1

Capitolo W15
prontuario: algebra [1]

Contenuti delle sezioni

10 pagine

W15 a. strutture algebriche c

W15a.01 operazioni algebriche

L'algebra odierna fa riferimento alle strutture, sistemi costituiti da uno o più insiemi detti terreni e da una o più operazioni tra elementi dei terreni (soprattutto operazioni binarie) e da un sistema di assiomi che li riguardano (soprattutto uguaglianze).

Data due strutture S e T, si dice che T è più ricca di S sse possiede più terreni e/o più operazioni e un sistema di assiomi più esteso; si dice che T è più stringente di S sse hanno analoghi terreni e operazioni e gli assiomi della T implicano quelli della S.

Siano a, b, c e d elementi di una struttura munita delle operazioni somma e prodotto $\mathsf{S} = \langle S, \oplus, \odot, ...\rangle$ potrebbe trattarsi di un semianello o di un suo arricchimento [a04].

proprietà commutative $\quad a \oplus b = b \oplus a \quad , \quad a \odot b = b \odot a$

proprietà associative $\quad (a \oplus b) \oplus c = a \oplus (b \oplus c) \quad , \quad (a \odot b) \odot c = a \odot (b \odot c)$

proprietà distributiva $\quad a \odot (b \oplus c) = a \odot b \oplus a \cdot c \quad , \quad (a \oplus b) \odot c = a \odot c \oplus b \odot c$

quindi $\quad (a \oplus b) \odot (c \oplus d) = a \odot c \oplus a \odot d \oplus b \odot c \oplus b \odot d$

La struttura S abbia la somma commutativa e sia munita anche di un elemento neutro per la somma denotato da 0, cioè di un elemento 0 tale che $\forall x \in \mathsf{S} \;\colon\; x \oplus 0 = 0 \oplus x = x$; la presenza di 0 induce a chiedersi se si ha l'operazione univoca passaggio da un elemento x al suo opposto $\ominus x$, elemento tale che $x \oplus (\ominus x) = 0$; essa è una involuzione, cioè $\forall x \in \mathsf{S} \;\colon\; \ominus(\ominus x) = x$.

Si può allora definire la differenza tra due elementi della struttura ponendo $a \ominus b \;:=\; a \oplus (\ominus b)$; la differenza si dice operazione inversa della somma

Per il passaggio all'opposto si ha $(a \ominus b) \oplus b = b \oplus (a \ominus b) = a \quad , \quad a \ominus (\ominus b) = a \oplus (\oplus b) = a \oplus b$

Per la relazione tra prodotto e zero si ha

$a \cdot 0 = 0 \cdot a = 0 \quad , \quad (\oplus a) \odot (+b) = a \odot b = (\ominus a) \odot (\ominus b) \quad , \quad (\oplus a) \odot (\ominus b) = \ominus a \odot b = \ominus(a \odot b)$

La S sia dotata anche di un elemento neutro bilatero per il prodotto che scriviamo 1, cioè sia $\forall x \;\colon\; x \odot 1 = x = 1 \odot x$;
nelle strutture costituite da trasformazioni per l'elemento neutro spesso si usa il termine **identità**

La S privata dello 0 sia munita anche dell'inversione rispetto al prodotto, operazione che trasforma x nell'elemento x^{-1} tale che $x \odot (x^{-1}) = (x^{-1}) \odot x = 1$; anche questa operazione è una involuzione, cioè $x \odot (x^{-1}) = (x^{-1}) \odot x = 1$.

Su questa struttura si può definire la divisione, operazione binaria definibile solo se il secondo operando è diverso da 0: $\quad \dfrac{a}{b} \;:=\; a \cdot (b^{-1})$

Si usano anche le notazioni $a/b \;:=\; a : b \;:=\; aob$; la divisione si dice operazione inversa del prodotto.

Proprietà $\quad \dfrac{a}{b} \cdot b \;=\; b \cdot \dfrac{a}{b} \;=\; a$

$$\frac{a}{b} \pm \frac{c}{d} \;=\; \frac{a\,d \pm b\,c}{b\,d} \;\;,\;\; \frac{a}{b} \odot \frac{c}{d} \;=\; \frac{a\,c}{b\,d} \;\;,\;\; \frac{\frac{a}{b}}{\frac{c}{d}} \;=\; \frac{a}{b} \odot \frac{\mathrm{d}}{c} \;=\; \frac{a\,d}{b\,c} \;\;,\;\; \frac{-a}{-b} \;=\; \frac{a}{b} \;\;,\;\; \frac{-a}{b} \;=\; \frac{a}{-b} \;=\; -\frac{a}{b}$$

