NUMERI COMPLESSI E POLINOMI

CARLANGELO LIVERANI

1. Perchè i numeri complessi

Sappiamo tutti (?) cosa sono i numeri reali ($\mathbb{R}$) ma che sono i numeri complessi ($\mathbb{C}$) e a che servono? Non potevamo vivere felicemente anche senza numeri complessi?

Si consideri l'equazione $x^2+1=0$. Se si agisce meccanicamente si sarebbe tentati di scrivere che la soluzione è $x=\pm\sqrt{-1}$. Peccato che non abbia alcun senso. Tuttavia se avesse senso si avrebbe, ad esempio,

$$x^4=(\sqrt{-1})^2(\sqrt{-1})^2=(-1)^2=1.$$

D'altro canto

$$0=(x^2+1)^2=x^4+2x^2+1=x^4-1+2(x^2+1)=x^4-1.$$

Abbiamo calcolato formalmente una quantità in due modi diversi e abbiamo ottenuto lo stesso risultato. Un risultato che però lascia perplessi visto che la soluzione di $x^4=1$ è ±1 e non $\sqrt{-1}$, che non si sa che sia.

Tuttavia queste considerazioni producono inevitabilmente almeno due dubbi

(1) Non è che per caso si possa veramente fare finta che $\sqrt{-1}$ sia un numero?
(2) Siamo veramente sicuri di capire tutto sulle radici dei polinomi?

2. Dubbio uno

Che significa *fare finta che* $\sqrt{-1}$ *sia un numero*? essenzialmente vuole dire che si comporta come tale, ovvero si possono fare tutte le operazioni che si fanno coi numeri: somme, moltiplicazioni e relative operazioni inverse.

Cominciamo con la moltiplicazione per un numero reale. Sia $a\in\mathbb{R}$, Se moltiplichiamo $x^2+1=0$ per a^2 otteniamo $(ax)^2=-a^2$. D'altro canto $(a\sqrt{-1})^2=-a^2$, quindi sembra che non ci sia alcun problema. Cosa succede se sommiamo a a $b\sqrt{-1}$. Questo non è chiaro, la cosa più naturale sembra decidere che abbiamo il nuovo oggetto $a+b\sqrt{-1}$.

Siamo perciò portati a considerare oggetti del tipo $a+b\sqrt{-1}$ con $a,b\in\mathbb{R}$. Se li volgiamo considerare numeri dobbiamo dire come si sommano e si moltiplicano. Se deve valere la proprietà associativa e distributiva allora, per ogni $a,b,c,d\in\mathbb{R}$,

$$\begin{aligned}(a+b\sqrt{-1})+(c+d\sqrt{-1})&=(a+c)+(b+d)\sqrt{-1}\\(a+b\sqrt{-1})(c+d\sqrt{-1})&=ac+bd(\sqrt{-1})^2+(ad+bc)\sqrt{-1}\\&=(ac-bd)+(ad+bc)\sqrt{-1}.\end{aligned}\tag{2.1}$$

Questo è interessante: sembra si possano definire somme e moltiplicazioni che producono lo stesso tipo di oggetti.

Date: March 12, 2019.

Se ci pensate un poco e fate uno sforzo di astrazione, vi rendete conto che questi oggetti sono null'altro che una coppia di numeri reali (a, b) che definiscono l'oggetto $a + b\sqrt{-1}$, qualunque cosa esso sia.

A questo punto occorre una idea, una vera astrazione: dimentichiamoci di tutte le nostre considerazioni e consideriamo (2.1) in sè: cosa ci dice? È semplicemente la definizione di due operazioni binarie su $\mathbb{R}^2$.[1] Chiamiamo la prima *csomma*, e indichiamola con $\boxplus$, e la seconda *cmoltiplicazione*, e indichiamola con $\boxdot$, così definite

$$(a, b) \boxplus (c, d) = (a + c, b + d)$$
$$(a, b) \boxdot (c, d) = (ac - bd, ad + bc).$$

Problem 2.1. *Si mostri che per ogni* $x, y, z \in \mathbb{R}^2$

$$x \boxplus (y \boxplus z) = (x \boxplus y) \boxplus z \; ; \;\; e \quad\; x \boxdot (y \boxdot z) = (x \boxdot y) \boxdot z$$
$$x \boxplus y = y \boxplus x \; ; \;\; e \quad\; x \boxdot y = y \boxdot x$$
$$x \boxplus (0, 0) = x \; ; \;\; e \quad\; x \boxdot (1, 0) = x$$
$$x \boxdot (y \boxplus z) = (x \boxdot y) \boxplus (x \boxdot z)$$

