

$$3^n > 1 + 2n$$

$$n \in \mathbb{N}, \quad \underline{n \geq 2}$$

Passo base: $P(2)$ vero

$$P(2): \quad 3^2 > 1 + 2 \cdot 2$$

$$9 > 5 \quad \text{vero}$$

$P(n)$ vero

Passo induttivo

$$P(n) \text{ vero} \\ 3^n > 1 + 2n$$

allora

$$P(n+1) \text{ vero}$$

$$3^{n+1} > \underbrace{1 + 2(n+1)}$$

$$1 + 2n + 2 = 2n + 3$$

$$3^{n+1} > 2n + 3$$

$$\underbrace{3 \cdot 2n = 6n + 2 \cdot 2n}$$

$$3^{n+1} = 3^n \cdot 3 > (1 + 2n) \cdot 3 = 3 + 3 \cdot 2n = 3 + 2n + 2 \cdot 2n = \\ = (2n + 3) + 6n > (2n + 3) + 0 = 2n + 3$$

perciò $2n > 0$

$$3^{n+1} > 2n + 3 \quad \text{ovvero} \quad P(n+1) \text{ è vero.}$$

$$3^0 > 1 + 2 \cdot 0 \quad \Leftrightarrow \quad 1 \geq 1 \quad \text{vero} \quad \Rightarrow 3^n \geq 1 + 2n$$

$$3^1 \geq 1 + 2 \cdot 1 \quad \Leftrightarrow \quad 3 \geq 3 \quad \text{vero} \quad \forall n \in \mathbb{N}$$

$$6 \mid n(2n^2 - 3n + 1) \quad \forall n \in \mathbb{N}$$

Passo base $P(0): 6 \mid 0 \cdot (2 \cdot 0^2 - 3 \cdot 0 + 1) \Leftrightarrow 6 \mid 0$ vero

Passo induttivo

$$P(n) \text{ vero} \Rightarrow P(n+1) \text{ vero}$$

$$6 \mid n(2n^2 - 3n + 1) \Rightarrow 6 \mid (n+1)(2(n+1)^2 - 3(n+1) + 1)$$

$$\underbrace{(n+1)(2(n+1)^2 - 3(n+1) + 1)}_{= (n+1)(2n^2 + 4n + 2 - 3n - 3 + 1)} =$$

$$= (n+1)((2n^2 - 3n + 1) + 4n - 1) = n(2n^2 - 3n + 1) + \cancel{4n^2} - \cancel{n}$$

$$+ \cancel{2n^2} - \cancel{3n} + \cancel{1} + \cancel{4n} - \cancel{1} = \underbrace{n(2n^2 - 3n + 1) + 6n^2}_{\text{ipotesi d'induzione}}$$

$$(6 \mid n(2n^2 - 3n + 1) \quad \wedge \quad 6 \mid 6n^2) \Rightarrow$$

ipotesi d'induzione

$$6 \mid n(2n^2 - 3n + 1) + 6n^2 \Leftrightarrow 6 \mid (n+1)(2(n+1)^2 - 3(n+1) + 1)$$

$$f: \mathbb{N} \rightarrow \mathbb{N}$$

$\nearrow y$

$$\forall n \in \mathbb{N} \quad f(n) = n^2 + 1$$

Siamo $n, m \in \mathbb{N}$ tali che $f(n) = f(m)$. Allora $n^2 + 1 = m^2 + 1$

cioè $n^2 = m^2$ e quindi $n = m$ (perché $n, m \in \mathbb{N}$)

quindi f è iniettiva.

f è surgettiva: sia $y \in \mathbb{N}$ cerchiamo, se esiste, $n \in \mathbb{N}$

tale che $f(n) = y$ ovvero $n^2 + 1 = y$, cioè $n^2 = y - 1$

Per $y = 4$ l'ugualianza diventa

$$n^2 = 4 - 1$$

$$n^2 = 3$$

non esiste alcun numero naturale il cui quadrato sia 3, per cui $\forall n \in \mathbb{N} \quad f(n) \neq 4$. Quindi f non è surgettiva.

Calcolare il resto della divisione di

$$57 \cdot 632^{1142}$$

per 9

$$57 \cdot 632 = 9 \cdot \underbrace{6381}_{57629} + 3$$

$$\begin{array}{r} 1142 \\ 576 \end{array} \Big| 2$$

$$57 \cdot 632 \equiv 3 \pmod{9}$$

M.C.D.(3,9) ≠ 1

$$3^2 \equiv 0 \pmod{9}$$

$$57 \cdot 632^{1.142} \equiv 3^{1.142} \pmod{9}$$

$$1.142 = 576 \cdot 2$$

$$3^2 \equiv 0 \pmod{9}$$

$$3^{1.142} = (3^2)^{576} \equiv 0 \pmod{9}$$

il resto della divisione è 0.

$$h^{3.816} \stackrel{20.321}{\equiv}$$

$\mu \equiv 10$

$$h^{3.816} \equiv 6 \pmod{10}$$

$$\text{M.C.D.}(6, 10) \neq 1$$

$$6^3 \equiv 6 \pmod{10}$$

$$6^2 \equiv 36 \equiv 6 \pmod{10}$$

$$6^{20.321} = (6^4)^{5.080} \cdot 6 \equiv 6^{5.080} \cdot 6 \pmod{10}$$

per induzione completa

$$\boxed{6^{2n} \equiv 6 \pmod{10}} \quad ? \quad n \geq 1$$

$$6^{2n} \equiv 6 \pmod{10} \quad \begin{matrix} n=1 \\ 6^2 \equiv 6 \pmod{10} \end{matrix} \quad \text{viiste}$$

$$6^{2(n+1)} = 6^{2n+2} = \underbrace{6^{2n} \cdot 6^2}_{\text{: passo d'induz}} \equiv 6 \cdot 6 = 6^2 \equiv 6 \pmod{10}$$

: passo d'induz

$$\forall n \in \mathbb{N} \quad 6^{2n} \equiv 6 \pmod{10}$$

$$6^{5.080} \equiv 6 \pmod{10}$$

$$6^{20 \cdot 32^1} \equiv 6 \cdot 6 = 6^2 \equiv 6 \pmod{10}$$

il resto è 6.

Proviamo per induzione completa che se A è un insieme finito con $|A| = n$, allora $|\mathcal{P}(A)| = 2^n$.

Dico Passo base $|A|=0$, $A=\emptyset$

$\mathcal{P}(A) = \{\emptyset\}$ e quindi $|\mathcal{P}(A)| = 1 = 2^0$.

Passo induttivo

Supponiamo che B insieme con $|B| = n$ risulti

$|\mathcal{P}(B)| = 2^n$ e proviamo che se A è un insieme finito con $|A| = n+1$, allora $|\mathcal{P}(A)| = 2^{n+1}$.

Sia A insieme, $|A| = n+1$ e sia $x_0 \in A$.

Sia $B = A - \{x_0\}$; $|B| = n$

$$|\mathcal{P}(B)| = 2^{n+1}$$

$C \subset A \Leftrightarrow (\exists D \subset B \text{ tale che } C = D \cup \{x_0\}) \vee (C \subset B)$

Esempio: $A = \{x_0, x_1, x_2, x_3\}$ $B = \{x_1, x_2, x_3\}$

$$\mathcal{P}(B) = \{\emptyset, \{x_1\}, \{x_2\}, \{x_3\}, \{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}, \{x_1, x_2, x_3\}\}$$

$$\left\{ \underbrace{\{\emptyset \cup \{x_0\}, \{x_1\} \cup \{x_0\}, \{x_2\} \cup \{x_0\}, \{x_3\} \cup \{x_0\}, \{x_1, x_2\} \cup \{x_0\}, \{x_1, x_3\} \cup \{x_0\}, \{x_2, x_3\} \cup \{x_0\}}_{\{x_1, x_2, x_3\} \cup \{x_0\} = \{x_1, x_2, x_3\} \cup \{x_0\}}, \{x_1, x_2, x_3\} \cup \{x_0\} \right\}$$

$$\mathcal{P}(A) = \mathcal{P}(B) \cup \{\{x_0\}, \{x_1, x_0\}, \{x_2, x_0\}, \{x_3, x_0\}, \{x_1, x_2, x_0\}, \\ \{x_1, x_3, x_0\}, \{x_2, x_3, x_0\}, \{x_1, x_2, x_3, x_0\}\}$$

$$\mathcal{P}(A) = \mathcal{P}(B) \cup \{D \cup \{x_0\} : D \subset B\}, \quad \mathcal{P}(B) \cap \{D \cup \{x_0\} : D \subset B\} = \emptyset$$

$$|\mathcal{P}(A)| = |\mathcal{P}(B) \cup \{D \cup \{x_0\} : D \subset B\}| = |\mathcal{P}(B)| + |\{D \cup \{x_0\} : D \subset B\}|$$

$$= |\mathcal{P}(B)| + |\mathcal{P}(B)| = 2^n + 2^n = 2 \cdot 2^n = 2^{n+1}.$$

STRUTTURE ALGEBRICALI

Def. Sia A un insieme $A \neq \emptyset$. Si dice legge di composizione interna su A o operazione su A una funzione:

$$*: A \times A \rightarrow A$$

$$\forall a, b \in A \quad * (a, b) = a * b \in A$$

per esempio $+ : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ è una legge di composizione interna.

Le coppie ordinate $(A, *)$ si dice struttura algebrica.

$(\mathbb{N}, +)$, $(\mathbb{Z}, +)$ sono strutture algebriche.

Def. Sia $(A, *)$ una struttura algebrica. Si dice che la legge di composizione interna $*$ è associativa se

$$\forall a, b, c \in A \quad a * (b * c) = (a * b) * c.$$

Esempio La somma + usata su \mathbb{N} (e su \mathbb{Z}) è

associativa $\forall a, b, c \in \mathbb{N} \quad (a+b)+c = a+(b+c)$

$$(7+3)+11 = 7+(3+11).$$

$$(-2+3)+(-7) = -2+(3+(-7)).$$

Def. Sia $(A, *)$ una struttura algebrica. Si dice che $*$ ammette elemento neutro se esiste $e \in A$ tale che $\forall x \in A \quad x * e = e * x = x$.

Pn esempio $(\mathbb{N}, +)$ c'è l'elemento neutro che è 0 perché $\forall n \in \mathbb{N} \quad n+0 = 0+n = n$.

Osserv. Sia $(A, *)$ una struttura algebrica. Se $*$ ammette elemento neutro, esso è unico.

Siano infatti e, e' elementi neutri per $*$

$$\begin{aligned} e &= e * e' = \underline{e} \\ &\rightarrow \text{può essere } e' \text{ è elem. neutro} \\ \text{perciò } e &\text{ è elem. neutro} \end{aligned}$$

$$\text{quindi } e' = e.$$

Def. Sia $(A, *)$ una struttura algebrica. Si dice che $(A, *)$ è un monoido se $*$ è associativa e ammette elemento neutro. $(A, *)$ è un monoido se:

$$\forall a, b, c \in A \quad a * (b * c) = (a * b) * c$$

$$\exists e \in A \text{ tale ch } \forall a \in A \quad a * e = e * a = a$$

Esempi $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sono tutti monoidi.

1. $(\mathbb{N}, +)$ non va oltre l'essere un monoido.

$$A^A = \{f : A \rightarrow A\}$$

$$\circ : A^A \times A^A \longrightarrow A^A$$

$\xrightarrow{(f, g)} g \circ f$

2. (A^A, \circ) è un monoido

$$\forall f, g, h \in A^A \quad f \circ (g \circ h) = (f \circ g) \circ h$$

$$\exists i_A : A \rightarrow A^A \quad \text{tale ch} \quad \forall f \in A^A \quad i_A \circ f = f \circ i_A = f.$$

3. Monoido delle parole. Si dice parola di lunghezza $n \in \mathbb{N}^*$ su un insieme A una n -pla ordinata di elementi di A

$$a_1, a_2, \dots, a_n$$

dove $a_1, a_2, \dots, a_n \in A$. Esiste un'unica parola di lunghezza

O che che le parole suono W_0 .

A inizio $\forall h \in \mathbb{N} \quad W_h = \text{insieme delle parole di lunghezza } h \text{ che si possono formare con elementi di } A$.

$$\bigcup_{h \in \mathbb{N}} W_h = W$$

W insieme di tutte le parole in A .

W si munisce di una legge di composizione interna, detta giustapposizione

$$\cdot : W \times W \longrightarrow W$$

Siano $v, w \in W$, allora esistono $h, k \in \mathbb{N}$ tali che
 $v \in W_h$ e $w \in W_k$

$\exists a_1, \dots, a_n \in A \quad \exists b_1, \dots, b_k \in A$ tali che

$$v = a_1 \dots a_n \quad w = b_1 \dots b_k$$

$$v \cdot w = a_1 \dots a_n b_1 \dots b_k \in W_{h+k} \in W.$$

Vale la proprietà associativa.

Siano $v = a_1 \dots a_n \in W_n$, $w = b_1 \dots b_k \in W_k$
 $z = c_1 \dots c_r \in W_r$

$$(v \cdot w) \cdot z = (a_1 \dots a_n b_1 \dots b_k) c_1 \dots c_r = \\ = a_1 \dots a_n b_1 \dots b_k c_1 \dots c_r = a_1 \dots a_n (b_1 \dots b_k c_1 \dots c_r) = \\ = v \cdot (w \cdot z)$$

\exists l'elemento neutro che è la parola vuota W_0

$$\forall v \in W \quad v \cdot W_0 = v = W_0 \cdot v.$$

(W, \cdot) è un monoido che si chiama
 monoido delle parole su A o
 monoido libero su A -
dotate di elem. neutro e.

Def. Sia $(A, *)$ una struttura algebrica \checkmark Un elemento
 $a \in A$ si dice simmetizzabile se esiste
 $a' \in A$ tale che $a * a' = a' * a = e$.
 a' si dice simmetrico di a .

Osserv. Sia $(A, *)$ un monoido. Se un elemento $a \in A$
 è simmetizzabile, allora c'è un unico simmetrico
 di a .

D'inv. Siano a' , a'' due simmetri di a

$$a' + a = a * a' = e$$

$$a'' * a = \underline{a * a''} = e$$

$$a' = a' + e = a' * (a * a'') = (a' + a) * a'' = e * a'' = a''$$

↑
associatività

$$\text{quindi } a' = a''.$$

Portanto se $a \in A$, a simmetricabile si può parlare del simmetrico di a (unico).

Def. Sia $(A, *)$ una struttura algebrica - Si dice che $(A, *)$ è un gruppo se : vale le proprietà associatività, esiste l'elemento neutro e ogni elemento è simmetricabile - In simboli : $(A, *)$ è un gruppo se :

$$(G_1) \forall a, b, c \in A \quad (a + b) * c = a * (b * c)$$

$$(G_2) \exists e \in A \text{ tale che } \forall a \in A \quad a * e = e * a = a$$

$$(G_3) \forall a \in A \quad \exists a' \in A \text{ tale che } a * a' = a' * a = e.$$

Def. Sia (A, \star) una struttura algebrica. Si dice ch \star è commutativa se

$$\forall a, b \in A \quad a \star b = b \star a.$$

Def. Un gruppo (A, \star) tale ch \star non commutativa si dice gruppo abeliano.

Esempi:

$(\mathbb{N}, +)$ è un monoido commutativo

$$\left\{ \begin{array}{ll} n \in \mathbb{N} & m+0 \\ \forall m \in \mathbb{N} & m+n = n+m \neq 0. \\ \text{quindi } (\mathbb{N}, +) \text{ non è} & \text{gruppo} \end{array} \right.$$

(A^+, \circ) è un monoido non commutativo

non è gruppo, perché gli unici elementi di A^+ definiti di simmetria sono le funzioni bigettive.

$f \in A^+$ f è simmetricabile vuol dire

che $\exists f' \in A^+$ tale ch $f \circ f' = f' \circ f = id_A$

cioè ch f è invertibile: ciò avviene se e solo se f è bigettive. Non è commutativo perché in genere se $f, g \in A^+$ $f \circ g \neq g \circ f$.

(\mathcal{W}, \cdot) è un monoido non commutativo.

$$\text{Se } v = a_1 \dots a_n \in \mathcal{W}_n \quad w = b_1 \dots b_k \in \mathcal{W}_k$$

$$v \cdot w = a_1 \dots a_n b_1 \dots b_k \neq b_1 \dots b_k a_1 \dots a_n = w \cdot v.$$

$(\mathbb{Z}, +)$ è un gruppo abeliano perché
 $\forall n \in \mathbb{Z} \exists -n \in \mathbb{Z}$ tale che $n + (-n) = (-n) + n = 0$.

$(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sono gruppi abeliani.

(\mathbb{N}, \cdot) (\mathbb{Z}, \cdot) sono monoidi commutativi

$$\forall a, b, c \in \mathbb{N} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c) \quad (\text{lo stesso in } \mathbb{Z})$$

$$\exists 1 \in \mathbb{N} \text{ tale che } \forall a \in \mathbb{N} \quad a \cdot 1 = 1 \cdot a = a \quad (\dots \dots \dots)$$

(\mathbb{N}, \cdot) (\mathbb{Z}, \cdot) non sono gruppi

$$\text{Se } m \in \mathbb{N} (m \in \mathbb{Z}) \quad m \neq \pm 1, \quad \forall n \in \mathbb{N} \quad (n \in \mathbb{Z})$$

$$m \cdot m = m \cdot m \neq 1$$

(\mathbb{Q}, \cdot) (\mathbb{R}, \cdot) sono monoidi commutativi.

$$\begin{matrix} q \neq 0 \\ p \neq 0 \end{matrix} \quad \frac{p}{q} \cdot \frac{q}{p} = 1$$

$$\exists 0 \in \mathbb{Q} \text{ tale che } \forall x \in \mathbb{Q} \quad 0 \cdot x = x \cdot 0 \neq 1$$

quindi (\mathbb{Q}, \cdot) , (\mathbb{R}, \cdot) non sono gruppi.

$$\mathbb{Q}^* = \{x \in \mathbb{Q} : x \neq 0\}$$

$$(\mathbb{Q}^*, \cdot) \quad \forall x \in \mathbb{Q}^* \quad \exists \frac{1}{x} \in \mathbb{Q}^* \text{ tale che } x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$$

Lo stesso avviene su (\mathbb{R}^*, \cdot)

(\mathbb{Q}^*, \cdot) e (\mathbb{R}^*, \cdot) sono gruppi abeliani.

Osserv. Una operazione di gruppo su un insieme A in generale si può denotare moltiplicativamente:

con $\cdot, *, \circ, \odot, \dots$

e additivamente con $+, \oplus, \dots$

Nel caso della moltiplicazione moltiplicativa, normalmente si denota con 1 l'elemento neutro e si parla di inverso di un elemento per parlare del simmetrico:
a $\in A$ l'inverso di a (ovvero il simmetrico di a)
si indica con a^{-1} :

$$a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Nel caso della notazione additiva, normalmente si parla di opposto di un elemento per parlare del simmetrico:

se $a \in A$ l'opposto di a si indica con $-a$:

$a + (-a) = (-a) + a = 0$.
0 in genere indice l'elemento neutro-

$$\begin{array}{c} (G_i) \\ (G, +) \\ 1_G \\ 0 \\ a^{-1} \\ -a \end{array}$$

Def. Sia (G_i) un gruppo e sia $a \in G$. Si pone

$$a^0 = 1_G$$

$$a^n = a \cdot a^{n-1} \quad \forall n \in \mathbb{N}$$

$$a^m = (\bar{a}^m)^{-1} \quad \forall m \in \mathbb{Z}, \quad m < 0$$

↳ inverso di a^m .

esempio: $a^{-3} = (a^3)^{-1} = a$

Notazione additive $(G, +)$ gruppo

si definisce il multiplo di un elemento $a \in G$:

$$0 \cdot a = 0$$

$$n \cdot a = a + (n-1)a$$

$$n \in \mathbb{N}$$

$$n \cdot a = -(-n)a$$

$$n \in \mathbb{Z} \quad n < 0$$

Prop. Sia (G, \cdot) un gruppo. Allora

1. $\forall g \in G \quad \forall n, m \in \mathbb{Z} \quad g^n \cdot g^m = g^{n+m}$
2. $\forall g \in G \quad \forall n, m \in \mathbb{Z} \quad (g^n)^m = g^{n \cdot m}$

In notazione additive: $(G, +)$ gruppo

1. $\forall g \in G \quad \forall n, m \in \mathbb{Z} \quad n \cdot g + m \cdot g = (n+m) \cdot g$
2. $\forall g \in G \quad \forall n, m \in \mathbb{Z} \quad n \cdot (mg) = (n \cdot m) \cdot g$