Algebra astratta

A. *Introduzione*

Abbiamo visto come dai numeri Naturali siamo passati ai numeri Interi poi ai numeri razionali e quindi ai numeri reali e complessi costruendo strutture via via piu' complicate.
Vediamo ora di studiare tali strutture per vedere se possiamo individuarle anche su altri oggetti matematici diversi dai numeri.
Visto che abbiamo ampliato il concetto di numero per poter sempre eseguire le operazioni partiremo dalle operazioni interne ad un insieme, individueremo le principali strutture cui danno luogo tali operazioni e quindi parleremo di morfismi fra insiemi.

Prima pero' sara' opportuno un piccolo ripasso sulle principali proprieta' delle operazioni elementari sui numeri naturali.
Naturalmente se ti senti ben preparato puoi passare direttamente alle strutture algebriche.

B. *Ripasso sulle proprieta' delle operazioni elementari*

Vediamo quindi le principali proprieta' delle operazioni che abbiamo definito inizialmente come operazioni interne nell'insieme **N** dei numeri naturali.

Per ora facciamo un semplice riepilogo delle regole: in futuro fare un link ad aritmetica razionale (quando sviluppata) per vedere sia le regole che la loro dimostrazione .

---

1. Operazioni elementari

Chiamiamo **operazioni elementari** le operazioni interne nell'insieme **N** dei numeri naturali: cioe':

- L'addizione; Collegamento ad **N**
- La moltiplicazione Collegamento ad **N**

Anche se non e' molto preciso chiameremo l'**addizione** anche con il termine **somma**: non e' molto preciso perche' la somma e' il risultato mentre l'operazione e' l'addizione, ma ormai e' un errore di uso comune
Similmente chiameremo la **moltiplicazione** anche con il termine **prodotto**: anche qui non e' molto preciso perche' il prodotto e' il risultato mentre l'operazione e' la moltiplicazione.

---

2. Proprieta' dell' addizione

Elenchiamo semplicemente le proprieta' che ci interesseranno con un semplice esempio semplificativo: dimostreremo poi le varie proprieta' nella sezione dedicata ad aritmetica razionale:

- Proprieta' **associativa**
  Dire che vale la proprieta' associativa significa che sommando tre o piu' numeri e' indifferente quali di essi siano sommati prima o dopo; esempio:
  $3+2+5=(3+2)+5=3+(2+5)$
- Proprieta' **commutativa**
  Dire che vale la proprieta' commutativa significa che, nella somma di due numeri, la somma del primo col secondo numero e' uguale alla somma del secondo numero con il primo; esempio:
  $3+2=2+3$
- Esistenza dell' **elemento neutro**
  Dire che esiste l'elenento neutro significa che esiste un elemento che sommato a qualunque altro non ne varia il valore (nella somma lo zero); esempio:
  $3+0=0+3=3$
- Esistenza dell' **elemento inverso** (qui pero' siamo nell'insieme **Z** dei numeri Interi)
  Dire che esiste l'elenento inverso significa che esiste un elemento che sommato ad un altro ha come risultato l'elemento neutro (lo zero); esempio:
  $(-3)+(+3)=(+3)+(-3)=0$

3. Proprieta' della moltiplicazione

Elenchiamo semplicemente le proprieta' che ci interesseranno con un semplice esempio semplificativo:

- Proprieta' ***associativa***
  Dire che vale la proprieta' associativa significa che moltiplicando tre o piu' numeri e' indifferente quali di essi siano moltiplicati prima o dopo; esempio:
  $3\cdot 2\cdot 5=(3\cdot 2)\cdot 5=3\cdot(2\cdot 5)$
- Proprieta' ***commutativa***
  Dire che vale la proprieta' commutativa significa che, nel prodotto di due numeri, il prodotto del primo col secondo numero e' uguale al prodotto del secondo numero con il primo; esempio:
  $3\cdot 2=2\cdot 3$
- Esistenza dell' ***elemento neutro***
  Dire che esiste l'elenento neutro significa che esiste un elemento che moltiplicato a qualunque altro non ne varia il valore (nel prodotto l' uno): esempio
  $3\cdot 1=1\cdot 3=3$
- Esistenza dell' ***elemento inverso*** (qui pero' siamo nell'insieme **Q** dei numeri Razionali).
  Dire che esiste l'elemento inverso significa che esiste un elemento che moltiplicato ad un altro ha come risultato l'elemento neutro (l' uno); esempio:
  $3\cdot\frac{1}{3}=\frac{1}{3}\cdot 3=1$
- Esistenza dell' ***elemento assorbente***
  Dire che esiste l'elemento assorbente significa che esiste un elemento (lo zero) che

moltiplicato a qualunque altro trasforma il risultato in zero: esempio
$3 \cdot 0 = 0 \cdot 3 = 0$

4. Mutue proprieta' di somma e prodotto

Anche qui elenchiamo semplicemente la proprieta' che ci interessa con un semplice esempio semplificativo:

- Proprieta' **distributiva** della moltiplicazione rispetto all'addizione
  Significa che posso distribuire la moltiplicazione rispetto ai termini dell'addizione; esempio:
  $3 \cdot (2 + 5) = (3 \cdot 2) + (3 \cdot 5)$

C. *Strutture algebriche*

In questo capitolo, prendendo spunto dai numeri che abbiamo visto in aritmentica (naturali, interi, razionali, reali e complessi) evidenzieremo delle strutture che potranno essere applicate a vari enti ed insiemi matematici;
in questo modo potremo catalogare vari enti ed ampliare la conoscenza delle proprieta' degli insiemi stessi

---

- metodo operativo e nomenclatura
- struttura algebrica
- semigruppo
- gruppo
- anello
- corpo
- spazi vettoriali

1. Metodo operativo e nomenclatura

Inizieremo percorrendo passo passo la strada gia' percorsa con i numeri Naturali, Interi, Razionali e Reali, partendo dalle strutture piu' semplici fino ad arrivare a strutture piu' complesse; infine vedremo che le strutture trovate non sono esclusive dei numeri ma si ritrovano anche nelle matrici, nei vettori ed in altri enti matematici.

Per indicare una operazione generica utilizzeremo il simbolo $\textcircled{T}$, mentre se avremo bisogno di due operazioni contemporaneamente useremo i due simboli: $\oplus$ $\otimes$
Indicheremo un insieme con le lettere maiuscole dell'alfabeto latino **A, B, C, ...** mentre ne Indicheremo gli elementi con le lettere minuscole **a, b, c, ...**

---

2. Struttura algebrica

Prima di introdurre il concetto fondamentale di struttura algebrica esaminiamo alcuni concetti che ci saranno necessari.

- Legge di composizione interna
- Elemento neutro
- Elemento simmetrico
- Concetto di struttura algebrica

a) Legge di composizione interna

Dato un insieme di enti **A,** diremo che un' operazione Ⓣ e' di **composizione interna** se presi comunque due elementi di **A** quali **a**, **b**, esiste l'elemento **c** appartenente ad **A** tale che vale:

$$a \text{ Ⓣ } b = c$$

In pratica significa che il risultato dell'operazione e' anche lui un elemento dell'insieme di partenza

---

Si dice in modo equivalente che l'insieme **A** e' chiuso rispetto all'operazione Ⓣ.

Cioe' l'operazione agisce sul prodotto cartesiano **A x A** e lo trasforma ancora in **A:**

$$\text{Ⓣ}: A \times A \rightarrow A$$

Si puo' anche dire che componendo tramite l'operazione Ⓣ una coppia di elementi di **A** il risultato appartiene ancora ad **A:**

$$\text{Ⓣ}: (a, b) \rightarrow c \quad \text{con } a,b,c \in A$$

Esempi:
1) Considero l'insieme **N** dei numeri naturali con l'operazione di somma:
la somma e' un'operazione di composizione interna, infatti posso sempre sommare tra loro due numeri naturali ed il risultato e' sempre un numero naturale. Vedere anche somma in **N** .

2) Considero l'insieme **N** dei numeri naturali con l'operazione di differenza:
la differenza non e' un'operazione di composizione interna in **N**, infatti posso fare la differenza fra due numeri naturali solamente se il primo ha un valore maggiore del secondo mentre non posso sottrarre un numero maggiore da un numero minore. Vedere anche differenza in **N**.