Se ci pensate un poco vedete che il problema precedente non fa altro che verificare, per queste nuove operazioni, le proprietà: associativa, commutativa, esistenza dell'elemento neutro e distributiva. Inoltre dato $(a, b) \in \mathbb{R}^2$ si ha

$$(a, b) \boxplus (0, 0) = (a, b)$$
$$(a, b) \boxdot (1, 0) = (a, b)$$
$$(a, b) \boxplus (-a, -b) = (a - a, b - b) = (0, 0)$$
$$(a, b) \boxdot \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right) = (1, 0).$$

Cioè, le operazioni hanno un elemento neutro, ogni elemento ha un inverso rispetto a $\boxplus$ e ogni elemento diverso da $(0, 0)$ ha un inverso rispetto a $\boxdot$.

In altre parole $\boxplus$ e $\boxdot$ hanno esattamente le stesse proprietà della somma e moltiplicazione tra numeri reali.

D'altro canto per ogni $a, b \in \mathbb{R}$ si ha

$$(a, 0) \boxplus (b, 0) = (a + b, 0)$$
$$(a, 0) \boxdot (b, 0) = (a \cdot b, 0).$$

Il che significa che l'algebra dei numeri reali che conosciamo dalle medie è contenuta in questa nuova algebra come caso particolare. Per di più se $a, b, c \in \mathbb{R}$ si ha

$$(a, 0) \boxdot (c, d) = (a \cdot c, a \cdot d).$$

Se riflettete un poco su quanto detto vi renderete conto che tanto vale chiamare $\boxplus$ e $\boxdot$ coi nomi già noti di $+$ e $\cdot$. Inoltre, è più comodo scrivere $a\mathbb{1} + ib$ che (a, b), dove $\mathbb{1}$ sta per $(1, 0)$ e i sta per $(0, 1)$. Di più, si può tranquillamente non scrivere $\mathbb{1}$ senza che questo crei alcuna confusione. Infine si noti che

$$i^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1$$

ovvero i si comporta come vorremmo che si comporti $\sqrt{-1}$, solo che ora sappiamo esattamente di cosa stiamo parlando.

[1] Ovvero di due funzioni da $\mathbb{R}^2 \times \mathbb{R}^2 \to \mathbb{R}^2$.

Abbiamo quindi visto che si può dare un senso preciso all'idea che $\sqrt{-1}$ è un numero e che si possono fare con tali numeri operazioni del tutto simili a quelle che si fanno coi numeri reali. Infatti si possono tranquillamente identificare i reali con gli elementi $(a, 0)$.

Inoltre abbiamo visto che questi nuovi oggetti si possono interpretare come punti del piano.

C'è un oggetto naturale e utilissimo per i numeri reali che non abbiamo definito per i numeri complessi: il valore assoluto. Non è a priori ovvio cosa sia la definizione naturale, tuttavia se pensiamo al valore assoluto di un numero come alla sua distanza da zero (ovvero $|x| = \sqrt{x^2}$), allora sembra ragionevole definire

$$|a + ib| = \sqrt{a^2 + b^2}.$$

Problem 2.2. *Si mostri che, per ogni $z, w \in \mathbb{C}$,*

$$|z| = 0 \iff z = 0$$
$$|z + w| \leq |z| + |w|$$
$$|zw| = |z||w|$$

Dunque $|\cdot|$ si comporta esattamente come il valore assoluto e si chiama *modulo* del numero complesso. Ovviamente il modulo di un numero reale è esattamente il valore assoluto del numero.

A questo punto viene naturale domandarsi quali funzioni si possono costruire da $\mathbb{C} \to \mathbb{C}$. Una ovvia possibilità sono i polinomi: per ogni $z \in \mathbb{C}$ si può definire, per esempio,

$$p(z) = \sum_{i=0}^{n} a_n z^i$$

dove $a_i \in \mathbb{C}$. Se volgiamo andare oltre i polinomi il primo candidato interessante è l'esponenziale. È quindi naturale definire

$$e^z = \sum_{k=0}^{\infty} \frac{z^n}{n!}.$$

Si noti che

$$\left| \sum_{k=0}^{\infty} \frac{z^n}{n!} \right| \leq \sum_{k=0}^{\infty} \frac{|z|^n}{n!}$$

e dunque è una serie assolutamente convergente, quindi ben definita.

