Polinomi

CCF

28 gennaio 2010

1 Introduzione

Poniamoci in un ambiente molto familiare: l'insieme dei polinomi nella variabile x. Di tale insieme vogliamo studiare alcune proprietà, legate a nozioni altrettanto familiari quali quella di radice o di scomposizione in fattori irriducibili. Cercheremo di mettere in evidenza che molte delle proprietà più rilevanti dipendono in definitiva dalla struttura dell'insieme in cui scegliamo i coefficienti dei nostri polinomi.

Consideriamo ad esempio il polinomio $p(x) = 7x^2 - 14$. Possiamo riscrivere tale polinomio in tante forme fra loro equivalenti, elenchiamone alcune:

- $p(x) = 7 \cdot (x^2 - 2)$
- $p(x) = -7 \cdot (2 - x^2)$
- $p(x) = -21 \cdot (\frac{2}{3} - \frac{x^2}{3})$
- $p(x) = 7 \cdot (x - \sqrt{2}) \cdot (x + \sqrt{2})$

e così via in infinite varianti...

Armati di uno spirito un po' radicale, potremmo porci alcune domande: hanno qualcosa in comune tutte queste decomposizioni ? Che legame esiste fra le decomposizioni di $p(x)$ in cui intervengono solo numeri interi e quelle in cui intervengono anche numeri razionali o irrazionali ? In ogni caso, oltre alle decomposizioni che abbiamo elencato e a tutte quelle simili che si possono ricavare in modo analogo moltiplicando per degli ulteriori coefficienti, ne esistono di realmente differenti ? E se invece considerassimo un altro polinomio - diciamo ad esempio $q(x) = 2x^{14} - 7$ - cosa saremmo in grado di affermare ? Cosa ci assicurerebbe di poter infine giungere anche per $q(x)$ ad una decomposizione di questo stesso tipo ?

In estrema sintesi, ciò che vogliamo arrivare a mettere in luce in queste note è che l'insieme dei polinomi gode in definitiva di molte proprietà simili a quelle che sappiamo essere valide per i numeri interi. Più precisamente i suoi elementi possono sempre essere fattorizzati in modo essenzialmente unico come prodotti di potenze di certi elementi fondamentali, vale a dire dei "polinomi irriducibili". La fattorizzazione - proprio come nel caso della fattorizzazione in $\mathbb{Z}$ - risulterà unica a meno dell'ordine dei fattori e della moltiplicazione per degli "elementi invertibili".
Cominciamo a fissare qualche notazione. Per indicare il generico polinomio

$$f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n,$$

spesso utilizzeremo il simbolo di *sommatoria*

$$f(x) = \sum_{i=0}^{n} a_i x^i.$$

Denoteremo poi rispettivamente con $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ e $\mathbb{R}[x]$ gli insiemi dei polinomi a coefficienti interi, razionali e reali:

$$\mathbb{Z}[x] = \{\sum_{i=0}^{n} a_i x^i \ \mid \ a_i \in \mathbb{Z}\},$$

$$\mathbb{Q}[x] = \{\sum_{i=0}^{n} a_i x^i \ \mid \ a_i \in \mathbb{Q}\},$$

$$\mathbb{R}[x] = \{\sum_{i=0}^{n} a_i x^i \ \mid \ a_i \in \mathbb{R}\}.$$

Più in generale denoteremo con

$$\mathbf{D}[x] = \{\sum_{i=0}^{n} a_i x^i \ \mid \ a_i \in \mathbf{D}\},$$

l'insieme dei polinomi a coefficienti in $\mathbf{D}$ quando non sarà necessario specificare se $\mathbf{D} = \mathbb{Z},\ \mathbb{Q}$ o $\mathbb{R}$.
Come vedremo, una circostanza che determinerà qualche differenza abbastanza importante fra le proprietà di $\mathbb{Z}[x]$ e quelle di $\mathbb{Q}[x]$ e $\mathbb{R}[x]$, è dovuta al fatto che in $\mathbb{Z}$ ci sono solo due elementi *invertibili*: $+1$ e -1. Invece, in $\mathbb{Q}$ e in $\mathbb{R}$ tutti gli elementi diversi da zero sono invertibili. In generale, se

$\mathbf{D} = \mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$ l'insieme degli elementi invertibili di $\mathbf{D}$ sarà denotato con il simbolo $\mathbf{D}^\times$:

$$\mathbf{D}^\times = \{x \in \mathbf{D} \ \mid \ \exists y \in \mathbf{D} \mid x \cdot y = 1\}.$$

Osserviamo ora che l'insieme dei polinomi $\mathbf{D}[x]$ è dotato evidentemente di due operazioni interne: vale a dire *la somma e il prodotto*. Un'altra operazione - questa volta esterna - usuale quando si ha a che fare con i polinomi è la cosiddetta *sostituzione*. Fissato comunque un numero $c \in \mathbf{D}$ risulta definita una funzione

$$S_c : \mathbf{D}[x] \to \mathbf{D}$$

che al generico polinomio $f(x)$ associa il suo *valore in c*: $S_c(f(x)) = f(c)$. Nella prossima sezione vedremo però che per comprendere meglio la struttura dell'insieme dei polinomi è indispensabile studiare un'ulteriore operazione: *la divisione*.

2 Grado e divisione con resto

In questa prima sezione introduciamo due strumenti basilari: il concetto di grado di un polinomio e l'algoritmo di divisione con resto. Per cominciare diamo però una serie di definizioni che ci saranno utili nel corso di questa trattazione.

2.1 Definizione. Dati due polinomi $a(x), b(x) \in \mathbf{D}[x]$ diremo che $a(x)$ *divide* $b(x)$ - in simboli $a(x) \mid b(x)$ - se esiste $c(x) \in \mathbf{D}[x]$ tale che

$$a(x) \cdot c(x) = b(x).$$

2.2 Definizione. Un polinomio $f(x) \in \mathbf{D}[x]$ è detto *invertibile in* $\mathbf{D}[x]$ se $f(x) \mid 1$.

2.3 Definizione. Un polinomio $f(x) \in \mathbf{D}[x]$ si dice *irriducibile* se in ogni sua fattorizzazione $f = g \cdot h$ almeno uno fra g e h è un elemento invertibile in $\mathbf{D}[x]$.

2.4 Definizione. Consideriamo il monomio non nullo $a \cdot x^k \in \mathbf{D}[x]$: definiamo il suo *grado* come l'intero non negativo k. Più in generale, il grado del polinomio $f(x) = \sum_{i=0}^{n} a_i x^i$, con $a_n \neq 0$, è n. Il grado di un polinomio

f viene denotato con il simbolo[1] $\deg(f)$. Chiaramente, un polinomio non nullo f ha grado zero se e soltanto se è un polinomio costante $f = a_0 = a_0x^0$. Per delle ragioni tecniche è opportuno definire il grado del polinomio (identicamente) nullo come $-\infty$. In simboli: $\deg(0) := -\infty$. Si adottano inoltre le seguenti convenzioni: $-\infty < n$ e $-\infty + n = -\infty$, $\forall n \in \mathbb{Z}$.

