Strutture algebriche

Definizione

Una **operazione interna** (binaria) di un insieme S è una applicazione

$$* : S \times S \to S, \quad (s, s') \mapsto s * s'.$$

$* (s, s') = s * s'$

Osservazioni:

- Le operazioni tipicamente si indicano non con delle lettere ma con dei simboli, ad esempio l'asterisco di sopra. Altre possibilità (lista naturalmente illimitata)

$$+, \cdot, \times, \div, \cap, \cup, \setminus, \text{ etc.}$$

- Quindi, se il simbolo scelto per l'operazione è $+$, scriveremo l'immagine di (s, s') come $s + s'$, se il simbolo è $\div$ scriveremo $s \div s'$, etc.)

Esempi

Operazioni aritmetiche:

- Somma e prodotto fra numeri naturali, interi, razionali, reali, complessi sono operazioni interne rispettivamente di $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- La sottrazione è una operazione interna di $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, ma non è una operazione interna di $\mathbb{N}$, poiché la differenza fra due numeri naturali non è sempre un numero naturale (esempio: $2 - 7 = -5$ è un intero negativo). $\in \mathbb{N} \quad \in \mathbb{N} \quad \in \mathbb{Z}$ $* := -$
- La divisione non è una operazione interna di $\mathbb{N}$ o di $\mathbb{Z}$ (il rapporto fra due numeri naturali/interi non è sempre un numero naturale/intero), né di $\mathbb{Q}$ o $\mathbb{R}$ (non si può dividere per 0). È una operazione, ad esempio, di $\mathbb{Q}\setminus\{0\}$ ed $\mathbb{R}\setminus\{0\}$.

Operazioni fra matrici:

- La somma di matrici reali è una operazione interna di $\mathcal{M}_{m,n}(\mathbb{R})$, per ogni $m, n \geq 1$.
- Il prodotto righe per colonne è una operazione interna di $\mathcal{M}_n(\mathbb{R})$, per ogni $n \geq 1$.

Operazioni insiemistiche:

- Sia S un insieme e indichiamo con $\mathcal{P}(S)$ la collezione dei sottoinsiemi di S, detto **insieme delle parti** di S; intersezione e unione sono operazioni interne di $\mathcal{P}(S)$.

$\cap \quad \cup$

Definizione

Siano K e S due insiemi. Una **operazione esterna** di S ad operatori in K è una applicazione

$$K \times S \to S, \quad (k, s) \mapsto ks.$$

Esempio:

- Il prodotto di una matrice reale $m \times n$ per uno scalare $\lambda \in \mathbb{R}$ è una operazione esterna di $\mathbb{R} \times \mathcal{M}_{m,n}(\mathbb{R}) \to \mathcal{M}_{m,n}(\mathbb{R})$ ad operatori in $\mathbb{R}$.

Definizione

Un insieme con delle operazioni (interne o esterne) è detto **struttura algebrica**.

Esempi:

- $(\mathbb{N}, +, \cdot)$ è una struttura algebrica con due operazioni (entrambe interne).
- L'insieme $\{\text{FALSO}, \text{VERO}\}$ con le operazioni **OR** e **AND** è una struttura algebrica detta **algebra di Boole** (alla base, fra le altre cose, del funzionamento dei computer).

Proprietà delle operazioni interne

Definizione

Una operazione interna $*$ di un insieme S si dice **commutativa** se $\forall\, r, s \in S$ si ha

$$r * s = s * r,$$

e si dice **associativa** se per ogni $r, s, t \in S$ si ha

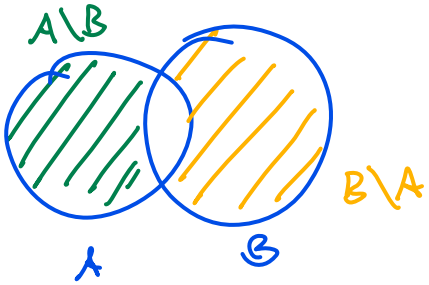
$$r * (s * t) = (r * s) * t.$$

In tal caso scriveremo semplicemente $r * s * t$ per indicare il risultato dell'operazione.