W15a.02 potenze e radici

potenze

Siano h, m ed n numeri interi e sia k un intero positivo.

$$a^0 \;:=\; 1 \quad , \quad a^1 \;:=\; a \quad , \quad a^n \;:=\; a^{n-1}\cdot a$$
$$a^{m+n} = a^m \cdot a^n \quad , \quad a^{-n} \;:=\; \frac{1}{a^n} \quad , \quad (a\cdot b)^n = a^n\cdot b^n$$
$$\frac{a^m}{a^n} \;=\; a^{m-n} \quad , \quad (a^m)^n \;=\; a^{m\,n}$$
$$(a\cdot b)^n \;=\; a^n\cdot b^n \quad , \quad \left(\frac{a}{b}\right)^n \;=\; \frac{a^n}{b^n} \quad , \quad (-a)^{2\,h} = a^{2\,h} \quad , \quad (-a)^{2\,h+1} = -a^{2\,h+1}$$

radici

Consideriamo n e k interi positivi, m intero, a ed r reali nonnegativi.
$\sqrt[n]{a} = r \iff r^n = a$ si usa anche la scrittura $a^{1/n} \;:=\; \sqrt[n]{a}$

$$a^{\frac{m}{n}} \;:=\; \sqrt[n]{a^m} \;=\; \left(\sqrt[n]{a}\right)^m \quad , \quad \sqrt[n]{a\,b} \;=\; \sqrt[n]{a}\cdot\sqrt[n]{b} \quad , \quad \sqrt[n]{\frac{a}{b}} \;=\; \frac{\sqrt[n]{a}}{\sqrt[n]{b}}$$
$$\sqrt[n]{a^n\,b} \;=\; a\;\sqrt[n]{b} \quad , \quad \sqrt[n]{a}\cdot\sqrt[k]{a} \;=\; \sqrt[n\,k]{a^{n+k}}$$

W15a.03 specie di strutture algebriche

magma o **gruppoide** struttura costituita da un insieme terreno e da un'operazione binaria che in genere si chiama prodotto e che scriviamo $\odot$; presentata formalmente con una notazione della forma $\langle M, \odot\rangle$

quasigruppo magma $\langle Q, \odot\rangle$ nel quale per ogni $a, b \in Q$ sono univocamente definiti gli elementi c e d tali che $a \odot c = b$ e $d \odot a = b$; in parole povere magma nel quale sono sempre definite una divisione a sinistra e una a destra. Un magma è un quasigruppo sse la sua tavola di composizione è un quadrato latino [D63].

loop quasigruppo unifero, cioè semigruppo che possiede un elemento neutro bilatero, una identità.

semigruppo magma con $\odot$ associativo
Esempi: $\langle \mathbb{P}, +\rangle$, $\langle \mathbb{P}, \cdot\rangle$, razionali positivi muniti di somma o di prodotto, reali positivi muniti di somma o di prodotto

monoide semigruppo unifero; formalmente presentato con una notazione della forma $\langle M, \odot, e\rangle$.
esempi: numeri naturali, razionali nonnegativi, reali nonnegativi muniti di somma; numeri positivi, razionali positivi, reali positivi muniti di prodotto; booleano di un insieme munito di unione; insieme delle relazioni entro un insieme munito del prodotto di composizione; classi di resti

gruppo monoide con tutti gli elementi dotati di inverso; forma tipica $\langle G, \odot, e, {}^{-1}\rangle$
Esempi: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ munito di somma; $\mathbb{Q}_+$, $\mathbb{Q}_{nz}$, $\mathbb{R}_+$, $\mathbb{R}_{nz}$ muniti di prodotto; insieme delle permutazioni di un insieme munito del prodotto di composizione; simmetrie di un poligono regolare o di altro tipo di figura dotata di qualche regolarità; insieme delle classi di resti modulo p con p numero primo munito del prodotto modulo p

semianello struttura munita di due operazioni presentabile con una notazione come $\langle S, \oplus, \odot\rangle$, con $\langle S, \oplus\rangle$ semigruppo abeliano, $\langle S, \odot\rangle$ semigruppo con $\odot$ distributivo su $\oplus$
Esempi: insieme delle matrici quadrate di dato profilo e classi di resti per un generico intero positivo

anello semianello con l'operazione somma $\oplus$ commutativa.

anello unifero semianello con l'operazione somma $\oplus$ che è operazione di gruppo abeliano e l'operazione prodotto $\odot$ dotata di unità.
Esempi: insieme degli interi, dei razionali, dei reali, dei complessi muniti di somma e prodotto usuali.

campo anello tale che, tolto lo 0, il suo prodotto costituisce operazione di gruppo abeliano
Esempi: insieme dei razionali, dei reali, dei complessi, delle classi di resti per un numero intero primo.