Problem 2.3. *Si mostri che, per ogni $z, w \in \mathbb{C}$,*

$$e^{z+w} = e^z e^w.$$

Problem 2.4. *Si mostri che, per ogni $\theta \in \mathbb{R}$,*

$$e^{i\theta} = \cos\theta + i \sin\theta.$$

Questo è piuttosto interessante, significa che per ogni $a + ib \in \mathbb{C}$, possiamo scrivere $a + ib = \rho(\cos\theta + i\sin\theta)$ usando le coordiante polari, dove, chiaramente, $\rho^2 = |a + ib|$. Quindi, ponendo $\alpha = \ln\rho$ si ha

$$a + ib = e^{\alpha + i\theta} = e^\alpha e^{i\theta} = \rho(\cos\theta + i\sin\theta).$$

In altre parole tutti i numeri, meno 0, si possono scrive come un esponenziale.

3. Dubbio due

A questo punto domandiamoci cosa questa estensione dei numeri implica per le radici (gli zeri) di un polinomio. Cominciamo dal nostro esempio iniziale: $z^2+1=0$, ma ora consideriamo il problema con $z \in \mathbb{C}$. Poichè

$$1 = |z^2| = |z|^2$$

deve essere $|z| = 1$. Possiamo quindi scrivere $z = e^{i\theta}$. Quindi l'equazione diventa $e^{2i\theta} = -1$, ovvero $2\theta = (2k+1)\pi$ per $k \in \mathbb{Z}$. Abbiamo quindi le soluzioni $z = e^{i(k+1/2)\pi}$, ovvero $z = \pm i$. Questo rende finalmente preciso in che senso l'equazione $x^2 + 1 = 0$ ha due soluzioni.

Problem 3.1. *Si mostri che le soluzioni dell'equazione $z^4 = 1$ sono $\{\pm 1, \pm i\}$.*

Finalmente tutto torna ed è consistente.

A questo punto viene naturale domandarsi: ma un polinomio complesso di grado n quanti zeri può avere? La risposta è data dal *Teorema fondamentale dell'algebra*:

Theorem 3.2. *Un polinomio complesso di grado n ha esattamente n zeri contanti con molteplicità.*

Proof. Il primo passo nella dimostrazione è mostrare che, in contrasto con quello che succede per i reali, tutti i polinomi complessi hanno almeno uno zero.

Sia $p_n(z) = \sum_{k=0}^n a_k z^k$ con $a_k \in \mathbb{C}$ e $a_n \neq 0$. Prima di tutto notiamo che, per ogni $r > 1$,

$$|p_n(re^{i\theta})| \geq |a_n| r^n - \sum_{k=0}^{n-1} |a_k| r^k = r^n \left(|a_n| - \sum_{k=0}^{n-1} |a_k| r^{-1} \right) \geq \frac{|a_n|}{2} r^n$$

a patto che r sia più grande di un qualche $r_* > 1$ sufficientemente grande.

Ora scegliamo $r_0 \geq r_*$ tale che $\frac{|a_n|}{2} r_0^n > |p_n(0)|$. Ne segue che il minimo di $|p(z)|$ nel disco $D = \{z \in \mathbb{C} \,:\, |z| \leq r_0\}$ deve essere nell'interno del disco e che $p(z)$ non si può annullare all'esterno di D. Sia $z_0 \in \mathring{D}$ un punto dove $|p_n|$ attiene il minimo, volgiamo dimostrare che $p(z_0) = 0$. Ragioneremo per assurdo: supponiamo che $p(z_0) \neq 0$.

Allora conviene scrivere

$$\begin{aligned} p_n(z) &= \sum_{k=0}^n a_k (z - z_0 + z_0)^k = \sum_{k=0}^n a_k \sum_{j=0}^k \binom{k}{j} (z-z_0)^j z_0^{k-j} \\ &= \sum_{j=0}^n \left[\sum_{k=j}^n \binom{k}{j} a_k z_0^{k-j} \right] (z-z_0)^j =: \sum_{j=0}^n b_j (z-z_0)^j \end{aligned}$$

dove abbiamo usato il binomio di Newton. Studiamo ora il valore di $|p_n(z)|$ in un piccolo intorno do z_0. Si noti che, per ipotesi, $b_0 \neq 0$. Per semplictà consideriamo il caso in cui $b_1 \neq 0$, il caso generale è simile ed è lasciato al lettore come esercizio che gli permetterà di verificare se ha compreso l'argomento.

Sia $r > 0$ sufficientemente piccolo, allora esiste $M > 0$ tale che

$$|p_n(z_0 + re^{i\theta})| = \left| \sum_{j=0}^n b_j r^j e^{ij\theta} \right| \leq |b_0 + b_1 re^{i\theta}| + Mr^2.$$

Per continuare è conveniente scrivere $b_l = \rho_l e^{i\alpha_l}$. Allora

$$|p_n(z_0 + re^{i\theta})| \leq |e^{i\alpha_0}(\rho_0 + r\rho_1 e^{i(\alpha_1 - \alpha_0 + \theta)})| + Mr^2 = |\rho_0 + \rho_1 re^{i(\alpha_1 - \alpha_0 + \theta)}| + Mr^2.$$

Ora possiamo scegliere $\theta = \alpha_0 - \alpha_1 + \pi$, quindi, per r sufficientemente piccolo,

$$|p_n(z_0 + re^{i\theta})| \leq |\rho_0 - r\rho_1| + Mr^2 < |\rho_0| = |p_n(z_0)| = |b_0|$$

che è una contraddizione. Segue quindi che deve essere $b_0 = 0$ e perciò

$$p_n(z) = \sum_{j=1}^{n} b_j (z - z_0)^j = (z - z_0) \sum_{j=0}^{n-1} b_{j+1}(z - z_0)^j =: (z - z_0) p_{n-1}(z).$$

Abbiamo quindi concluso la dimostrazione che i polinomi complessi hanno sempre almeno uno zero. Applicando questo fatto a p_{n-1} possiamo scrivere

$$p_n(z) = (z - z_0)(z - z_1) p_{n-2}(z).$$

Per induzione segue che esistono $\{z_i\}_{i=0}^{n-1}$, non necessariamente distinti, tali che

$$p_n(z) = \prod_{i=0}^{n-1} (z - z_i)$$

che dimostra il teorema. □

4. E i polinomi reali allora?

Consideriamo il polinomio

$$p_n(x) = \sum_{k=0}^{n} a_k x^k$$

dove $a_k, x \in \mathbb{R}$. Possiamo dire qualcosa su come lo si può fattorizzare?

L'idea è di considerare il polinomio sui complessi $p_n(z)$, $z \in \mathbb{C}$. Allora sappiamo che esistono numeri complessi z_i tali che

$$p_n(z) = \prod_{k=1}^{n} (z - z_i)$$

Per continuare introduciamo una nuova nozione, quella di *complesso coniugato*: per ogni numero complesso $z = x + iy$ il compleso coniugato è il numero $x - iy$ e si designa con $\overline{z}$.

Problem 4.1. *Si mostri che per ogni $z, w \in \mathbb{C}$ si ha*

$$|z|^2 = z \cdot \overline{z}$$
$$\overline{z + w} = \overline{z} + \overline{w}$$
$$\overline{z \cdot w} = \overline{z} \cdot \overline{w}$$

Ovviamente se un numero è reale il suo complesso coniugato è lui stesso.

Usando questa nuova nozione si ha $\overline{p_n(z)} = p_n(\overline{z})$, dunque

$$0 = p(z_j) = p(\overline{z}_j)$$

in altre parole: se un polinomio reale ha uno zero complesso allora anche il complesso coniugato è uno zero.

Allora deve essere che existe $m \leq n/2$ tale che gli zeri di p_n si possono scrivere come $z_{2m+1}, \dots, z_n \in \mathbb{R}$ e $z_j = x_j + iy_j = \overline{z}_{j+m} \in \mathbb{C}$, $j \leq m$. Perciò, per ogni $x \in \mathbb{R}$

$$\begin{aligned} p_n(x) &= \prod_{j=1}^{m} (x - x_j - iy_j)(x - x_i + iy_j) \prod_{j=2m+1}^{n} (x - z_j) \\ &= \prod_{j=1}^{m} \left[(x - x_j)^2 + y_j^2 \right] \prod_{j=2m+1}^{n} (x - z_j) \end{aligned}$$

Abbiamo così dimostrato che ogni polinomio reale si può fattorizzare come prodotto di polinomi di primo grado oppure di secondo grado che non hanno zeri nel campo reale. In altre parole l'unica ragione per cui un polinomio reale di grado n può non avere n zeri (contati con molteplicità) è se contiene un fattore del tipo (è divisibile per) $(x - a)^2 + b^2$.

Problem 4.2. *Si mostri che tutti i polinomi reali di grado dispari hanno almeno uno zero.*

Carlangelo Liverani, Dipartimento di Matematica, II Università di Roma (Tor Vergata), Via della Ricerca Scientifica, 00133 Roma, Italy.

E-mail address: liverani@mat.uniroma2.it