Esempi:

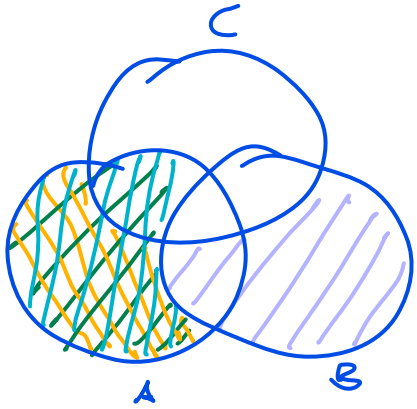
	commutativa	associativa
Somma di due numeri / n-uple / matrici	✓	✓
Unione e intersezione	✓	✓
Prodotto di due numeri	✓	✓
Prodotto fra matrici	✗	✓
Differenza fra insiemi	✗	✗
Divisione $:$	✗	✗
	$2:1 \neq 1:2$	$(1:2):2 \neq 1:(2:2)$

DIFFERENZA PRA INSIEMI.



$A \setminus B \neq B \setminus A$

$\Rightarrow$ OP. NON COMMUTATIVA



$(A \setminus B) \setminus C \neq A \setminus (B \setminus C)$

$\Rightarrow$ OP. NON ASSOCIATIVA

Elemento neutro

Definizione

Sia $(G, *)$ un insieme con una operazione interna. Un elemento $e \in G$ è detto **elemento neutro** rispetto all'operazione considerata se:

$$\forall\, g \in G\,, \quad g * e = e * g = g\,.$$

Esempi:

- il numero intero 0 è elemento neutro rispetto alla somma di due numeri;
- il numero intero 1 è elemento neutro rispetto al prodotto di due numeri;
- la matrice nulla $0_{\mathcal{M}_{m,n}(\mathbb{R})}$ è elemento neutro rispetto alla somma di matrici $m \times n$;
- la matrice identica $\mathbb{1}_n$ è elemento neutro rispetto al prodotto di matrici $n \times n$.

Proposizione

Se $(G, *)$ ha un elemento neutro, questo è unico.

Dimostrazione (per assurdo). SIANO e E e' DUE ELEMENTI NEUTRI ALLORA

$e = e * e' = e' \quad \Rightarrow \quad e = e'$

e' NEUTRO $\qquad$ e NEUTRO

Elementi invertibili

Sia $(G, *, e)$ un insieme con una operazione interna ed un elemento neutro.

Definizione

Un elemento $g \in G$ si dice **invertibile** in $(G, *, e)$ se esiste un elemento $h \in G$ tale che

$$g * h = h * g = e.$$

In tal caso h si dice **inverso** di g e si scrive $h = g^{-1}$.

Esempi:

- Ogni elemento n di $(\mathbb{Z}, +, 0)$ è invertibile, ed il inverso è il suo **opposto** $-n$.
- Ogni elemento non nullo x di $(\mathbb{Q}, \cdot, 1)$ è invertibile, ed il suo inverso è l'**inverso** x^{-1}. L'elemento $0 \in \mathbb{Q}$ non è invertibile (rispetto al prodotto).
- Ogni elemento $A \in \mathcal{M}_{m,n}(\mathbb{R})$ è invertibile rispetto alla somma, ed il inverso è dato dalla matrice opposta $-A$. $-A := (-a_{ij})$
- Se $A \in \mathcal{M}_n(\mathbb{R})$ è una matrice invertibile, il suo inverso rispetto al prodotto è A^{-1}. (MA NON OGNI MATRICE È INVERTIBILE)

Definizione

Sia $(G, *, e)$ un insieme con una operazione associativa ed un elemento neutro. Una struttura algebrica di questo tipo è detta **monoide**.

Proposizione (Unicità dell'inverso)

In un monoide, (ASSOC.) se un elemento è invertibile allora il suo inverso è unico.