semireticolo inferiore struttura munita di una operazione binaria chiamata incontro (*meet*) o massimo dei minoranti denotata spesso con $\wedge$, la quale è associativa, commutativa e idempotente
Esempi: controarborescenza.

semireticolo superiore struttura munita di una operazione binaria chiamata giunzione (*join*) o minimo dei maggioranti, denotata spesso con $\vee$, la quale è associativa, commutativa e idempotente.

reticolo struttura presentabile come $\langle L, \wedge, \vee\rangle$ ove $\wedge$ e $\vee$ sono due operazioni binarie che chiamiamo, risp., giunzione e incontro tali che Ł$, \wedge\rangle$ è un semireticolo inferiore e $\langle L, \vee\rangle$ è un semireticolo superiore; inoltre si chiede che valgano le due leggi di assorbimento:

$$\forall a, b \in L \;\colon\; a \vee (a \wedge b \;=\; a \;,\; a \wedge (a \vee b \;=\; a \;.$$

Esempi: collezione dei sottoinsiemi di un dato insieme munito delle operazioni di intersezione e unione; insieme delle partizioni di un insieme ordinato per raffinamento; $\mathbb{N} \times \mathbb{N}$ ordinato parzialmemte sulle due componenti

reticolo di Boole reticolo sul cui terreno è definita una involuzione $\sim$ tale che $\sim (a \wedge b) = (\sim a) \vee (\sim b)$ e $\sim (a \vee b) = (\sim a) \wedge (\sim b)$
Esempi: reticolo dei sottoinsiemi di un dato insieme munito della complementazione

modulo sinistro su anello se $\boldsymbol{R} = \langle R, +, 0, -, \cdot, 1\rangle$ è un anello, è una struttura della forma $\left\langle\, \boldsymbol{R}, \oplus, \ominus, \mathbf{0}, {\scriptscriptstyle\perp} \,\right\rangle$ tale che $r{\scriptscriptstyle\perp}(\mathbf{v} + \mathbf{w}) = r{\scriptscriptstyle\perp}\mathbf{v} + r{\scriptscriptstyle\perp}\mathbf{w}$, $(r + s){\scriptscriptstyle\perp}\mathbf{v} = r{\scriptscriptstyle\perp}\mathbf{v} + s{\scriptscriptstyle\perp}\mathbf{v}$, $r \cdot s){\scriptscriptstyle\perp}\mathbf{v} = r{\scriptscriptstyle\perp}(s{\scriptscriptstyle\perp}\mathbf{v})$ e $1{\scriptscriptstyle\perp}\mathbf{v} = \mathbf{v}$
Esempi: trasformazioni lineari

modulo destro su anello struttura simile al modulo sinistro nella quale la moltiplicazione vede gli elementi dell'anello posti a destra

spazio vettoriale o **spazio lineare** modulo su un anello arricchibile a campo $\boldsymbol{F} = \left\langle F, +, 0, -, \cdot, ^{-1}\right\rangle$ e tale che $r{\scriptscriptstyle\perp}\mathbf{v} = \mathbf{v}{\scriptscriptstyle\perp}r$
Esempi: insieme delle funzioni da un dato dominio a valori su un campo munito di tale campo e delle estensioni funzionali della somma di vettori e della moltiplicazione per elementi del campo; in particolare per ogni d intero positivo, l'insieme delle d-uple di elementi del campo; più in particolare gli insiemi delle d-uple di numeri razionali, reali o complessi

algebra su campo spazio vettoriale munito di un prodotto distributivo sulla somma
Esempi: insieme delle matrici a entrate su un campo; insieme delle trasformazioni lineari tra due spazi vettoriali; insieme dei polinomi in una o più variabii su un dato campo; insieme dei polinomi di grado inferiore a d su un dato campo; insieme delle serie formali su un dato campo

morfismi

Consideriamo due strutture algebriche che si possono considerare magmi $\left\langle S_1, \odot_1, ...\right\rangle$ ed $\left\langle S_2, \odot_2, ...\right\rangle$. Una funzione $m \in \left\lceil\, S_1 \longrightarrow S_2 \,\right\rceil$ si dice:

omomorfismo sse mantiene la struttura algebrica, cioè sse $\forall x_1, x_2 \in \mathsf{dom}(m) \;\colon\; x_1 \odot_2 x_2 = m(x_1 \odot_1 x_2)$;

endomorfismo sse $\mathsf{cod}(m) \subseteq S_1$

epimorfismo sse è suriettiva, cioè sse $\mathsf{cod}(m) = S_2$;

monomorfismo sse è funzione iniettiva, cioè sse $m \in \left\lceil\, \mathsf{dom}(m) \;\triangleleft\!\!\longrightarrow\!\!\triangleright\; \mathsf{cod}(m) \,\right\rceil$;

isomorfismo sse è funzione biiettiva, cioè sse $m \in \left\lceil\, S_1 \triangleleft\!\!\longrightarrow\!\!\triangleright S_2 \,\right\rceil$;

automorfismo sse è una permutazione e $S_1 = S_2$, cioè sse m è endomorfismo e isomorfismo.

