(24/12/19)

Numeri algebrici e non numerabilità di $\mathbb{R}$

Definizione *Un numero α si dice* **algebrico** *se è radice di un polinomio a coefficienti interi (cioè, se esiste un polinomio $x \to P(x)$ di grado $d \geq 1$ a coefficienti in $\mathbb{Z}$ tale che $P(\alpha) = 0$).*

Esempi: (i) Un numero razionale p/q ($p \in \mathbb{Z}$, $q \in \mathbb{N}$) è algebrico essendo radice del polinomio $P(x) = qx - p$.
(ii) Più in generale, r^s con $r, s \in \mathbb{Q}_+$ è algebrico: se $r = p/q$ e $s = n/m$, r^s è radice di $P(x) = q^n x^m - p^n$. In particolare, se p è primo e $n \geq 2$, $\sqrt[n]{p}$ è un irrazionale algebrico.
I numeri irrazionali non algebrici si dicono **trascendenti**.

Teorema 1 *I numeri algebrici sono numerabili.*

Nel corso della dimostrazione useremo il fatto che il numero di radici di un polinomio[1] non eccede il suo grado:

Lemma (i) *Se $x \to P(x)$ è un polinomio di grado $d \geq 1$, $\alpha \in \mathbb{R}$ e $P(\alpha) = 0$, allora $P(x) = (x - \alpha) \cdot Q(x)$ con Q polinomio di grado $d - 1$.*
(ii) *Sia P un polinomio di grado $d \geq 1$ e sia m il numero delle sue radici reali. Allora*[2] *$0 \leq m \leq d$.*
Dimostrazione
(i): Sia $\hat{P}(y) := P(\alpha + y)$: $\hat{P}$ è un polinomio di grado d in y; infatti se

$$P(x) = a_d x^d + a_{d-1} x^{d-1} + \cdots + a_0 \ ,$$

allora, $\hat{P}(y) = a_d y^d + \hat{a}_{d-1} y^{d-1} + \cdots + \hat{a}_0$ (ossia P e $\hat{P}$ hanno lo stesso coefficiente del grado massimo). Ora, $P(\alpha) = 0$ equivale a $\hat{P}(0) = 0$, ma questo significa che il termine noto di $\hat{P}$ è nullo ($\hat{a}_0 = 0$) e dunque possiamo fattorizzare y, ossia,

$$\hat{P}(y) = y \cdot \hat{Q}(y) \ , \qquad \hat{Q}(y) = a_d y^{d-1} + \cdots + \hat{a}_1 \ ,$$

e dunque (ponendo $x = y - \alpha$)

$$P(x) = \hat{P}(x - \alpha) = (x - \alpha)\hat{Q}(x - \alpha) =: (x - \alpha)Q(x)$$

con $Q(x) = a_d x^{d-1} + \cdots$.
(ii) Per induzione su d. Se $d = 1$, P ha una radice. Assumiamo l'asserto vero per $d - 1 \geq 1$ e dimostriamolo per d. Se P non ha nessuna radice reale, la tesi è vera. Se $m \geq 1$, sia α una radice di P. Dal punto (i) segue che $P(x) = (x-\alpha)Q(x)$ con Q di grado $d-1$, che, per ipotesi induttiva, ha al più $d - 1$ radici e quindi P ha al più d radici. ∎

Dimostrazione (del Teorema 1) Sia $\mathcal{P}_n$ la famiglia di tutti i polinomi di grado al più n con coefficienti, in modulo, minori uguali a n. La cardinalità di $\mathcal{P}_n$ è finita (infatti, è al più

[1] Se non specificato altrimenti, qui i polinomi si intendono a coefficienti in $\mathbb{R}$.
[2] Tutti i casi sono possibili: x^2+1 non ha nessuna radice reale ($m = 0$), mentre $(x-1)(x-2)\cdots(x-m)^{d+1-m}$ è un polinomio di grado d che ha esattamente $1 \leq m \leq d$ radici distinte (e cioè, $1, 2, ..., m$); ma se d è dispari, per il teorema di esistenza degli zeri per funzioni continue, $m \geq 1$ (perché?).

$(2n+1)^{n+1}$) e $\bigcup_{n\in\mathbb{N}} \mathcal{P}_n$ coincide con l'insieme dei polinomi a coefficienti in $\mathbb{Z}$. La tesi segue dunque dal fatto che l'unione numerabile di insiemi finiti è al più numerabile. ∎

Teorema 2. $\mathbb{R}$ *non è numerabile.*
Dimostrazione Dimostriamo un asserto equivalente, ossia, che[3] *l'intervallo* $[0,1]$ *non è numerabile.*

Supponiamo, per assurdo, che $I_0 := [0,1]$ sia numerabile, ossia, che $[0,1] = \{x_n \big| n \in \mathbb{N}\}$ con $x_n \neq x_m$ se $n \neq m$.
Dividiamo I_0 in tre parti uguali lunghe $1/3$, e poniamo $I_1 := [a_1, b_1] := [0, 1/3]$, se $x_1 \geq 1/2$, mentre, se $x_1 < 1/2$, poniamo $I_1 := [a_1, b_1] := [2/3, 1]$. Chiaramente[4],

$$0 =: a_0 \leq a_1 < a_1 + 1/3 = b_1 \leq b_0 := 1 \ , \quad \text{e} \quad d(x_1, I_1) \geq \frac{1}{6} \ .$$

Iteriamo: dato l'intervallo $I_{j-1} = [a_{j-1}, b_{j-1}] \subseteq [0,1]$, $(j \geq 1)$, lungo $1/3^{j-1}$ (ossia, $b_{j-1} = a_{j-1} + 1/3^{j-1}$), definiamo I_j come segue[5]:

$$I_j := \begin{cases} [a_j, b_j] := \left[a_{j-1}, a_{j-1} + \dfrac{1}{3^j}\right] \ , & \text{se } x_j \geq \dfrac{a_{j-1}+b_{j-1}}{2} \ , \\ [a_j, b_j] := \left[b_{j-1} - \dfrac{1}{3^j}, b_{j-1}\right] \ , & \text{se } x_j < \dfrac{a_{j-1}+b_{j-1}}{2} \ . \end{cases}$$

In tal modo abbiamo costruito una successione di intervalli $I_j \subseteq I_{j-1} \subseteq \cdots \subseteq I_0 = [0,1]$ tali che $x_k \notin I_j$, $\forall\ 1 \leq k \leq j$. Infatti, è immediato verificare che gli intervalli I_j verificano:

(i) $I_j = [a_j, b_j] \ , \quad \text{con} \quad 0 = a_0 \leq a_1 \leq \cdots \leq a_j < b_j := a_j + \dfrac{1}{3^j} \leq b_{j-1} \leq \cdots \leq b_0 = 1,$

(ii) $d(x_j, I_j) \geq \dfrac{1}{2 \cdot 3^{j+1}} \ .$

La successione $\{a_j\}$ è monotona crescente con maggiorante 1 e quindi ha limite $\alpha = \lim a_j \in [0,1]$. Ma $\alpha \neq x_n$ per ogni $n \in \mathbb{N}$: essendo $I_j \subseteq I_n$ per ogni $j \geq n$, si ha che $a_n \leq a_j \leq b_n$ per ogni $j \geq n$ e quindi $\alpha \in I_n$ e da (ii) segue che $d(x_n, I_n) \geq \frac{1}{2\cdot 3^{n+1}}$; dunque, $x_n \notin I_n$ e $\alpha \neq x_n$. Ma questo contraddice l'ipotesi che $[0,1] = \{x_n \big| n \in \mathbb{N}\}$. ∎

[3] Un sottoinsieme di un insieme numerabile è al più numerabile (e quindi se $[0,1]$ non è numerabile, non lo è neanche $\mathbb{R}$); viceversa se $[0,1]$ è numerabile lo sarebbe anche $\mathbb{R} = \bigcup_{j\in\mathbb{Z}} j + [0,1]$.

[4] Si ricorda che $d(x,A) := \inf_{y\in A} |x-y|$; $x \in A \implies d(x,A) = 0$, $d(x,A) > 0 \implies x \notin A$.

[5] Si noti che , $a_{j-1} + \dfrac{1}{3^j} < \dfrac{a_{j-1}+b_{j-1}}{2} = a_{j-1} + \dfrac{3}{2}\dfrac{1}{3^j} < b_{j-1} - \dfrac{1}{3^j} = a_{j-1} + \dfrac{2}{3^j}$.