---

b) Elemento neutro

Dato un insieme di enti **A** e su di esso un' operazione Ⓣ, diremo che **n** appartenente ad **A** e' l'**elemento neutro** rispetto all'operazione se per qualunque elemento **a** di **A** vale:

$$a \text{ Ⓣ } n = n \text{ Ⓣ } a = a$$

cioe' la composizione di qualunque elemento di **a** di **A** con **n** restituisce sempre lo stesso elemento **a**.

Esempi:
1) Considero l'insieme **N** dei numeri naturali con l'operazione di somma.
In questo caso l'elemento neutro e' lo zero; infatti chiamato a un qualunque numero naturale ho:
$a + 0 = 0 + a = a$

2) Considero l'insieme **N** dei numeri naturali con l'operazione di prodotto.
In questo caso l'elemento neutro e' l'uno; infatti chiamato a un qualunque numero naturale ho:
$a \times 1 = 1 \times a = a$

---

c) Elemento simmetrico

Dato un insieme di enti **A** e su di esso un' operazione Ⓣ, diremo che **a'** appartenente ad **A** e' l'**elemento simmetrico** rispetto all' elemento **a** di **A** vale:

$$a \text{ Ⓣ } a' = a' \text{ Ⓣ } a = n$$

cioe' la composizione di qualunque elemento di **a** di **A** con il proprio simmetrico restituisce sempre l'elemento neutro **n.**

Esempi:

1) Considero l'insieme **Z** dei numeri interi con l'operazione di somma.
In questo caso l'elemento simmetrico di un qualunque numero e' lo stesso numero cambiato di segno; infatti chiamato **a** un qualunque numero naturale ho:

$$a + (-a) = (-a) + a = 0$$

2) Considero l'insieme **Q** dei numeri razionali con l'operazione di prodotto.
In questo caso l'elemento simmetrico di un qualunque elemento **a** e' il suo inverso **1/a** ; infatti componendo ogni elemento con il suo inverso ottengo l'elemento neutro 1:

$$a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$$

d) Concetto di struttura algebrica

Su ogni insieme non vuoto **A** si possono definire una o piu' leggi di composizione interna;
Si definisce **struttura algebrica** un insieme non vuoto **A** su cui siano definite una o piu' leggi di composizione interna.

Semplificando:
Struttura algebrica = Insieme con operazione (i)

Indicheremo una struttura algebrica nei seguenti modi:

$(A ; Ⓣ)$ Struttura con una legge di composizione interna

$(A ; \oplus, \otimes)$ Struttura con due leggi di composizione interna.

3. Semigruppo

La prima struttura e' ricalcata sull'insieme **N** con l'operazione di addizione od anche con l'operazione di moltiplicazione: e' la struttura piu' semplice ed e' possibile individuarla in moltissimi argomenti.

Si definisce ***semigruppo*** ogni insieme di enti **A** su cui sia definita un' operazione interna Ⓣ associativa; cioe' $(A ; Ⓣ)$ e' semigruppo se Ⓣ e' associativa; vale a dire che per ogni elemento **a**, **b**, **c** di **A** vale:

$$(a \text{ Ⓣ } b) \text{ Ⓣ } c = a \text{ Ⓣ } (b \text{ Ⓣ } c)$$

Se l'operazione e' commutativa il semigruppo si dice **commutativo** od anche **abeliano.**
Se inoltre un semigruppo e' dotato di **elemento neutro** allora si chiama **monoide.**

Esempi:
1) Considero l'insieme **N** dei numeri naturali con l'operazione di addizione.
In questo caso ho:
- un semigruppo perche' l'addizione e' associativa
- e' abeliano perche' l'addizione e' commutativa
- e' un monoide perche' esiste l'elemento neutro (lo zero).

---

2) Considero l'insieme **N** dei numeri naturali con l'operazione di moltiplicazione.
In questo caso ho:
- un semigruppo perche' la moltiplicazione e' associativa
- e' abeliano perche' la moltiplicazione e' commutativa
- e' un monoide perche' esiste l'elemento neutro (l' uno).

---

3) Considero l'insieme **P** dei numeri naturali pari con l'operazione di prodotto.
In questo caso ho:
- un semigruppo perche' la moltiplicazione e' associativa
- e' abeliano perche' la moltiplicazione e' commutativa
- non e' un monoide perche'in **P** non esiste l'elemento neutro (l'uno non e' pari).

---

4) Considero l'insieme **Q** dei numeri Razionali con l'operazione di divisione.
L'operazione di divisione non e' associativa infatti:
$(12 : 6) : 2 \neq 12 : (6 : 2)$
Eseguendo i calcoli nel primo caso ottengo:
$(12 : 6) : 2 = 2 : 2 = 1$
nel secondo caso ottengo:
$12 : (6 : 2) = 12 : 3 = 4$
Quindi l'insieme dei numeri razionali con l'operazione di divisione non forma semigruppo.

a) Un esempio da illusionista: i tre bicchieri

Per farti capire l'importanza delle strutture ti faccio un semplice esempio; un gioco di prestigio, da fare ad un amico una volta sola, altrimenti si capisce il trucco.
Prendi 3 bicchieri (possibilmente a calice: fa piu' scena) e ponili nel seguente modo:

Poi dici al tuo amico:
"Guarda come faccio: prendo due bicchieri vicini e li rovescio finche' non ho tutti e tre i bicchieri con il calice in alto"
Ed esegui nel seguente modo:
- prima rovesci i primi due a sinistra:

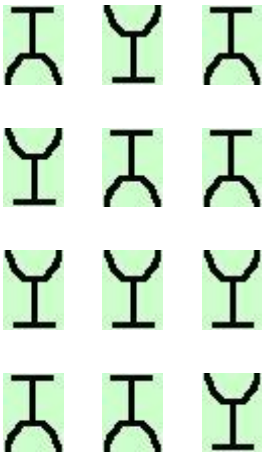
- poi rovesci il secondo ed il terzo ed ottieni il risultato:

Adesso prendi il bicchiere centrale, lo rovesci e dici al tuo amico:
"Hai visto come e' semplice; adesso fallo tu" Siccome adesso la configurazione e':

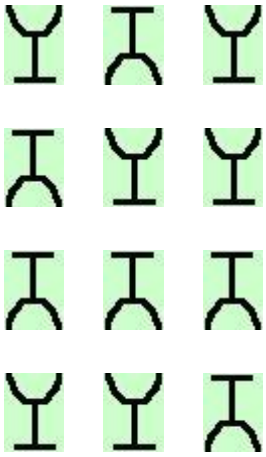
Potrai divertirti a vedere il tuo amico cercare di portare i tre bicchieri con il calice in alto, senza potervi riuscire, ma tu rifiuta di spiegarlo.

Perche' non puo' riuscire? Semplicemente perche' le varie configurazioni dei due calici fanno parte di due semigruppi diversi e il rovesciare due bicchieri adiacenti e' l'operazione associativa sull'insieme delle configurazioni ed e' un'operazione interna nel senso che partendo da un oggetto del semigruppo ottieni sempre e solo elementi del semigruppo.
Ti mostro i due semigruppi delle configurazioni possibili.

Configurazioni del primo semigruppo



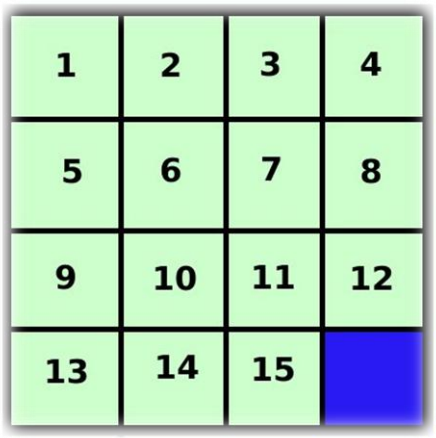
Configurazioni del secondo semigruppo



Sono 8 possibili configurazioni perche' sono disposizioni con ripetizione su due elementi (diritto e rovescio) di classe 3 (numero dei bicchieri) (calici): $2^3=8$

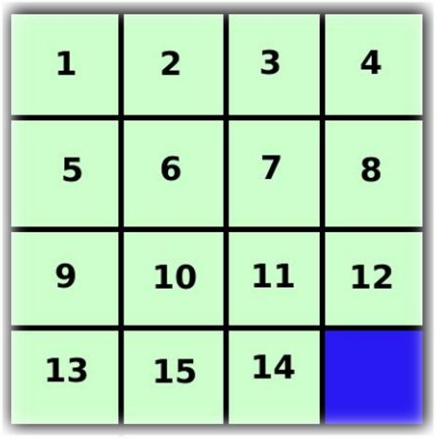
b) Il gioco del 15

E' un vecchio gioco degli anni 60: si tratta di una cornice con 15 tesserine identiche numerate da 1 a 15 in disordine e devono essere messe in ordine dall'1 al 15; utilizzando il quadratino vuoto puoi fare scorrere le tessere adiacenti. La configurazione giusta da ottenere e' la seguente:



Partendo da questa e spostando le varie tessere utilizzando la casella vuota e' sempre possibile tornale alla configurazione iniziale.