Nei casi precedenti le due strutture si dicono, risp., strutture omomorfe, endomorfe, epimorfe, monomorfe, isomorfe e automorfe.

W15 b. polinomi ed equazioni polinomiali

W15b.01 polinomi

Sia n un intero nonnegativo e consideriamo una sequenza $\mathsf{a} = \langle a_n, a_{n-1}, ..., a_2, a_1, a_0 \rangle$ elementi di un semianello $\mathbb{K}$ con $a_n \neq 0$; in particolare interessano i casi $\mathbb{K} = \mathbb{R}$, $\mathbb{K} = \mathbb{C}$ e $\mathbb{K} = \mathbb{F}_p$ per p numero primo.

Si dice polinomio nella z variabile in $\mathbb{K}$ l'espressione

$$\overline{P}(z) = b_n\, z^n + b_{n-1}\, z^{n-1} + \cdots + b_2\, z^2 + b_1\, z + b_0 = \sum_{j=0}^{n} b_j\, z^j$$

La sequenza a si dice sequenza dei coefficienti del polinomio $\overline{P}(z)$ ed n grado del polinomio; tale intero naturale si denota con $deg(\overline{P})$. Affermare che $deg(\overline{P}) = n$ equivale a enunciare $a_n \neq 0$.

Un polinomio si può interpretare come funzione polinomiale del genere $\lceil \mathbb{K} \longmapsto \mathbb{K} \rceil$.

I polinomi di grado 0 corrispondono alle funzioni costanti entro $\mathbb{K}$; i polinomi di grado 1, della forma $a_1\, z + a_0$ corrispondono alle funzioni lineari entro $\mathbb{K}$; quelli di grado 2, $a_2\, z^2 + a_1\, z + a_0$, alle cosiddette funzioni quadratiche; quelli di grado 3 alle funzioni cubiche; quelli di grado 4 alle cosiddette funzioni quartiche; quelli di grado 5 alle cosiddette quintiche e così via.
Particolarmente utili sono le funzioni polinomiali su reali.

Conviene includere tra i polinomi su $\mathbb{K}$ anche il polinomio nullo $P(z) \equiv 0$ e assegnargli il grado -1.

Spesso le considerazioni sui polinomi e sulle funzioni polinomiali si semplificano identificando le due nozioni.

Sui polinomi si definiscono varie operazioni algebriche. Per questo consideriamo i generici polinomi $\overline{P}(z)$ e $\overline{Q}(z) = \sum_{j=r}^{0} q_k\, z^k$ e, quando serve, identifichiamo il polinomio di quest'ultima forma con l'espressione $\sum_{j=R}^{0} q_k\, z^k$ con $R > r$, intendendo sia $q_k = 0$ per $k = r+1, ..., R$.

somma di polinomi $\overline{P}(z) + \overline{Q}(z) \;:=\; \sum_{k=M}^{0} (a_k + q_k)\, z^k$.

Chiaramente la soma di polinomi è commutativa e associativa.
Inoltre $deg(\overline{P}) \neq deg(\overline{Q}) \implies deg(Pol + \overline{Q}) = \max(deg(\overline{P}), deg(\overline{Q})$, mentre $deg(\overline{P}) = deg(\overline{Q}) \implies deg(Pol + \overline{Q}) \leq \max(deg(\overline{P}), deg(\overline{Q})$.

moltiplicazione di un polinomio per un elemento f di $\mathbb{K}$ $f \cdot \overline{P}(z) \;:=\; \sum_{j=n}^{0} (f\, a_j)\, z^j$.

Se $f \neq 0$, allora $deg\Big(f\, \overline{P}(z)\Big) = deg(\overline{P})$; altrimenti $deg\Big(0\, \overline{P}(z)\Big) = -1$.

La moltiplicazione per -1 porta al polinomio opposto: $(-1)\, \overline{P}(z) = -\, \overline{P}(z) = \sum_{j=n}^{0} (-a_j)\, z^j$ avente lo stesso grado di $\overline{P}(z)$.

prodotto di polinomi: se i due polinomi fattori non sono nulli $P(z) \cdot Q(z) \;:=\; \sum_{jn}^{0} \sum_{h=q}^{0} (a_j\, q_h)\, z^{j+h}$ e $deg(P(z) \cdot Q(z) = deg(P) + deg(Q)$.
Invece il prodotto con un fattore nullo porta al polinomio nullo.

