

Corso di geometria (per fisici)

ANNO ACCADEMICO 2009/2010
CANALE C

Esercizi - Settimana 1 - Foglio A

Gruppo 1.

- $x \in (A \cap B) \cap C \iff x \in (A \cap B) \text{ e } x \in C \iff x \in A \text{ e } x \in B \text{ e } x \in C \iff x \in (A \cap C) \text{ e } x \in (B \cap C) \iff x \in (A \cap C) \cap (B \cap C)$
- $x \in (A \cap B) \cup C \iff x \in (A \cap B) \text{ o } x \in C \iff (x \in A \text{ e } x \in B) \text{ o } x \in C \iff (x \in A \text{ o } x \in C) \text{ e } (x \in B \text{ o } x \in C) \iff x \in (A \cup C) \text{ e } x \in (B \cup C) \iff x \in (A \cup C) \cap (B \cup C)$
- $x \in A \setminus (B \cup C) \iff x \in A \text{ e } x \notin (B \cup C) \iff x \in A \text{ e } x \notin B \text{ e } x \notin C \iff (x \in A \text{ e } x \notin B) \text{ e } (x \in A \text{ e } x \notin C) \iff x \in (A \setminus B) \text{ e } x \in (A \setminus C) \iff x \in (A \setminus B) \cap (A \setminus C)$
- $x \in A \times (B \cap C) \iff x = (a, y) \text{ con } a \in A \text{ e } y \in B \cap C \iff x = (a, y) \text{ con } a \in A \text{ e } (y \in B \text{ e } y \in C) \iff (x = (a, y) \text{ con } a \in A \text{ e } y \in B) \text{ e } (x = (a, y) \text{ con } a \in A \text{ e } y \in C) \iff x \in A \times B \text{ e } x \in A \times C \iff x \in (A \times B) \cap (A \times C)$

Gruppo 2.

- $g \circ f$ suriettiva $\implies \forall c \in C$ esiste $a \in A$ tale che $(g \circ f)(a) = c$. In particolare, $g(b) = c$, dove $b = f(a)$, e quindi g è suriettiva.
- Siano $a_1, a_2 \in A$ e supponiamo $f(a_1) = f(a_2)$. Allora $(g \circ f)(a_1) = (g \circ f)(a_2)$. Ora, $g \circ f$ iniettiva $\implies a_1 = a_2$. Quindi f è iniettiva.
- Se $g \circ h = id_C$, allora g è suriettiva, perché id_C lo è. Viceversa, se g è suriettiva, per ogni $c \in C$ scegliamo un $b \in B$ tale che $g(b) = c$ (sappiamo che tale b esiste perché g è suriettiva) e definiamo $h(c) := b$. È chiaro che $g(h(c)) = c$ per ogni $c \in C$ per costruzione.

