scelta $f: \mathcal{P}^{\neq\emptyset}(S) \to S$, e, fissato un $a_0 \in S$ qualunque, definiamo per ricorsione $a_{n+1} = f(\{x \in S \mid x < a_n\})$.
Siccome S non ha minimo, l'insieme a cui è applicata f non è mai vuoto, per cui la sequenza a_n è ben definita ∎

Esempi di applicazione di AC

Vediamo qui alcuni esempi di applicazione di AC al di fuori del contesto, strettamente, della teoria degli insiemi. Un primo esempio, molto facile, è dimostrare che, in uno spazio primo-numerabile (ossia, ogni punto ha una base di intorni numerabile, per esempio uno spazio metrico, per via delle palle di raggio $\frac{1}{n}$) un punto x è nella chiusura $\bar{A}$ di A se è limite di una successione di punti di A.
Considerando, per concretezza, lo spazio $\mathbb{R}$, abbiamo:

Prop. Sia $A \subseteq \mathbb{R}$, allora

$$x \in \bar{A} \iff \exists \{x_i\}_{i\in\omega} \left(\forall i \in \omega\ x_i \in A\right) \wedge \left(\lim_{i\to\infty} x_i = x\right)$$

$$\overset{\text{def.}}{=} \forall \varepsilon > 0 \quad]x-\varepsilon, x+\varepsilon[\cap A \neq \emptyset$$

Dim.

$\leftarrow$ $\forall \varepsilon > 0 \ \exists i \ x_i \in]x-\varepsilon, x+\varepsilon[\cap A$

quindi $\forall \varepsilon > 0 \ ]x-\varepsilon, x+\varepsilon[\cap A \neq \emptyset$ ossia, per definizione, $x \in \bar{A}$.

$\rightarrow$ Sia f una funzione di scelta per $\mathcal{P}(A) \setminus \{\emptyset\}$.
Definiamo $x_i = f\left(A \cap \left]x - \frac{1}{i+1}, x + \frac{1}{i+1}\right[\right)$ ∎

Un'altra applicazione è l'esistenza di basi degli spazi vettoriali

infinito-dimensionali. Questo ragionamento, in realtà, si applica non solo alla dipendenza lineare, ma a qualunque relazione di dipendenza che soddisfi il lemma dello scambio di Steinitz, per esempio la dipendenza algebrica.

Promemoria.

Sia F un campo e V uno spazio vettoriale su F.

$A \subseteq V$ è linearmente indipendente se per ogni $a_1 \dots a_n \in A$ e $x_1 \dots x_n \in F$ $\quad x_1 a_1 + \dots + x_n a_n = 0 \leftrightarrow x_1 = \dots = x_n = 0$

$B \subseteq V$ linearmente indipendente è una base se dato $v \in V$ esistono $b_1 \dots b_n \in B$ $x_1 \dots x_n \in F$ tali che $v = x_1 b_1 + \dots + x_n b_n$

Ossia B è una base di V se ogni elemento di V si scrive in modo unico come combinazione lineare FINITA di elementi di B.

Non avrebbe senso, in generale, parlare di combinazioni lineari se non finite.

L'osservazione seguente è la chiave per applicare il lemma di Zorn

Oss. B è una base se e solo se è un sottoinsieme linearmente indipendente di V massimale rispetto all'inclusione.

Dim

($\text{base} \to \text{massimale}$) Se B non fosse massimale, ci sarebbe $v \in V$ tale che $B \cup \{v\}$ è linearmente indipendente. Ma $v = b_1 x_1 + \dots + b_n x_n$

per opportuni $b_1 \dots b_n \in B$ e $x_1 \dots x_n \in F$. Quindi $B \cup \{v\}$ non è indipendente perché $b_1 x_1 + \dots + b_n x_n + v \cdot (-1) = 0$ ∎

(massimale → base) Sia B massimale, $v \in V$. Se $v \in B$, chiaramente $v = v \cdot 1$. Altrimenti, per la massimalità di B, $B \cup \{v\}$ non è indipendente. Di conseguenza esistono $b_1 \dots b_n \in B$ $x_1 \dots x_n, y \in F$ tali che $x_1 b_1 + \dots + x_n b_n + y v = 0$ ma non $x_1 = \dots = x_n = y = 0$.
Se y fosse $= 0$, avremmo $x_1 = \dots = x_n = 0$ per l'indipendenza di B.
Quindi $y \neq 0$ e $v = \left(-\frac{x_1}{y}\right) b_1 + \dots + \left(-\frac{x_n}{y}\right) b_n$ ∎

Prop Dato uno spazio vettoriale V e $X \subseteq V$ linearmente indipendente, esiste una base B di V tale che $X \subseteq B$.
Dim Applichiamo il lemma di Zorn all'insieme dei sottoinsiemi A di V linearmente indipendenti tali che $X \subseteq A$, ordinati per inclusione. Occorre dimostrare che l'unione di una catena di insiemi linearmente indipendenti C è linearmente indipendente.