Dimostrazione. (PER ASSURDO)

SIA $g \in G$ E SUPPONIAMO CHE $h, h' \in G$ SIANO DUE INVERSI DI g. QUINDI,

$g * h = e$ $\quad$ $h' * g = e$

PER DEF. DI ELEMENTO NEUTRO, SI HA

$$h' = h' * e \overset{\text{EL. NEUTRO}}{=} h' * (g * h) \overset{\text{ASSOC.}}{=} (h' * g) * h = e * h \overset{\text{EL. NEUTRO}}{=} h$$

$\Rightarrow h' = h$ ✓

Gruppi

Definizione

Un insieme G con una operazione interna $*$ ed elemento neutro e si dice **gruppo** se:

i) l'operazione $*$ è associativa;

ii) ogni elemento di G è invertibile.

MONOIDE

Se l'operazione $*$ è commutativa, diremo che $(G, *, e)$ è **commutativo** o **abeliano**.

Osservazione: un gruppo è un monoide in cui ogni elemento è invertibile.

Primi esempi:

- $(\mathbb{Z}, +, 0)$ e $(\mathbb{Q}\backslash\{0\}, \cdot, 1)$ sono gruppi commutativi.
- $(\mathcal{M}_{m,n}(\mathbb{R}), +, 0_{\mathcal{M}_{m,n}(\mathbb{R})})$ è un gruppo commutativo.
- L'insieme $S(n)$ delle permutazioni è un gruppo (il cosiddetto **gruppo simmetrico**), con operazione data dalla composizione di due permutazioni: $\sigma * \tau := \sigma \circ \tau$. Ogni permutazione è una applicazione biunivoca e questo fornisce l'inverso, mentre l'elemento neutro è dato dalla permutazione identica. Per $n \geq 2$, il gruppo $S(n)$ **non** è commutativo. AD ESEMPIO $S(3)$: $\sigma: (1,2,3) \mapsto (2,1,3)$, $\tau: (1,2,3) \mapsto (2,3,1)$

$\sigma \circ \tau: (1,2,3) \mapsto (3,2,1)$ $\quad$ $\tau \circ \sigma: (1,2,3) \mapsto (1,3,2)$ $\Rightarrow \sigma * \tau \neq \tau * \sigma$

I seguenti insiemi diventano tutti gruppi tramite la moltiplicazione di matrici, la matrice identica $\mathbb{1}_n$ come elemento neutro e l'inversa di una matrice come inverso. L'unico aspetto da verificare è che la moltiplicazione sia effettivamente un'operazione interna.

- $\mathrm{GL}(n, \mathbb{R}) := \{A \in \mathcal{M}_n(\mathbb{R}) \mid \det(A) \neq 0\}$ si chiama **gruppo lineare generale**.

DA DIMOSTRARE: IL PRODOTTO FRA DUE MATRICI INVERTIBILI È NUOVAM. INVERTIBILE E QUINDI DEFINISCE UN'OPERAZ. INTERNA

$$GL(n,\mathbb{R}) \times GL(n,\mathbb{R}) \longrightarrow GL(n,\mathbb{R})$$
$$(A, B) \longmapsto AB$$

$$\det(AB) \overset{\text{BINET}}{=} \det(A)\cdot\det(B) \neq 0$$ PERCHÉ PER IPOTESI $\det(A) \neq 0$, $\det(B) \neq 0$

$\Rightarrow AB \in GL(n,\mathbb{R})$

- $\mathrm{SL}(n, \mathbb{R}) := \{A \in \mathcal{M}_n(\mathbb{R}) \mid \det(A) = 1\}$ si chiama **gruppo lineare speciale**.