4. Se $k \circ f = id_A$, allora f è iniettiva, perché id_A lo è.
Viceversa, se f è iniettiva, allora definiamo k nel modo seguente. Dato $b \in B$, esiste al più un elemento $a \in A$ tale che $f(a) = b$. Se tale elemento esiste, definiamo $k(b) := a$. Altrimenti definiamo $k(b) \in A$ come vogliamo. Per costruzione, avremo $k \circ f = id_A$.
5. Dai punti precedenti segue che un'inversa esiste se e solo se f è iniettiva e suriettiva, ossia biiettiva. Per l'unicità, se avessi due inverse k e k' di f , allora $k = id_A \circ k(k' \circ f) \circ k = k' \circ (f \circ k) = k' \circ id_B = k'$.
6. $a \in f^{-1}(B_1) \cap f^{-1}(B_2) \iff a \in f^{-1}(B_1) \text{ e } a \in f^{-1}(B_2) \iff f(a) \in B_1 \text{ e } f(a) \in B_2 \iff f(a) \in B_1 \cap B_2 \iff a \in f^{-1}(B_1 \cap B_2)$.
 $a \in f^{-1}(B_1) \cup f^{-1}(B_2) \iff a \in f^{-1}(B_1) \text{ o } a \in f^{-1}(B_2) \iff f(a) \in B_1 \text{ o } f(a) \in B_2 \iff f(a) \in B_1 \cup B_2 \iff a \in f^{-1}(B_1 \cup B_2)$.
7. $b \in f(A_1 \cup A_2) \iff \exists a \in A_1 \cup A_2$ tale che $f(a) = b \iff \exists a_1 \in A_1$ tale che $f(a_1) = b$ oppure $\exists a_2 \in A_2$ tale che $f(a_2) = b \iff b \in f(A_1)$ oppure $b \in f(A_2) \iff b \in f(A_1) \cup f(A_2)$.
Se $b \in f(A_1 \cap A_2)$, allora $\exists a \in A_1 \cap A_2$ tale che $f(a) = b$. Quindi $\exists a_1 \in A_1$ tale che $f(a_1) = b$ e $\exists a_2 \in A_2$ tale che $f(a_2) = b$, ovvero basta prendere $a_1 = a_2 = a$. Ne segue che $b \in f(A_1)$ e $b \in f(A_2)$, ossia $b \in f(A_1) \cap f(A_2)$.
Il viceversa non vale: se consideriamo l'unica $f : \{1, 2\} \rightarrow \{0\}$ e prendiamo $A_1 = \{1\}$ e $A_2 = \{2\}$, otteniamo che $A_1 \cap A_2 = \emptyset$ e quindi $f(A_1 \cap A_2) = \emptyset$, mentre $f(A_1) = f(A_2) = \{0\}$ e quindi $f(A_1) \cap f(A_2) = \{0\}$.
Tuttavia, se f è iniettiva, allora $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$. Infatti, se $b \in f(A_1) \cap f(A_2)$, allora $\exists a_1 \in A_1$ such that $f(a_1) = b$ and $\exists a_2 \in A_2$ tale che $f(a_2) = b$. Dato che f è iniettiva, $a_1 = a_2$ e quindi $a_1 = a_2 \in A_1 \cap A_2$, ossia $b \in f(A_1 \cap A_2)$.
8. Vedere foglio B di esercizi.
9. Vedere foglio B di esercizi.

Gruppo 3.

1. L'applicazione \bar{f} è ben definita. Infatti, se $[x_1] = [x_2]$ per $x_1, x_2 \in X$, allora $x_1 \sim x_2$. Di conseguenza, $\bar{f}([x_1]) = f(x_1) = f(x_2) = \bar{f}([x_2]) \in$

$f(X)$.

\bar{f} è iniettiva. Infatti, se $\bar{f}([x_1]) = \bar{f}([x_2])$, allora $f(x_1) = f(x_2)$ e quindi $x_1 \sim x_2$, ovvero $[x_1] = [x_2]$.

\bar{f} è suriettiva. Infatti, se $y \in f(X)$, allora $\exists x \in X$ tale che $f(x) = y$. Ne segue che $\bar{f}([x]) = y$.

- \sim è riflessiva perché $x^2 \geq 0$ per ogni $x \in \mathbb{Q}$ ed è chiaramente simmetrica. Però non è transitiva: infatti, se $x > 0$ e $y < 0$, allora $x \sim 0$ e $0 \sim y$, però $x \not\sim y$. Quindi \sim non è una relazione di equivalenza.
- \sim è riflessiva perché $x - x = 0 \in \mathbb{N}$, però non è simmetrica, perché $2 \sim 1$ (dato che $2 - 1 = 1 \in \mathbb{N}$) ma $1 \not\sim 2$ (dato che $1 - 2 = -1 \notin \mathbb{N}$). Quindi \sim non è una relazione di equivalenza.

- \sim è riflessiva perché $x - x = 0 \in \mathbb{Z}$; è simmetrica, perché $x \sim y \implies x - y \in \mathbb{Z} \implies y - x \in \mathbb{Z} \implies y \sim x$. Infine, \sim è transitiva: se $x \sim y$ e $y \sim z$, allora $x - y \in \mathbb{Z}$ e $y - z \in \mathbb{Z}$; quindi $z - x = (z - y) + (y - x) \in \mathbb{Z}$. Quindi \sim è una relazione di equivalenza.