2.5 Lemma. Siano $f, g \in \mathbf{D}[x]$ due polinomi.

- $\deg(-f) = \deg(f)$;
- $\deg(f+g) \leq \max(\deg(f), \deg(g))$;
- $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Dimostrazione. Per esercizio, facendo attenzione al polinomio nullo. □

Avendo a disposizione la nozione di grado non è difficile dimostrare i seguenti risultati.

2.6 Esercizio. Utilizzando il Lemma precedente dimostra che

- gli invertibili in $\mathbf{D}[x]$ sono esattamente i polinomi costanti che sono invertibili in $\mathbf{D}$;
- se $c \in \mathbf{D}$ e c è irriducibile in $\mathbf{D}$ allora il polinomio costante $c \in \mathbf{D}[x]$ è irriducibile in $\mathbf{D}[x]$;
- ogni polinomio di grado 1 il cui coefficiente direttore è invertibile in $\mathbf{D}$ è irriducibile.

Parliamo ora della divisione con resto. Stabilire l'esistenza e l'unicità del quoziente e del resto nella divisione fra polinomi è un costituirà un passo cruciale per il nostro programma di esplorazione delle analogie fra i polinomi e i numeri interi. Come vedremo è da tale risultato che discenderanno le proprietà di fattorizzazione. Sottolineiamo inoltre che esso ci permette di fornire un esempio niente affatto banale di dimostrazione per induzione.

2.7 Teorema. Siano

$$f(x) = \sum_{i=0}^{n} a_i x^i, \quad g(x) = \sum_{j=0}^{m} b_j x^j$$

due polinomi di $\mathbf{D}[x]$ tali che $b_m \in \mathbf{D}^\times$. Allora esistono e sono unici due polinomi $q(x), r(x) \in \mathbf{D}[x]$ tali che

$$f(x) = q(x) \cdot g(x) + r(x), \quad \text{e} \quad \deg(r) < \deg(g).$$

[1] Derivato dalla parola inglese "degree", che appunto significa grado.

Dimostrazione. Se $\deg(f) < \deg(g)$, possiamo prendere $q = 0$ e $r = f$.

Se invece $\deg(f) \geq \deg(g)$, sia allora $f(x) = \sum_{i=0}^{n} a_i x^i$, $g(x) = \sum_{j=0}^{m} b_j x^j$, con $a_n \neq 0$ e $b_m \in \mathbf{D}^\times$, $n \geq m \geq 0$. Procederemo per induzione su $n = \deg(f)$. Se $n = 0$, allora $m = 0$, $f = a_0$ e $g = b_0$. Si può dunque scegliere $q = a_0 \cdot b_0^{-1}$ e $r = 0$, ottenendo infatti $\deg(r) < \deg(g)$ e $q \cdot g + r = (a_0 b_0^{-1}) b_0 = a_0 = f$.

Assumiamo ora che la parte del teorema che riguarda l'esistenza sia vera per i polinomi di grado minore di $n = \deg(f)$. Un calcolo immediato mostra che il polinomio $(a_n b_m^{-1} x^{n-m}) \cdot g$ ha grado n e coefficiente di grado massimo a_n. Quindi

$$f - (a_n b_m^{-1} x^{n-m}) \cdot g = (a_n x^n + \cdots + a_0) - (a_n x^n + \cdots + a_n b_m^{-1} b_0 x^{n-m})$$

è un polinomio di grado minore di n. L'ipotesi induttiva assicura allora che esistono dei polinomi q' e r tali che

$$f - (a_n b_m^{-1} x^{n-m}) \cdot g = q'g + r \quad \text{e} \quad \deg(r) < \deg(g).$$

Possiamo allora porre $q = (a_n b_m^{-1} x^{n-m}) + q'$, ottenendo

$$f = (a_n b_m^{-1} x^{n-m}) \cdot g + q'g + r = q \cdot g + r.$$

Passiamo ora a provare la parte del teorema che riguarda l'unicità. Supponiamo che sia $f = q_1 \cdot g + r_1$ e $f = q_2 \cdot g + r_2$, con $\deg(r_1) < \deg(g)$ e $\deg(r_2) < \deg(g)$. L'uguaglianza $q_1 \cdot g + r_1 = q_2 \cdot g + r_2$ implica che

$$(q_1 - q_2) \cdot g = r_2 - r_1.$$

Il Lemma 2.5 assicura allora che

$$\deg(q_1 - q_2) + \deg(g) = \deg(r_2 - r_1) \leq \max(\deg(r_2), \deg(r_1)) < \deg(g).$$

Pertanto necessariamente $\deg(q_1 - q_2) = -\infty = \deg(r_2 - r_1)$. In altri termini $q_1 - q_2 = 0$ e $r_1 - r_2 = 0$. □

2.8 Corollario. (*Teorema del resto.*) Sia $f \in \mathbf{D}[x]$ un polinomio. Per ogni $c \in \mathbf{D}$, esiste un unico polinomio $q \in \mathbf{D}(x)$ tale che

$$f(x) = q(x) \cdot (x - c) + f(c).$$

Dimostrazione. Se $f = 0$, allora $q = 0$. Se invece $f \neq 0$, possiamo usare il Teorema 2.7 e concludere che esistono e sono unici due polinomi $q(x)$ e $r(x)$ in $\mathbf{D}[x]$ tali che $f(x) = q(x) \cdot (x - c) + r(x)$ con $\deg(r) < \deg(x - c) = 1$. Pertanto $r(x)$ è un polinomio costante $r(x) = r_0$ (eventualmente nullo). Ora, ovviamente risulta

$$f(c) = q(c) \cdot (c - c) + r_0 = r_0.$$

□

Fattorizzazione unica in $\mathbb{Q}[x]$ e $\mathbb{R}[x]$ e massimo comun divisore

Il Teorema 2.7 ha delle conseguenze importanti. Per cominciare, esso implica che la struttura di $\mathbb{Q}[x]$ e di $\mathbb{R}[x]$ hanno delle analogie molto strette con quella di $\mathbb{Z}$. Esso ci assicura infatti che - similmente a quanto capita in $\mathbb{Z}$ - si può effettuare la divisione fra due qualsivoglia elementi in $\mathbb{Q}[x]$ o $\mathbb{R}[x]$ (purché il secondo non sia nullo) trovando un resto di grado inferiore a quello del divisore. Non è difficile allora, a partire da tale proprietà, vedere che ogni polinomio in $\mathbb{Q}[x]$ o in $\mathbb{R}[x]$ si può *fattorizzare* come prodotto di un numero finito di fattori irriducibili (o "primi"). Inoltre tale fattorizzazione risulterà necessariamente unica a meno dell'ordine dei fattori e della moltiplicazione per eventuali elementi invertibili.