Il prodotto di polinomi è commutativo e associativo.

La divisione conduce a entità più generali, le cosiddette funzioni razionali della forma $\dfrac{\overline{P}(z)}{\overline{Q}(z)}$.

W15b.02 equazioni polinomiali

Una equazione polinomiale di grado $n \in \mathbb{N}$ ha la forma

(1) $$\overline{P}(z) \;=\; a_n\, z^n + a_{n-1}\, z^{n-1} + \cdots + a_2\, z^2 + a_1\, z + a_0 \;=\; 0\ .$$

Qui supponiamo che $\forall i = 0, 1, 2, ..., n \;\vdots\; z \in \mathbb{C}$ e che l'incognita z appartenga a $\mathbb{C}$.

L'insieme delle soluzioni della (1) coincide con l'insieme delle soluzioni della corrispondente **equazione monica**, equazione caratterizzata dal polinomio monico

(2) $$P(z) \;:=\; \frac{\overline{P}(z)}{a_n} = x^n + b_{n-1}\, x^{n-1} + \cdots + b_2\, b^2 + b_1\, z + b_n = 0\ .$$

La (2) si ricava subito dalla (1) e in genere si tratta un po' più facilmente.

Un numero complesso s si dice **zero del polinomio** o **radice del polinomio** $P(z)$ di molteplicità $m \in \mathbb{P}$ sse si può scrivere $P(z) = (z-s)^m\, Q(z)$ con $Q(z)$ polinomio (nonnullo) tale che $Q(s) \neq 0$. Il polinomio $Q(z)$ si ottiene come $\dfrac{P(z)}{(z-s)^m}$ mediante l'algoritmo euclideo.

Se s è radice di molteplicità m di $P(z)$, allora s è radice di molteplicità $m-1$ della $P'(z) = 0$.

$P(z)$ presenta il fattore $(z-s)^m$ sse $P(s) = P'(s) = \cdots = P^{(m-1)}(s) = 0$.
In particolare $P(z)$ presenta il fattore $z - s$ sse $P(s) = 0$.

teorema fondamentale dell'algebra L'equazione algebrica $\overline{P}(x) = 0$ di grado n presenta esattamente n radici nel campo complesso, quando ciascuna radice di molteplicità m si conta m volte. Se le radici sono $s_1, s_2, ..., s_n$ si ha $\overline{P}(z) = a_n\,(z-s_1)\,(z-s_2)\,\cdots\,(z-s_n)$.

Ovviamente l'equazione di primo grado $a_1\, z + a_0 = 0$ ha l'unica soluzione $z = -\dfrac{a_0}{a_1}$.

Si trova che le equazioni dei gradi 2, 3 e 4 posseggono soluzioni date da espressioni generali nelle quali intervengono dei radicali nei coefficienti. Per gradi superiori, come dimostra il teorema di Ruffini-Abel, risulta impossibile trovare espressioni generali contenenti radicali per le soluzioni; si trovano soluzioni mediante radicali solo per equazioni particolari; di una generica equazione si possono ottenere solo soluzioni approssimate.

Con le notazioni precedenti si hanno i seguenti collegamenti polinomiali tra coefficienti e radici (**uguaglianze di Viéte**).

$$\begin{aligned}
s_1 + s_2 + \cdots + s_n &= -\frac{a_{n-1}}{a_n} \\
s_1\, s_2 + s_1\, s_3 + \cdots + s_{n-1}\, s_n &= \sum_{1\le i<j\le n} s_i\, s_j = \frac{a_{n-2}}{a_n} \\
s_1\, s_2\, s_3 + s_1\, s_2\, s_4 + \cdots + s_{n-2}\, s_{n-1}\, s_n &= \sum_{1\le i<j<k\le n} s_i\, s_j\, s_k = -\frac{a_{n-3}}{a_n} \\
&\cdots\cdots\cdots\cdots \\
s_1\, s_2\, \cdots\, s_n &= (-1)^n\, \frac{a_0}{a_n}
\end{aligned}$$

W15b.03 equazioni polinomiali con coefficienti reali

Consideriamo un polinomio reale $\overline{P}(x)$. Se s è una sua radice non reale, allora è radice anche il suo complesso coniugato s^*, ossia

$$\overline{P}(s) = 0 \implies \overline{P}(s^*) = 0 \ .$$

Quindi un polinomio reale possiede un numero pari di radici non reali e se s è una di queste presenta come fattore reale il binomio della forma $z^2 - 2\,\Re(s)\,z + (\Re(s)^2 + \Im(s)^2)$.

