

Numeri complessi e polinomi

1 Numeri complessi

L'insieme dei numeri reali si identifica con la retta della geometria: in altri termini la retta si può dotare delle operazioni $+$ e \times e divenire un insieme che soddisfa le seguenti regole di calcolo.

- (1) La somma è commutativa: $x + y = y + x$
- (2) la somma è associativa: $x + (y + z) = (x + y) + z$
- (3) la somma possiede un elemento neutro: $x + 0 = x$
- (4) la somma si può invertire: $x + (-x) = 0$
- (5) la moltiplicazione è commutativa: $xy = yx$
- (6) la moltiplicazione è associativa: $x(yz) = (xy)z$
- (7) la moltiplicazione possiede un elemento neutro: $x \times 1 = x$
- (8) la moltiplicazione si inverte sugli elementi non nulli: $x \times (x^{-1}) = 1$
- (9) la somma si può raccogliere nel prodotto: $xy + xz = x(y + z)$

Vogliamo ora notare come anche il piano cartesiano $\mathbb{R} \times \mathbb{R}$ possieda una coppia di operazioni $+$ e \times che soddisfano queste proprietà.

Definizione 1.1 *L'insieme dei numeri complessi \mathbb{C} è il piano $\mathbb{R} \times \mathbb{R}$.*

Definiamo la somma come

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$$

Dato che si tratta semplicemente della somma di vettori in \mathbb{R}^2 , sappiamo che soddisfa le (1)-(4).

Per definire il prodotto usiamo il fatto che $\mathbb{C} = \mathbb{R}^2$ è uno spazio vettoriale: consideriamo la sua base canonica (e_1, e_2) , sicché possiamo scrivere per ogni $z \in \mathbb{C}$:

$$z = xe_1 + ye_2$$

Notiamo ora che lo spazio vettoriale dei numeri reali si può considerare un sottospazio dei numeri complessi: basta considerare un numero reale $x \in \mathbb{R}$

come il numero complesso $(x, 0)$; questo vuol dire che l'elemento $1 \in \mathbb{R}$ è identificato con e_1 ; scriviamo quindi

$$x = x1 + yi = x + yi$$

dove con i abbiamo denominato $e_2 = (0, 1)$.

La somma di numeri complessi si può quindi scrivere come

$$(a + bi) + (c + di) = (a + c) + i(b + d)$$

Ora notiamo che il prodotto di due numeri reali consiste in una operazione geometrica: quello che ci interessa notare è che un numero reale è determinato dal suo valore assoluto e dal suo segno.

Possiamo immaginare il segno come un angolo: se è $+$ allora l'angolo è di 0° , altrimenti è di 180° . In effetti cambiare segno ad un numero vuol dire ruotarlo di 180° intorno all'origine (immaginiamo i numeri reali come l'asse delle x); questo spiega perché $-(-x) = x$: ruotare di due volte di 180° è come ruotare di 360° cioè tornare al punto di partenza.

Ora consideriamo il vettore $i = e_2$: per passare da $1 = e_1$ a e_2 si ruota di 90° ; quindi ruotando due volte di 90° è come ruotarlo di 180° : dato che ruotare vuol dire moltiplicare, abbiamo che $i^2 = -1$.

Ora per definire il prodotto fra numeri complessi, scriviamoli in termini della base canonica $\{1, i\}$ e trattiamoli come polinomi nella variabile i :

$$(a + bi)(c + di) = ac + i^2bd + adi + bci = ac - bd + i(ad + bc)$$

(perché $i^2 = -1$). In questo modo abbiamo scritto una operazione che soddisfa le proprietà del prodotto, perché è un caso particolare del prodotto di polinomi, e quindi abbiamo dotato \mathbb{C} di una moltiplicazione.

Interpretando i numeri complessi come coppie di numeri reali il prodotto si scrive

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 - y_1y_2, x_1y_2 + x_2y_1)$$

Scriviamo esplicitamente l'inverso di un numero complesso.

Abbiamo detto che il prodotto di numeri reali si scrive facilmente in termini della loro lunghezza e del segno: la lunghezza di un numero reale, visto come vettore, è il suo valore assoluto $|x|$, mentre il suo segno rappresenta un angolo di 0 o di $\pi = 180^\circ$ (d'ora in avanti misuriamo gli angoli inj radianti piuttosto che in gradi).

Per essere precisi possiamo scrivere

$$x = |x| \cos \sigma$$

dove $\sigma \in \{0, \pi\}$ è il segno. La moltiplicazione di numeri reali si scrive allora come

$$xy = |x||y| \cos \sigma \cos \tau = |xy| \cos(\sigma + \tau)$$

(infatti $\cos(\sigma + \tau) = \cos \sigma \cos \tau - \sin \sigma \sin \tau$, ma dato che $\sigma, \tau \in \{0, \pi\}$ il loro seno è zero).

Quindi moltiplicare numeri reali vuol dire fare il prodotto delle lunghezze e sommare i rispettivi angoli.

Vediamo che anche nel caso di numeri complessi questo è vero.

Definizione 1.2 *Il modulo di un numero complesso $z = (x, y) = x + iy$ è la sua lunghezza*

$$|z| = \sqrt{x^2 + y^2}$$

Il modulo soddisfa a queste proprietà, analoghe a quelle del valore assoluto fra numeri reali:

$$\begin{aligned} |z_1 z_2| &= |z_1| |z_2| \\ |z_1 + z_2| &\leq |z_1| + |z_2| \\ |z| = 0 &\iff z = 0 \end{aligned}$$

(si noti che il modulo è sempre un numero reale non negativo).

Un qualsiasi numero complesso si può scrivere come

$$z = |z|(\cos \theta + i \sin \theta)$$

(rappresentazione polare o trigonometrica del numero complesso).

Infatti ogni punto del piano si scrive in questo modo: questo perché per ogni punto del piano passa una ed una sola retta che passa anche per l'origine; l'angolo θ è quello formato da questa retta e dall'asse delle x , e il modulo è la distanza fra il punto z e l'origine.

Possiamo scrivere tutto ciò in termini di prodotto scalare: dato che

$$z = x + iy$$

e $\{1, i\}$ è una base ortonormale, abbiamo che

$$z = \langle z, 1 \rangle 1 + \langle z, i \rangle i$$

e $\langle z, 1 \rangle = x$, $\langle z, i \rangle = y$, dato che x e y sono la coordinata rispetto a 1 e rispetto a i , che si dice *unità immaginaria*.