Un'altra conseguenza notevole del Teorema 2.7 consiste nel fatto che esso consente di applicare il cosiddetto *algoritmo euclideo* delle divisioni successive per determinare il massimo comune divisore fra due polinomi in $\mathbb{Q}[x]$ e in $\mathbb{R}[x]$. Per completezza, richiamiamo brevemente tale procedura. Dati due polinomi a e b con $b \neq 0$, applicando iterativamente il Teorema 2.7 avremo

$$\begin{aligned}
a &= q_0 b + r_1, \text{ con } \deg(r_1) < \deg(b);\\
b &= q_1 r_1 + r_2, \text{ con } \deg(r_2) < \deg(r_1);\\
r_1 &= q_2 r_2 + r_3, \text{ con } \deg(r_3) < \deg(r_2);\\
&\vdots\\
r_n &= q_{n+1} r_{n+1} + r_{n+2}, \text{ con } \deg(r_{n+2}) < \deg(r_{n+1});\\
&\vdots
\end{aligned}$$

Ponendo se necessario $r_0 = b$, il massimo comun divisore di a e b, in simboli $\mathrm{MCD}(a, b)$, risulta essere r_k se k è il minimo intero tale che $r_{k+1} = 0$. Un tale

k dovendo esistere necessariamente visto che i gradi formano una sequenza decrescente di interi. Vale la pena sottolineare che dall'algoritmo euclideo segue poi anche il cosiddetto *teorema di Bezout*. Dati cioè $a, b \in \mathbb{Q}[x]$, ovvero $a, b \in \mathbb{R}[x]$, esistono dei polinomi $c, d \in \mathbb{Q}[x]$ o, rispettivamente, $c, d \in \mathbb{R}[x]$ tali che

$$\mathrm{MCD}(a, b) = a \cdot c + b \cdot d.$$

2.9 Osservazione. Il massimo comun divisore $\mathrm{MCD}(a(x), b(x))$ di due polinomi $a(x)$ e $b(x)$ è definito a meno di invertibili in $\mathbb{Q}$ (ovvero in $\mathbb{R}$). Ovvero, la scrittura $\mathrm{MCD}(a(x), b(x)) = c(x)$ equivale a qualunque scrittura del tipo $\mathrm{MCD}(a(x), b(x)) = d \cdot c(x)$ per ogni $d \in \mathbb{Q}^\times$ ($\mathbb{R}^\times$, rispettivamente).

2.10 Esercizio. Per definizione, dati due polinomi $a(x), b(x) \in \mathbf{D}[x]$ un polinomio $d(x) \in \mathbf{D}[x]$ è un massimo comun divisore di $a(x)$ e $b(x)$ se soddisfa le seguenti due proprietà:

- $d(x) \mid a(x) \ \wedge \ d(x) \mid b(x)$;
- $(c(x) \mid a(x) \ \wedge \ c(x) \mid b(x)) \implies c(x) \mid d(x)$.

Dimostra che se $\mathbf{D} = \mathbb{Q}$ o $\mathbb{R}$ il MCD fra due polinomi si ottiene effettivamente applicando l'algoritmo euclideo delle divisoni successive.

2.11 Esempio. Siano $a(x) = 2x^3 - x + 1$ e $b(x) = 3x^2 + 4x + 1$. Dividendo $a(x)$ per $b(x)$ si ottiene

$$\begin{array}{r|l}
2x^3 - x + 1 & 3x^2 + 4x + 1 \\
\hline
2x^3 + \frac{8}{3}x^2 + \frac{2}{3}x & \frac{2}{3}x - \frac{8}{9} \\
\hline
-\frac{8}{3}x^2 - \frac{5}{3}x + 1 & \\
-\frac{8}{3}x^2 - \frac{32}{9}x - \frac{8}{9} & \\
\hline
\frac{17}{9}x + \frac{17}{9} &
\end{array}$$

Ovvero $2x^3 - x + 1 = (3x^2 + 4x + 1) \cdot (\frac{2}{3}x - \frac{8}{9}) + (\frac{17}{9}x + \frac{17}{9})$. Ora, dividendo ancora $b(x)$ per il resto che abbiamo trovato, avremo

$$\begin{array}{r|l}
3x^2 + 4x + 1 & \frac{17}{9}x + \frac{17}{9} \\
\hline
3x^2 + 3x & \frac{27}{17}x + \frac{9}{17} \\
\hline
x + 1 & \\
x + 1 & \\
\hline
0 &
\end{array}$$

Ne segue che $\mathrm{MCD}(a(x), b(x)) = \frac{17}{9}x + \frac{17}{9}$. Per l'Osservazione 2.9, si ha anche $\mathrm{MCD}(a(x), b(x)) = x + 1$.

3 Radici

3.1 Definizione. Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbf{D}[x]$ e sia $c \in \mathbb{R}$ un numero tale che $f(c) = 0$, allora c è detta *radice* di f.

3.2 Teorema. (*Teorema di Ruffini.*) Sia $f \in \mathbf{D}[x]$ un polinomio. Allora $c \in \mathbf{D}$ è una radice di f se e soltanto se $(x - c)$ divide f.

Dimostrazione. Per il Corollario 2.8, possiamo scrivere

$$f(x) = q(x) \cdot (x - c) + f(c),$$

con un polinomio $q(x)$ univocamente determinato.

Ora, se $(x-c)$ divide $f(x)$, per definizione si avrà che $f(x) = (x-c)\cdot h(x)$, per un opportuno polinomio $h(x) \in \mathbf{D}[x]$. Quindi

$$f(c) = (h(x) - q(x)) \cdot (x - c).$$

Se $h(x) = q(x)$, allora $f(c) = 0$ e c è radice di f. Se invece $h(x) \neq q(x)$ si ottiene un assurdo confrontando i gradi.

Viceversa, se $f(c) = 0$, $f(x) = q(x) \cdot (x - c)$, e dunque $(x - c)$ divide $f(x)$. □

3.3 Teorema. Sia $f(x) \in \mathbf{D}[x]$ un polinomio di grado n. Allora $f(x)$ ha al più n radici distinte.

Dimostrazione. Siano $c_1, c_2, \ldots, c_m$ le radici distinte di f. Per il Teorema 3.2, avremo

$$f(x) = q_1(x) \cdot (x - c_1),$$

e quindi

$$0 = f(c_2) = q_1(c_2)(c_2 - c_1).$$

Visto che $c_2 - c_1 \neq 0$, necessariamente $q_1(c_2) = 0$, cioè $(x - c_2)$ divide q_1. Potremo allora scrivere

$$f(x) = q_2(x) \cdot (x - c_2) \cdot (x - c_1).$$

Iterando questo procedimento, si ottiene che se $c_1, c_2, \ldots, c_m$ sono radici distinte di $f(x)$ allora $g_m(x) = (x - c_m) \cdots (x - c_2) \cdot (x - c_1)$ divide $f(x)$. Ma $\deg(g_m) = m$, e quindi, per il Lemma 2.5 $m \leq n$. □

3.4 Proposizione. Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ un polinomio di grado n. Se $u = \frac{c}{d}$ è una radice razionale di $f(x)$ (con c e d interi e coprimi) allora c divide a_0 e d divide a_n.

