

Alcune informazioni importanti sui polinomi

1. Radici e molteplicità

Sia \mathbb{K} un campo. Denotiamo con 1 e 0 rispettivamente l'unità moltiplicativa e l'elemento neutro additivo del campo \mathbb{K} .

Consideriamo l'insieme $\mathbb{K}[\lambda]$ dei polinomi a coefficienti in \mathbb{K} . Con le usuali operazioni di somma e prodotto l'insieme $\mathbb{K}[\lambda]$ ha una struttura di anello commutativo unitario, con unità il polinomio $1 \equiv 1\lambda^0 + 0\lambda^1 + 0\lambda^2 + \dots$ ed elemento neutro additivo il polinomio nullo $0 \equiv 0\lambda^0 + 0\lambda^1 + 0\lambda^2 + \dots$.

Un elemento $\lambda_0 \in \mathbb{K}$ è una radice di un polinomio $P(\lambda)$ se $P(\lambda_0) = 0$. Vale la seguente importante

Proposizione 1. $\lambda_0 \in \mathbb{K}$ è una radice di $P(\lambda)$ se e solo se esiste $Q(\lambda) \in \mathbb{K}[\lambda]$ tale che

$$P(\lambda) = (\lambda - \lambda_0)Q(\lambda).$$

Dimostrazione. Se esiste $Q(\lambda) \in \mathbb{K}[\lambda]$ tale che $P(\lambda) = (\lambda - \lambda_0)Q(\lambda)$ allora è ovvio che $P(\lambda_0) = 0$ e che λ_0 è quindi una radice. Vediamo il viceversa. Supponiamo quindi che λ_0 sia una radice di $P(\lambda)$ e facciamo vedere che esiste $Q(\lambda) \in \mathbb{K}[\lambda]$ tale che $P(\lambda) = (\lambda - \lambda_0)Q(\lambda)$. Se $\lambda_0 = 0$ allora $P(0) = 0$ e quindi $P(\lambda)$ non ha termine noto. Si ha quindi

$$P(\lambda) = a_n\lambda^n + a_{n-1}\lambda^{n-1} + \dots + a_2\lambda^2 + a_1\lambda = \lambda(a_n\lambda^{n-1} + a_{n-1}\lambda^{n-2} + \dots + a_2\lambda + a_1)$$

e quindi la tesi con $Q(\lambda) = a_n\lambda^{n-1} + a_{n-1}\lambda^{n-2} + \dots + a_2\lambda + a_1$. Passiamo al caso generale. Fissiamo un qualsiasi $\alpha \in \mathbb{K}$; possiamo scrivere $P(\lambda) = P((\lambda - \alpha) + \alpha)$; sostituiamo $(\lambda - \alpha) + \alpha$ nell'espressione di P e sviluppiamo le potenze di tutti i binomi. Otteniamo un nuovo polinomio $R(\mu)$ tale che $P((\lambda - \alpha) + \alpha) = R(\lambda - \alpha)$. Notiamo che $R(0) = P(\alpha)$.¹ Scegliamo in particolare $\alpha = \lambda_0$; per costruzione abbiamo che $R(0) = P(\lambda_0) = 0$, perché λ_0 è una radice di P . Ma allora, per il caso precedente, esiste un polinomio S tale che $R(\mu) = \mu S(\mu)$ e quindi

$$R(\lambda - \lambda_0) = (\lambda - \lambda_0)S(\lambda - \lambda_0)$$

A sinistra, per definizione, abbiamo $P(\lambda)$. Inoltre, ragionando come sopra, capiamo che $S(\lambda - \lambda_0) = Q(\lambda)$ per un qualche polinomio $Q(\lambda)$. Riassumendo: $P(\lambda) = (\lambda - \lambda_0)Q(\lambda)$ che è quello che dovevamo dimostrare.

Ovviamente può accadere che λ_0 sia anche una radice di $Q(\lambda)$ e quindi esiste un polinomio $G(\lambda)$ tale che $Q(\lambda) = (\lambda - \lambda_0)G(\lambda)$. Otteniamo allora

$$P(\lambda) = (\lambda - \lambda_0)^2 G(\lambda).$$

Procedendo induttivamente possiamo dare la seguente

Definizione 1. Sia $\lambda_0 \in \mathbb{K}$ una radice di $P(\lambda)$. Allora λ_0 ha molteplicità h come radice di $P(\lambda)$ se esiste $F(\lambda) \in \mathbb{K}[\lambda]$ tale che $F(\lambda_0) \neq 0$ e

$$P(\lambda) = (\lambda - \lambda_0)^h F(\lambda).$$

¹Vediamo un esempio: sia $P(\lambda) = 3\lambda^2 + 2\lambda - 4$ e sia $\alpha = 1$; sostituiamo al posto di λ il binomio $(\lambda - 1) + 1$ e sviluppiamo $3((\lambda - 1) + 1)^2 + 2((\lambda - 1) + 1) - 4$ ottenendo $3(\lambda - 1)^2 + 8(\lambda - 1) + 1$ che è il polinomio $R(\mu) = 3\mu^2 + 8\mu + 1$ calcolato in $(\lambda - 1)$; si ha $R(0) = 1$; notiamo che $P(1)$ è anche uguale a 1, come enunciato.