Quindi ogni polinomio reale si può fattorizzare mediante polinomi reali che possono essere solo di grado 1 e di grado 2; ossia a ogni polinomio reale monico si può dare la forma

$$P(z) \ = \ (x - s_1)^{\alpha_1} \cdots (x - s_v)^{\alpha_v}\,(x^2 + t_1\,x + u_1)^{\beta_1} \cdots (x^2 + t_w\,x + u_w)^{\beta_w} \ ,$$

dove $\alpha_1 + \cdots + \alpha_v + 2(\beta_1 + \cdots + \beta_w) \ = \ n$.
Dato che i fattori quadratici assumono solo valori positivi, un polinomio $\overline{P}(x)$ privo di radici reali (di grado pari) assume solo valori con il segno di a_n.
Dunque un polinomio reale di grado pari e con $\dfrac{a_0}{a_n} < 0$ possiede almeno due radici reali di segno opposto.

Se tutti gli a_j sono interi e se una radice è $s = \dfrac{s_n}{s_d}$ con s_n ed s_d coprimi, allora s_n divide b_0 e s_d divide b_n.

Vale la **regola dei segni di Cartesio**: il numero delle radici reali positive, tenuto conto delle molteplicità, è uguale al numero k dei cambiamenti di segno nella sequenza $\langle a_0, a_1, ..., a_n\rangle$ oppure è uguale a k diminuito di un intero positivo pari. Se tutte le radici sono reali il numero delle positive è k.

W15**b.04** **equazioni quadratiche**

Consideriamo sia l'equazione generale che l'equazione monica:

$$\overline{P}(x) \ = \ a\,x^2 + b\,x + c \ = \ 0 \qquad\qquad P(x) \ = \ x^2 + \beta\,x + \gamma \ = \ 0 \ .$$

Attraverso il cosiddetto "completamento del quadrato", cioè scrivendo $P(x) \ = \ \left(x + \frac{\beta}{2}\right)^2 - \left(\frac{\beta}{2}\right)^2 + \gamma$, per le soluzioni si ottengono, risp., le espressioni

$$x \ = \ \frac{-b \pm \sqrt{b^2 - 4\,a\,c}}{2\,a} \qquad\qquad x \ = \ -\frac{\beta}{2} \pm \sqrt{\left(\frac{\beta}{2}\right)^2 - \gamma}$$

L'espressione $b^2 - 4\,a\,c$ si dice discriminante dell'equazione $\overline{P}(x) = 0$.

– se $b^2 - 4\,a\,c > 0$ si hanno due radici reali diverse;
– se $b^2 - 4\,a\,c = 0$ si ha una radice reale di molteplicità 2;
– se $b^2 - 4\,a\,c < 0$ si hanno due radici complesse non reali coniugate diverse.

Denotiamo con x_1 e x_2 le due soluzioni della $\overline{P}(x) = 0$ ossia della $P(x) = 0$; abbiamo $P(x) = (x - x_1)(x - x_2) = 0$ e quindi $x_1 + x_2 = \beta$ e $x_1\,x_2 = \gamma$.

W15**b.05** **equazioni cubiche**

Consideriamo l'equazione monica $P(x) \ = \ x^3 + r\,x^2 + s\,x + t \ = \ 0$; essa con la sostituzione $y := x + \dfrac{r}{3}$ conduce alla equazione ridotta $y^3 + p\,y + q = 0$, ove $p := s - \dfrac{r^2}{3}$ e $q := \dfrac{2\,r^3}{27} - \dfrac{r\,s}{3} + t$.

Le soluzioni dell'equazione ridotta sono date dalle **formule di Cardano**:

$$\begin{aligned} y_1 &= u+v \\ y_2 &= \epsilon\, u + \eta\, v \\ y_3 &= \eta\, u + \epsilon\, v \end{aligned} \qquad \text{ove} \qquad \begin{aligned} u &:= \sqrt[3]{-\frac{q}{2}+\sqrt{D}} \\ u &:= \sqrt[3]{-\frac{q}{2}-\sqrt{D}} \end{aligned} \quad , \quad \begin{aligned} D &:= \left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2 \\ \epsilon &:= -\frac{1}{2} + \mathrm{i}\sqrt{\frac{3}{2}} \\ \eta &:= -\frac{1}{2} - \mathrm{i}\sqrt{\frac{3}{2}} \end{aligned}$$

La loro collocazione nel piano complesso dipende dal discriminante D:

- se $D > 0$ si ha una soluzione reale $x_1 = u + v + \frac{r}{3}$ e due soluzioni complesse coniugate $x_{2,3} = -\frac{u+v}{2} + \frac{r}{3} \pm \mathrm{i}\sqrt{\frac{3}{2}}\,(u-v)$;
- se $D = 0$ si ha una soluzione reale x_1 e una soluzione reale di molteplicità 2 $x_2 = x_3$, eccetto il caso $p = q = 0$ per il quale si ha una sola radice reale molteplicità 3;
- se $D < 0$ si hanno tre radici reali.