$[x] + [y] := [x + y]$ è ben definita su \mathbb{Q}/\sim . Infatti, se $[x'] = [x]$ e $[y'] = [y]$, ovvero se $x' \sim x$ e $y' \sim y$, allora $\exists n, m \in \mathbb{Z}$ tali che $x' = x + n$ e $y' = y + m$. Quindi $[x' + y'] = [x + n + y + m] = [x + y]$. È chiaro che $[0]$ è l'elemento neutro, che la somma è associativa e commutativa e che $[-x]$ è l'inverso additivo di $[x]$. Quindi $(\mathbb{Q}, +)$ è un gruppo abeliano.

Invece, $[x] \cdot [y] := [x \cdot y]$ non è ben definita. Infatti, se considero $x = 1$ e $y = 1/2$, allora $[x] \cdot [y] = [xy] = [y]$. Tuttavia, $[x] = [0]$ e quindi dovranno anche avere $[x] \cdot [y] = [0] \cdot [y] = [0]$. Ma $[y] \neq [0]$ perché $y - 0 = y \notin \mathbb{Z}$.

- Se $a \neq b$, la relazione \sim non è riflessiva. Infatti, il polinomio $p(t) = t - a$ soddisferebbe $p(a) = 0 \neq b - a = p(b)$ e quindi $p(t) \not\sim p(t)$.

Tuttavia, se scelgo $a = b \in \mathbb{Q}$, allora \sim è una relazione di equivalenza. Infatti, $p(a) = p(a)$ e quindi $p(t) \sim p(t)$; $p(a) = q(a) \iff q(a) = p(a)$ e quindi $p(t) \sim q(t) \iff q(t) \sim p(t)$; infine, se $p(t) \sim q(t)$ e $q(t) \sim r(t)$, questo vuol dire che $p(a) = q(a)$ e $q(a) = r(a)$ e quindi $p(a) = r(a)$, ossia $p(t) \sim r(t)$.

Gruppo 4.

1. Chiaramente $(\mathbb{Q}[\eta], +)$ è un gruppo abeliano. Infatti $0 \in \mathbb{Q}[\eta]$, la somma è commutativa e associativa e l'inverso additivo di $a + b\eta + c\eta^2 \in \mathbb{Q}[\eta]$ è $-a - b\eta - c\eta^2 \in \mathbb{Q}[\eta]$.

La moltiplicazione $(a + b\eta + c\eta^2)(a' + b'\eta + c'\eta^2) = (aa' + bc' + b'c) + (ab' + a'b + cc')\eta + (ac' + a'c + bb')\eta^2$ è associativa, commutativa e distributiva rispetto alla somma. L'elemento neutro per la moltiplicazione è 1. Infine, $(\mathbb{Q}[\eta]^*, \cdot)$ è un gruppo abeliano, ossia esiste l'inverso moltiplicativo di ogni numero non nullo. Infatti, se voglio invertire $a + b\eta + c\eta^2 \neq 0$, posso supporre che $a \neq 0$ (i casi $b \neq 0$ oppure $c \neq 0$ sono analoghi). Voglio trovare $a' + b'\eta + c'\eta^2 \in \mathbb{Q}[\eta]$ non nullo tale che il prodotto $(a + b\eta + c\eta^2)(a' + b'\eta + c'\eta^2) = (aa' + bc' + b'c) + (ab' + a'b + cc')\eta + (ac' + a'c + bb')\eta^2$ sia uguale a $q \in \mathbb{Q}$. Infatti, da questo concluderei che

$$\frac{1}{a + b\eta + c\eta^2} = \frac{a'}{q} + \frac{b'}{q}\eta + \frac{c'}{q}\eta^2.$$

Nel caso $a \neq 0$, posso scegliere $a' \in \mathbb{Q}$ a piacere (per esempio $a' = 1$), $b' = \frac{-a'b - cc'}{a}$ e $c' = \frac{-a'c - bb'}{a}$.

2. No, $(\mathbb{Q}[t], +)$ è un gruppo abeliano. La moltiplicazione dei polinomi è associativa, distributiva, commutativa e con elemento neutro (il polinomio costante 1). Ma i polinomi di grado almeno 1 non hanno un inverso moltiplicativo. Infatti, se $\deg(p(t)) \geq 1$, per ogni $q(t) \neq 0$, $\deg(p(t)q(t)) \geq 1$, e quindi non potremmo mai avere $p(t)q(t) = 1$. La struttura di $(\mathbb{Q}[t], +, \cdot)$ è quella di *anello commutativo con unità*.

$(\mathbb{Q}[t, t^{-1}], +)$ è ancora un gruppo abeliano e la moltiplicazione è associativa, distributiva, commutativa e con unità 1. Inoltre, i polinomi del tipo t^k hanno un inverso moltiplicativo, ossia t^{-k} . Tuttavia, $p(t) = t - 1$ non ha un inverso moltiplicativo. Infatti, se $q(t) = a_{-k}t^{-k} + \dots + a_d t^d$ fosse l'inverso moltiplicativo di $p(t)$, dove $a_i \in \mathbb{Q}$ e $d \geq 0$ e $k \geq 1$ sono interi, allora avremmo necessariamente $1 = p(t)q(t) = -a_{-k}t^{-k} + \dots + a_d t^{d+1}$, che è chiaramente assurdo.

3. Visto a lezione.
4. Visto a lezione.
5. Supponiamo $p(t) \neq 0$ e sia $d = \deg(p) \geq 0$. Consideriamo $a_1, \dots, a_{d+1} \in \mathbb{K}$ elementi distinti (che esistono, perché \mathbb{K} ha infiniti elementi). Poiché

$p(a_i) = 0$, allora $(t - a_i) | p(t)$. Poiché gli a_i sono tutti distinti, allora $\text{mcd}(t - a_i, t - a_j) = \text{mcd}(t - a_i, a_i - a_j) = 1$ per $i \neq j$, ossia i polinomi $(t - a_i)$ sono a due a due relativamente primi fra loro e quindi $(t - a_1)(t - a_2) \cdots (t - a_{d+1}) | p(t)$, la qual cosa è assurda per ragioni di grado. L'assurdo viene dall'aver supposto $p(t) \neq 0$. Dunque $p(t) = 0$.

6. Basta prendere $q(t) = t(t - \bar{1})(t - \bar{2}) \cdots (t - \overline{p-1}) \in \mathbb{Z}/p[t]$. Questo è un polinomio di grado p tale che $q(a) = 0$ per ogni $a \in \mathbb{Z}/p$.
7. Se $p(t)$ è costante (ossia $b = c = 0$), allora la funzione associata non è né iniettiva né suriettiva.

Se $p(t) = a + bt$ con $b \neq 0$ (ossia $c = 0$), allora la funzione è biiettiva. Infatti, per ogni $y \in \mathbb{R}$, $p(t) = a + bt = y$ se e solo se $t = (y - a)/b$.

Se $c \neq 0$, allora la funzione non è né iniettiva né suriettiva. Infatti, l'equazione $p(t) = a + bt + ct^2 = y$ nella variabile t ha due soluzioni reali e distinte quando $b^2 - 4(a - y)c > 0$, ovvero quando $y > a - b^2/4c$ (il che mostra che la funzione non è iniettiva), e non ha soluzioni reali quando $y < a - b^2/4c$ (il che mostra che la funzione non è suriettiva).

Nel caso invece della cubica con $d \neq 0$, la funzione è sempre suriettiva, perché l'equazione $a + bt + ct^2 + dt^3 = y$ nella variabile t ha almeno una soluzione reale per ogni $y \in \mathbb{R}$ per il teorema fondamentale dell'algebra. L'iniettività però è più sottile e richiede uno studio di funzione. In effetti, la funzione sarà iniettiva se e solo se sarà strettamente crescente o strettamente decrescente, ovvero se e solo se la derivata di $q'(t) = b + 2ct + 3dt^2$ di $q(t)$ non avrà due radici reali distinte, ovvero se e solo se $c^2 - 3bd \leq 0$.