Definizione 1.3 *Se $z = x + iy \in \mathbb{C}$ allora x si dice parte reale e y si dice parte immaginaria del numero complesso z , e si denotano rispettivamente con $x = \operatorname{Re} z$ e $y = \operatorname{Im} z$; se $\operatorname{Re} z = 0$ il numero complesso si dice puramente immaginario o semplicemente immaginario.*

Ma sappiamo che

$$\langle v, w \rangle = |v||w| \cos \theta$$

dove θ è l'angolo fra w e v . Ora applichiamo questa formula ai prodotti $\langle z, 1 \rangle = |z| \cos \theta$ e $\langle z, i \rangle = |z| \cos(\pi/2 - \theta)$ (dato che l'angolo fra 1 e i è $\pi/2$), quindi troviamo che

$$z = \langle z, 1 \rangle 1 + \langle z, i \rangle i = |z| \cos \theta + i|z| \cos \left(\frac{\pi}{2} - \theta \right) = |z|(\cos \theta + i \operatorname{sen} \theta)$$

Abbiamo quindi dimostrato che un numero complesso si scrive in forma trigonometrica. Notiamo che l'angolo θ non è unico: ogni angolo del tipo $\theta + 2k\pi$ va bene, come al solito quando si ha a che fare con seni e coseni. Scegliamo sempre l'unico θ compreso fra 0 (incluso) e 2π (escluso).

Il legame fra parti reali ed immaginarie di un numero complesso e fra il suo modulo e il suo angolo è dato dalle

$$\begin{cases} x = |z| \cos \theta \\ y = |z| \operatorname{sen} \theta \end{cases}$$

Ora possiamo scrivere il prodotto di numeri complessi $z_1 = x_1 + iy_1$ e $z_2 = x_2 + iy_2$ in forma trigonometrica:

$$\begin{aligned} z_1 z_2 &= (x_1 x_2 - y_1 y_2) + i(x_1 y_2 + x_2 y_1) \\ &= (|z_1| \cos \theta_1 |z_2| \cos \theta_2 - |z_1| \operatorname{sen} \theta_1 |z_2| \operatorname{sen} \theta_2) \\ &\quad + i(|z_1| \cos \theta_1 |z_2| \operatorname{sen} \theta_2 + |z_2| \cos \theta_2 |z_1| \operatorname{sen} \theta_1) \\ &= |z_1 z_2| ((\cos \theta_1 \cos \theta_2 - \operatorname{sen} \theta_1 \operatorname{sen} \theta_2) + i(\cos \theta_1 \operatorname{sen} \theta_2 + \operatorname{sen} \theta_1 \cos \theta_2)) \\ &= |z_1 z_2| (\cos(\theta_1 + \theta_2) + i \operatorname{sen}(\theta_1 + \theta_2)) \end{aligned}$$

Cioè per fare il prodotto di numeri complessi si moltiplicano i moduli e si sommano gli angoli.

Così, dato che il numero complesso 1 ha modulo 1 e angolo 0 , dato un numero complesso non nullo z , il suo inverso w sarà tale che $zw = 1$ cioè $|zw| = 1$ e $\theta + \rho = 0$, vale a dire $|w| = 1/|z|$ e $\rho = -\theta$; quindi per fare l'inverso di un numero complesso si fa l'inverso del modulo e si cambia segno all'angolo (sommando 2π se si ottiene un angolo negativo, in modo da ricadere sempre nell'intervallo $[0, 2\pi)$).

Notiamo che, dato il legame fra coseno e prodotto scalare, abbiamo che

$$\cos \theta = \frac{\langle z, 1 \rangle}{|z|} = \frac{x}{\sqrt{x^2 + y^2}}$$

e quindi

$$\operatorname{sen} \theta = \frac{\langle z, i \rangle}{|z|} = \frac{y}{\sqrt{x^2 + y^2}}$$

Ne segue che

$$\begin{aligned} z^{-1} &= \frac{1}{|z|} (\cos(-\theta) + i \operatorname{sen}(-\theta)) = \frac{1}{|z|} (\cos(\theta) - i \operatorname{sen}(\theta)) \\ &= \frac{1}{\sqrt{x^2 + y^2}} \left(\frac{x}{\sqrt{x^2 + y^2}} - i \frac{y}{\sqrt{x^2 + y^2}} \right) = \frac{1}{x^2 + y^2} (x - iy) \end{aligned}$$

Definizione 1.4 Se $z = x + iy \in \mathbb{C}$ definiamo il suo complesso coniugato come il numero $\bar{z} = x - iy$.

Evidentemente un numero coincide col proprio coniugato se e solo se la sua parte immaginaria è zero, cioè se è reale: $z = \bar{z} \iff \operatorname{Im} z = 0 \iff z \in \mathbb{R}$; analogamente un numero complesso è puramente immaginario se e solo se $z = -\bar{z}$.

Notiamo che $z\bar{z} = |z|^2$, quindi

$$\frac{1}{|z|^2} z\bar{z} = 1$$

da cui ritroviamo che

$$z^{-1} = \frac{\bar{z}}{|z|^2}$$

Ad esempio calcoliamo $1/i$: abbiamo dalla formula precedente che

$$\frac{1}{i} = \frac{\bar{i}}{|i|^2} = -i$$

Trigonometricamente, $i = \cos \pi/2 + i \operatorname{sen} \pi/2$, quindi

$$\frac{1}{i} = \cos -\frac{\pi}{2} + i \operatorname{sen} -\frac{\pi}{2} = -i \operatorname{sen} \frac{\pi}{2} = -i$$

I numeri complessi sono fondamentali perché consentono di estrarre radici qualsiasi: il lettore avrà già notato che $\sqrt{-1} = i$; dato che $i^2 = -1$. In effetti un numero complesso possiede sempre due radici quadrate, ed in generale possiede n radici n -esime.

Un numero complesso di modulo 1 è, geometricamente, un punto della circonferenza di centro l'origine e raggio 1; è quindi determinato solo dall'angolo, ed infatti ha sempre la forma

$$\cos \theta + i \operatorname{sen} \theta$$

Le sue radici n -esime si scrivono facilmente: sono i numeri complessi

$$\cos \frac{k\theta}{n} + i \operatorname{sen} \frac{k\theta}{n}$$

dove $k = 0, \dots, n-1$. In effetti è facile notare come le potenze n -esime di questi numeri siano il numero di partenza.