Se pero' estrai una tesserina e la rimonti ad esempio in questo modo:



(ho scambiato il 15 con il 14), allora non sara' piu' possibile ottenere la configurazione delle tesserine numerate da 1 a 15.

Anche qui, come nell'esempio precedente rispetto all'operazione di fare scorrere le tesserine utilizzando la casella vuota otteniamo due diversi semigruppi di configurazioni uno indipendente dall'altro.

4. Gruppo

Abbiamo qui una struttura un po' piu' complessa che ci e' suggerita dall'insieme **Z** con l'operazione di addizione od anche dall'insieme **Q-{0}** (Insieme dei razionali escluso il numero 0) con l'operazione di moltiplicazione

---

Si definisce ***gruppo*** **(A ; Ⓣ)** un insieme di enti **A** su cui sia definita un' operazione Ⓣ che goda delle seguenti proprieta':

1. Ⓣ e' interna cioe'

   (a Ⓣ b) ∈ A

2. Ⓣ e' associativa, cioe'

   (a Ⓣ b) Ⓣ c = a Ⓣ (b Ⓣ c)

3. Ⓣ possiede l'elemento neutro **n**

   a Ⓣ n = n Ⓣ a = a

4. ogni elemento **a** possiede inⓉ l'elemento simmetrico **a'** tale che:

   a Ⓣ a' = a' Ⓣ a = n

Se il gruppo gode della proprieta' commutativa allora il gruppo si dice ***commutativo*** o ***abeliano.***
Se il gruppo ha un numero finito di elementi allora si chiama ***gruppo finito*** e dal numero **n** dei suoi elementi si dice anche ***gruppo di ordine n*** .

Nella prossima pagina qualche esempio servira' a chiarire meglio in concetto.

---

a) Esempi di strutture di gruppo

1) Consideriamo l'insieme **Z** dei numeri interi con l'operazione di addizione: allora la struttura **(Z; +)** e' una struttura di gruppo; infatti:

- La somma in **Z** e' un'operazione interna; il risultato della somma appartiene sempre a **Z**
- La somma in **Z** e' associativa, infatti presi comunque tre numeri interi **a**, **b** e **c**, vale sempre la proprieta':
  $(a + b) + c = a + (b + c)$
- Lo zero **0** e' l'elemento neutro per la somma in **Z**, infatti preso comunque un numero intero **a** vale sempre la proprieta':
  $a + 0 = 0 + a = a$
- L'elemento simmetrico rispetto alla somma in **Z** e' l'elemento che ha il segno cambiato (opposto), infatti preso comunque un numero intero **a** vale sempre la proprieta':
  $a + (-a) = (-a) + a = 0$

---

2) Consideriamo l'insieme **Q** dei numeri razionali con l'operazione di moltiplicazione $\cdot$. Allora la struttura **(Q; $\cdot$)** non e' una struttura di gruppo. Infatti, sono verificate la prima e la seconda proprieta' ma esiste un elemento, lo zero **0** che non possiede l'elemento inverso e quindi non e' verificata la terza proprieta' dei gruppi.

Mentre per mostrare che una proprieta' e' vera devi dimostrarla per tutti gli elementi su cui agisce; per dimostrare che una proprieta' e' falsa e' sufficiente far vedere che esiste un elemento per cui tale proprieta' non e' valida.

---

3) Consideriamo invece l'insieme **Q - {0}** dei numeri interi senza lo zero con l'operazione di moltiplicazione; allora la struttura **(Q - {0}; $\cdot$)** e' una struttura di gruppo. Infatti:

- Il prodotto in **Q - {0}** e' un'operazione interna; il risultato del prodotto fra due numeri in **Q - {0}** appartiene sempre a **Q - {0}**
- Il prodotto in **Q - {0}** e' associativo; infatti presi comunque tre numeri interi **a**, **b** e **c**, vale sempre la proprieta':
  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- L'uno **1** e' l'elemento neutro per il prodotto in **Q - {0}**; infatti preso comunque un numero razionale **a** vale sempre la proprieta':
  $a \cdot 1 = 1 \cdot a = a$
- L'elemento simmetrico rispetto al prodotto in **Q - {0}** e' l'elemento del tipo 1/a (inverso); infatti preso comunque un numero intero **a** vale sempre la proprieta':
  $a \cdot \frac{1}{a} = \frac{1}{a} \cdot a = 1$
  e, non essendoci lo zero, ogni elemento ha un suo inverso.

---

4) Vediamo un gruppo parecchio "strano".
Prendiamo l'insieme composto dal solo numero uno **{ 1 }** con l'operazione di moltiplicazione; **({ 1 } , $\cdot$)** e' un gruppo. Infatti:

- L'operazione di prodotto e' interna: il risultato e' sempre **1**
- Il prodotto in **{ 1 }** e' associativo; infatti:
  $(1 \cdot 1) \cdot 1 = 1 \cdot (1 \cdot 1)$

- L'uno **1** e' l'elemento neutro per il prodotto in **{ 1 }**; infatti:
  $1 \cdot 1 = 1 \cdot 1 = 1$
- L'elemento simmetrico rispetto al prodotto in **{ 1 }** e' lo stesso 1; infatti:
  $1 \cdot 1 = 1 \cdot 1 = 1$
  essendo l'1 finale l'elemento neutro.

Esercizio:
Prova a dimostrare che l'insieme composto dal solo numero zero **{ 0 }** con l'operazione di addizione **+**
({ 0 } , +) e' un gruppo. Questo ed il gruppo precedente vengono anche chiamati ***gruppo banale***.

b) Proprieta' dei gruppi

Vediamo ora alcune proprieta' dei gruppi e facciamone la dimostrazione. Vedrai un tipo di ragionamento piuttosto "originale" ma che porta ad ottimi risultati:

- Unicita' dell'elemento neutro
- Unicita' dell'elemento simmetrico
- Ogni elemento e' semplificabile

(1) Unicita' dell'elemento neutro

Proprieta':

In ogni gruppo (A ; Ⓣ) l'elemento neutro e' unico.

Cioe' in ogni gruppo c'e' un elemento neutro ed uno solo.

Dimostrazione:

Ipotesi: (A ;Ⓣ) e' un gruppo

Tesi: l'elemento neutro **n** e' unico

Per definizione di gruppo un elemento neutro deve esistere quindi bastera' dimostrare che c'e n'e' uno solo (e' unico).
Per assurdo supponiamo che esistano due elementi neutri **n** ed **u**; allora avro' per ogni elemento **a** di **A**:

1) $n \text{ Ⓣ } a = a \text{ Ⓣ } n = a$
2) $u \text{ Ⓣ } a = a \text{ Ⓣ } u = a$

Ora, essendo **u** un elemento di **A** considero **a = u** ed ottengo dalla prima:

$n \text{ Ⓣ } u = u \text{ Ⓣ } n = u$

Poi essendo **n** un elemento di **A** considero **a = n** ed ottengo dalla seconda:

$u \text{ Ⓣ } n = n \text{ Ⓣ } u = n$

Confrontando le uguaglianze sopra ottengo:

$n = u$

Cioe', se esistono due elementi neutri, essi sono uguali. Come volevamo dimostrare.

(2) Unicita' dell'elemento simmetrico

Proprieta':

In ogni gruppo (A ; Ⓣ) per ogni elemento a esiste un solo elemento simmetrico.