Dimostrazione. Se u è radice allora vale le relazione

$$a_0 d^n + \sum_{i=1}^{n-1} a_i c^i d^{n-i} + a_n c^n = 0,$$

dalla quale discende da un lato che

$$a_0 d^n = c\Big(\sum_{i=1}^{n} -a_i c^{i-1} d^{n-i}\Big),$$

e dall'altro che

$$-a_n c^n = \Big(\sum_{i=0}^{n-1} a_i c^i d^{n-i-1}\Big) d.$$

Conseguentemente, visto che c e d sono coprimi, c deve dividere a_0 e d deve dividere a_n. □

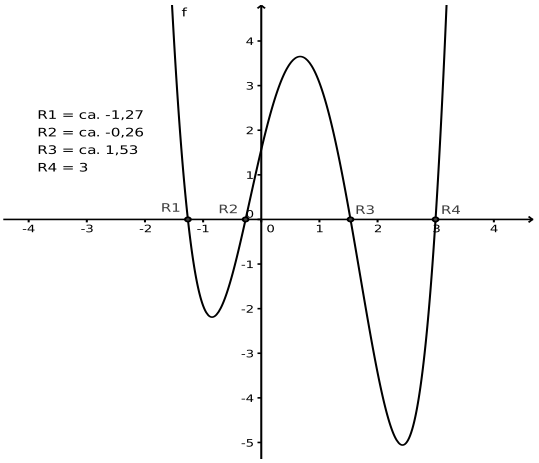
3.5 Esempio. È bene osservare che la precedente proposizione può essere applicata anche per trovare le radici razionali di un polinomio a coefficienti razionali. Per esempio consideriamo il polinomio $f(x) = x^4 - 3x^3 - 2x^2 + \frac{11}{2}x + \frac{3}{2} \in \mathbb{Q}[x]$. Evidentemente tale polinomio ha le stesse radici di $2f = 2x^4 - 6x^3 - 4x^2 + 11x + 3 \in \mathbb{Z}[x]$. La proposizione 3.4 ci assicura che le possibili radici razionali di $3f$ sono da trovarsi in $\{\pm 1, \pm 3, \pm\frac{1}{2}, \pm\frac{3}{2}\}$. Procedendo per tentativi si mostra che l'unica radice razionale è in effetti 3. Come curiosità presentiamo il grafico di $f(x)$.

3.6 Esercizio. Cosa si può dire riguardo alle radici razionali di $f(x) = x^4 - 2x^3 - 7x^2 - \frac{11}{3}x - \frac{4}{3}$?

Radici multiple

Parliamo ora di "radici multiple". Consideriamo un polinomio $f \in \mathbf{D}[x]$, e sia c una sua radice. L'uso ripetuto del Teorema 3.2 mostra che esiste un intero positivo massimo $0 < m \leq \deg(f)$ tale che

$$f(x) = (x - c)^m \cdot g(x),$$



dove $g(x) \in \mathbf{D}[x]$ e $(x - c)$ non divide $g(x)$ (ovvero $g(c) \neq 0$). L'intero m viene allora detto *molteplicità della radice* c. Se $m = 1$ allora c viene detta *radice semplice*. Se invece $m > 1$, si parlerà di c come di una *radice multipla*.

Per caratterizzare i polinomi che hanno radici multiple ci serve introdurre un nuovo strumento.

3.7 Lemma. Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbf{D}[x]$. Sia

$$f'(x) = \sum_{i=1}^{n} i \cdot a_i x^{i-1} = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + n a_n x^{n-1}.$$

Allora $\forall f, g \in \mathbf{D}[x]$ e $\forall c \in \mathbf{D}$

(i) $(c \cdot f)' = c \cdot f'$;

(ii) $(f + g)' = f' + g'$;

(iii) $(f \cdot g)' = f' \cdot g + f \cdot g'$;

(iv) $(g^h)' = h \cdot g^{h-1} \cdot g', \quad (h \in \mathbb{N})$.

Dimostrazione. Per esercizio. □

Il polinomio f' viene detto *derivata formale* di f. Il termine formale sta a sottolineare il fatto che la definizione di f' non coinvolge il concetto di limite.

3.8 Teorema. Sia $f(x) \in \mathbb{R}[x]$.

(i) Se c è una radice di f, c è multipla se e solo se $f'(c) = 0$;

(ii) se f è coprimo con f' allora f non ha radici multiple;

(iii) se f è irriducibile di grado positivo, allora f non ha radici multiple.

Dimostrazione.

(i) Se c ha molteplicità m allora $f(x) = (x-c)^m \cdot g(x)$ con $g(c) \neq 0$. Usando il Lemma 3.7

$$f'(x) = m(x-c)^{m-1}g(x) + (x-c)^m g'(x).$$

Ora, se $m > 1$, allora $f'(c) = 0$. Se $m = 1$ $f'(c) = g(c) \neq 0$.

(ii) dall'ipotesi segue che esistono[2] dei polinomi $a, b \in \mathbb{R}[x]$ tali che

$$a(x) \cdot f(x) + b(x) \cdot f'(x) = 1.$$

Quindi se c è una radice multipla $1 = a(c) \cdot f(c) + b(c) \cdot f'(c) = 0$, il che è evidentemente assurdo.

(iii) Se f è irriducibile di grado positivo, f e f' sono sicuramente coprimi, perché $0 \leq \deg(f') < \deg(f)$.

□

4 Invertibili e Irriducibili

Il passo successivo consiste ora nel cercare di comprendere meglio quali sono gli elementi irriducibili in $\mathbf{D}[x]$. Si tratta in generale di una questione abbastanza delicata. Cominciamo a considerare il caso di $\mathbb{Z}[x]$ e quello di $\mathbb{Q}[x]$. Più specificamente cominciamo a osservare quanto segue.

Non sorprende che un polinomio sia irriducibile in $\mathbb{Z}[x]$ senza esserlo una volta considerato in un insieme di polinomi più grande: per esempio si consideri $x^2-2 = (x-\sqrt{2})\cdot(x+\sqrt{2})$. D'altra parte occorre fare attenzione al fatto che si può presentare anche la situazione opposta. Cioè, un polinomio può ad esempio essere irriducibile in $\mathbb{Q}[x]$ senza esserlo in $\mathbb{Z}[x]$: per esempio $2x+2$ ha la fattorizzazione $2 \cdot (x+1)$ che è una vera fattorizzazione solo in $\mathbb{Z}[x]$ (2 è invertibile in $\mathbb{Q}$).

Lo scopo di questa sezione consiste in effetti nel dimostrare che l'unica differenza fra le fattorizzazioni in $\mathbb{Z}[x]$ e quelle in $\mathbb{Q}[x]$ è in effetti quella a cui si è accennato nella precedente osservazione.