In particolare il numero 1 ha n radici n -esime (per esempio le sue radici quadrate sono ± 1). Dato che il suo angolo è 0, o se si vuole 2π , le possiamo determinare facilmente:

$$\sqrt[n]{1} = \cos \frac{2k\pi}{n} + i \operatorname{sen} \frac{2k\pi}{n}$$

Ad esempio le radici cubiche dell'unità sono

$$\begin{aligned} \cos \frac{0}{3} + i \operatorname{sen} \frac{0}{3} &= 1, & \cos \frac{2\pi}{3} + i \operatorname{sen} \frac{2\pi}{3} &= -\frac{1}{2} + i \frac{\sqrt{3}}{2}, \\ \cos \frac{4k\pi}{3} + i \operatorname{sen} \frac{4k\pi}{3} &= -\frac{1}{2} - i \frac{\sqrt{3}}{2} \end{aligned}$$

Con i numeri complessi si possono quindi risolvere, a priori, tutte le equazioni algebriche.

Quello che deve essere chiaro è che, dato che i numeri complessi comprendono i reali come caso particolare (cioè li estendono), e dato che fra numeri complessi si possono compiere le stesse operazioni algebriche che si compiono fra numeri reali, anzi meglio dato che si possono sempre estrarre le radici, tutte le costruzioni puramente algebriche che si fanno con i numeri reali si possono fare con i numeri complessi.

Ad esempio si possono considerare polinomi a coefficienti complessi, matrici a coefficienti complessi, vettori a coefficienti complessi e così via.

2 Esercizi

- 1) Trovare i moduli dei seguenti numeri complessi: (a) $z = 4 + 3i$, (b) $z = \cos \alpha - i \operatorname{sen} \alpha$, (c) $z = -2 + 2\sqrt{3}i$.
- 2) Mettere in forma trigonometrica i seguenti numeri complessi: (a) $-1 - i\sqrt{3}$, (b) $-\sqrt{2} + i\sqrt{2}$.
- 3) Calcolare $(-1 + i\sqrt{3})^{60}$
- 4) Mettere nella forma $x + iy$ i seguenti numeri complessi: (a) $(1/2 - i\sqrt{3}/2)^3$, (b) $(1/\sqrt{2} + i/\sqrt{2})^4$, (c) $(5 + 5i)(5i - 5)$, (d) $(i/\sqrt{2} - 1/\sqrt{2})^8$, (e) $(2+i)/(2-i)$.

5) Risolvere in \mathbb{C} le seguenti equazioni: (a) $z = 2 + i\sqrt{5}$, (b) $(1 - i)z^3 = 1 + i$, (c) $z^2 + 5i = 12$, (d) $z^2 - (1 + i)z + 2 - i = 0$

6) Risolvere l'equazione

$$(1 + i)^2 \left(z^2 - \frac{i}{2} \right) = 1 - i$$

3 Risposte

1) (a) 5, (b) 1, (c) 4.

2) (a) $2 \cos(-2\pi/3) + 2i \operatorname{sen}(-2\pi/3)$, (b) $2 \cos(3\pi/4) + 2i \operatorname{sen}(3\pi/4)$.

3) 2^{60} .

4) (a) -1 , (b) -1 , (c) -50 , (d) 1 , (e) $3/5 + 4i/5$.

5) (a) $\pm(\sqrt{5} + i)/\sqrt{2}$, (b) $(\pm\sqrt{3}/2 + i/2)$, $-i$, (c) $\pm(5 - i)/\sqrt{2}$, (d) $-i$, $1 + 2i$.

6) $\pm i/\sqrt{2}$.

4 Aritmetica dei polinomi

Considereremo qui polinomi a coefficienti complessi; molte cose che diremo sono vere anche se i coefficienti sono solo reali, ma alcune proprietà fondamentali sono vere solo per polinomi complessi.

Definizione 4.1 *Le radici di un polinomio $p \in \mathbb{C}[x]$ sono gli elementi $c \in \mathbb{C}$ tali che $p(c) = 0$.*

Talora le radici dei polinomi si chiamano anche *zeri*, perché si ottengono risolvendo l'equazione $p(x) = 0$.

Ovviamente consideriamo polinomi di grado positivo: un polinomio di grado nullo a coefficienti in \mathbb{C} è esattamente un elemento di \mathbb{C} , e non ha molto senso chiedersi quali siano le sue radici.

Si dimostri per esercizio che il polinomio $p(x) = p_0 + p_1x + \dots + p_nx^n$ ha le stesse radici del polinomio

$$\frac{p_0}{p_n} + \frac{p_1}{p_n}x + \dots + x^n$$

Dunque, se vogliamo studiare le radici di un polinomio, possiamo sempre supporre che il polinomio sia *monico*, cioè che il suo *coefficiente direttore* sia 1, dove il coefficiente direttore è il numero che moltiplica la potenza di grado deg p del polinomio: se $p(x) = p_0 + p_1x + \dots + p_nx^n$ il suo coefficiente direttore è p_n .

I polinomi di grado uno, che sono della forma $ax + b$ non presentano particolari problemi: infatti, dato che a e b stanno in un campo, e dato che $a \neq 0$ (altrimenti il polinomio si ridurrebbe alla costante b) possiamo determinare l'unica soluzione, che è $x = -b/a$.

I polinomi quadratici talvolta possiedono radici, talvolta no: ad esempio $x^2 + 1$ non può possedere radici reali, perché per ogni $r \in \mathbb{R}$ si ha $r^2 \geq 0$, e quindi $r^2 + 1 > 0$, mentre possiede due radici complesse, $\pm i$.

Discutiamo le operazioni algebriche fra polinomi: già sappiamo che i polinomi formano uno spazio vettoriale, cioè possiamo sommarli fra loro e moltiplicarli per numeri (complessi).