Nell'ultimo caso le formula di Cardano forniscono due soluzioni reali mediante espressioni contenenti immaginari. Si può rimanere nel campo reale servendosi di funzioni trigonometriche e iperboliche.

Introdotto $R := (\mathrm{sign}(q))\sqrt{\frac{|p|}{3}}$, si giunge alla seguente casistica

	$p < 0 \wedge D \le 0$	$p < 0 \wedge D > 0$	$p > 0$
	$\cos\phi = \frac{q}{2R^3}$	$\cosh\phi = \frac{q}{2R^3}$	$\sinh, \phi = \frac{q}{2R^3}$
$y_1 =$	$-2R\cos\frac{\phi}{3}$	$-2R\cosh\frac{\phi}{3}$	$-2R\sinh\frac{\phi}{3}$
$y_2 =$	$-2R\cos(\phi/3 + 4\pi/3)$	$R\cosh\left(\frac{\phi}{3}\right) - \mathrm{i}\sqrt{3}\,R\sinh\left(\frac{\phi}{3}\right)$	$R\sinh\left(\frac{\phi}{3}\right) - \mathrm{i}\sqrt{3}\,R\cosh\left(\frac{\phi}{3}\right)$
$y_3 =$	$-2R\cos(\phi/3 + 4\pi/3)$	$R\cosh\left(\frac{\phi}{3}\right) - \mathrm{i}\sqrt{3}\,R\sinh\left(\frac{\phi}{3}\right)$	$R\sinh\left(\frac{\phi}{3}\right) - \mathrm{i}\sqrt{3}\,R\cosh\left(\frac{\phi}{3}\right)$

W15b.06 equazioni quartiche

Consideriamo l'equazione $P(x) = a\,x^4 + b\,x^3 + c\,x^2 + d\,x + e = 0$; essa con la sostituzione $y := x + \frac{b}{4}$ conduce alla equazione ridotta $y^4 + p\,y^2 + q\,y + 0 + r = 0$, ove p, q ed r sono dati da espressioni algebriche nei coefficienti.

Le soluzioni di questa dipendono dalle soluzioni z_1, z_2 e z_3 della cosiddetta **risolvente cubica**:

$$z^3 + 2\,p\,z^2 + (p^2 - 4\,r)\,z - q^2 = 0$$

Se tutte le z_i sono reali positive la quartica possiede quattro soluzioni reali.

Se tutte le z_i sono reali, ma una è positiva e due negative, allora la quartica possiede di due coppie di soluzioni complesse coniugate.

Se una delle z_i è reale e due sono complesse coniugate, allora la quartica possiede due soluzioni reali e una coppia di soluzioni complesse coniugate.

Conosciute le z_i, le soluzioni della equazione quartica ridotta sono date da

$$\begin{aligned}
y_1 &= \frac{1}{2}\,(\sqrt{z_1}+\sqrt{z_2}+\sqrt{z_3})\\
y_2 &= \frac{1}{2}\,(\sqrt{z_1}-\sqrt{z_2}-\sqrt{z_3})\\
y_3 &= \frac{1}{2}\,(-\sqrt{z_1}+\sqrt{z_2}-\sqrt{z_3})\\
y_4 &= \frac{1}{2}\,(-\sqrt{z_1}-\sqrt{z_2}+\sqrt{z_3})
\end{aligned}$$

Quando in particolare $b = D = 0$ si ha la cosiddetta **equazione biquadratica** la quale equivale a una equazione quadratica nella incognita $v := x^2$, $a\,v^2 + c\,v + e \;=\; 0$; le soluzioni della biquadratica si ottengono quindi come radici quadrate delle soluzioni di quest'ultima.

Si giunge a soluzioni ricavabili da due equazioni quadratiche anche per le particolari equazioni quartiche i che nella forma monica $x^4 + r\,x^3 + s\,x^4 + t\,x + u \;=\; 0$ hanno coefficienti che soddisfano la relazione $r^2 + 8\,t \;=\; 4\,r\,s$. in tal caso si giunge all'equazione biquadratica

$$w^2 + \left(s - \frac{r^2}{4}\right) w + u \;=\; 0 \qquad \text{ove} \qquad w \;:=\; x^2 + \frac{r\,x}{2}\ .$$

Ciascuna delle soluzioni w_1 e w_2 di questa porta a un'equazione quadratica $x^2 + \dfrac{r}{2}\,x - w_i \;=\; 0$ e le loro soluzioni forniscono le radici della quartica ora in esame.