[2] Per il Teorema di Bezout e per l'Osservazione 2.9.

4.1 Definizione. Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ un polinomio non nullo. Il massimo comun divisore dei coefficienti $a_1, a_2, \ldots, a_n$, viene detto *contenuto di* f e denotato con il simbolo $C(f)$. Il polinomio f si dirà poi *primitivo* quando $C(f) = 1$.

4.2 Lemma. Siano $f(x) \in \mathbb{Z}[x]$, $f(x) \neq 0$ e $a \in \mathbb{Z}^*$, allora

$$C(a \cdot f) = a \cdot C(f)$$

e

$$f = C(f) \cdot f_1,$$

dove f_1 è un polinomio primitivo.

Dimostrazione. Per esercizio. □

4.3 Teorema. Siano $f(x), g(x) \in \mathbb{Z}[x]$ due polinomi non nulli. Allora $C(f \cdot g) = C(f) \cdot C(g)$. In particolare il prodotto di due polinomi primitivi è un polinomio primitivo.

Dimostrazione. Sappiamo che $f = C(f) \cdot f_1$ e che $g = C(g) \cdot g_1$ con f_1 e g_1 primitivi. Quindi

$$C(f \cdot g) = C(C(f) \cdot f_1 \cdot C(g) \cdot g_1) = C(f) \cdot C(g) \cdot C(f_1 \cdot g_1).$$

Quindi è sufficiente dimostrare la seconda parte del teorema. Procediamo "per assurdo". Siano dunque $f_1 = \sum_{i=0}^{n} a_i x^i$ e $g_1 = \sum_{i=0}^{m} b_j x^j$ due polinomi primitivi, e supponiamo che il loro prodotto

$$f_1 \cdot g_1 = \sum_{k=0}^{n+m} c_k x^k, \quad \text{con } c_k = \sum_{i+j=k} a_i \cdot b_j$$

non sia primitivo. Esiste allora un numero primo p che divide tutti i coefficienti c_k. Visto che f_1 e g_1 sono primitivi, esisteranno degli interi minimi s e t tali che

$$p \mid a_i \quad \text{per } i < s, \quad \text{e } p \nmid a_s,$$
$$p \mid b_j \quad \text{per } j < t, \quad \text{e } p \nmid b_t.$$

Ora, però sappiamo che

$$p \mid c_{s+t} = a_0 b_{s+t} + \cdots + a_{s-1} b_{t+1} + a_s b_t + a_{s+1} b_{t-1} + \cdots a_{s+t} b_0,$$

e quindi p deve dividere anche $a_s b_t$, e questo è assurdo perché $p \nmid a_s$ e $p \nmid b_t$. □

4.4 Teorema.("*Lemma di Gauss.*") Sia $f(x) \in \mathbb{Z}[x]$ un polinomio primitivo di grado positivo. Allora f è irriducibile in $\mathbb{Z}[x]$ se e solo se lo è in $\mathbb{Q}[x]$.

Dimostrazione. Supponiamo che f sia irriducibile in $\mathbb{Z}[x]$ ma che esistano dei polinomi di grado positivo $g, h \in \mathbb{Q}[x]$ tali che $f = g \cdot h$. Avremo allora

$$g(x) = \sum_{i=0}^{n} \frac{a_i}{b_i} x^i, \quad h(x) = \sum_{j=0}^{m} \frac{c_j}{d_j} x^j,$$

con $a_i, c_j \in \mathbb{Z}$ e $b_i, d_j \in \mathbb{Z}^*$. Consideriamo il prodotto di tutti i denominatori $b = b_0 \cdot b_1 \cdots b_n$ e il polinomio $\widetilde{g} = b \cdot g \in \mathbb{Z}[x]$. Se poniamo $a = C(\widetilde{g})$, avremo che $\widetilde{g} = a \cdot g_1$ per un certo polinomio primitivo g_1. Dunque abbiamo che

$$g = \frac{a}{b} \cdot g_1.$$

Analogamente avremo che

$$h = \frac{c}{d} \cdot h_1.$$

con c e d interi, h_1 primitivo e $\deg h = \deg h_1$. Quindi

$$f = g \cdot h = \frac{ac}{bd} f_1 \cdot h_1,$$

cioè $bd \cdot f = ac \cdot g_1 h_1$. Ma ora sia f (per ipotesi) che $f_1 \cdot h_1$ (per il Teorema 4.3) sono primitivi, quindi

$$bd = \pm C(bd \cdot f) = \pm C(ac \cdot h_1 \cdot g_1) = \pm ac.$$

Pertanto $f = \pm g_1 \cdot h_1$, cioè f è riducibile in $\mathbb{Z}[x]$.

Viceversa se f è irriducibile in $\mathbb{Q}[x]$, ma $f = g \cdot h$, con $g, h \in \mathbb{Z}[x]$, allora visto che in $\mathbb{Q}[x]$ le fattorizzazioni sono uniche, almeno uno fra g e h, diciamo g, deve essere costante. Quindi, visto che f è primitivo, $1 = C(f) = g \cdot C(h)$, cioè $g = \pm 1$ e f è irriducibile in $\mathbb{Z}[x]$. □

4.5 Osservazione. Anche se non lo dimostriamo in dettaglio, vale la pena sottolineare che i risultati visti finora sarebbero sufficienti a dimostrare che anche in $\mathbb{Z}[x]$ ogni polinomio può essere fattorizzato in modo unico come prodotto di polinomi irriducibili di $\mathbb{Z}[x]$. In estrema sintesi, il risultato segue dall'esistenza e unicità delle fattorizzazioni in $\mathbb{Q}[x]$ e in $\mathbb{Z}$ e dal Lemma di Gauss.

Criterio di Eisenstein

In generale non è facile capire se un dato polinomio sia irriducibile. Per quanto riguarda i polinomi a coefficienti interi, uno dei pochi strumenti disponibili è dato dal seguente criterio.

4.6 Teorema.(“*Criterio di Eisenstein.*”) Sia $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$ un polinomio di grado positivo e sia p un numero primo tale che

$$p \nmid a_n; \quad p \mid a_i \text{ per } i = 0, 1, \ldots, n-1; \quad p^2 \nmid a_0,$$

allora f è irriducibile in $\mathbb{Q}[x]$. Se f è primitivo allora è irriducibile anche in $\mathbb{Z}[x]$.

Dimostrazione. Cominciamo con lo scrivere come al solito $f = C(f) \cdot f_1$, con f_1 primitivo (in particolare $f_1 = f$ se f è primitivo). Vogliamo dimostrare che f_1 è irriducibile in $\mathbb{Q}[x]$, ovvero, equivalentemente (per il Teorema 4.4), in $\mathbb{Z}[x]$.