Per definire il prodotto fra polinomi ci facciamo guidare dal principio secondo il quale questo prodotto deve, nel caso di polinomi costanti, coincidere con l'usuale prodotto di numeri, cioè ponendo al posto della x un numero, dobbiamo ottenere il prodotto di numeri in \mathbb{C} : partiamo da un esempio, che sviluppiamo in tutti i dettagli sperando che il lettore non si offenda per l'eccessiva semplicità del calcolo:

$$\begin{aligned} (1 + x^2 - 3x^3)(x + 2x^2 + 3x^3 + 4x^4) &= (1 + (x^2 - 3x^3))(x + 2x^2 + 3x^3 + 4x^4) \\ &= (x + 2x^2 + 3x^3 + 4x^4) + (x^2 - 3x^3)(x + 2x^2 + 3x^3 + 4x^4) \\ &= (x + 2x^2 + 3x^3 + 4x^4) + x^2(x + 2x^2 + 3x^3 + 4x^4) - 3x^3(x + 2x^2 + 3x^3 + 4x^4) \\ &= (x + 2x^2 + 3x^3 + 4x^4) + (x^3 + 2x^4 + 3x^5 + 4x^6) + (-3x^4 - 6x^5 - 9x^6 - 12x^7) \\ &= x + 2x^2 + 4x^3 + 3x^4 - 4x^5 - 5x^6 - 12x^7 \end{aligned}$$

Abbiamo usato a ripetizione la proprietà distributiva: in generale questo calcolo si scrive come

$$(*) \quad \left(\sum_{i=1}^n a_i \right) \times \left(\sum_{j=1}^m b_j \right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$$

Ora consideriamo due polinomi $p(x) = \sum_i p_i x^i$ e $q(x) = \sum_j q_j x^j$: se vogliamo moltiplicarli poniamo nella (*) $a_i = p_i x^i$ e $b_j = q_j x^j$, sicché $a_i b_j = p_i q_j x^{i+j}$ e troviamo

$$(**) \quad \left(\sum_{i=0}^n p_i x^i \right) \times \left(\sum_{j=0}^m q_j x^j \right) = \sum_{i=0}^n \sum_{j=0}^m p_i q_j x^{i+j}$$

Scriviamo come un polinomio questo prodotto: poniamo $k = i + j$ e troviamo

$$\sum_{i=0}^n \sum_{j=0}^m p_i q_j x^{i+j} = \sum_{k=0}^{n+m} \left(\sum_{i=0}^k p_i q_{k-i} \right) x^k$$

Possiamo anche scriverlo come

$$\sum_{i=0}^n \sum_{j=0}^m p_i q_j x^{i+j} = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} p_i q_j \right) x^k$$

Per maggiore chiarezza ne scriviamo esplicitamente alcuni termini del prodotto: ad esempio se supponiamo $n < m$:

$$\begin{cases} c_0 = p_0 q_0 \\ c_1 = p_0 q_1 + p_1 q_0 \\ c_2 = p_0 q_2 + p_1 q_1 + p_2 q_0 \\ \vdots \\ c_n = p_0 q_n + p_1 q_{n-1} + \cdots + p_n q_0 \\ c_{n+1} = p_0 q_{n+1} + p_1 q_n + \cdots + p_n q_1 \\ \vdots \\ c_m = p_0 q_m \end{cases}$$

Si tratta quindi semplicemente di considerare le somme dei prodotti di p_i e q_j tali che la somma dei loro indici sia uguale ad uno stesso indice k , per ottenere c_k .

Ricordiamo che il grado di un polinomio è la massima potenza dell'incognita il cui coefficiente non sia nullo: lo indichiamo con $\deg p$, (dall'inglese *degree*)

Corollario 4.1 *Se $p, q \in C[x]$ sono polinomi non nulli allora $\deg(p \times q) = \deg p + \deg q$.*

DIMOSTRAZIONE: Se $p(x) = \sum_i p_i x^i$ e $q(x) = \sum_j q_j x^j$ allora $(pq)(x) = \sum_k c_k x^k$, con $c_{\deg p + \deg q} = p_{\deg p} q_{\deg q}$ che è diverso da zero, perché se $p_{\deg p} = 0$ allora $p = 0$ e se $q_{\deg q} = 0$ allora $q = 0$.

CVD

Si noti che se uno dei due polinomi è zero allora $pq = 0$ e quindi il grado del prodotto è pure zero.

Verificare per esercizio che se $p(x) = x^n$ e $q(x) = x^m$ allora $(p \times q)(x) = x^{n+m}$.

Teorema 4.2 *Il prodotto fra polinomi soddisfa la proprietà commutativa, associativa, possiede un elemento neutro (il polinomio costante 1), la proprietà distributiva e la legge di annullamento del prodotto.*

Affrontiamo ora la questione dell'inversione di un polinomio, cioè di risolvere l'equazione $p(x)q(x) = 1$ dato $p(x)$; questa non è sempre risolvibile,

in effetti basta considerare il polinomio x per accorgersi che non ha inverso moltiplicativo: se l'avesse esisterebbe $q(x)$ tale che $xq(x) = 1$: allora, per il corollario precedente, dato che ovviamente deve essere $q \neq 0$, si ha $1 + \deg q = 0$, che è assurdo, dato che $\deg q \geq 0$; più in generale, dato che il prodotto di polinomi ha come grado la somma dei gradi dei suoi fattori, un polinomio di grado positivo non sarà mai invertibile:

Teorema 4.3 *Un polinomio $p \in \mathbb{C}[x]$ è invertibile se e solo se è costante e non nullo.*

DIMOSTRAZIONE: Ovviamente un polinomio costante e non nullo p_0 è invertibile: $p_0 p_0^{-1} = 1$; se $p = \sum_i p_i x^i$ è invertibile, allora esiste $q \in \mathbb{C}[x]$ non nullo tale che $pq = 1$: quindi, per il corollario precedente, $\deg p + \deg q = 0$; ne segue che, $\deg p = \deg q = 0$, e quindi che p_0 e $q = q_0$ sono costanti, tali che $p_0 q_0 = 1$, cioè $q_0 = p_0^{-1}$.

CVD

Quindi gli elementi invertibili nell'insieme dei polinomi sono pochissimi: solo i polinomi costanti non nulli; il lettore dovrebbe comunque notare che questo fatto è del tutto analogo a quel che succede in \mathbb{Z} : gli unici elementi di \mathbb{Z} che ammettono inverso moltiplicativo sono 1 e -1 . In effetti molti lettori avranno già notato un fatto interessantissimo: la somma e il prodotto di polinomi soddisfano le stesse regole della somma e del prodotto di numeri interi.