$A \in GL(n,\mathbb{R})$

IL PRODOTTO FRA DUE MATRICI È UN'OPERAZ. INTERNA

$$SL(n,\mathbb{R}) \times SL(n,\mathbb{R}) \longrightarrow SL(n,\mathbb{R})$$

SE $A, B \in SL(n,\mathbb{R}) \Rightarrow \det(A) = \det(B) = 1$

$$\Rightarrow \det(AB) \overset{\text{BINET}}{=} \det(A)\det(B) = 1\cdot 1 = 1$$

$\Rightarrow AB \in SL(n,\mathbb{R})$

- $\mathrm{O}(n,\mathbb{R}) := \{A \in \mathcal{M}_n(\mathbb{R}) \mid A^{-1} = A^T\}$ si chiama **gruppo ortogonale**.

$A \in GL(n,\mathbb{R})$

IL PROD. FRA MATRICI INDUCE UN'OP. INTERNA $O(n,\mathbb{R}) \times O(n,\mathbb{R}) \to O(n,\mathbb{R})$?

VERIFICHIAMO:

$(AB)^{-1} = B^{-1}A^{-1} = B^T A^T = (AB)^T \Rightarrow (AB)^{-1} = (AB)^T \Rightarrow AB \in O(n,\mathbb{R})$ ✓

(4. LEZIONE (!)) (IPOTESI $A,B \in O(n,\mathbb{R})$) (3. LEZIONE (?))

- $\mathrm{SO}(n,\mathbb{R}) := \{A \in \mathrm{O}(n,\mathbb{R}) \mid \det(A) = 1\}$ si chiama **gruppo ortogonale speciale**.

(DIM. COME SOPRA)

COMMENTO: SE $A \in O(n,\mathbb{R}) \Rightarrow \det(A) = \pm 1$

DIMOSTRAZ.: $1 = \det(1_n) = \det(A A^{-1}) = \det(A A^T) = \det(A)\det(A^T)$ ($A \in O(n,\mathbb{R})$, BINET)

$= (\det(A))^2 \Rightarrow \det(A) = \pm 1$ ✓ ($\det(A) = \det(A^T)$)

- **Controesempio**: L'insieme $X = \{A \in \mathrm{O}(n,\mathbb{R}) \mid \det(A) = -1\}$ **non** è un gruppo:

SE $A,B \in X$, ALLORA $\det(AB) = \det(A)\det(B) = (-1)\cdot(-1) = 1$

$\Rightarrow AB \notin X \Rightarrow X$ NON È UN GRUPPO.

Anelli

Definizione

Sia $\mathcal{A}$ un insieme dotato di **due** operazioni interne, che chiameremo **somma** (indicata con $+$) e **prodotto** (indicato con $\cdot$), e di due elementi $0_\mathcal{A}$ e $1_\mathcal{A}$. La struttura algebrica $(\mathcal{A}, +, 0_\mathcal{A}, \cdot, 1_\mathcal{A})$ si dice **anello** (con unità) se le seguenti proprietà sono soddisfatte:

1. $(\mathcal{A}, +, 0_\mathcal{A})$ è un gruppo commutativo;
2. il prodotto è associativo;
3. $1_\mathcal{A}$ è elemento neutro rispetto al prodotto;

} $(A, \cdot, 1_A)$ È UN MONOIDE

4. per ogni $a, b, c \in \mathcal{A}$ si ha (**proprietà distributiva**):

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad (a + b) \cdot c = a \cdot c + b \cdot c$$

Un anello si dice **commutativo** se il prodotto è commutativo.

Esempi:

- $(\mathbb{Z}, +, 0, \cdot, 1)$ è un anello commutativo;
- per $n \geq 2$, le matrici $n \times n$ formano un anello non commutativo.

(DISTRIB. VERIFICATA ALLA SECONDA LEZ.)

Campi

$(\mathbb{Q}, +, 0, \cdot, 1)$ è un altro esempio di anello commutativo. Rispetto a $\mathbb{Z}$ gode di una proprietà aggiuntiva: ogni elemento non nullo di $\mathbb{Q}$ è invertibile rispetto al prodotto.