Siano $a_1 \dots a_n \in \bigcup C$. Consideriamo $A_1 \dots A_n \in C$ tali che per ogni $i = 1 \dots n$ $a_i \in A_i$. Siccome C è una catena per inclusione, c'è un $j \in \{1 \dots n\}$ tale che A_j include tutti gli altri A_i.
Quindi $a_1 \dots a_n \in A_j$ e, siccome A_j è indipendente,

$x_1 a_1 + \dots + x_n a_n = 0 \iff x_1 = \dots = x_n = 0$ ∎

Esercizio Sia B una base di $\mathbb{R}$ come $\mathbb{Q}$-spazio vettoriale, determina $|B|$.

Esempio Esiste una funzione $f : \mathbb{R} \to \mathbb{R}$ tale che

$$\forall x, y \in \mathbb{R} \quad f(x+y) = f(x) + f(y)$$

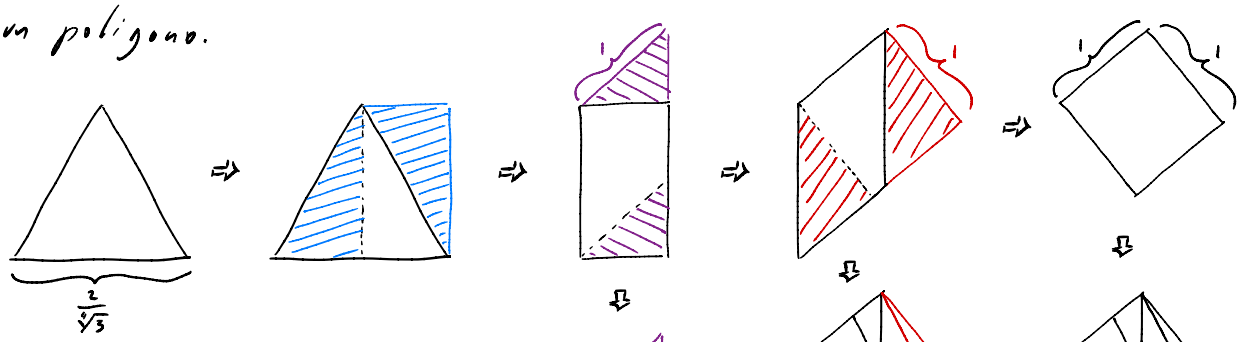
tuttavia f **non** è della forma $f(x) = k \cdot x$.

Dim Sia B una base di $\mathbb{R}$ come $\mathbb{Q}$-spazio vettoriale. Fissiamo $b_1 \in B$. Consideriamo la funzione

$$f : \mathbb{R} \to \mathbb{Q}$$

$$x \longmapsto y_1 \text{ tale che } \exists y_2 \dots y_n \; x = b_1 y_1 + \dots + b_n y_n. \qquad \blacksquare$$

È noto dall'antichità che due poligoni aventi la stessa area sono scomponibili in un numero finito di poligoni congruenti — *equiscomponibili* — questa si può considerare, anzi, la definizione stessa di area di un poligono.



Per passare da un poligono ad un quadrato equivalente, spezzalo in triangoli, poi trasforma i triangoli in rettangoli, poi passando per un parallelogramma, poi trasforma un rettangolo in un altro con uno dei due lati arbitrario. Porta tutti i rettangoli ad avere un

lato uguale, unisci li, e trasforma il nuovo rettangolo in un quadrato, di nuovo col trucco del parallelogramma.

Nota Curiosamente, Euclide non definisce l'area, ma, dal momento che ci ragiona aggiungendo e togliendo pezzi congruenti, possiamo adattare, a posteriori, una definizione basata sull'equiscomponibilità alla matematica classica. Ancora più curiosamente, i ragionamenti di Euclide richiedono, in realtà di definire $Area(A) = Area(B)$ se e solo se esistono due poligoni C e D, rispettivamente non sovrapposti ad A e B, equiscomponibili fra loro, tali che $A \cup C$ e $B \cup D$ sono equiscomponibili. Per dedurre che, in realtà, due poligoni con la stessa area sono equiscomponibili serve l'assioma di Archimede, che Euclide non aveva. La sistemazione formale di questi concetti è dovuta a Hilbert, e al XIX secolo.