Possiamo quindi usare questa analogia per definire una divisione con resto fra polinomi, esattamente come si fa per gli interi.

Teorema 4.4 *Se $a, b \in \mathbb{C}[x]$ sono polinomi e $b \neq 0$ allora esistono due unici polinomi $q, r \in \mathbb{C}[x]$ tali che*

$$* \quad a(x) = b(x)q(x) + r(x) \quad \text{con} \quad \deg r < \deg b$$

DIMOSTRAZIONE: Scriviamo $a(x) = \sum_i a_i x^i$ e $b(x) = \sum_j b_j x^j$, e ragioniamo per induzione su $\deg a$: considereremo $b(x)$ come un polinomio fissato nel corso della dimostrazione.

Se $\deg a = 0$ allora a è costante, quindi possiamo porre $q = 0$ e $r = a = a_0$ se $\deg b > 0$, oppure $q = a_0 b_0^{-1}$ e $r = 0$ se $\deg b = 0$, ottenendo la (*).

Sia ora $\deg a = n$ e supponiamo che il teorema sia vero per i polinomi $a(x)$ di grado $< n$: intanto notiamo che se $n = \deg a < \deg b$ allora prendendo $q = 0$ e $r = a$ otteniamo la tesi. Supponiamo quindi $m \leq n$ e consideriamo il polinomio

$$c(x) = a(x) - \frac{a_0}{b_0} x^{n-m} b(x)$$

che ha grado $< n$: infatti il termine di grado più alto del polinomio $a_0 b_0^{-1} x^{n-m} b(x)$ è quello di grado $n - m + \deg b = n$, che è proprio $a_0 b_0^{-1} b_0 = a_0$; ne segue che il termine di grado n di $c(x)$ è zero, e, dato che $\deg c \leq n$, che $\deg c < n$.

Possiamo quindi applicare a $c(x)$ l'ipotesi induttiva, cioè determinare due polinomi $d, r \in \mathbb{C}[x]$ tali che

$$c(x) = b(x)d(x) + r(x) \quad \text{con} \quad \deg r < \deg b$$

A questo punto usiamo la definizione di $c(x)$ per dedurne che

$$a(x) = \frac{a_0}{b_0} x^{n-m} b(x) + b(x)d(x) + r(x) = b(x) \left(\frac{a_0}{b_0} x^{n-m} + d(x) \right) + r(x)$$

e quindi, ponendo

$$q(x) = \frac{a_0}{b_0} x^{n-m} + d(x)$$

abbiamo due polinomi $q, r \in \mathbb{C}[x]$ che soddisfano la (*).

Resta da provarne l'unicità: al solito, supponiamo che esistano $q', r' \in \mathbb{C}[x]$ in modo che

$$a(x) = b(x)q(x) + r(x) = b(x)q'(x) + r'(x)$$

con $\deg r, \deg r' < \deg b$; ne segue allora che

$$b(x)(q(x) - q'(x)) = r'(x) - r(x)$$

e quindi che, supponendo $q(x) \neq q'(x)$

$$\deg b + \deg(q - q') = \deg(r' - r)$$

Ma $\deg r, \deg r' < \deg b$ e quindi $\deg(r - r') \leq \max\{\deg r, \deg r'\} < \deg b$, sicché avremmo $\deg(q - q') < 0$, che è un assurdo.

Siamo quindi costretti ad ammettere che $q = q'$, da cui $r = r'$.

CVD

Abbiamo cioè dimostrato che anche per i polinomi si può effettuare la divisione, esattamente come per i numeri interi: questo fatto cruciale ha una serie di conseguenze immediate ma fondamentali. Al solito diciamo che q è il *quoziente* e r è il *resto* della divisione di a per b .

Si noti che questo risultato come tutti quelli fin qui esposti, è valido sia per polinomi reali che per polinomi complessi.

La dimostrazione del teorema suggerisce anche il metodo di calcolo, che sarà del tutto analogo all'algoritmo della divisione fra numeri interi: il lettore comprenderà meglio questo procedimento se lo vedrà in azione su un esempio specifico.

Esempio 4.1 Consideriamo $a(x) = 2x^5 - 3x^4 + 5x^3 - 7x^2 + 11x - 13$ e $b(x) = 2x^2 + x + 1$ e supponiamo di voler dividere a per b , cioè di voler determinare $a = bq + r$ secondo l'algoritmo euclideo. Come abbiamo appena spiegato, determiniamo q dando i suoi coefficienti a partire da quello direttore; per prima cosa vogliamo $q_3 \in \mathbb{C}$ tale che

$$a(x) - q_3x^3b(x) = 2x^5 - 3x^4 + 5x^3 - 7x^2 + 11x - 13 - q_3x^3(2x^2 + x + 1)$$

abbia grado < 5 , dunque $q_3 = 1$; otteniamo il polinomio

$$2x^5 - 3x^4 + 5x^3 - 7x^2 + 11x - 13 - x^3(2x^2 + x + 1) = -4x^4 + 4x^3 - 7x^2 + 11x - 13$$

e vogliamo stavolta un numero q_2 tale che

$$-4x^4 + 4x^3 - 7x^2 + 11x - 13 - q_2x^2(2x^2 + x + 1)$$

abbia grado < 4 , dunque $q_2 = -2$; otteniamo il polinomio

$$-4x^4 + 4x^3 - 7x^2 + 11x - 13 + 2x^2(2x^2 + x + 1) = 6x^3 - 5x^2 + 11x - 13$$

e vogliamo un numero q_1 tale che

$$6x^3 - 5x^2 + 11x - 13 - q_1x(2x^2 + x + 1)$$

abbia grado < 3 , dunque $q_1 = 3$; otteniamo il polinomio

$$6x^3 - 5x^2 + 11x - 13 - 3x(2x^2 + x + 1) = -8x^2 + 8x - 13$$

e vogliamo un numero q_0 tale che

$$-8x^2 + 8x - 13 - q_0(2x^2 + x + 1)$$

abbia grado < 2 , dunque $q_0 = -4$; a questo punto ci fermiamo, perché siamo giunti a un grado minore del grado di $b(x)$, e calcoliamo il resto:

$$-8x^2 + 8x - 13 + 4(2x^2 + x + 1) = 12x - 9$$

I coefficienti che abbiamo trovato sono quelli del polinomio q , così che

$$a(x) = q(x)b(x) + r(x) = (x^3 - 2x^2 + 3x - 4)(2x^2 + x + 1) + (12x - 9)$$

Se il lettore vuole, può svolgere il prodotto come verifica.