Definizione

Un anello **commutativo** (con unità) K si dice **campo** se ogni elemento diverso da zero è invertibile rispetto al prodotto. Ovvero,

1. $(\mathcal{A}, +, 0_{\mathcal{A}})$ è un gruppo commutativo;
2. $(\mathcal{A}\backslash\{0\}, \cdot, 1_{\mathcal{A}})$ è un gruppo commutativo;
3. per ogni $a, b, c \in \mathcal{A}$ si ha:

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad (a + b) \cdot c = a \cdot c + b \cdot c.$$

Gli insiemi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ con le usuali operazioni sono campi.

Gli insiemi $\mathbb{Z}$ e $\mathcal{M}_n(\mathbb{R})$ (con $n \geq 2$) sono anelli, ma non sono campi.

NON TUTTI GLI ELEMENTI IN $M_n(\mathbb{R})$ SONO INVERTIBILI.

$M_{m,n}(\mathbb{C})$
$M_{m,n}(\mathbb{Q})$

Osservazione

Si possono considerare matrici con elementi in un campo K qualsiasi, e sistemi di equazioni lineari con coefficienti in un campo K arbitrario. I teoremi enunciati sono validi nel caso in cui invece di $\mathbb{R}$ si consideri un campo K arbitrario (ad esempio $K = \mathbb{C}$ o $K = \mathbb{Q}$).

Estensione di $\mathbb{Q}$ mediante $\sqrt{2}$

PROPRIO

$\mathbb{Q} \subset \mathbb{R}$ non solo costituisce un campo, ma anche un **sottocampo** in $\mathbb{R}$. Visto che $\sqrt{2} \neq \mathbb{Q}$, si può "estendere" $\mathbb{Q}$ mediante $\sqrt{2}$ nel seguente modo per ottenere un nuovo campo $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$:

L'insieme

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$$

con le operazioni ereditate da $\mathbb{R}$ costituisce un campo.

Verifica. DEVO DIMOSTRARE CHE LE OPERAZ. DI SOMMA E PRODOTTO DEFINITE IN $\mathbb{R}$ SI RESTRINGONO AD OPERAZ INTERNE DI $\mathbb{Q}(\sqrt{2})$.

PRENDO $x = a_1 + b_1\sqrt{2}$, $y = a_2 + b_2\sqrt{2}$, $a_1, a_2, b_1, b_2 \in \mathbb{Q}$

DEVO DIMOSTR.: $x + y \in \mathbb{Q}(\sqrt{2})$

$$x + y = (a_1 + b_1\sqrt{2}) + (a_2 + b_2\sqrt{2}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$$
$$=: c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

VISTO CHE $a_1 + a_2 \in \mathbb{Q}$, $b_1 + b_2 \in \mathbb{Q}$.

IDEM RISPETTO AL PRODOTTO

$$x \cdot y = (a_1 + b_1\sqrt{2}) \cdot (a_2 + b_2\sqrt{2}) = \underbrace{(a_1 a_2 + 2 b_1 b_2)}_{\in \mathbb{Q}} + \underbrace{(a_1 b_2 + b_1 a_2)}_{\in \mathbb{Q}}\sqrt{2} \in \mathbb{Q}(\sqrt{2})$$

$\Rightarrow$ SOMMA E PRODOTTO SONO "CHIUSI" IN $\mathbb{Q}(\sqrt{2})$.

L'INVERSO RISPETTO ALLA SOMMA È SEMPLICEM. $-x = -a - b\sqrt{2}$

I DUE ELEMENTI NEUTRI: 0 $(a = b = 0)$ E 1 $(a = 1, b = 0)$

L'INVERSO RISPETTO AL PRODOTTO:

DOVREBBE ESSERE $x^{-1} = \frac{1}{a + b\sqrt{2}}$, MA STA IN $\mathbb{Q}(\sqrt{2})$?