Supponiamo per assurdo che f_1 sia fattorizzabile come $g \cdot h$, con

$$g(x) = b_r x^r + \ldots b_0 \in \mathbb{Z}[x], \ \deg(g) = r \geq 1;$$

e

$$h(x) = c_s x^s + \ldots c_0 \in \mathbb{Z}[x], \ \deg(h) = s \geq 1.$$

Ora, il numero primo p non divide $C(f)$ perché $p \nmid a_n$, quindi i coefficienti di $f_1(x) = \sum_{i=0}^{n} \widehat{a}_i x^i$ soddisfano le stesse proprietà di divisibilità rispetto a p di quelli di f. Visto che p divide dunque $\widehat{a}_0 = b_0 \cdot c_0$, p dividerà sicuramente almeno uno fra b_0 e c_0, diciamo $p \mid b_0$. Visto che però $p^2 \nmid \widehat{a}_0$, c_0 non può essere divisibile per p. Osserviamo ora che non tutti i coefficienti di g possono essere divisibili per p, altrimenti f_1 non sarebbe primitivo. Sia dunque k il minimo intero positivo tale che

$$p \mid b_i \text{ per } i < k, \text{ e } p \nmid b_k.$$

Visto che $1 \leq k \leq r < n$, per ipotesi $p \mid \widehat{a}_k = b_0 c_k + b_1 c_{k-1} + \ldots b_{k-1} c_1 + b_k c_0$. Ma allora necessariamente $p \mid b_k c_0$, che è assurdo perché p non divide né b_k né c_0. Siamo quindi giunti ad una contraddizione e pertanto possiamo concludere che f_1 deve essere irriducibile in $\mathbb{Q}[x]$ e in $\mathbb{Z}[x]$. □

4.7 Esempio. Il polinomio $f(x) = 3x^6 - 8x^5 + 4x^2 + 10$ è sicuramente irriducibile in $\mathbb{Q}[x]$ e in $\mathbb{Z}[x]$. Basta usare il criterio di Eisenstein con $p = 2$.

4.8 Esempio. Tutti i polinomi del tipo $x^n \pm p$ (n intero positivo, p primo) sono irriducibili in $\mathbb{Z}[x]$. (Pertanto, per ogni n esistono infiniti polinomi di grado n irriducibili in $\mathbb{Z}[x]$.)

5 Lagrange e Kronecker

A priori non è chiaro se dato un polinomio si riesca a trovare la sua fattorizzazione in fattori irriducibili. Lo scopo di questa sezione è di illustrare una possibile procedura che, per quanto laboriosa, permette di fattorizzare in un numero finito di passi qualunque polinomio a coefficienti interi (o razionali). L'interesse principale di questa procedura è per così dire di carattere "teorico", nel senso che fornisce una risposta positiva alla questione della fattorizzabilità. D'altra parte, la quantità di calcoli e verifiche da fare cresce in modo talmente rapido al crescere del grado, da rendere di scarsa rilevanza pratica la procedura.

1. *Interpolazione di Lagrange.*

   Se $c_0, c_1, \ldots c_n$ sono numeri razionali distinti e $d_0, d_1, \ldots d_n$ sono numeri razionali, allora esiste al più un polinomio $f(x) \in \mathbb{Q}[x]$ di grado n tale che $f(c_i) = d_i$ per $i = 0, \ldots, n$.

   Il precedente enunciato vale immutato se si sostituisce $\mathbb{Q}$ con $\mathbb{R}$.

   In effetti, se poniamo

   $$g_i(x) = (x - c_0) \cdots (x - c_{i-1})(x - c_{i+1}) \cdots (x - c_n) \quad (i = 0, 1, \ldots, n)$$

   vediamo che $g_i(c_j) = 0$ se $i \neq j$ e quindi il polinomio

   $$f(x) = \sum_{i=0}^{n} \frac{g_i(x)}{g_i(c_i)} d_i$$

   è l'unico in $\mathbb{Q}[x]$ (o in $\mathbb{R}[x]$) di grado al più n tale che $f(c_i) = d_i$, $\forall i$.

2. *Metodo di Kronecker.* Sia ora $f(x) \in \mathbb{Z}[x]$ di grado n. Per quanto appena detto, fissati $n+1$ interi distinti $c_0, c_1, \ldots c_n$, il polinomio $f(x)$ è univocamente determinato dai valori $f(c_0)$, $f(c_1)$, $\ldots$, $f(c_n)$. Quello che segue è il cosiddetto metodo di Kronecker per determinare tutti i fattori irriducibili di $f(x)$ in $\mathbb{Z}[x]$.

(a) È sufficiente trovare i fattori di grado al più $n/2$.

(b) I polinomi $g \in \mathbb{Z}[x]$ che dividono f, vanno cercati fra i polinomi tali che $g(c)$ divide $f(c)$ ($c \in \mathbb{Z}$).

(c) Sia m il massimo intero non superiore a $n/2$. Si fissano gli interi distinti $c_0, c_1, \ldots, c_m$ e si calcolano i valori $f(c_0), f(c_1), \ldots, f(c_m)$. Si scelgono degli interi $d_0, d_1, \ldots, d_m$ in modo che d_i divide $f(c_i)$. Si determina il solo polinomio (a coefficienti razionali) di grado al più m tale che $g(c_i) = d_i$ con l'interpolazione di Lagrange.

(d) Si controlla se il polinomio $g(x) \in \mathbb{Q}[x]$ appena determinato divide $f(x)$. Se non lo divide, si fa una nuova scelta per i divisori $d_0, d_1, \ldots, d_m$. Si noti che c'è solo un numero finito di scelte possibili. Se invece $f = g \cdot h$, allora si ripete il procedimento su g e su h.

(e) Dopo un numero finito di passi tutti i fattori irriducibili di f in $\mathbb{Q}[x]$ saranno stati trovati. Se $g \in \mathbb{Q}[x]$ è uno di tali fattori (di grado positivo) ed r è il prodotto dei denominatori dei coefficienti di g allora $r \cdot g \in \mathbb{Z}[x]$. Se C è il contenuto di $r \cdot g$ allora $g_1 = (r/C)g$ è un fattore irriducibile di f in $\mathbb{Z}[x]$.

Esempi

Fattorizziamo il polinomio $f(x) = x^5 + x + 1$. Visto che il grado è 5 cerchiamo un possibile fattore g di f che abbia grado 2. Se scegliamo $c_0 = 0$, $c_1 = 1$ e $c_2 = -1$, troviamo i valori $f(c_0) = 1$, $f(c_1) = 3$ e $f(c_2) = -1$. Per trovare i possibili fattori g con l'interpolazione di Lagrange avremo al più sedici possibilità, relative ai seguenti possibili valori di $d_0 \in \{1, -1\}$, $d_1 \in \{1, -1, 3, -3\}$ e $d_2 \in \{1, -1\}$. Dai calcoli risulta che la terna $d_0 = 1$, $d_1 = 3$, $d_2 = 1$ ci fornisce il polinomio

$$\frac{(x-1)\cdot(x+1)}{(-1)\cdot(1)} \cdot 1 + \frac{(x)\cdot(x+1)}{(1)\cdot(2)} \cdot 3 + \frac{(x)\cdot(x-1)}{(1)\cdot(2)} \cdot 1$$

troviamo cioè $g(x) = x^2 + x + 1$. Effettuando la divisione troviamo che effettivamente questo $g(x)$ divide il nostro polinomio. Risulta infatti che $x^5 + x + 1 = (x^2 + x + 1) \cdot (x^3 - x^2 + 1)$. Ora, il polinomio $g(x)$ è sicuramente irriducibile perché le sole possibili radici razionali sarebbero 1 e -1, ma $g(1) = g(-1) = 1$. Analogamente si verifica che anche $x^3 - x^2 + 1$ è irriducibile, e quindi la fattorizzazione di $f(x)$ è completa.