Quando si effettua questa operazione con carta e penna si usa la stessa notazione che per la divisione fra numeri imparata alle scuole elementari: nel caso precedente cominciamo a dividere il monomio di grado più alto in a (che è $2x^5$) per il monomio di grado più alto in b che è $2x^2$, ottenendo x^3 : poi moltiplichiamo b per x^3 e lo sottraiamo da a :

$$\begin{array}{r|l} 2x^5 - 3x^4 + 5x^3 - 7x^2 + 11x - 13 & 2x^2 + x + 1 \\ -2x^5 - x^4 - x^3 & x^3 \\ \hline -4x^4 + 4x^3 - 7x^2 + 11x - 13 & \end{array}$$

Ora ripetiamo il processo di divisione su questo polinomio differenza (quello scritto in basso, sotto la riga): stavolta dividiamo $-4x^4$ per $2x^2$ ottenendo $-2x^2$:

$$\begin{array}{r|l} 2x^5 - 3x^4 + 5x^3 - 7x^2 + 11x - 13 & 2x^2 + x + 1 \\ -2x^5 - x^4 - x^3 & x^3 \\ \hline -4x^4 + 4x^3 - 7x^2 + 11x - 13 & \\ 4x^4 + 2x^3 + 3x^2 & -2x^2 \\ \hline 6x^3 - 5x^2 + 11x - 13 & \end{array}$$

Proseguiamo ancora e stavolta dividiamo $6x^3$ per $2x^2$ ottenendo $3x$:

$$\begin{array}{r|l} 2x^5 - 3x^4 + 5x^3 - 7x^2 + 11x - 13 & 2x^2 + x + 1 \\ -2x^5 - x^4 - x^3 & x^3 \\ \hline -4x^4 + 4x^3 - 7x^2 + 11x - 13 & \\ 4x^4 + 2x^3 + 3x^2 & -2x^2 \\ \hline 6x^3 - 5x^2 + 11x - 13 & \\ -6x^3 - 3x^2 - 3x & +3x \\ \hline -8x^2 + 8x - 13 & \end{array}$$

Infine nell'ultimo passaggio i coefficienti direttori del dividendo e del divisore sono $-8x^2$ e $2x^2$ il cui quoziente è -4 :

$$\begin{array}{r|l} 2x^5 - 3x^4 + 5x^3 - 7x^2 + 11x - 13 & 2x^2 + x + 1 \\ -2x^5 - x^4 - x^3 & x^3 \\ \hline -4x^4 + 4x^3 - 7x^2 + 11x - 13 & \\ 4x^4 + 2x^3 + 3x^2 & -2x^2 \\ \hline 6x^3 - 5x^2 + 11x - 13 & \\ -6x^3 - 3x^2 - 3x & +3x \\ \hline -8x^2 + 8x - 13 & \\ 8x^2 + 4x + 4 & -4 \\ \hline 12x - 9 & \end{array}$$

Col che abbiamo completato la “divisione lunga” ed ottenuto un resto (non nullo), dato dall'ultimo polinomio $12x - 9$ che ha grado minore del grado del dividendo $2x^2 + x + 1$.

Il lettore dovrebbe a questo punto provare a prendere polinomi e dividerli in questo modo: c'è sempre il modo di verificare se la divisione $a = bq + r$ è stata fatta correttamente, ed è quello di calcolare $bq + r$ e verificare che si tratta di a .

Definizione 4.2 Se $p, q \in \mathbb{C}[x]$ allora p divide q se esiste $s \in \mathbb{C}[x]$ tale che $p(x)s(x) = q(x)$; scriviamo $p|q$.

Corollario 4.5 Se $p \in \mathbb{C}[x]$ allora $c \in \mathbb{C}$ è una radice del polinomio p se e solo se $(x - c)|p$.

DIMOSTRAZIONE: Si noti che, per il teorema, possiamo in ogni caso determinare q e r tali che

$$p(x) = (x - c)q(x) + r(x)$$

con $\deg r < \deg(x - c) = 1$, cioè r deve essere costante.

Supponiamo ora che c sia una radice di p , cioè che $p(c) = 0$: allora

$$0 = p(c) = (c - c)q(c) + r = r$$

cioè $r = 0$ e quindi $(x - c)|p$. Viceversa, se $(x - c)|p$ allora $p(x) = (x - c)q(x)$ e quindi $p(c) = (c - c)q(c) = 0$.

CVD

Dunque determinare una radice di un polinomio è la stessa cosa che determinare un fattore lineare del polinomio (con “lineare” si intende “di grado uno”).

Un fatto molto importante è il seguente

Corollario 4.6 *Se $p \in \mathbb{C}[x]$ allora p può avere al più $\deg p$ radici distinte.*

DIMOSTRAZIONE: per assurdo, supponiamo che $p \in \mathbb{C}[x]$ abbia almeno $n = 1 + \deg p$ radici distinte, diciamo c_1, \dots, c_n : allora, per il corollario precedente, $(x - c_i)|p$ per $i = 1, \dots, n$, cioè

$$p(x) = (x - c_1)(x - c_2) \cdots (x - c_n)q(x)$$

Ma il polinomio a secondo membro ha almeno grado $n = \deg p + 1$ mentre quello a primo membro ha grado $\deg p$: quindi non possono esistere più di $\deg p$ radici distinte.

CVD

Quindi, dato un polinomio qualsiasi, potrà avere al più n radici (magari non ne avrà nessuna): ad esempio, dato $x^3 - x^2 + x - 1$ in $\mathbb{R}[x]$, sappiamo certamente che, se ha radici, ne ha al più tre: in effetti si vede “ad occhio” che 1 ne è una radice, quindi

$$x^3 - x^2 + x - 1 = (x - 1)q(x)$$

ed è facile determinare $q(x)$: infatti deve avere grado due (poiché il suo prodotto con un polinomio di grado uno è un polinomio di grado tre), sicché lo scriviamo come $q(x) = q_0 + q_1x + q_2x^2$, svolgiamo il prodotto ed uguagliamo i coefficienti di questo prodotto a quelli di $x^3 - x^2 + x - 1$: in questo caso, comunque, basta raccogliere x^2 dai primi due termini per avere

$$x^3 - x^2 + x - 1 = x^2(x - 1) + (x - 1) = (x^2 + 1)(x - 1)$$

e quest'ultimo polinomio $x^2 + 1$ non ha radici in \mathbb{R} , dunque il polinomio $x^3 - x^2 + x - 1$ ha solo una radice in \mathbb{R} .