Diamo un classico corollario della Proposizione 1:

Proposizione 2. Se $P \in \mathbb{K}[\lambda]$ non è il polinomio nullo ed ha grado n , allora P ammette al più n radici in \mathbb{K} , contate con la loro molteplicità.

Dimostrazione. Procediamo per induzione sul grado n . Se $n = 1$ allora P ammette precisamente una radice oppure non ha radici, e quindi la proposizione è vera.² Supponiamo ora vera la Proposizione per polinomi di grado $n-1$ e dimostriamola per polinomi di grado n . Se P non ammette radici, abbiamo finito. Altrimenti P ammette una radice $\lambda_0 \in \mathbb{K}$. Ma allora per la Proposizione 1 esiste un polinomio $Q(\lambda)$, necessariamente di grado $n-1$, tale che

$$P(\lambda) = (\lambda - \lambda_0)Q(\lambda)$$

Per ipotesi induttiva $Q(\lambda)$ ha al più $n-1$ radici. Ne segue la tesi.

2. Polinomi reali e complessi

Sia $P(\lambda)$ un polinomio di grado n : $P(\lambda) = a_n\lambda^n + \dots + a_1\lambda + a_0$. Possiamo supporre senza perdita di generalità per quanto segue che $a_n = 1$. Si dice che il polinomio è *monico*. Vi invito a ripassare autonomamente quello che abbiamo visto sul campo dei numeri complessi e ad aggiungere la nozione di *coniugio*³. In particolare, il coniugato di $z = a + ib$, $a, b \in \mathbb{R}$ è per definizione $\overline{a + ib} := a - ib$; si ha

$$\overline{\overline{z}} = z, \quad \overline{z + w} = \overline{z} + \overline{w}, \quad \overline{zw} = \overline{z}\overline{w}$$

come si verifica immediatamente. Inoltre,

$$|z|^2 \equiv |a + ib|^2 := a^2 + b^2 = (a + ib) \cdot \overline{(a + ib)} \equiv z\overline{z};$$

$$z \neq 0 \Rightarrow z^{-1} = \overline{z}/|z|^2.$$

Infine,

$$z \in \mathbb{R} \text{ se e solo se } z = \overline{z}.$$

Notiamo anche che $z + \overline{z} = 2a \in \mathbb{R}$.

Teorema fondamentale dell'algebra. *Sia $P(\lambda)$ un polinomio monico a coefficienti complessi; esistono n numeri complessi $\lambda_1, \dots, \lambda_n$ tali che*

$$P(\lambda) = (\lambda - \lambda_1) \cdots (\lambda - \lambda_n).$$

Questi numeri $\lambda_j \in \mathbb{C}$ sono quindi le radici di $P(\lambda)$ e cioè sono tutte e sole le soluzioni dell'equazione $P(\lambda) = 0$. Le radici di un polinomio complesso di grado n sono quindi in numero di n . Fra questi λ_j alcuni saranno coincidenti. Siano $\{\lambda_1, \dots, \lambda_k\}$ le radici distinte; allora

$$P(\lambda) = (\lambda - \lambda_1)^{h(\lambda_1)} \cdots (\lambda - \lambda_k)^{h(\lambda_k)}.$$

È ovvio che il numero intero $h(\lambda_j)$ è la molteplicità di λ_j come radice del polinomio $P(\lambda)$. Il Teorema fondamentale dell'algebra viene anche enunciato come segue: *ogni polinomio complesso di grado n ammette n radici contate con la loro molteplicità.*

²infatti, essendo di grado 1, P si scrive come $P(\lambda) = \alpha\lambda + \beta$ con $\alpha, \beta \in \mathbb{K}$ non entrambi nulli. Se $\alpha = 0$ e $\beta \neq 0$ allora P non ha radici, perché l'equazione $0\lambda + \beta = 0$ non ha soluzioni. Se $\beta = 0$ e $\alpha \neq 0$ allora P ha la radice $\lambda_0 = 0$. Se $\alpha \neq 0$ e $\beta \neq 0$ allora P ha la radice $\lambda_0 = -\beta/\alpha$.