W15b.07 equazioni binomiche

Hanno la forma $z^n = c$ con c numero complesso.

In generale si ha una soluzione che si serve dell'espressione di c in coordinate polari, $c = r\,\mathsf{e}^{\mathsf{i}\,\theta}$: per $h = 0, 1, ..., n-1$ si può scrivere $z^n = c = r\,\mathsf{e}^{\mathsf{i}(\theta+2\,\pi\,h)}$ e quindi

$$z \;=\; \sqrt[n]{r}\,\mathsf{e}^{\mathsf{i}(\theta+2\,\pi\,h)/n} \;=\; \sqrt[n]{r}\left(\cos\,\frac{\theta+2\,\pi\,h}{n} + \mathsf{i}\,\sin\,\frac{\theta+2\,\pi\,h}{n}\right)$$

Nel piano complesso le n radici z_h per $h = 0, 1, 2, ..., n-1$ sono i vertici del poligono regolare di n lati con centro nell'origine, vertici sul circumcerchio di raggio $\sqrt[n]{r}$ e anomalia di z_0 pari a $\dfrac{\theta}{n}$.

In particolare l'equazione $z^2 = c$ definiti $x := \Re(z^2)$, $y := \Im(z^2)$ e $\rho := |z^2| = \sqrt{x^2+y^2}$, si trovano le radici

$$z \;=\; \pm\sqrt{x+\mathsf{i}\,y} = \begin{cases} \pm\left(\sqrt{\frac{\rho+x}{2}} + \mathsf{i}\sqrt{\frac{\rho-x}{2}}\right) & \text{se } y \geq 0\\ \pm\left(\sqrt{\frac{\rho+x}{2}} - \mathsf{i}\sqrt{\frac{\rho-x}{2}}\right) & \text{se } y \leq 0 \end{cases}$$

W15b.08 decomposizioni dei polinomi

Ogni polinomio con coefficienti reali $D(x)$ si può decomporre in fattori di primo o secondo grado con coefficienti reali.

$$D(x) \;=\; d\,(x-r_1)^{m_1}\cdots(x-r_h)^{m_h}\,(x^2+2\,a_1\,x+b_1)^{n_1}\,\cdots\,(x^2+2\,a_k\,x+b_k)^{n_k} \qquad ,$$

ove $h, k \geq 0$, $\forall j = 1, ..., k \;\colon\; {a_j}^2 < b_j$ e $\displaystyle\sum_{i=1}^{h} m_i + 2\sum_{j=1}^{k} n_j = deg(D)$.

W15 c. quozienti di polinomi e loro decomposizioni

W15c.01 Siano $N(x)$ e $D(x)$ due polinomi con $deg(D(x)) > 0$; la loro divisione si dice **funzione razionale** e per essa si ha univocamente

$$Q(x) \;:=\; \frac{N(x)}{D(x)} \;=\; P(x) + \frac{R(x)}{D(x)} \quad \text{con} \quad deg(R) < deg(D) \;\;,\;\; deg(P) = deg(N) - deg(D) \;.$$

$Q(x)$ si dice polinomio quoziente e $R(x)$ polinomio resto di $N(x)$ e $D(x)$.

Consideriamo i polinomi reali $R(x)$ e $D(x)$ con $deg(R(x)) < deg(D(x))$ e si abbia la decomposizione di $D(x)$ in polinomi real dei gradi 1 e 2 data in ca.08. Allora si trova univocamente la seguente decomposizione
I coefficienti $\rho_{1,1}$, $\rho_{1,2}$,..., σ_{k,n_k}, τ_{k,n_k} che, in numero di $\delta := deg(D)$, compaiono nei numeratori del secondo membro si ottengono risolvendo l'equazione della forma $R(x) = \overline{R}(x)$, ove $\overline{R}(x)$ denota il polinomio lineare nei suddetti coefficienti ottenuto riducendo a un unico denominatore la somma a secondo membro della decomposizione richiesta. Si osserva che dalla uguaglianza dei coefficienti delle δ potenze x^i per i=0,1,...,$\delta - 1$ nella $R(x) = \overline{R}(x)$ si ottiene un sistema di δ equazioni negli altrettanti coefficienti incogniti.

L'esposizione in https://www.mi.imati.cnr.it/alberto/ e https://arm.mi.imati.cnr.it/Matexp/matexp_main.php