Dimostrazione:

Ipotesi: (A ;Ⓣ) e' un gruppo

Tesi: per ogni elemento **a** e' unico **a'** tale che **a Ⓣ a'= n**

Per definizione di gruppo, dato un elemento **a,** il simmetrico deve esistere, quindi bastera' dimostrare che c'e n'e' uno solo (e' unico).
Per assurdo supponiamo che, dato l'elemento **a** esistano due elementi simmetrici **a'** ed **a"**; allora avro' per definizione di elemento simmetrico :

1) **a Ⓣ a' = a' Ⓣ a = n**
2) **a Ⓣ a" = a" Ⓣ a = n**

Sviluppo **a'** fino ad ottenere **a":**

a' = a' Ⓣ n =

al posto di **n** metto **(a Ⓣ a")**

= a' Ⓣ (a Ⓣ a") =

Uso la proprieta' associativa per collegare **a** con **a':**

= (a' Ⓣ a) Ⓣ a" =

Ma **(a' Ⓣ a) = n** quindi:

= n Ⓣ a" =

e, per la proprieta' dell'elemento neutro **n** :

= a"

Quindi leggendo il primo e l'ultimo termine dell'uguaglianza ottengo:

a' = a"

Cioe', se esistono due elementi simmetrici, essi sono uguali. Come volevamo dimostrare.

(3) Ogni elemento e' semplificabile

Proprieta':

In ogni gruppo (A ;Ⓣ) per ogni elemento a, b, c da

a Ⓣ b = a Ⓣ c

segue b = c

Cioe' posso togliere la **a**; sarebbe a dire che ogni elemento si ottiene da un altro in modo unico.

Dimostrazione:

Ipotesi: **(A ;Ⓣ)** e' un gruppo, **a Ⓣ b = a Ⓣ c**

Tesi: **b = c**

Partiamo dall'uguaglianza dell'ipotesi.
Per arrivare alla tesi dobbiamo eliminare la **a;** quindi componiamo i due membri dell'uguaglianza con **a'** (un elemento si elimina con il suo inverso) :

a' Ⓣ (a Ⓣ b) = a' Ⓣ (a Ⓣ c)

Ora applico la proprieta' associativa in modo da mettere **a'** con **a** :

(a' Ⓣ a) Ⓣ b = (a' Ⓣ a) Ⓣ c

Ora so che **(a' Ⓣ a)** e' l'elemento neutro **n** :

n Ⓣ b = n Ⓣ c

E per definizione di elemento neutro:

b = c

Come volevamo dimostrare.

c) Insieme dei resti modulo **p** o relazione di congruenza modulo **p**

Dipendentemente dal tuo libro di testo avrai la prima o la seconda denominazione.

Ricordo quando all'Universita' incontrai per la prima volta l'algebra astratta: non riuscivo a dare un senso a tutta quella teoria campata in aria: semigruppi, gruppi... non ci vedevo nient'altro che una generalizzazione degli insiemi numerici!
Poi finalmente il Professore ci fece una lezione sull'insieme dei resti modulo p e, finalmente, tutto quanto mi apparve sotto una nuova luce: non si trattava solo di una generalizzazione degli insiemi numerici, ma di di una nuova costruzione logica che prometteva grandi risultati.

Per comprendere bene lo svolgimento e' necessario conoscere bene la teoria degli insiemi in generale e le relazioni di equivalenza; in particolare:

- Cosa significa resto modulo p
- Relazione di equivalenza ed insieme quoziente su N
- Collegamento ai sistemi di numerazione
- Rappresentazione di un gruppo finito mediante la tabella di Cayley
- Insieme dei resti modulo p (o relazione di congruenza modulo p)

(1) Cosa significa resto modulo p

Consideriamo l'insieme **N** dei numeri naturali con l'operazione di divisione per un numero ad esempio divisione per 5: allora per ogni numero naturale otterro' un quoziente ed un resto; ad esempio:

7 : 5 da' quoziente 1 e resto 2
10 : 5 da' quoziente 2 e resto 0
12 : 5 da' quoziente 2 e resto 2
19 : 5 da' quoziente 3 e resto 4

In pratica, per i quozienti posso ottenere vari risultati mentre per i resti i risultati saranno solamente:

0, 1, 2, 3, 4.

Se non hai capito, ecco:
Facciamo la divisione per 5 per tutti i numeri naturali:

0 : 5 da' quoziente 0 e resto 0
1 : 5 da' quoziente 0 e resto 1
2 : 5 da' quoziente 0 e resto 2
3 : 5 da' quoziente 0 e resto 3
4 : 5 da' quoziente 0 e resto 4
5 : 5 da' quoziente 1 e resto 0
6 : 5 da' quoziente 1 e resto 1
7 : 5 da' quoziente 1 e resto 2
8 : 5 da' quoziente 1 e resto 3
9 : 5 da' quoziente 1 e resto 4

10 : 5 da' quoziente 2 e resto 0
11 : 5 da' quoziente 2 e resto 1
. . . . . .
. . . . . .
Se osservi i resti essi sono:
0, 1, 2, 3, 4, 0, 1, 2, 3, 4, 0, 1, ...
Cioe' partono da **0** fino a **4** poi si ripetono
Quindi i resti possibili sono solamente:
0, 1, 2, 3, 4.

Se la divisione la facciamo per 4, allora anche qui otterro' per ogni numero naturale un quoziente ed un resto. Esempio:

7 : 4 da' quoziente 1 e resto 3
10 : 4 da' quoziente 2 e resto 2
12 : 4 da' quoziente 3 e resto 0
19 : 4 da' quoziente 4 e resto 3

In questo caso per i quozienti posso ottenere vari risultati, mentre per i resti i risultati saranno solamente:
0, 1, 2, 3.

Se non hai capito, ecco:
Facciamo la divisione per 4 per tutti i numeri naturali:
0 : 4 da' quoziente 0 e resto 0
1 : 4 da' quoziente 0 e resto 1
2 : 4 da' quoziente 0 e resto 2
3 : 4 da' quoziente 0 e resto 3
4 : 4 da' quoziente 1 e resto 0
5 : 4 da' quoziente 1 e resto 1
6 : 4 da' quoziente 1 e resto 2
7 : 4 da' quoziente 1 e resto 3
8 : 4 da' quoziente 2 e resto 0
9 : 4 da' quoziente 2 e resto 1
10 : 4 da' quoziente 2 e resto 2
11 : 4 da' quoziente 2 e resto 3
. . . . . .
. . . . . .
Se osservi i resti essi sono:
0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3 . . . . .
Cioe' partono da **0** fino a **3** poi si ripetono.
Quindi i resti possibili sono solamente:
0, 1, 2, 3.

Proviamo la divisione per 9, anche qui otterro' per ogni numero naturale un quoziente ed un resto. Esempio:

7 : 9 da' quoziente 0 e resto 7
10 : 9 da' quoziente 1 e resto 1
12 : 9 da' quoziente 1 e resto 3
19 : 9 da' quoziente 2 e resto 1

In questo caso per i quozienti posso ottenere vari risultati, mentre per i resti i risultati saranno solamente:
0, 1, 2, 3, 4, 5, 6, 7, 8.

Per capire meglio, ecco:
Facciamo la divisione per 9 per tutti i numeri naturali:
0 : 9 da' quoziente 0 e resto 0
1 : 9 da' quoziente 0 e resto 1
2 : 9 da' quoziente 0 e resto 2
3 : 9 da' quoziente 0 e resto 3
4 : 9 da' quoziente 0 e resto 4
5 : 9 da' quoziente 0 e resto 5
6 : 9 da' quoziente 0 e resto 6

7 : 9 da' quoziente 0 e resto 7
8 : 9 da' quoziente 0 e resto 8
9 : 9 da' quoziente 1 e resto 0
10 : 9 da' quoziente 1 e resto 1
11 : 9 da' quoziente 1 e resto 2
12 : 9 da' quoziente 1 e resto 3
13 : 9 da' quoziente 1 e resto 4
14 : 9 da' quoziente 1 e resto 5
15 : 9 da' quoziente 1 e resto 6
16 : 9 da' quoziente 1 e resto 7
17 : 9 da' quoziente 1 e resto 8
18 : 9 da' quoziente 2 e resto 0
19 : 9 da' quoziente 2 e resto 1
11 : 9 da' quoziente 1 e resto 2
. . . . . .
. . . . . .
Se osservi i resti essi sono:
0, 1, 2, 3, 4, 5, 6, 7, 8, 0, 1, 2, 3, 4, 5, 6, 7, 8, 0, 1 . . . . .
Cioe' partono da **0** fino a **8** poi si ripetono.
Quindi i resti possibili sono solamente:
0, 1, 2, 3, 4, 5, 6, 7, 8.