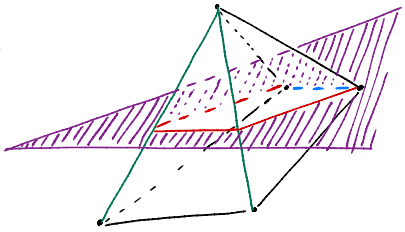
Ebbene, tutti questi anacronismi solo per dire che in tre dimensioni non funziona.

Teo (Dehn)
Un cubo ed un tetraedro regolare (sia pure aventi il medesimo volume) non si possono scomporre in un numero finito di poliedri congruenti.

Dim
Supponiamo di avere una funzione $f: \mathbb{R} \to \mathbb{R}$ additiva tale che $f(x) = 0$ se e solo se x è un multiplo razionale di π — $x = k\pi$ con $k \in \mathbb{Q}$.

Definiamo il valore di un poliedro come la somma dei valori dei suoi spigoli, definiti, a loro volta, dicendo che il valore di uno spigolo di lunghezza l che forma un angolo diedro di ampiezza α è $l \cdot f(\alpha)$.

Quando tagliamo un poliedro A con un piano, ottenendo così due nuovi poliedri B e C, la somma dei valori di B e C equivale al valore di A. Infatti, il taglio dà luogo ad alcuni spigoli nuovi, in rosso, ma la somma dei due angoli diedri, poniamo α_1 e α_2, che insistono su uno qualunque di essi è π e $l \cdot f(\alpha_1) + l \cdot f(\alpha_2) = l \cdot f(\alpha_1 + \alpha_2) = 0$. Può dividere spigoli vecchi, in verde, in due, poniamo di lunghezza l_1 e l_2, senza alterare l'angolo diedro, per cui $(l_1 + l_2) f(\alpha) = l_1 f(\alpha) + l_2 f(\alpha)$. Infine, in azzurro, può spezzare l'angolo diedro lasciando inalterata la lunghezza, e si conclude similmente.



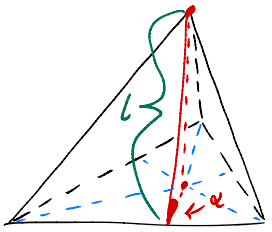
Abbiamo concluso che il valore è invariante per equiscomposizioni, ci resta da costruire f. Fissiamo una base B di $\mathbb{R}$ come spazio vettoriale su $\mathbb{Q}$ tale che $\pi \in B$ — ossia estendendo l'insieme linearmente indipendente $\{\pi\}$. Definiamo

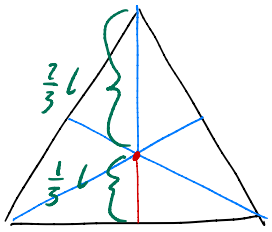
$$f(\pi q_0 + b_1 q_1 + \dots + b_n q_n) = b_1 q_1 + \dots + b_n q_n$$

per ogni $q_0 \dots q_n \in \mathbb{Q}$ e $b_1 \dots b_n \in B \setminus \{\pi\}$

f è quindi la proiezione su un complemento del sottospazio $\pi\mathbb{Q}$.
L'additività di f è conseguenza immediata della $\mathbb{Q}$-linearità.
Inoltre, per definizione, $f(x)=0$ se e solo se x si scrive nella forma πq_0 con $q_0 \in \mathbb{Q}$.

Ora si chiama che il valore di un cubo è nullo, perché tutti i diedri hanno ampiezza $\frac{1}{2}\pi$. Occorre quindi dimostrare che il valore di un tetraedro regolare è non nullo. Si vede facilmente che i diedri del tetraedro valgono $\alpha = \arccos\frac{1}{3}$ quindi basta dire che questo α non è multiplo razionale di π. In altri termini, che, se $n \in \mathbb{N}$, $n\alpha$ non è multiplo intero di π.





Questo fatto si può esprimere, altresì, dicendo che $z^n \notin \mathbb{R}$ dove $z \overset{\text{def}}{=} \cos\alpha + i\cdot\sin\alpha \in \mathbb{C}$. Ora, $z = \frac{1}{3}(1+2i\sqrt{2})$. Si vede immediatamente, per induzione, che $(1+2i\sqrt{2})^n = x_n + y_n i\sqrt{2}$ per qualche $x_n, y_n \in \mathbb{Z}$. Inoltre, sempre per induzione, riducendo x_n e y_n modulo 3, otteniamo che, per n dispari $x_n \equiv 1\ (3)$ $y_n \equiv 2\ (3)$, per n pari e $\neq 0$ $x_n \equiv 2\ (3)$ $y_n \equiv 1\ (3)$. In nessun caso, in particolare $y_n = 0$. ∎