³quindi Proposizione 4.19 in [A-dF] e poi quello che segue fino alla fine della Sezione 4.6; richiamo comunque qui le nozioni fondamentali sul coniugio

Supponiamo ora che $P(\lambda)$ sia un polinomio *reale*; questo vuol dire che i coefficienti a_j sono numeri reali. Se consideriamo $P(\lambda)$ come polinomio a coefficienti complessi (cosa lecita dato che $\mathbb{R} \subset \mathbb{C}$) allora possiamo applicare quanto appena visto e concludere che esistono n numeri complessi $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ tali che

$$P(\lambda) = (\lambda - \lambda_1) \cdots (\lambda - \lambda_n).$$

Dato che il polinomio ha i coefficienti reali si ha che se $\mu \in \mathbb{C}$ è una radice complessa di $P(\lambda)$ allora anche $\bar{\mu} \in \mathbb{C}$ è una radice complessa di $P(\lambda)$.⁴ Quindi le radici di $P(\lambda)$ sono reali oppure complesse-coniugate (non-reali). Siano

$$c_1 = \lambda_1, \quad \bar{c}_1 = \lambda_2, \dots, \quad c_k = \lambda_{2k-1}, \quad \bar{c}_k = \lambda_{2k}, \quad 0 \leq 2k \leq n$$

le radici complesse coniugate, e siano

$$r_1 = \lambda_{2k+1}, \dots, r_{n-2k} = \lambda_n$$

le radici reali. Allora

$$P(\lambda) = (\lambda - c_1) \cdot (\lambda - \bar{c}_1) \cdots (\lambda - c_k) \cdot (\lambda - \bar{c}_k) \cdot (\lambda - r_1) \cdots (\lambda - r_{n-2k}).$$

Quindi

$$P(\lambda) = (\lambda^2 - (c_1 + \bar{c}_1)\lambda + |c_1|^2) \cdots (\lambda^2 - (c_k + \bar{c}_k)\lambda + |c_k|^2) \cdot (\lambda - r_1) \cdots (\lambda - r_{n-2k}).$$

In parole: ogni polinomio reale si decompone nel prodotto di polinomi *reali* di secondo grado⁵ che non ammettono radici reali e di polinomi reali di primo grado (che quindi ammettono un'unica radice reale). Se $k = 0$ le radici sono tutte reali; in altre parole, in questo caso il polinomio reale ha tutte le sue radici nel campo \mathbb{R} ; notiamo che $P(\lambda)$ ha tutte le sue radici in \mathbb{R} se e solo se *la somma delle molteplicità delle sue radici reali è proprio n* . Notiamo anche che se $2k < n$ allora esiste almeno una radice reale.

È importante notare che se $n = 2m + 1$ allora, ovviamente, $2k < 2m + 1 \equiv n$; quindi un polinomio reale di grado *dispari* ammette sempre (almeno) una radice reale.⁶

Sia ora V uno spazio vettoriale **reale** di dimensione n . Sia $F : V \rightarrow V$ lineare e sia $P_F(\lambda)$ il polinomio caratteristico di F ; $P_F(\lambda)$ è un polinomio a coefficienti reali di grado n e le sue radici **reali** sono tutti e soli gli autovalori di F . La molteplicità algebrica di un autovalore è la sua molteplicità in quanto radice del polinomio caratteristico. Diciamo che F ammette tutti gli autovalori in \mathbb{R} se $k = 0$; in tal caso possiamo scrivere

$$P_F(\lambda) = (r_1 - \lambda)(r_2 - \lambda) \cdots (r_n - \lambda), \quad \text{con } r_j \in \mathbb{R}.$$

(Ritroviamo in questo modo la definizione di [A-dF]. Notare che scriviamo i fattori come $(r_j - \lambda)$, e non come $(\lambda - r_j)$, perché se T è diagonalizzabile allora questa è precisamente l'espressione di $P_T(\lambda)$.)

Notiamo che se $\dim V = 2m + 1$ allora F ammette autovettori (perché esiste almeno un autovalore).

⁴Infatti: $P(\mu) = 0 \Rightarrow a_n \mu^n + \cdots + a_1 \mu + a_0 = 0 \Rightarrow \overline{a_n \mu^n + \cdots + a_1 \mu + a_0} = 0 \Rightarrow a_n \bar{\mu}^n + \cdots + a_1 \bar{\mu} + a_0 = 0$ (perché $a_j \in \mathbb{R}$) $\Rightarrow P(\bar{\mu}) = 0$.

⁵Perché $c_j \bar{c}_j = |c_j|^2 \in \mathbb{R}$ e $(c_j + \bar{c}_j) \in \mathbb{R}$

⁶Intuitivamente: le radici complesse non reali vengono in coppie complesse-coniugate e se il grado del polinomio è dispari allora rimane qualche radice "spaiata" che deve essere necessariamente reale.