(2) Relazione di equivalenza ed insieme quoziente su N

Ora procediamo su un esempio numerico per il divisore (5); poi potremo generalizzare a tutti i naturali maggiori di 1 (Nota):

Nota! Posso considerare solo i numeri Naturali maggiori di 1 perche':
- Non posso considerare lo zero perche' non ha senso la divisione di un numero per zero
- Se faccio la divisione per 1, essendo 1 il divisore di tutti i numeri, ottengo come resto sempre lo zero; quindi, per i resti, non avrebbe senso considerare la divisione per 1

Considero il resto dell'operazione di divisione su **N** per 5.
La relazione:
"Avere lo stesso resto nell'operazione di divisione di un numero naturale per 5"
e' una relazione di equivalenza: Dimostrazione (*Scheda C1*)
Questa relazione di equivalenza, applicata all'insieme **N**, lo suddivide nei sottoinsiemi (partizione di **N**):

- Sottoinsieme degli elementi che hanno come resto **0**
- Sottoinsieme degli elementi che hanno come resto **1**
- Sottoinsieme degli elementi che hanno come resto **2**
- Sottoinsieme degli elementi che hanno come resto **3**
- Sottoinsieme degli elementi che hanno come resto **4**

Se ora considero l'insieme quoziente, allora da **N** ottengo l'**insieme dei resti modulo 5**
$r_5 = \{ 0, 1, 2, 3, 4 \}$

Lo chiamo con la lettera minuscola per non confonderlo con l'insieme **R** dei numeri reali.

Potro' applicare lo stesso ragionamento con qualunque divisore che sia un elemento di **N** diverso da 0 ed 1.
Nelle prossime pagine su questi insiemi $r_5, r_4, r_3, r_2, r_6, r_7, r_8, r_9, \ldots$ studieremo nei particolari le strutture di gruppo con le operazioni $\oplus$ $\otimes$.

Inizio prima da r_5 perche' siamo partiti da questo esempio, poi sviluppero' r_4 r_3 e, particolarmente importante, r_2, poi riprendero' da r_6 e continuero' fino ad r_9, ma potrei continuare tranquillamente fin dove voglio.

Scheda n. C1

Dimostriamo che la relazione su **N**:
"Avere lo stesso resto nell'operazione di divisione di un numero naturale per 5"
e' una relazione di equivalenza:
Dobbiamo dimostrare che la relazione e' riflessiva, simmetrica e transitiva :

- E' ***riflessiva*** perche' lo stesso numero diviso per 5 avra' sempre lo stesso resto.
- E' ***simmetrica*** perche', se il numero **a** ha lo stesso resto del numero **b,** allora anche il numero **b** ha lo stesso resto del numero **a**. Esempio se 7 ha lo stesso resto di 12 allora anche 12 ha lo stesso resto di 7
- E' ***transitiva*** : se **a** ha lo stesso resto di **b** e **b** ha lo stesso resto di **c** allora **a** ha lo stesso resto di **c** esempio se 7 ha lo stesso resto di 12 e 12 ha lo stesso resto di 27 allora 7 ha lo stesso resto di 27

(3) Collegamento ai sistemi di numerazione

Non posso procedere senza fare notare i profondi collegamenti che esistono fra i resti modulo **p** e i sistemi di numerazione in base **p** .
Dopo sviluppati i sistemi di numerazione sostituire la pagina con un link ai sistemi di numerazione.

Vedremo, nei sistemi di numerazione, che , per trovare le cifre di un numero in base qualunque **p** (sistema di numerazione in base **p**) bastera' calcolarne i successivi resti della divisione del numero per **p** e poi considerare tali resti in ordine inverso: cio' deriva dal fatto che consideriamo i numeri in forma polinomiale e quindi, dividendo un numero per **p** troviamo i successivi termini con le potenze di p.
Due esempi serviranno a rendere meglio l'idea.

Prima un esempio banale. Consideriamo il numero decimale:
34567
in forma polinomiale posso scriverlo come:
$3\cdot10^4 + 4\cdot10^3 + 5\cdot10^2 + 6\cdot10^1 + 7\cdot10^0$
Se ora divido questo numero per 10, ottengo che tutte le potenze del 10 diminuiscono di 1 e l'ultimo termine e' il resto:
- quoziente = $3\cdot10^3 + 4\cdot10^2 + 5\cdot10^1 + 6\cdot10^0$
- resto = 7

Dividendo ancora per 10 avro':
- quoziente = $3\cdot10^2 + 4\cdot10^1 + 5\cdot10^0$
- resto = 6

Dividendo ancora per 10 avro':
- quoziente = $3\cdot10^1 + 4\cdot10^0$
- resto = 5

Divido ancora per 10 ed ho:
- quoziente = $3\cdot10^0$
- resto = 4

Divido ancora per 10 ed ho:
- quoziente = 0
- resto = 3

Se scrivo i resti in ordine inverso, ottengo il numero in base 10 (naturalmente coincide con il numero di partenza:
34567

Proviamo ora a scrivere lo stesso numero in base 5:
$(34567)_{10} = (\dots)_5$
Divido il numero per 5 una prima volta:
- quoziente = **6913** - resto = **2**
Divido per 5
- quoziente = **1382** - resto = **3**
Divido per 5
- quoziente = **276** - resto = **2**
Divido per 5
- quoziente = **55** - resto = **1**
Divido per 5
- quoziente = **11** - resto = **0**
Divido per 5
- quoziente = **2** - resto = **1**
Divido per 5
- quoziente = **0** - resto = **2**
Quindi ottengo:
$(34567)_{10} = (2101232)_5$
Equivale a dire che:
$3\cdot10^4 + 4\cdot10^3 + 5\cdot10^2 + 6\cdot10^1 + 7\cdot10^0 = 2\cdot5^6 + 1\cdot5^5 + 0\cdot5^4 + 1\cdot5^3 + 2\cdot5^2 + 3\cdot5^1 + 2\cdot5^0$

Quoziente	Resto
34567	
6913	2
1382	3
276	2
55	1
11	0
2	1
0	2

Visti questi legami potremo anche considerare le tabelle di Cayley (che faremo nella prossima pagina) come le tavole pitagoriche per la somma e per la moltiplicazione dei vari sistemi di numerazione, pero' ristrette al solo numero finale.

(4) Rappresentazione di un gruppo finito mediante la tabella di Cayley

E' possibile rappresentare i gruppi finiti (gruppi con un numero finito di elementi) mediante dei particolari diagrammi chiamati diagrammi di Cayley. Vediamoli su un paio di gruppi.

Considero l'insieme A che ha come elementi:
- primo elemento = insieme dei numeri pari = **p**
- secondo elemento = insieme di numeri dispari = **d**

$A = \{ p , d \}$
Considero l'operazione di addizione $\oplus$
Allora $\{ A , \oplus \}$ e' un gruppo.
Posso rappresentarlo come:

$\oplus$	p	d
p	p	d
d	d	p

E' come una tavola pitagorica: i dati sono quelli neri; quelli rossi li trovo come incrocio, ad esempio:
$p \oplus p = p$ pari piu' pari uguale pari
$p \oplus d = d$ pari piu' dispari uguale dispari
$d \oplus p = d$ dispari piu' pari uguale dispari
$d \oplus d = p$ dispari piu' dispari uguale pari

Osservando la tabella di Cayley, vedi la struttura di gruppo; nel nostro caso **p** e' l'elemento neutro. L'elemento inverso lo trovi guardando le caselle che hanno come risultato l'elemento neutro: nel nostro caso l'inverso di **d** e' **d**.

Altro esempio: (devi saper usare i numeri immaginari)
Considero l'insieme $A = \{ i, -1, -i, 1 \}$ sono le potenze di i
con l'operazione di moltiplicazione $\otimes$.
La struttura $\{ A , \otimes \}$ e' un gruppo.
Posso rappresentarlo come:

$\otimes$	1	i	-1	-i
1	1	i	-1	-i
i	i	-1	-i	1
-1	-1	-i	1	i
-i	-i	1	i	-1

Dalla tabella puoi vedere che:
1 e' l'elemento neutro (moltiplicandolo per gli altri non li cambia).
Per trovare l'inverso basta che guardi quando i risultati sono 1; gli 1 sono all'incrocio di elementi inversi. Quindi:
1 e' l'opposto di se' stesso
-1 e' l'opposto di se' stesso
i e' l'opposto di **-i**

Se il gruppo e' commutativo allora la tabella di Cayley e' simmetrica rispetto alla diagonale principale.

Vediamone un altro:
Consideriamo tutte le possibili rotazioni attorno al punto di incontro delle diagonali da far eseguire ad un quadrato in modo che i vertici siano sempre coincidenti.