Esercizio 4.7 *Determinare prima in \mathbb{R} e poi in \mathbb{C} le radici dei seguenti polinomi: $x^3 - x^2 - 2x + 2$; $x^4 + 4$; $x^n - 1$ (distinguere il caso n pari dal caso n dispari).*

Notiamo esplicitamente un fatto ovvio ma importante:

Corollario 4.8 *Se $r \in \mathbb{R}$ allora possiede al più n radici n -esime.*

Ad esempio 2 possiede due radici quadrate: $\sqrt{2}$ e $-\sqrt{2}$.

Corollario 4.9 *Un polinomio in $\mathbb{R}[x]$ è prodotto di fattori lineari se e solo se le sue radici sono elementi di \mathbb{R} .*

Cioè le proprietà di fattorizzazione di un polinomio dipendono fortemente dal tipo di numeri con i quali stiamo lavorando: il polinomio $x^2 + 1$ non ha nessuna radice in \mathbb{R} , quindi non è divisibile per nessun altro polinomio (è insomma una specie di “polinomio primo”), mentre in \mathbb{C} possiede le sue due radici, che sono $\pm i$: quindi $x^2 + 1 = (x - i)(x + i)$, sicché in \mathbb{C} risulta divisibile per polinomi non costanti.

Si noti che un polinomio è sempre divisibile per una costante non nulla, ovviamente, quindi la teoria della divisibilità dei polinomi si fa a meno di fattori costanti: è la stessa cosa che vale per gli interi, la cui teoria della divisibilità si faceva a meno del segno.

L’analogia fra \mathbb{Z} e $\mathbb{C}[x]$ è così perfetta che viene spontaneo chiedersi se l’intera teoria della divisibilità per gli interi non possa darsi *mutatis mutandis* nel caso dei polinomi¹. Qui ci contentiamo di dare alcuni frammenti della teoria della divisibilità dei polinomi.

Il concetto centrale della teoria dei numeri è quello di numero primo: per i polinomi l’analogo è il seguente.

Definizione 4.3 *Un polinomio $p \in \mathbb{R}[x]$ è irriducibile se ha grado positivo ed è divisibile solo per se stesso e per le costanti non nulle (la stessa definizione si dà per $\mathbb{C}[x]$).*

In altri termini, p è irriducibile se da qualsiasi equazione $p(x) = q(x)r(x)$ segue necessariamente che q oppure r sono costanti (per definizione un polinomio costante non è irriducibile: questa convenzione è analoga al fatto di non considerare 1 come un numero primo).

¹In effetti è così: si può formulare una teoria astratta che generalizza la teoria dei numeri e quella dei polinomi, e che si chiama *algebra commutativa*.

Ad esempio un polinomio di primo grado $x + a$ è sempre irriducibile; il polinomio $x^2 + 1$ è irriducibile in \mathbb{R} ma non in \mathbb{C} .

In modo perfettamente analogo alla convenzione che un numero primo sia sempre positivo, stabiliamo qui la convenzione che un polinomio irriducibile sia sempre monico, cioè la sua potenza di grado più alto abbia coefficiente 1.

Passiamo ora a considerare la nozione di massimo comune divisore fra polinomi: è quello che il lettore si aspetta.

Definizione 4.4 *Se $p, q \in \mathbb{C}[x]$ sono polinomi non nulli, allora $\text{MCD}(p, q)$ è il polinomio tale che*

- (1) $\text{MCD}(p, q) | p$ e $\text{MCD}(p, q) | q$;
- (2) Se $r | p$ e $r | q$ allora $r | \text{MCD}(p, q)$.

Dimostriamo ora l'esistenza e l'unicità (a meno di fattori costanti) del massimo comune divisore di due polinomi.

Teorema 4.10 *Se $p, q \in \mathbb{C}[x]$ sono non nulli allora esiste $\text{MCD}(p, q)$ ed è unico a meno di fattori costanti non nulli.*

DIMOSTRAZIONE: Consideriamo l'insieme

$$I(p, q) = \{ap + bq \mid a, b \in \mathbb{C}[x]\}$$

dei polinomi ottenuti come combinazioni lineari di p e q : si tratta di un insieme non vuoto, dato che contiene almeno p e q (per $a = 1, b = 0$ e $a = 0, b = 1$); ora consideriamo l'immagine $\deg_* I(p, q)$ di questo insieme per tramite della funzione $\deg: \mathbb{C}[x] \rightarrow \mathbb{N}$: si tratta dell'insieme dei numeri naturali che sono il grado di qualche polinomio che sta in $I(p, q)$: è un insieme non vuoto di numeri naturali (contiene almeno $\deg p$ e $\deg q$), quindi ha un minimo m .

Per definizione, esiste un polinomio $r \in I(p, q)$ che ha grado m , e quindi, per definizione di $I(p, q)$, esistono due polinomi $a, b \in \mathbb{C}[x]$ tali che

$$r = ap + bq$$

Ora dimostriamo che $r | p$ e $r | q$: infatti dividendo p per r otteniamo

$$p = sr + t$$

con $\deg t < \deg r$: quindi t non appartiene a $I(p, q)$ (perché un elemento che vi appartiene ha grado $\geq \deg r$). Ma l'equazione appena scritta equivale alla

$$t = p - sr = p - s(ap + bq) = p(1 - sa) + bq$$

e quindi ci presenta t come elemento di $I(p, q)$! L'unica scappatoia è che $t = 0$, e quindi che $p = sr$ cioè $r|p$; allo stesso modo si vede che $r|q$.

Verifichiamo infine che r non è semplicemente un divisore comune, ma il massimo divisore comune di p e q : se fosse $s|p$, $s|q$ allora $us = p$ e $vs = q$ per qualche $u, v \in \mathbb{C}[x]$; ma allora

$$r = ap + bq = aus + bvs = (au + bv)s$$

col che $s|r$, come volevamo dimostrare.

