C l'applicazione id_C è l'applicazione identità, definita come $\text{id}_C(c) := c$ per ogni $c \in C$.

Sia $a \in A$ per ipotesi $\exists b \in B \mid f(a) = b \wedge f^{-1}(b) = a$, considero $f \circ f^{-1} : B \rightarrow B$, ho che $\forall b \in B \quad f(f^{-1}(b)) = f(a) = b \Rightarrow f \circ f^{-1} = \text{id}_B$, analogamente, $\forall a \in A \quad f^{-1}(f(a)) = f^{-1}(b) = a$.

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

È un gruppo perché: ① \circ è associativa, $(f \circ g) \circ k = f(g(x)) \circ k = f(g(k(x))) = f \circ (g \circ k)$. ② esiste $\text{id}_x(x) = x$, tale che $f \circ \text{id}_x = f(\text{id}_x(x)) = f(x) = f \quad \forall f \in G$, quindi id_x è l'elemento neutro. ③ essendo f biettiva $\forall f \in G$, esiste $\forall f, f^{-1}$, ossia la sua inversa, tale che $\forall k \in A \quad f(k) = k'$ e $f^{-1}(k') = k$, b.c. $f(f^{-1}(k)) = k = \text{id}_x, \forall k \in A, f \in G$, quindi ogni elemento ha il suo inverso.

Esercizio 4. Sia ora $A = \{1, 2, \dots, n\}$.

Il gruppo G definito nell'esercizio precedente possiede allora una notazione specifica, che è S_n , ed un nome specifico che è il *gruppo simmetrico di n oggetti*.

Scrivere tutti gli elementi del gruppo S_3 (sono 6). Verificare che S_3 non è un gruppo commutativo.

Suggerimento: per scrivere, ad esempio, l'elemento di S_3 che manda 1 in 3, 2 in 2 e 3 in 1 potete scrivere

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

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

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.

Siano $(a, b) \neq (c, d)$ e $(e, f) \neq (g, h)$ quindi $ad \neq bc \wedge eh \neq fg$, dimostro che
 $(a, b) + (e, f) = (c, d) + (g, h) \Rightarrow (af + be, bf) = (ch + dg, dh)$
 $\Rightarrow (af + be) \cdot dh = (ch + dg) \cdot bf \Rightarrow afh + bedh = bch + bfgd = 0 \Rightarrow fh ad - fh bc = bdfg - bdeh$
 \Rightarrow USO LE IPOTESI $ad = bc \wedge eh = fg \Rightarrow fh bc - fh bc = bdeh - bdeh \Rightarrow 0 = 0$ verificato.
 $(a, b) \cdot (e, f) = (c, d) \cdot (g, h) \Rightarrow (ae, bf) = (cg, dh) \Rightarrow aedh = bfcg \Rightarrow bc fg = \underbrace{a} \underbrace{deh} = bc fg$

Esercizio 6. Consideriamo il campo dei numeri reali $(\mathbb{R}, +, \cdot)$. Consideriamo il sottoinsieme

$$\mathbb{Q}[\sqrt{2}] := \{\alpha + \sqrt{2}\beta, \alpha, \beta \in \mathbb{Q}\} \subset \mathbb{R}.$$

Verificare che le due operazioni di $(\mathbb{R}, +, \cdot)$ inducono in questo insieme una struttura di anello²; dimostrare che $\mathbb{Q}[\sqrt{2}]$ è un campo.

dimostro che $\mathbb{Q}[\sqrt{2}]$ sia un anello, come prima cosa, verifico che gli elementi di $\mathbb{Q}[\sqrt{2}]$ commutino rispetto alla somma.

$$a, b \in \mathbb{Q}[\sqrt{2}], a + b = (\alpha + \beta\sqrt{2}) + (\alpha' + \beta'\sqrt{2}) = \alpha + \beta\sqrt{2} + \alpha' + \beta'\sqrt{2} = \alpha' + \beta'\sqrt{2} + \alpha + \beta\sqrt{2} = b + a.$$

Sia $a \in \mathbb{Q}[\sqrt{2}]$, $a + \bar{a} = 0 \Rightarrow a = \alpha + \beta\sqrt{2} \wedge \bar{a} = -\alpha + (-\beta)\sqrt{2}$. lo zero è $0 \cdot 0\sqrt{2}$.

Dim inv. $a + \bar{a} \Rightarrow \alpha + \beta\sqrt{2} + (-\alpha + (-\beta)\sqrt{2}) = \alpha - \alpha + (\beta - \beta)\sqrt{2} = 0 + 0\sqrt{2} = 0$.

• e' associativa: $(a \cdot b) \cdot c = (\alpha + \beta\sqrt{2} \cdot \alpha' + \beta'\sqrt{2}) \cdot \alpha'' + \beta''\sqrt{2} = (\alpha + \beta\sqrt{2}) \cdot \alpha' + \beta'\sqrt{2} \cdot \alpha'' + \beta''\sqrt{2} = a \cdot (b \cdot c)$

Valgono le proprietà distributive:

$$a \cdot (b + c) = \alpha + \beta\sqrt{2} \cdot ((\alpha' + \beta'\sqrt{2}) + (\alpha'' + \beta''\sqrt{2})) = (\alpha + \beta\sqrt{2})(\alpha' + \beta'\sqrt{2}) + (\alpha + \beta\sqrt{2})(\alpha'' + \beta''\sqrt{2}) = ab + ac$$

l'elemento neutro rispetto al prodotto e' $\bar{1} = 1 + 0 \cdot \sqrt{2}$

ogni elemento ha un inverso: $\alpha + \beta\sqrt{2} \cdot (\alpha + \beta\sqrt{2})^{-1} = 1$

$$(\alpha + \beta\sqrt{2})^{-1} = \frac{\alpha + \beta\sqrt{2}}{(\alpha + \beta\sqrt{2})^2} = \frac{\alpha}{(\alpha + \beta\sqrt{2})^2} + \frac{\beta\sqrt{2}}{(\alpha + \beta\sqrt{2})^2}$$

Esercizio 7. Abbiamo visto che in un anello $(A, +, \cdot)$ con elemento neutro additivo 0 si ha sempre che $a \cdot 0 = 0 = 0 \cdot a$. Denotiamo con $-a$ l'inverso additivo di un elemento $a \in A$. Verificare che si ha sempre:

- $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$
- $(-a) \cdot (-b) = ab$
- denotiamo brevemente $(b + (-c))$ con $b - c$; verificare che $a \cdot (b - c) = a \cdot b - a \cdot c$

$$a \cdot (-b) = (-a) \cdot b \Leftrightarrow a \cdot (-b) + ((-a) \cdot b)^{-1} = 0 \Leftrightarrow a \cdot (-b) + (-b \cdot a) = 0$$

$$\Leftrightarrow a \cdot (-b) + b \cdot (-a) = 0 \Leftrightarrow (a \cdot (-b))^{-1} = b \cdot (-a) \text{ ma so che}$$

$$(a \cdot (-b))^{-1} = b \cdot (-a) \text{ quindi: } a \cdot (-b) = (-a) \cdot b.$$

$$(-a) \cdot (-b) = a \cdot b \Leftrightarrow \underbrace{(-a) \cdot (-b)}_{\text{PER IL PUNTO 1}} + ab = 0 \Leftrightarrow \underbrace{a \cdot (-b)}_{\text{PUNTO 1}} + ab = 0 \Leftrightarrow -(a \cdot b) + a \cdot b = 0 \Leftrightarrow 0 = 0.$$

$$a \cdot (b + (-c)) = a \cdot b + a \cdot (-c) = \underbrace{\text{PER IL PUNTO 1}}_{\rightarrow -(a \cdot c) = a \cdot (-c)} a \cdot b + (-a \cdot c) = ab - ac$$

Esercizio 8. Sia A un anello unitario e sia $\mathcal{U}(A)$ l'insieme degli elementi invertibili di A :

$$\mathcal{U}(A) := \{a \in A : \exists a' \in A \text{ tale che } a \cdot a' = 1 = a' \cdot a\}$$

Dimostrate da soli, senza guardare gli appunti, che il prodotto di due elementi in $\mathcal{U}(A)$ è ancora in $\mathcal{U}(A)$ e che quindi la moltiplicazione in A induce in $\mathcal{U}(A)$ una struttura di gruppo (il gruppo degli invertibili di A). Suggerimento: utilizzate l'esercizio 1.3.

Siano $a, b \in \mathcal{U}(A)$, $\exists! a', b' \mid a \cdot a' = 1 = a' \cdot a \wedge b \cdot b' = 1 = b' \cdot b$.

So che $(a \cdot b)^{-1} = b' \cdot a'$, assumo che $(ab)^{-1}$ sia l'inverso di ab :

$$ab \cdot (ab)^{-1} = (a \cdot b) \cdot (b' \cdot a') = (a \cdot b) \cdot (b' \cdot a') \stackrel{\circ}{=} a \cdot b \cdot b' \cdot a' = a \cdot 1 \cdot a' = a \cdot a' = 1$$

\rightarrow ASSOCIATIVITA'

$$(ab)^{-1} \cdot ab = (b' \cdot a') \cdot ab = (b' \cdot a') \cdot a \cdot b \stackrel{\circ}{=} b' \cdot (a' \cdot a) \cdot b = b' \cdot 1 \cdot b = b' \cdot b = 1$$

Quindi, se a e b sono invertibili, anche $a \cdot b$ lo è.