L'operazione di rotazione Ⓣ avra' solamente 4 valori (essendo ciclica per 360° cioe' dopo 360 ° si ripete): $a_1 = 0°$ $a_2 = 90°$ $a_3 = 180°$ $a_4 = 270°$
La tabella di Cayley sara' quindi:

Ⓣ	a_1	a_2	a_3	a_4
a_1	a_1	a_2	a_3	a_4
a_2	a_2	a_3	a_4	a_1
a_3	a_3	a_4	a_1	a_2
a_4	a_4	a_1	a_2	a_3

Da notare che ponendo:
$a_1 = 1 \quad a_2 = i \quad a_3 = -1 \quad a_4 = -i$
i due gruppi precedenti coincidono. Infatti, i numeri complessi e le rotazioni nel piano sono diversi aspetti della stessa realta'.

(5) Insieme dei resti modulo p (o relazione di congruenza modulo p)

Per ogni insieme di resti $\mathbf{r_p}$ considereremo sia la struttura con operazione additiva $(\mathbf{r_p}, \oplus)$ che la struttura con operazione moltiplicativa $(\mathbf{r_p}, \otimes)$

- Insieme dei resti modulo 5
- Insieme dei resti modulo 4
- Insieme dei resti modulo 3
- Insieme dei resti modulo 2
- Insieme dei resti modulo 6
- Insieme dei resti modulo 7
- Insieme dei resti modulo 8
- Insieme dei resti modulo 9
- Insieme dei resti modulo 10

(a) Insieme dei resti modulo 5

Vediamo prima il gruppo additivo $(\mathbf{r_5}, \oplus)$

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Dalla tabella puoi vedere che:
0 e' l'elemento neutro (sommandolo per gli altri non li cambia).
Per trovare l'inverso basta che guardi quando i risultati sono 0; gli 0 sono all'incrocio di elementi inversi. Quindi:
2 e' l'opposto di **3** e viceversa
1 e' l'opposto di **4** e viceversa
0 e' l'opposto di se' stesso
Quando abbiamo un gruppo additivo l'elemento inverso si chiama anche opposto.

Vediamo quindi la tabella di Cayley per $(\mathbf{r_5}, \otimes)$

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Dalla tabella puoi vedere che:
0 e' l'elemento assorbente (moltiplicandolo per gli altri li fa diventare 0 (li assorbe); per poter avere la struttura di gruppo dovresti togliere lo zero, $(r_5 - \{0\}, \otimes)$ perche' lo zero non ha elemento inverso.
Questo ragionamento sara' possibile farlo quando l'ordine del gruppo e' un numero primo, invece per basi quali 4,6,8,9,... vedremo che nella tabella moltiplicativa compariranno dei divisori dello zero, di conseguenza non potremo piu' parlare di gruppo.
1 e' l'elemento neutro (moltiplicandolo per gli altri non li cambia.
Per trovare l'inverso basta che guardi quando i risultati sono 1; gli 1 sono all'incrocio di elementi inversi. Quindi:
2 e' l'inverso di **3** e viceversa
1 e' l'inverso di se' stesso
4 e' l'inverso di se' stesso
Tabelle di questo tipo ci suggeriscono una nuova struttura: l'anello.

(b) *Insieme dei resti modulo 4*

Vediamo prima il gruppo additivo $(r_4, \oplus)$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Dalla tabella puoi vedere che:
0 e' l'elemento neutro (sommandolo per gli altri non li cambia).
Per trovare l'inverso basta che guardi quando i risultati sono 0; gli 0 sono all'incrocio di elementi inversi. Quindi:
1 e' l'opposto di **3** e viceversa

2 e' l'opposto di se' stesso
Quando abbiamo un gruppo additivo l'elemento inverso si chiama anche opposto.

Vediamo quindi la tabella di Cayley per $(r_4, \otimes)$

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Dalla tabella puoi vedere che:
0 e' l'elemento assorbente: moltiplicandolo per gli altri li fa diventare 0 (li assorbe).
Qui non puoi avere la struttura di gruppo nemmeno togliendo lo zero, $(r_4 - \{0\}, \otimes)$ perche' il valore 2 e' un divisore dello zero : $2 \otimes 2 = 0$.
1 e' l'elemento neutro (moltiplicandolo per gli altri non li cambia
Per trovare l'inverso basta che guardi quando i risultati sono 1; gli 1 sono all'incrocio di elementi inversi. Quindi:
0 non ha inverso
2 non ha inverso
1 e' l'inverso di se' stesso
3 e' l'inverso di se' stesso

Da notare che troveremo un numero divisore dello zero quando il numero p di r_p non e' primo, cioe' troveremo divisori dello zero in $r_4, r_6, r_8, r_9, \ldots$ inoltre il numero per se' stesso dara' 0 quando p e' un quadrato perfetto, cioe' in $r_4, r_9, r_{16}, \ldots$

(c) *Insieme dei resti modulo 3*

Vediamo prima il gruppo additivo $(r_3, \oplus)$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Dalla tabella puoi vedere che:
0 e' l'elemento neutro (sommandolo per gli altri non li cambia).
Per trovare l'inverso basta che guardi quando i risultati sono 0; gli 0 sono all'incrocio di elementi inversi. Quindi:

0 e' l'opposto di se' stesso
1 e' l'opposto di **2** e viceversa

Vediamo quindi la tabella di Cayley per $(r_3, \otimes)$

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Dalla tabella puoi vedere che:
0 e' l'elemento assorbente: moltiplicandolo per gli altri li fa diventare 0 (li assorbe).
Per poter avere la struttura di gruppo dovresti togliere lo zero, $(r_3 - \{0\}, \otimes)$ perche' lo zero non ha elemento inverso.
1 e' l'elemento neutro (moltiplicandolo per gli altri non li cambia.
Per trovare l'inverso basta che guardi quando i risultati sono 1; gli 1 sono all'incrocio di elementi inversi. Quindi:
0 non ha inverso
1 e' l'inverso di se' stesso
2 e' l'inverso di se' stesso.

(d) *Insieme dei resti modulo 2*

Questa e'importantissima: e' alla base del sistema di numerazione a base 2, cioe' del sistema di numerazione su cui si basa l'Informatica. Inoltre, puoi trovarne strutture isomorfe in varie discipline.

Vediamo prima il gruppo additivo $(r_2, \oplus)$

$\oplus$	0	1
0	0	1
1	1	0

Dalla tabella puoi vedere che:
0 e' l'elemento neutro (sommandolo per gli altri non li cambia).
Per trovare l'inverso basta che guardi quando i risultati sono 0; gli 0 sono all'incrocio di elementi inversi. Quindi:
0 e' l'inverso di se' stesso
1 e' l'inverso di se' stesso

Vediamo quindi la tabella di Cayley per $(r_2, \otimes)$

$\otimes$	0	1
0	0	0
1	0	1

Dalla tabella puoi vedere che:
0 e' l'elemento assorbente: moltiplicandolo per gli altri li fa diventare 0 (li assorbe).
Per poter avere la struttura di gruppo dovresti togliere lo zero, $(r_3 - \{0\}, \otimes)$ perche' lo zero non ha elemento inverso, ma ottieni il gruppo banale (vedi il 4º esempio e l'esercizio della pagina).
1 e' l'elemento neutro (moltiplicandolo per gli altri non li cambia)
Per trovare l'inverso basta che guardi quando i risultati sono 1; gli 1 sono all'incrocio di elementi inversi. Quindi:
0 non ha inverso
1 e' l'inverso di se' stesso.

(e) *Insieme dei resti modulo 6*

Vediamo prima il gruppo additivo $(r_6, \oplus)$

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Dalla tabella puoi vedere che:
0 e' l'elemento neutro (sommandolo per gli altri non li cambia).
Per trovare l'inverso basta che guardi quando i risultati sono 0; gli 0 sono all'incrocio di elementi inversi. Quindi:
1 e' l'opposto di **5** e viceversa
2 e' l'opposto di **4** e viceversa
3 e' l'opposto di se' stesso
0 e' l'opposto di se' stesso
Quando abbiamo un gruppo additivo l'elemento inverso si chiama anche opposto.