INFATTI,

$$\frac{1}{a + b\sqrt{2}} = \frac{1}{a + b\sqrt{2}} \cdot \frac{a - b\sqrt{2}}{a - b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \underbrace{\frac{a}{a^2 - 2b^2}}_{\in \mathbb{Q}} + \underbrace{\frac{-b}{a^2 - 2b^2}}_{\in \mathbb{Q}}\sqrt{2} =: a' + b'\sqrt{2}$$

CON $a', b' \in \mathbb{Q}$

$\Rightarrow x^{-1} \in \mathbb{Q}(\sqrt{2})$

Esempio

Nello stesso modo si costruisce

$$\mathbb{R} \subset \mathbb{C} := \{a + bi \mid a, b \in \mathbb{R},\ i = \sqrt{-1}\}$$

come estensione di $\mathbb{R}$ mediante $\sqrt{-1}$.

L'anello dei polinomi $K[x]$

Definizione

- Un **polinomio** di grado $n \geq 0$ in una variabile x e a coefficienti in un campo K è una espressione del tipo

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0.$$

con $a_i \in K$ per ogni $i = 0, \ldots, n$, e $a_n \neq 0$.
- Un elemento $r \in K$ è detto **radice** del polinomio considerato se $P(r) = 0$.
- Una equazione del tipo $P(x) = 0$ è detta **algebrica** o **polinomiale** di grado n in x.

L'insieme dei polinomi (di grado arbitrario) in una variabile x e a coefficienti in un campo K viene indicato con $K[x]$. A noi interesserà il caso $K = \mathbb{R}$.

$K[x]$ come anello commutativo

DOBBIAMO DEFINIRE SOMMA E PRODOTTO COME OP. INTERNE DI $K[x]$.

DUE POLINOM. $P(x) = \sum_{k=0}^{m} a_k x^k$, $Q(x) = \sum_{k=0}^{n} b_k x^k$

SUPPONIAMO $m \geq n$.

SOMMA: $(P+Q)(x) = P(x) + Q(x) = \sum_{k=0}^{n} (a_k + b_k) x^k + \sum_{k=n+1}^{m} a_k x^k$

PRODOTTO: $(P \cdot Q)(x) = \left(\sum_{k=0}^{m} a_k x^k\right) \cdot \left(\sum_{k=0}^{n} b_k x^k\right) = \sum_{k=0}^{m+n} \left(\sum_{j=0}^{k} a_j b_{k-j}\right) x^k$

IN ALTERNATIVA, TRAMITE LE SUCCESSIONI DI CAUCHY:

SCRIVO $P(x) = (a_0, a_1, \ldots, a_m, 0, \ldots, 0)$ (x^0, x^1, x^m) $Q(x) = (b_0, \ldots, b_n, 0, \ldots, 0)$

$(P+Q)(x) = (a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, a_{n+1}, \ldots, a_m, 0, \ldots, 0)$

$(P \cdot Q)(x) = (a_0 \cdot b_0, (a_0 \cdot b_1 + a_1 \cdot b_0), (a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0), \ldots, \ldots)$ (x^0, x^1, x^2)

SOMMA DEGLI INDICI: 0, 1, 2

"PRODOTTO DI CONVOLUZIONE"

$\mathbb{R}[x]$

Un polinomio reale può non avere radici reali. Esempio: $P(x) = x^2 + 1$ non ha radici reali; ammette però due radici complesse. Diciamo che $\mathbb{C}$ è **algebricamente chiuso**, poiché ogni equazione algebrica in $\mathbb{C}$ (di grado $n \geq 1$) ammette soluzioni.

Teorema fondamentale dell'algebra

Un polinomio di grado $n \geq 1$ a coefficienti in $\mathbb{C}$ può sempre essere scritto nella forma

$$P(x) = c(x - r_1)(x - r_2) \dots (x - r_n) \,,$$

"FATTORI LINEARI"

dove $r_1, \dots, r_n \in \mathbb{C}$ sono le radici e $c \in \mathbb{C}$ un coefficiente non nullo.

Le radici di un polinomio non sono necessariamente tutte distinte. Ad esempio $x^2 - 6x + 9 = (x - 3)^2$ ha due radici, entrambe uguali a 3.