Il polinomio $f(x) = x^5 - x + 1$ è invece irriducibile. Scegliendo ancora $c_0 = 0$, $c_1 = 1$ e $c_2 = -1$, troviamo i valori $f(c_0) = 1$, $f(c_1) = 1$ e $f(c_2) = 1$. Procedendo come sopra si troveranno al più otto possibili fattori g relativi ai possibili valori di $d_0, d_1, d_2 \in \{1, -1\}$. In effetti un calcolo diretto mostra che, a meno del segno, i fattori possibili di grado positivo risultano essere $2x^2 - 1$, $x^2 - x - 1$ e $x^2 + x - 1$. Ma nessuno di essi divide $f(x)$.

6 Radici complesse

Consideriamo l'insieme dei *numeri complessi*

$$\mathbb{C} = \{a + i \cdot b \mid a, b \in \mathbb{R}\}$$

dove il simbolo i - la cosiddetta *unità immaginaria* - soddisfa la seguente relazione fondamentale

$$i^2 = -1.$$

Nell'insieme $\mathbb{C}$ è molto semplice svolgere qualunque calcolo: basta utilizzare le solite proprietà delle operazioni in $\mathbb{R}$ (commutativa, associativa, distributiva, etc.) e ricordarsi che $i^2 = -1$. Ad esempio

$$(a + ib) + (c + id) = (a + c) + i(b + d);$$

$$(a + ib) \cdot (c + id) = ac + iad + ibc + i^2bd = (ac - bd) + i(ad + bc);$$

$$\frac{1}{a + ib} = \frac{a - ib}{(a - ib)(a + ib)} = \frac{a - ib}{a^2 + b^2}.$$

L'insieme $\mathbb{C}$ munito delle operazioni di somma e moltiplicazione, risulta in definitiva avere una struttura analoga a quella di $\mathbb{R}$ (o $\mathbb{Q}$): è quello che in matematica si dice *campo*. In particolare tutti i risultati che nelle sezioni precedenti abbiamo visto valere in $\mathbb{R}[x]$ si possono estendere senza difficoltà a $\mathbb{C}[x]$.
La proprietà che però rende estremamente interessanti i numeri complessi è mostrata nel seguente enunciato.

6.1 Teorema.(“*Teorema fondamentale dell'algebra.*”) Sia $f(x) \in \mathbb{C}[x]$ un polinomio di grado n, allora $f(x)$ ammette esattamente n radici in $\mathbb{C}$, contate con la relativa molteplicità.

Esistono numerose dimostrazioni differenti di questo importante risultato, ma nessuna completamente elementare. Inoltre nessuna fra queste dimostrazioni è puramente algebrica. In effetti, anche quelle più semplici si basano almeno in qualche punto su argomentazioni di natura analitica (occorre quanto meno utilizzare il fatto che i polinomi sono "funzioni continue" e il Teorema di Weierstrass) ed esulano comunque dai limiti di questa trattazione.

Ci accontenteremo invece di vedere una semplice conseguenza del Teorema 6.1 al riguardo dei polinomi a coefficienti reali. Premettiamo un'ultima definizione.

6.2 Definizione. Il *complesso coniugato* del numero complesso $z = a + ib \in \mathbb{C}$ è il numero complesso $\overline{z} = a - ib$.

6.3 Lemma. Siano $z_1, z_2 \in \mathbb{C}$ due numeri complessi. Allora

- $\overline{\overline{z_1}} = z_1$;
- $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$;
- $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$;
- $\overline{z_1} = z_1$ se e solo se $z_1 \in \mathbb{R}$;
- $z_1 + \overline{z_1} \in \mathbb{R}$;
- $z_1 \cdot \overline{z_1} \in \mathbb{R}$.

Dimostrazione. Per esercizio. □

6.4 Proposizione. Sia $f(x) \in \mathbb{R}[x]$. Allora $c \in \mathbb{C}$ è radice di $f(x)$ se e solo anche $\overline{c}$ lo è. Inoltre c e $\overline{c}$ hanno la stessa molteplicità. In particolare un polinomio a coefficienti reali ha necessariamente un numero pari (eventualmente nullo) di radici complesse non reali.

Dimostrazione. Sia $f(x) = \sum_{i=0}^{n} a_i x^i$ con $a_i \in \mathbb{R}$. Allora, usando il Lemma 6.3,

$$f(\overline{c}) = \sum_{i=0}^{n} a_i \overline{c}^i = \overline{\sum_{i=0}^{n} a_i c^i} = \overline{f(c)}.$$

Qundi c è radice di f se e solo se lo è $\overline{c}$.
Ora se c è radice complessa non reale, potremo scrivere

$$f(x) = (x - c) \cdot (x - \overline{c}) \cdot g(x),$$

per un certo polinomio $g(x)$ che a priori appartiene a $\mathbb{C}[x]$. Osserviamo però che

$$(x-c)\cdot(x-\overline{c}) = x^2 - (c+\overline{c})x + c\cdot\overline{c} \in \mathbb{R}[x],$$

e quindi anche $g(x) \in \mathbb{R}[x]$. Ripetendo per $g(x)$ lo stesso procedimento fatto per $f(x)$ si ottiene la tesi. □

6.5 Corollario. Sia $f(x) \in \mathbb{R}[x]$ di grado dispari. Allora $f(x)$ ammette almeno una radice reale.

Dimostrazione. Infatti f avrà un numero dispari di radici complesse per il Teorema 6.1, ma fra queste solo un numero pari potranno essere non reali. □

6.6 Esercizio. Sia $f(x) \in \mathbb{R}[x]$ irriducibile. Dimostra che $f(x)$ ha grado al più 2.

7 Appendice: Metodo risolutivo per equazioni di terzo grado

Si definisce equazione di terzo grado o cubica un'equazione polinomiale in cui il grado massimo dell'incognita sia di. Nella forma canonica, si presenta come

$$ax^3 + bx^2 + cx + d = 0.$$

La prima soluzione generale dell'equazione di terzo grado si deve al matematico italiano Scipione del Ferro, ma lo scopritore per così dire ufficiale è Girolamo Cardano, dal quale la formula risolutiva prende il nome.