CVD

Poiché il massimo comune divisore è unico a meno di una costante, possiamo fissarne uno canonico scegliendo quello che ha come coefficiente direttore 1: cioè, nel séguito, supporremo sempre che $\text{MCD}(p, q)$ sia l'unico polinomio monico che soddisfa la definizione di massimo comune divisore di p e q .

Esercizio 4.11 *L'insieme $I(p, q)$ definito nella dimostrazione precedente ha le seguenti proprietà: 1) se $x \in I(p, q)$ e $y \in \mathbb{C}[x]$ allora $xy \in I(p, q)$; 2) se $x, y \in I(p, q)$ allora $x - y \in I(p, q)$; 3) $0 \in I(p, q)$; 4) $1 \in I(p, q) \iff I(p, q) = \mathbb{C}[x]$.*

Esercizio 4.12 *Dimostrare il lemma di Bézout per i polinomi: se $p, q \in \mathbb{C}[x]$ non sono nulli allora esistono $a, b \in \mathbb{C}[x]$ tali che $\text{MCD}(p, q) = ap + bq$.*

Diamo ora la versione polinomiale del lemma di Euclide:

Teorema 4.13 *Se $p \in \mathbb{C}[x]$ è irriducibile e $q, r \in \mathbb{C}[x]$ non sono nulli allora se $p|qr$ si ha $p|q$ oppure $p|r$.*

DIMOSTRAZIONE: Sia $p|qr$ e supponiamo che $p \nmid q$ (altrimenti la tesi è verificata): vogliamo dimostrare che in questo caso si ha $p|r$; dato che $p \nmid q$, $\text{MCD}(p, q) = 1$ e quindi, per il lemma di Bézout, esistono due polinomi $a, b \in \mathbb{C}[x]$ tali che

$$ap + bq = 1$$

Ora moltiplichiamo questa equazione per il polinomio r ed abbiamo

$$apr + bqr = r$$

e sfruttiamo l'ipotesi $p|qr$ (cosa che non abbiamo ancora fatto) per dedurne l'esistenza di un polinomio $c \in \mathbb{C}[x]$ tale che $pc = qr$, e quindi che

$$r = apr + bqr = apr + cpr = (ar + cr)p$$

il che vuol dire $p|r$, come volevamo.

CVD

Possiamo ora dimostrare il teorema fondamentale dell'aritmetica dei polinomi:

Teorema 4.14 *Se $p \in \mathbb{C}[x]$ è un polinomio di grado positivo allora esistono $p_1, \dots, p_n \in \mathbb{C}[x]$ irriducibili tali che*

$$p(x) = p_1(x)p_2(x) \cdots p_n(x)$$

e p_1, \dots, p_n sono unici a meno dell'ordine e di un fattore costante non nullo.

DIMOSTRAZIONE: La dimostrazione è praticamente la stessa del teorema fondamentale dell'Aritmetica, e procede per induzione sul grado: se p ha grado uno allora è già irriducibile; supponiamo quindi che il teorema sia vero per un polinomio di grado minore di $\deg p$: se p è irriducibile si pone $p_1 = p$ ed il teorema è dimostrato; altrimenti vuol dire che esistono $q, r \in \mathbb{C}[x]$ di gradi positivi tali che $p(x) = q(x)r(x)$: ciascuno di essi, per ipotesi induttiva, è prodotto di polinomi irriducibili q_1, \dots, q_k e r_1, \dots, r_h , e questi sono anche fattori irriducibili di p .

Vediamo l'unicità, e, come nel caso di \mathbb{Z} , dovremo usare il lemma di Euclide: supponiamo che uno stesso polinomio ammetta due fattorizzazioni in polinomi irriducibili:

$$p_1 \cdots p_n = q_1 \cdots q_m$$

Dimostriamo, per induzione su n , che $n = m$ e che, a meno di scambiare l'ordine (cioè riordinando gli indici $1, \dots, n$), $p_i = q_i$.

Se $n = 1$ l'equazione diviene $p_1 = q_1 \cdots q_m$ e quindi, dato che p_1 è irriducibile ed anche q_1, \dots, q_m lo sono, deve essere $m = 1$ e $p_1 = c_1 q_1$ con $c_1 \in \mathbb{C}$ (si rammenti che un polinomio irriducibile ha grado positivo).

Ora supponiamo che la tesi sia vera per $n - 1$ e dimostriamola per n : consideriamo p_1 , che divide $q_1 \cdots q_m$: per il lemma di Euclide (o meglio una sua generalizzazione al caso di m polinomi che lasciamo al lettore), p_1 divide q_1 oppure q_2 , oppure q_m : supponiamo, appunto a meno di riordinare q_1, \dots, q_m , che $p_1 | q_1$, cioè, dato che entrambi sono irriducibili, $q_1 = c_1 p_1$, ove $c_1 \in \mathbb{C}$; allora l'equazione precedente diviene

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m \cdots q_m = c_1 p_1 q_2 \cdots q_m \Rightarrow p_2 \cdots p_n = c_1 q_2 \cdots q_m$$

Ma allora, per ipotesi induttiva, $m = n$ e $p_i = q_i$, col che l'unicità è dimostrata.

CVD

Dato che uno stesso polinomio irriducibile può comparire più volte nella fattorizzazione precedente, possiamo più precisamente scrivere

$$p = c p_1^{i_1} \cdots p_k^{i_k}$$

ove $i_1, \dots, i_n \in \mathbb{N}$ sono univocamente determinati e gli irriducibili p_1, \dots, p_n sono tutti distinti fra loro.

Esercizio: se $p \in \mathbb{R}[x]$ ha grado due allora è irriducibile oppure prodotto di fattori lineari; se ha grado tre è irriducibile oppure ha una radice.

Un teorema importantissimo afferma che i soli polinomi irriducibili in $\mathbb{C}[x]$ sono quelli lineari: questo si può riformulare dicendo che

Teorema Fondamentale dell'Algebra 4.15 *Se $p(x) \in \mathbb{C}[x]$ allora esiste sempre un $c \in \mathbb{C}$ tale che $p(c) = 0$.*

Questo teorema è falso in \mathbb{R} , basti pensare al polinomio $x^2 + 1$.