Vediamo quindi la tabella di Cayley per $(r_6, \otimes)$

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Dalla tabella puoi vedere che:
0 e' l'elemento assorbente (moltiplicandolo per gli altri li fa diventare 0 (li assorbe); stavolta anche togliendo lo 0 non hai strutture di gruppo.
1 e' l'elemento neutro (moltiplicandolo per gli altri non li cambia
Per trovare l'inverso basta che guardi quando i risultati sono 1; gli 1 sono all'incrocio di elementi inversi. Quindi:
2, 3 e **4** sono divisori dello zero e non hanno inversi
1 e' l'inverso di se' stesso
5 e' l'inverso di se' stesso.

(f) *Insieme dei resti modulo 7*

Vediamo prima il gruppo additivo $(r_7, \oplus)$

$\oplus$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Dalla tabella puoi vedere che:
0 e' l'elemento neutro (sommandolo per gli altri non li cambia).
Per trovare l'inverso basta che guardi quando i risultati sono 0; gli 0 sono all'incrocio di elementi inversi. Quindi:
1 e' l'opposto di **6** e viceversa
2 e' l'opposto di **5** e viceversa
3 e' l'opposto di **4** e viceversa
0 e' l'opposto di se' stesso
Quando abbiamo un gruppo additivo, l'elemento inverso si chiama anche opposto.

Vediamo quindi la tabella di Cayley per $(r_7, \otimes)$

$\otimes$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Dalla tabella puoi vedere che:
0 e' l'elemento assorbente (moltiplicandolo per gli altri li fa diventare 0 (li assorbe); per poter avere la struttura di gruppo dovresti togliere lo zero, $(r_7 - \{0\}, \otimes)$ perche' lo zero non ha elemento inverso.
1 e' l'elemento neutro (moltiplicandolo per gli altri non li cambia
Per trovare l'inverso basta che guardi quando i risultati sono 1; gli 1 sono all'incrocio di elementi inversi. Quindi:
2 e' l'inverso di **4** e viceversa
3 e' l'inverso di **5** e viceversa
6 e' l'inverso di se' stesso
Queste tabelle ci suggeriscono una nuova struttura: l'anello.

(g) *Insieme dei resti modulo 8*

Vediamo prima il gruppo additivo $(r_8, \oplus)$

$\oplus$	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	6	0
2	2	3	4	5	6	6	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	6	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Dalla tabella puoi vedere che:
0 e' l'elemento neutro (sommandolo per gli altri non li cambia).
Per trovare l'inverso basta che guardi quando i risultati sono 0; gli 0 sono all'incrocio di elementi inversi. Quindi:
1 e' l'opposto di 7 e viceversa
2 e' l'opposto di 6 e viceversa
3 e' l'opposto di 5 e viceversa
4 e' l'opposto di se' stesso
0 e' l'opposto di se' stesso
Quando abbiamo un gruppo additivo l'elemento inverso si chiama anche opposto.

Vediamo quindi la tabella di Cayley per $(r_8, \otimes)$

$\otimes$	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Dalla tabella puoi vedere che:
0 e' l'elemento assorbente (moltiplicandolo per gli altri li fa diventare 0 (li assorbe); anche togliendo lo zero stavolta non hai strutture di gruppo.
1 e' l'elemento neutro (moltiplicandolo per gli altri non li cambia
Per trovare l'inverso basta che guardi quando i risultati sono 1; gli 1 sono all'incrocio di elementi inversi. Quindi:

2 non ha inverso
4 non ha inverso
6 non ha inverso
0 non ha inverso
1 e' l'inverso di se' stesso
3 e' l'inverso di se' stesso
5 e' l'inverso di se' stesso
7 e' l'inverso di se' stesso

(h) *Insieme dei resti modulo 9*

Vediamo prima il gruppo additivo $(r_9, \oplus)$

$\oplus$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	6	8	0
2	2	3	4	5	6	6	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	6	0	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

Dalla tabella puoi vedere che:
0 e' l'elemento neutro (sommandolo per gli altri non li cambia).
Per trovare l'inverso basta che guardi quando i risultati sono 0; gli 0 sono all'incrocio di elementi inversi. Quindi:
1 e' l'opposto di **8** e viceversa
2 e' l'opposto di **7** e viceversa
3 e' l'opposto di **6** e viceversa
4 e' l'opposto di **5** e viceversa
0 e' l'opposto di se' stesso
Quando abbiamo un gruppo additivo l'elemento inverso si chiama anche opposto.

Vediamo quindi la tabella di Cayley per $(r_9, \otimes)$

⊗	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	7
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

Dalla tabella puoi vedere che:
0 e' l'elemento assorbente (moltiplicandolo per gli altri li fa diventare 0 (li assorbe); anche togliendo lo zero stavolta non hai strutture di gruppo.
1 e' l'elemento neutro (moltiplicandolo per gli altri non li cambia).
Per trovare l'inverso basta che guardi quando i risultati sono 1; gli 1 sono all'incrocio di elementi inversi. Quindi:
2 e' l'inverso di **5**
4 e' l'inverso di **7**
3 e' divisore dello zero e non ha inverso
6 e' divisore dello zero e non ha inverso
0 non ha inverso
1 e' l'inverso di se' stesso
8 e' l'inverso di se' stesso.

5. Anello

Veniamo quindi ad una struttura piu' complessa che corrisponde alla struttura dell'insieme **Z** con le due operazioni di addizione e moltiplicazione: la struttura ad **anello**. Consideriamo un insieme con due operazioni, una addittiva ed una moltiplicativa, pero' per la struttura moltiplicativa gli elementi non hanno inverso; quindi tale fatto impedira' di poter considerare un gruppo moltiplicativo e potremo considerare solo un semigruppo.

Si definisce **anello $(A ; \otimes, \otimes)$** un insieme di enti **A** su cui siano definite due operazioni $\otimes$, $\otimes$ che godano delle seguenti proprieta':

1) **$(A ; \otimes)$** e' un gruppo abeliano (commutativo)
2) **$(A ; \otimes)$** e' un semigruppo

3) L'operazione $\otimes$ e' distributiva rispetto all'operazione $\otimes$, sia a destra che a sinistra, cioe':

$$a \otimes (b \otimes c) = (a \otimes b) \otimes (a \otimes c)$$
$$(b \otimes c) \otimes a = (b \otimes a) \otimes (c \otimes a)$$

Attenzione: per la seconda operazione $\otimes$ non e' richiesta ne' la proprieta' commutativa, ne' che l'insieme **A** abbia l'elemento neutro.
Quindi avremo:
- se l'operazione $\otimes$ e' commutativa, allora l'anello si dice **commutativo**.
- se l'insieme **A** e' dotato di elemento neutro rispetto all'operazione $\otimes$, allora l'anello si dice **unitario** .

Facciamo il punto della situazione. Le strutture sono ricavate dagli insiemi dei numeri e poi vengono applicate e ricercate in vari enti matematici; per procedere in modo logico avremo bisogno di seguire l'evoluzione dei numeri partendo dai numeri naturali, passando agli interi, ai razionali eccetera; la struttura ad anello la troviamo nell'insieme **Z** dei numeri interi. Proseguendo oltre **Z**, avremo poi una struttura per i numeri razionali **Q**: il **campo** .

Senza approfondire le proprieta' degli anelli (lo farete all'universita') vediamo nella prossima pagina qualche semplice esempio della struttura ad anello.

a) Esempi di struttura ad anello

Consideriamo i seguenti esempi e mostriamo per ciascuno la presenza della struttura ad anello: per ognuno dovremo mostrare:

- la presenza di un gruppo commutativo con la prima operazione
- la presenza di un semigruppo con la seconda operazione
- il fatto che la seconda operazione e' distributiva rispetto alla prima

---

1) Insieme **Z** dei numeri interi con le operazioni di addizione (+) e moltiplicazione (·)

E' l'esempio piu' semplice perche' e' quello da cui abbiamo ricavato la struttura di anello, ma questo esempio ci servira' soprattutto per mostrare come bisogna procedere per mostrare la struttura ad anello su un qualunque altro insieme

---

Dimostrazione. Dovremo mostrare:
- la presenza di un gruppo commutativo con la prima operazione
- la presenza di un semigruppo con la seconda operazione
- il fatto che la seconda operazione e' distributiva rispetto alla prima

