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) se $e \in G$ e' l'elemento neutro, vale che $\forall s \in G \mid s \cdot e = s = e \cdot s$ ma sia $\tilde{e}$ un altro elemento neutro, quindi $\forall s \in G \mid s \cdot \tilde{e} = s = \tilde{e} \cdot s$, preso $s = e$ si ha: $\tilde{e} \cdot e = e = e \cdot \tilde{e}$, ma e' vero che $e \cdot \tilde{e} = \tilde{e} = e \cdot \tilde{e}$, quindi:

$$\begin{cases} \tilde{e} \cdot e = e = e \cdot \tilde{e} \\ e \cdot \tilde{e} = \tilde{e} = e \cdot \tilde{e} \end{cases} \Longrightarrow e = \tilde{e}$$ l'elemento neutro e' unico.

1.2) se $g \in G$, si ha $\exists g' \in G \mid g \cdot g' = e = g' \cdot g$, ma sia g'' un altro inverso di g, quindi: $g \cdot g'' = e = g'' \cdot g$, essendo $(G, \cdot)$ un gruppo, ogni elemento ha un inverso, quindi l'inverso di $g'^{-1} = g$ e $g''^{-1} = g$,

$$\begin{cases} g \cdot g'' = e = g'' \cdot g \\ g \cdot g' = e = g' \cdot g \end{cases} \Longrightarrow \begin{cases} g \cdot g' = e = g'' \cdot g \Rightarrow g \cdot g' = g'' \cdot g \\ g \cdot g'' = e = g' \cdot g \Rightarrow g \cdot g'' = g' \cdot g \end{cases} \Rightarrow g \cdot g'' = g \cdot g' \Rightarrow g' = g''$$

1.3) $(g \cdot h)^{-1} = g^{-1} \cdot h^{-1}$, esistono g' t.c. $g' \cdot g = e = g \cdot g'$ e h' t.c. $h' \cdot h = e = g \cdot g'$, quindi $(g^{-1} \cdot g) \cdot h^{-1} = e \cdot h^{-1} = h^{-1}$, quindi aggiungo ad entrambi i membri $(g \cdot h)$,

$$\Rightarrow (g \cdot h) \cdot (g \cdot h)^{-1} = g^{-1} \cdot h^{-1} \cdot (g \cdot h) = \boxed{\text{prop. assoc.}} \Rightarrow \underbrace{(g \cdot h) \cdot (g \cdot h)^{-1}}_{e} = \underbrace{g^{-1} \cdot g}_{e} \cdot \underbrace{h^{-1} \cdot h}_{e} =$$

$$\Rightarrow e = e \cdot e \Rightarrow e = e$$

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

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

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

Se f e' biunivoca $\forall a \in A$ $\exists b$ unico t.c. $f(a) = b$, analogamente, vale che $\forall b \in B$ $\exists a$ unico t.c. $f^{-1}(b) = a$. prendiamo un elemento k t.c. $f(k) = k'$, quindi $f^{-1}(k') = k$, per composizione, $f \circ f^{-1} = f(f^{-1}(x))$, preso $(f \circ f^{-1})(k) = f(f^{-1}(k)) = f(k') = k$, quindi $\forall a \in A$, $(f \circ f^{-1})(a) = a$.

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).

E' un gruppo perche': 1 $\circ$ e' associativa, $(f \circ g) \circ k = f(g(x)) \circ k = f(g(k(x))) = f \circ (g \circ k)$. 2 esiste $\mathrm{id}_x(x) = x$, tale che $f \circ \mathrm{id}_x = f(\mathrm{id}_x(x)) = f(x) = f$ $\forall f \in G$, quindi id_x e' l'elemento neutro. 3 essendo f biettiva $\forall f \in G$, esiste $\forall f$, f^{-1}, ossia la sua inversa, tale che, $\forall k \in A$ $f(k) = k'$ e $f^{-1}(k') = k$, t.c. $f(f^{-1}(k)) = k = \mathrm{id}_x$, $\forall k \in A, f \in G$, quindi ogni elemento ha il suo inverso.

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

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

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

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.

5.1) verifico che la somma sia ben posta, cio' vuol dire che, se
$(a,b)\sim(a',b')$ e $(c,d)\sim(c',d') \Rightarrow [(a,b)]+[(c,d)] = [(a',b')]+[(c',d')] \Rightarrow$
$\Rightarrow [(a\cdot d+b\cdot c, d\cdot b)] = [(a'\cdot d'+b'\cdot c', d'\cdot b')] \Longleftrightarrow (ad+bc, db)\sim(a'd'+b'c', d'b') \Leftarrow$
$\Rightarrow (ad+bc)\cdot d'b' = db\cdot(a'd'+b'c')$ ma dato $(a,b)\sim(a',b')$ e $(c,d)\sim(c',d')$ e' vero che:
$ab'=ba'$ e $cd'=dc'$, tornando a noi: $(ad+bc)\cdot d'b' = (db\cdot a'd'+b'c')$ $\Rightarrow$ distr.
$\Rightarrow add'b'+bcb'd' = dbb'c'+a'd'b'c' \Rightarrow dd'ba'+bb'dc' = dbb'c'+a'd'b'c' =$ per prop.
associativa e comm. $\Rightarrow dd'ba'+bb'dc' = dd'ba'+bb'dc'$ la somma e' ben posta

5.2) verifico che il prodotto sia ben posto, ossia che se
$(a,b)\sim(a',b')$ e $(c,d)\sim(c',d') \Rightarrow [(a,b)]\cdot[(c,d)] = [(a',b')]\cdot[(c',d')] \Rightarrow$
$\Rightarrow [(ac, bd)] = [(a'c', b'd')] \Rightarrow (ac, bd)\sim(a'c', b'd') \Rightarrow acb'd' = bda'c'$ ma
si ricordi che $ab'=ba'$ e $cd'=dc'$ $\Rightarrow$ $ba'cd' = ba'cd'$ (ass. e com.)