Indicando con $\mu_1, \dots, \mu_k$ le radici **distinte** del polinomio $P(x)$ ($k \leq n$), si avrà

$$P(x) = c(x - \mu_1)^{m_1}(x - \mu_2)^{m_2} \dots (x - \mu_k)^{m_k} \,,$$

dove $m_i \geq 1$ è detto **molteplicità** della radice μ_i, e si ha $m_1 + m_2 + \dots + m_k = n$.

Teorema delle radici razionali

Consideriamo un polinomio ($a_n \neq 0$) di grado n $\quad a_0, \dots, a_n \in \mathbb{Z}$

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

a **coefficienti interi**. Se un numero razionale $r = p/q \in \mathbb{Q}$ è una radice di $P(x)$, allora

i) p divide a_0;

ii) q divide a_n.

Le radici razionali si possono determinare considerando tutti i possibili valori di p/q, con p divisore di a_0 e q divisore di a_n, e verificando per sostituzione quali sono radici.

Esempio

Sia $P(x) = x^3 - 2x^2 - 5x + 6$.

$P(x) = a_3x^3 + a_2x^2 + a_1x + a_0$

$a_3 = 1$, $a_2 = -2$, $a_1 = -5$, $a_0 = 6$

I DIVISORI DI a_0 SONO $\pm 1, \pm 2, \pm 3, \pm 6$; I DIVISORI DI a_3 SONO ± 1. QUINDI

$$p/q \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

PER SOSTITUZIONE SI VERIFICA CHE LE RADICI SONO $1, 3, -2$.

$\Rightarrow \quad P(x) = (x-1)(x-3)(x+2)$

Regola di Ruffini

Dato uno scalare r e un polinomio $P(x)$ di grado n:

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

GRADO n

con $a_n \neq 0$, la regola di Ruffini permette di decomporre $P(x)$ nella forma

$$P(x) = (x - r)Q(x) + R$$

in cui

$$Q(x) = b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$$

GRADO $n-1$

è il **quoziente** della divisione ed R è una costante, detta **resto**. Si procede come segue:

	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_2	a_1	a_0
r		$b_{n-1}\cdot r$	$b_{n-2}\cdot r$		$b_2 r$	$b_1 \cdot r$	$b_0 \cdot r$
	$a_n = b_{n-1}$	$a_{n-1} + b_{n-1}\cdot r = b_{n-2}$	$a_{n-2} + b_{n-2}\cdot r = b_{n-3}$		$a_2 + b_2 \cdot r = b_1$	$a_1 + b_1 r = b_0$	$a_0 + b_0 \cdot r = R$

Se r è una radice di $P(x)$, allora il resto è $R = 0$.

Data una equazione di **3° grado**, la regola di Ruffini permette di ridurla ad una di 2° grado se almeno una soluzione è **nota a priori**.

Esercizio

Sia

$$P(x) = 2x^3 + x^2 - 4x - 2.$$

Usando il teorema delle radici razionali, scopriamo che una radice è $r = -\frac{1}{2}$. (ESERCIZIO)

Dividendo $P(x)$ per $x - r$ si ottiene:

	2	1	-4	-2
$-\frac{1}{2}$		$r b_2 = -1$	$r \cdot b_1 = 0$	$r \cdot b_0 = 2$
	$2 = b_2$	$a_2 + r b_2 = 0 = b_1$	$a_1 + r \cdot b_1 = -4 = b_0$	$a_0 + r b_0 = 0$

$\Rightarrow P(x) = \left(x + \frac{1}{2}\right) Q(x)$ con $Q(x) = 2x^2 + 0 \cdot x - 4 = 2x^2 - 4$

Esercizio

Sia

$$P(x) = 2x^3 + 2x^2 - x - 3.$$

Usando il teorema delle radici razionali, scopriamo che una radice è $r = 1$.

Dividendo $P(x)$ per $x - r$ si ottiene: