Il teorema fondamentale dell'algebra

Il "teorema fondamentale dell'algebra" è molto più un teorema di analisi che di algebra, almeno nella dimostrazione che andiamo a darne.

Teorema. *Ogni polinomio complesso di grado maggiore o uguale a 1 possiede almeno una radice complessa.*

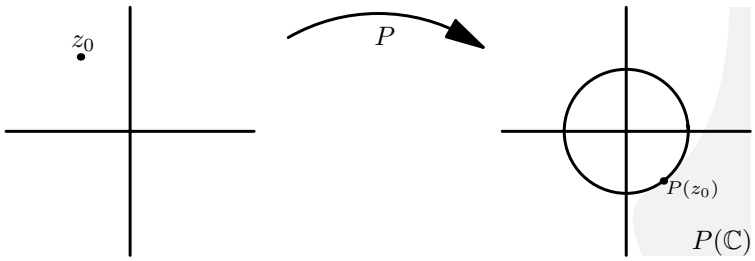
Dimostrazione. Sia $P\colon \mathbb{C} \to \mathbb{C}$ un polinomio complesso di grado $n \geq 1$:

$$P(z) := a_n z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0\,, \qquad a_n \in \mathbb{C} \setminus \{0\}\,, \quad a_i \in \mathbb{C} \quad \forall i < n\,.$$

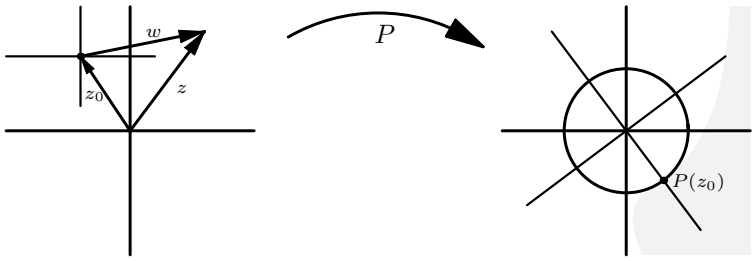
Dobbiamo dimostrare che esiste almeno un punto di $\mathbb{C}$ in cui P si annulla.
Cominciamo col notare che $|P(z)| \to \infty$ per $z \to \infty$. Infatti, raccogliendo il fattore z^n per $z \neq 0$ e ricordando che $a_i/z^{n-i} \to 0$ per $z \to \infty$ se $i < n$, possiamo scrivere:

$$|P(z)| = |z|^n \cdot \underbrace{\left| a_n + \frac{a_{n-1}}{z} + \ldots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n} \right|}_{\downarrow\ |a_n| \neq 0} \to +\infty \quad \text{per } z \to \infty\,.$$

Essendo $z \mapsto |P(z)|$ una funzione reale e continua su $\mathbb{C}$, per un corollario al teorema di Weierstrass essa ha un punto di minimo assoluto, che chiamiamo z_0. *Ci proponiamo di dimostrare che questo z_0 è una radice del polinomio. Procederemo per assurdo, supponendo che $P(z_0) \neq 0$.*
Poiché $|P(z)| \geq |P(z_0)|$ per ogni $z \in \mathbb{C}$, l'immagine $P(\mathbb{C})$ sta tutta al di fuori, o al massimo sul bordo, del cerchio di centro l'origine e raggio $|P(z_0)| > 0$:



Conviene cambiare coordinate in partenza e in arrivo: trasliamo l'origine in z_0 nel piano complesso di partenza, e facciamo una roto-omotetia (similitudine) nel piano di arrivo, in modo che l'origine rimanga invariata e il punto $P(z_0)$ vada nel punto 1, e il cerchio $\{z \in \mathbb{C} \,:\, |z| = |P(z_0)|\}$ diventi il cerchio unitario:



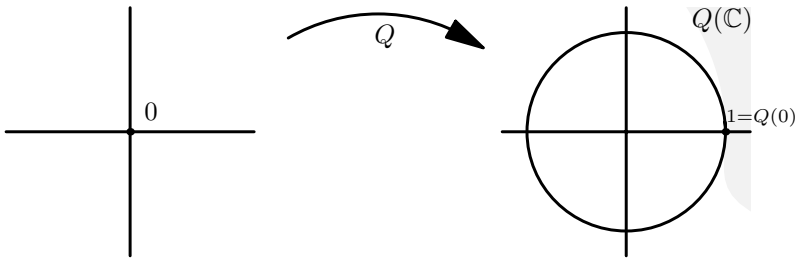
Nelle nuove coordinate il polinomio P diventa la funzione $Q\colon \mathbb{C} \to \mathbb{C}$ data dalla formula

$$Q(w) := \frac{P(z_0 + w)}{P(z_0)}\,,$$

(abbiamo usato una nuova variabile w al posto di z). Anche Q è un polinomio, e ha lo stesso grado di P. Si ha

$$Q(0) = 1 \quad \text{e} \quad |Q(w)| = \frac{|P(z_0 + w)|}{|P(z_0)|} \geq 1 \quad \text{per ogni } w \in \mathbb{C}\,.$$

In altre parole, l'immagine $Q(\mathbb{C})$ è esterna al cerchio unitario, e lo tocca nel punto $1 = Q(0)$



Scriviamo il polinomio Q come somma di monomi in ordine crescente di grado. P e Q hanno lo stesso grado, ma i coefficienti sono diversi: indichiamo con $c_0, c_1 \dots$ quelli di Q. Il termine noto di Q è $c_0 = Q(0) = 1$. Visto che Q ha grado $n \geq 1$, ci sono anche altri coefficienti non nulli oltre a quello noto: consideriamo quello di grado minimo, che sarà $c_m w^m$, dove $0 < m \leq n$ e $c_m \neq 0$. Isoliamo la somma dei primi due termini non nulli chiamandola $Q_0(w) := 1 + c_m w^m$, e indichiamo con $R(w)$ tutto il resto:

$$Q(w) = 1 + c_m w^m + c_{m+1} w^{m+1} + \ldots + c_n w^n = \underbrace{1 + c_m w^m}_{\equiv Q_0(w)} + \underbrace{c_{m+1} w^{m+1} + \ldots + c_n w^n}_{\equiv R(w)} .$$

(Eventualmente si ha $R(w) \equiv 0$ se $m = n$). La cosa da notare è che il resto è infinitesimo di ordine superiore a $Q_0(w)$ per $w \to 0$, perché somma finita di termini di termini di ordine superiore:

$$R(w) = o(w^m) \qquad \text{per } w \to 0 .$$

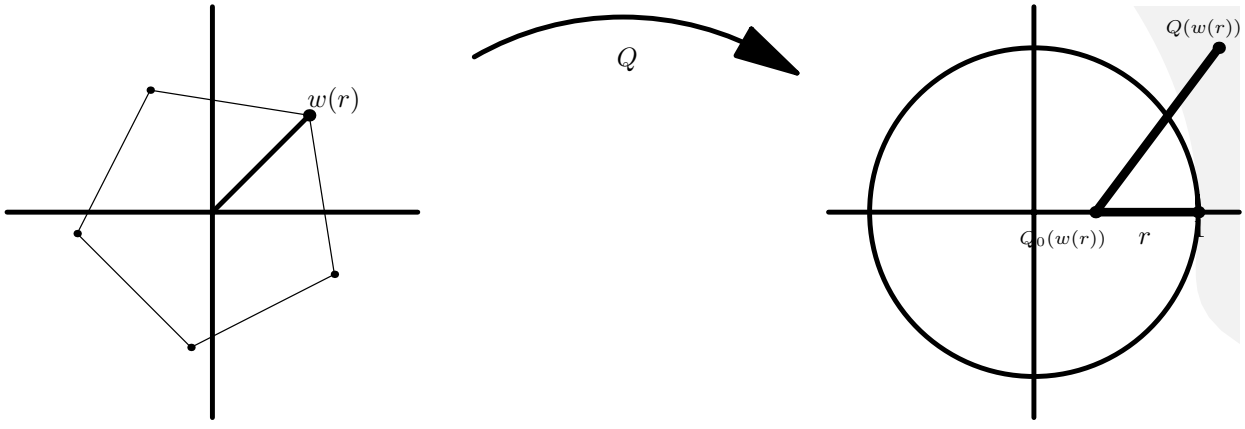
Prendiamo un punto sull'asse reale positivo del piano di arrivo, e che sia *interno* al cerchio unitario. Conviene indicare tale punto come $1 - r$, con $0 < r < 1$. *Questo punto appartiene all'immagine* $Q_0(\mathbb{C})$. Infatti l'equazione $Q_0(w) = 1 - r$ è risolubile elementarmente: (scrivendo in forma esponenziale $1 - r = 1 + re^{i\pi}$, $w = \rho e^{i\theta}$, $c_m = |c_m| e^{i\varphi}$):

$$\begin{aligned} Q_0(w) = 1 - r &\iff Q_0(\rho e^{i\theta}) = 1 + re^{i\pi} \iff 1 + c_m \rho^m e^{mi\theta} = 1 + re^{i\pi} \iff \\ &\iff 1 + |c_m| e^{i\varphi} \rho^m e^{mi\theta} = 1 + re^{i\pi} \iff \\ &\iff |c_m| \rho^m e^{i(\varphi + m\theta)} = re^{i\pi} \iff |c_m| \rho^m = r \quad \text{e } \exists k \in \mathbb{Z} : \quad \varphi + m\theta = \pi + 2k\pi \iff \\ &\iff \exists k \in \mathbb{Z} : \quad w = \sqrt[m]{\frac{r}{|c_m|}} \exp\Big(\frac{\pi + 2k\pi - \varphi}{m}\Big) . \end{aligned}$$

Ci sono m soluzioni dell'equazione $Q_0(w) = 1 - r$, disposte ai vertici di un poligono regolare di m lati centrato nell'origine. Indichiamo con $w(r)$ una di queste, per esempio quella con $k = 0$. Da tenere presente è la dipendenza di $w(r)$ da r:

$$w(r) := \sqrt[m]{\frac{r}{|c_m|}} \exp\Big(\frac{\pi - \varphi}{m}\Big) = \text{costante} \cdot \sqrt[m]{r} .$$

Se Q_0 non coincide con Q, $Q(w(r))$ non è necessariamente uguale a $1 - r$ e nulla vieta che sia esterno al cerchio unitario, come dovrebbe fare, visto che appartiene a $Q(\mathbb{C})$:

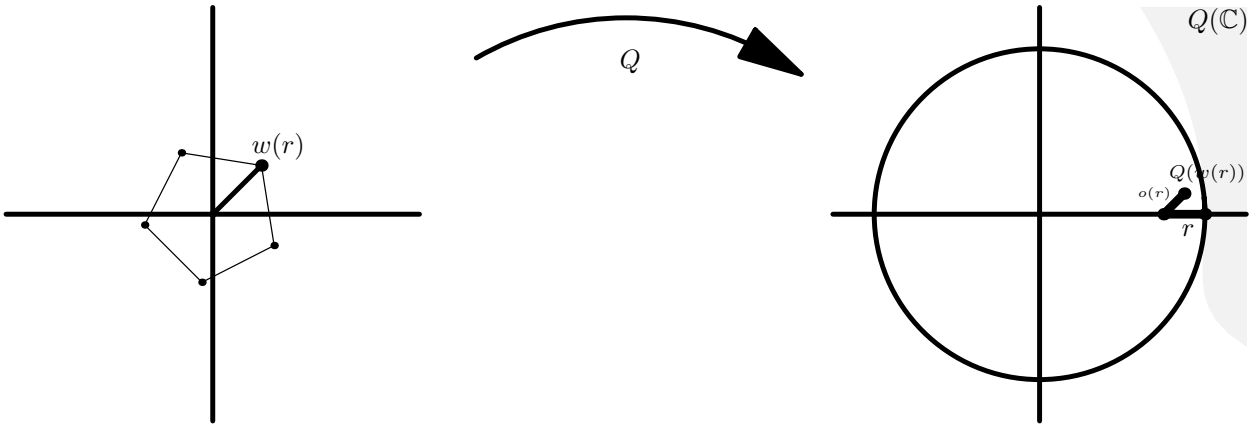


Però $Q(w(r))$ *deve essere dentro al cerchio unitario quando* r *è sufficientemente piccolo.* Infatti la distanza fra i punti $Q(w(r))$ e $1-r = Q_0(w(r))$ è un infinitesimo di ordine superiore a r quando $r \to 0^+$:

$$Q\big(w(r)\big) - Q_0\big(w(r)\big) = R\big(w(r)\big) = o\big(w(r)^m\big) = o\big((\sqrt[m]{r})^m\big) = o(r) \quad \text{per } r \to 0^+ .$$

e perciò

$$\begin{aligned}\big|Q(w(r))\big| &= \big|Q(w(r)) - Q_0(w(r)) + Q_0(w(r))\big| \le \big|Q(w(r)) - Q_0(w(r))\big| + \big|Q_0(w(r))\big| = \\ &= o(r) + (1-r) = 1 - r + o(r) = 1 - r \cdot \underbrace{\big(1 - o(1)\big)}_{>0} < 1 \qquad \text{se } r > 0 \text{ è abbastanza piccolo.}\end{aligned}$$



Questo mostra che $Q(\mathbb{C})$ ha anche dei punti *interni* al cerchio unitario, in contraddizione con quanto avevamo dedotto, per altre vie, dall'ipotesi che P non avesse radici. □

Esercizio. Tutti i polinomi $\mathbb{C} \to \mathbb{C}$ di grado ≥ 1 sono suriettivi.

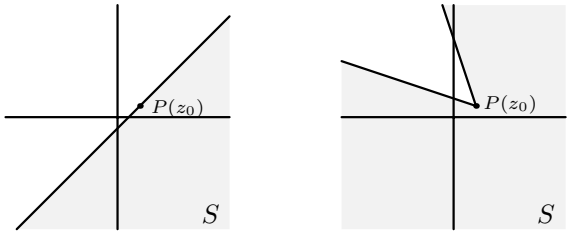
Esercizio. Dimostrare che se $z \mapsto P(z)$ è un polinomio su $\mathbb{C}$, $z_0 \in \mathbb{C}$ e $c \in \mathbb{C} \setminus \{0\}$, allora anche $w \mapsto P(z_0 + w)/c$ è un polinomio, dello stesso grado di P.

Esercizio. Nella dimostrazione del teorema fondamentale dell'algebra, esiste una costante $M \ge 0$ tale che $|w| \le 1 \Rightarrow |R(w)| \le M|w|^{m+1}$.

***Esercizio.** Sia $P\colon \mathbb{C} \to \mathbb{C}$ un polinomio complesso ed $r > 0$ tale che $|z| = r \Rightarrow |P(z)| > |P(0)|$. Dimostrare che P ha una radice z_0 di modulo minore di r. (Avvio: applicare Weierstraß al disco $\{z \in \mathbb{C} : |z| \le r\}$, che è chiuso e limitato in $\mathbb{C}$, e poi confluire nella dimostrazione del teorema fondamentale).

Esercizio. Se P è un polinomio complesso di grado ≥ 1, la funzione $z \mapsto |P(z)|$ non può avere punti z_0 di minimo locale in cui $P(z_0) \ne 0$. E punti di massimo locale? Le conclusioni rimangono vere per polinomi reali?

***Esercizio.** Sia P un polinomio complesso di grado ≥ 1, sia $z_0 \in \mathbb{C}$ e sia S un semipiano di $\mathbb{C}$ contenente $P(z_0)$ sul bordo. Dimostrare che per ogni $\varepsilon > 0$ l'immagine del disco di centro z_0 e raggio r non è sottinsieme di S. Generalizzare al caso in cui S è un angolo di ampiezza $< 2\pi$ e avente $P(z_0)$ come vertice. (Avvio: parte della dimostrazione del teorema fondamentale dell'algebra corrisponde al caso in cui S è l'esterno di un disco avente $P(z_0)$ sul bordo).



Esercizio. Se prendiamo un polinomio *reale* $P\colon \mathbb{R} \to \mathbb{R}$ e andiamo alla ricerca di sue radici reali, i passaggi della dimostrazione del teorema fondamentale dell'algebra si possono ripetere pari pari, o quasi, cambiando tutte le volte $\mathbb{C}$ in $\mathbb{R}$? E se abbiamo un polinomio *razionale* $\mathbb{Q} \to \mathbb{Q}$?