Il metodo risolutivo che intendiamo illustrare conduce alla risoluzione di un'equazione di terzo grado riconducendola, tramite una multipla sostituzione delle variabili, ad una particolare equazione quadratica. Il procedimento è il seguente. Si considera un'equazione del tipo

$$x^3 + ax^2 + bx + c = 0,$$

e la si trasforma inizialmente in un'equazione sempre cubica ma più semplice:

$$y^3 + py + q = 0.$$

Per essere più precisi, per ottenere l'equazione in y ridotta (priva di termini di secondo grado) si opera la sostituzione

$$x = y - \frac{a}{3}$$

che conduce ad un'equazione del tipo menzionato con

$$\begin{cases} p = -\frac{a^2}{3} + b \\ q = \frac{2a^3}{27} - \frac{ab}{3} + c \end{cases}.$$

Vale la pena di ricordare che le equazioni risolte da del Ferro erano esattamente quelle di tipo ridotto.

A questo punto si effettua un'ulteriore sostituzione: si pone

$$y = z - \frac{p}{3z}$$

e, con alcuni calcoli, e moltiplicando per z^3, si porta l'equazione in questa forma

$$z^6 + qz^3 - \frac{p^3}{27} = 0,$$

che è un'equazione trinomia in z^3, riconducibile ad una quadratica

$$t^2 + qt - \frac{p^3}{27} = 0,$$

effettuando la sostituzione $z^3 = t$. Il risultato sarà dunque dato da

$$t_{1,2} = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}.$$

Si osservi che, per delle ben note proprietà delle soluzioni di un'equazione quadratica, si ha

$$\begin{cases} t_1 + t_2 = -q, \\ t_1 \cdot t_2 = -\left(\frac{p}{3}\right)^3. \end{cases}$$

Definiamo ora

$$u = \sqrt[3]{t_1} = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

$$v = \sqrt[3]{t_2} = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

e supponiamo che il numero $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$, ovvero il radicando della radice quadrata all'interno della cubica, sia un numero maggiore od uguale a 0. Si

può verificare che il numero reale $u+v$ è una soluzione dell'equazione cubica ridotta. Infatti

$$\begin{aligned}(u+v)^3+p(u+v)+q &= u^3+v^3+3uv(u+v)+p(u+v)+q\\ &= t_1+t_2+\left(3\left(-\frac{p}{3}\right)+p\right)(u+v)+q\\ &= -q+(-p+p)(u+v)+q=0.\end{aligned}$$

Ora, se α è una soluzione reale dell'equazione cubica ridotta, possiamo senz'altro scrivere

$$\begin{aligned}y^3+py+q &= (y-\alpha)\left(y^2+\alpha y+\alpha^2+p\right)\\ &= (y-\alpha)\left(y+\frac{\alpha}{2}-\sqrt{-\frac{3\alpha^2}{4}-p}\right)\left(y+\frac{\alpha}{2}+\sqrt{-\frac{3\alpha^2}{4}-p}\right).\end{aligned}$$

Dunque, essendo $u+v$ una soluzione reale dell'equazione cubica ridotta, abbiamo che le altre due soluzioni sono complesse

$$\begin{cases}y_1=u+v\\ y_2=-\frac{u+v}{2}+i\cdot\frac{u-v}{2}\cdot\sqrt{3}\\ y_3=-\frac{u+v}{2}-i\cdot\frac{u-v}{2}\cdot\sqrt{3}\end{cases}$$

dove i è l'unità immaginaria.
Infatti

$$\begin{aligned}\sqrt{-\frac{3(u+v)^2}{4}-p} &= \sqrt{-\frac{3}{4}\left(u^2+2uv+v^2\right)-p}\\ &= \sqrt{-\frac{3}{4}\left(u^2+2uv+v^2\right)+3uv}\\ &= \sqrt{-\frac{3}{4}\left(u^2+v^2\right)+\frac{3}{2}uv}\\ &= \sqrt{-\frac{3}{4}\left(u^2-2uv+v^2\right)}\\ &= \sqrt{-\frac{3}{4}(u-v)^2}\\ &= \pm\, i\cdot\frac{u-v}{2}\cdot\sqrt{3}.\end{aligned}$$

In particolare il risultato del procedimento è la *formula di Cardano*

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

che fornisce la soluzione reale dell'equazione cubica ridotta. Da cui, la soluzione reale dell'equazione cubica è

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \frac{a}{3}.$$

Più in generale, le soluzioni dell'equazione di terzo grado sono date da

$$x_i = y_i - \frac{a}{3}$$

con $i = 1, 2, 3$.

Si noti che, come evidenziato nel procedimento risolutivo, non possono esistere tre soluzioni reali se $\Delta \geq 0$.

7.1 Problemi relativi alle soluzioni

Si consideri l'equazione

$$x^3 = 15x + 4.$$

Avremo dunque

$$\begin{cases} p = -15 \\ q = -4 \end{cases}$$

da cui $\Delta = \frac{16}{4} + -\left(\frac{15}{3}\right)^3 = 4 - 125 = -121 < 0$. Dunque le due soluzioni complesse dell'equazione quadratica associata sono

$$t_{1,2} = 2 \pm i \cdot 11,$$

e la formula risolutiva porterebbe a considerare numeri non reali. Tuttavia, si trova che una soluzione è $x = 4$, e di conseguenza altre due soluzioni sono ottenibili risolvendo l'equazione $x^2 + 4x + 1 = 0$. Quindi l'equazione ha tre radici reali, ovvero si ha la fattorizzazione

$$x^3 - 15x - 4 = (x - 4) \cdot (x + 2 - \sqrt{3}) \cdot (x + 2 + \sqrt{3}).$$

7.2 Il caso $\Delta < 0$

Se $\Delta < 0$, l'equazione cubica ridotta ha tre soluzioni reali

$$\begin{cases} y_1 = 2\sqrt{-\frac{p}{3}}\cos\frac{\theta}{3} \\ y_2 = 2\sqrt{-\frac{p}{3}}\cos\frac{\theta+2\pi}{3} \\ y_3 = 2\sqrt{-\frac{p}{3}}\cos\frac{\theta+4\pi}{3} \end{cases}$$

dove

$$\begin{cases} \theta = \arctan(\frac{-2\sqrt{-\Delta}}{q}) \text{ se } -\frac{q}{2} > 0, \\ \theta = \pi + \arctan(\frac{-2\sqrt{-\Delta}}{q}) \text{ se } -\frac{q}{2} < 0, \end{cases}$$

Riferimenti bibliografici

[1] M. Artin, *Algebra*. Collana "Programma di Matematica, Fisica, Elettronica". Bollati Boringhieri, 1997.

[2] I. N. Herstein, *Algebra*. Collana "Nuova Biblioteca di Cultura Scientifica". Editori Riuniti, 2003.

[3] G. Piacentini Cattaneo, *Algebra. Un approccio algoritmico*. Collana di Matematica. Testi e manuali. Zanichelli, 1996.