Cominciamo dal primo punto:
- Mostriamo che **(Z, +)** e' un gruppo; devono valere le proprieta':
  - **+** e' interna infatti chiamati **a** e **b** due elementi di **Z** allora anche **c = a+b** appartiene a **Z**
  - **+** e' associativa, infatti chiamati **a**, **b** e **c** tre elementi di **Z** abbiamo:
    $(a + b) + c = a + (b + c)$
    Infatti presi 3 numeri abbiamo sempre:
    $2 + (3 + 4) = (2 + 3) + 4$
    $2 + 7 = 5 + 4$
    $9 = 9$
    cioe' il primo membro e' uguale al secondo.
  - **+** possiede l'elemento neutro; infatti esiste l'elemento **0** tale che per ogni elemento **a** di **Z** abbiamo:
    $a + 0 = 0 + a = a$ cioe' per qualunque numero, ad esempio 3, vale sempre:
    $3 + 0 = 0 + 3 = 3$
  - ogni elemento **a** di **Z** possiede in **+** l'elemento simmetrico **a'** tale che:
    $a + a' = a' + a = 0$

Infatti, dato un numero, basta considerare lo stesso numero con segno contrario; es:
$3 + (-3) = (-3) + 3 = 0$
Quindi $(\mathbb{Z}, +)$ e' un gruppo; inoltre il gruppo e' commutativo perche' per ogni elemento a e b appartenenti a $\mathbb{Z}$ avremo che vale:
$a + b = b + a$

- Mostriamo che $(\mathbb{Z}, \cdot)$ e' un semigruppo.
  - Basta mostrare che $\cdot$ e' associativa, cioe' chiamati a, b e c tre elementi di $\mathbb{Z}$ abbiamo:
    $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
    Infatti presi 3 numeri abbiamo sempre:
    $2 \cdot (3 \cdot 4) = (2 \cdot 3) \cdot 4$
    $2 \cdot 12 = 6 \cdot 4$
    $24 = 24$
    Quindi $(\mathbb{Z}, \cdot)$ e' un semigruppo.
- Mostriamo infine che la seconda operazione e' distributiva rispetto alla prima, cioe' dati a, b e c appartenenti a $\mathbb{Z}$; avremo sempre:
  $a \cdot (b + c) = a \cdot b + a \cdot c$
  $(b + c) \cdot a = b \cdot a + c \cdot a$
  Infatti prendendo 3 numeri qualunque avremo:
  $2 \cdot (3 + 4) = 2 \cdot 3 + 2 \cdot 4$
  $2 \cdot 7 = 6 + 8$
  $14 = 14$

  $(3 + 4) \cdot 2 = 3 \cdot 2 + 4 \cdot 2$
  $7 \cdot 2 = 6 + 8$
  $14 = 14$
  Quindi la struttura $(\mathbb{Z}, +, \cdot)$ e' un anello.
  Siccome la moltiplicazione in $\mathbb{Z}$ e' commutativa avremo che l'anello e' commutativo.
  Poiche' la moltiplicazione in $\mathbb{Z}$ ha come elemento neutro l'elemento 1 l'anello e' unitario.

2) Insieme $A = \{ p, d \}$ composto da due elementi con p pari e d dispari con le operazioni di addizione e moltiplicazione.

E' l'anello piu' semplice che possiamo pensare: composto da due soli elementi: tale insieme e' inoltre isomorfo (fare link) all'insieme dei resti modulo 2 (basta porre $p = 0$ e $d = 1$)

Dimostrazione. Dovremo mostrare:

- la presenza di un gruppo commutativo con la prima operazione
- la presenza di un semigruppo con la seconda operazione
- il fatto che la seconda operazione e' distributiva rispetto alla prima

Cominciamo dal primo punto:

- Mostriamo che $(A, +)$ e' un gruppo; devono valere le proprieta':
  - $+$ e' interna infatti avremo sempre che
    $p + p = p \qquad p + d = d \qquad d + d = p$
    e tutti i risultati appartengono ad A
  - $+$ e' associativa, infatti chiamati a, b e c tre elementi di A abbiamo:
    $(a + b) + c = a + (b + c)$
    Per mostrarlo dovrei considerare le possibilita'.

    Veramente potrei fare ricorso al fatto che la somma e la moltiplicazione hanno qui le stesse proprieta' che hanno nell'insieme dei numeri naturali essendo in questo insieme una restrizione di tali operazioni, pero' come esercizio proviamo a sviluppare tutto il ragionamento.

    $(p + p) + p = p + (p + p)$
    $(p + p) + d = p + (p + d)$
    $(p + d) + p = p + (d + p)$
    $(d + p) + p = d + (p + p)$
    $(p + d) + d = p + (d + d)$
    $(d + p) + d = d + (p + d)$

$(d+d)+p=d+(d+p)$
$(d+d)+d=d+(d+d)$
e in tutte queste espressioni il primo membro e' uguale al secondo. Mostriamo come esempio la dimostrazione della validita' dell'ultima espressione sviluppando il primo membro ed il secondo membro e controllando che il risultato sia identico:
$(d+d)+d=p+d=d$
$d+(d+d)=d+p=d$
Ottengo lo stesso risultato:

- $+$ possiede l'elemento neutro: infatti esiste l'elemento $\mathbf{p}$ tale che per ogni elemento di $\mathbf{A}$ abbiamo:
  $p+p=p$
  $p+q=q$
  cioe' sommando $\mathbf{p}$ a qualunque elemento l'altro elemento non cambia
- ogni elemento di $\mathbf{A}$ possiede in $+$ l'elemento simmetrico: infatti
  $p+p=p$ e $\mathbf{p}$ e' simmetrico di se' stesso
  $d+d=p$ e $\mathbf{d}$ e' simmetrico di se' stesso

  Quindi $(\mathbf{A},+)$ e' un gruppo; inoltre il gruppo e' commutativo perche' per ogni elemento $\mathbf{p}$ e $\mathbf{q}$ appartenente a $\mathbf{A}$ avremo che vale:
  $p+q=q+p$

- Mostriamo che $(\mathbf{A},\cdot)$ e' un semigruppo
  - Basta mostrare che $\cdot$ e' associativa, cioe' chiamati $\mathbf{a}$, $\mathbf{b}$ e $\mathbf{c}$ tre elementi di $\mathbf{A}$ abbiamo:
    $(a\cdot b)\cdot c=a\cdot(b\cdot c)$
    Per mostrarlo dovrei considerare le possibilita':
    $(p\cdot p)\cdot p=p\cdot(p\cdot p)$
    $(p\cdot p)\cdot d=p\cdot(p\cdot d)$
    $(p\cdot d)\cdot p=p\cdot(d\cdot p)$
    $(d\cdot p)\cdot p=d\cdot(p\cdot p)$
    $(p\cdot d)\cdot d=p\cdot(d\cdot d)$
    $(d\cdot p)\cdot d=d\cdot(p\cdot d)$
    $(d\cdot d)\cdot p=d\cdot(d\cdot p)$
    $(d\cdot d)\cdot d=d\cdot(d\cdot d)$
    e in tutte queste espressioni il primo membro e' uguale al secondo; mostriamo come esempio la dimostrazione della validita' dell'ultima espressione:
    $(d\cdot d)\cdot d=d\cdot d=d$
    $d\cdot(d\cdot d)=d\cdot d=d$
    Quindi $(\mathbf{A},\cdot)$ e' un semigruppo.
- Mostriamo infine che la seconda operazione e' distributiva rispetto alla prima, cioe' dati $\mathbf{a}$, $\mathbf{b}$ e $\mathbf{c}$ appartenenti a $\mathbf{A}$ avremo sempre:
  $a\cdot(b+c)=a\cdot b+a\cdot c$
  $(b+c)\cdot a=b\cdot a+c\cdot a$
  Per mostrarlo dovrei considerare le possibilita':
  $p\cdot(p+p)=p\cdot p+p\cdot p$
  $p\cdot(p+d)=p\cdot p+p\cdot d$
  $p\cdot(d+p)=p\cdot d+p\cdot p$
  $d\cdot(p+p)=d\cdot p+d\cdot p$
  $p\cdot(d+d)=p\cdot d+p\cdot d$
  $d\cdot(p+d)=d\cdot p+d\cdot d$
  $d\cdot(d+p)=d\cdot d+d\cdot p$
  $d\cdot(d+d)=d\cdot d+d\cdot d$
  ed anche le commutate rispetto al $\cdot$
  $(p+p)\cdot p=p\cdot p+p\cdot p$
  $(p+d)\cdot p=p\cdot p+d\cdot p$
  $(d+p)\cdot p=d\cdot p+p\cdot p$
  $(p+p)\cdot d=p\cdot d+p\cdot d$
  $(d+d)\cdot p=d\cdot p+d\cdot p$
  $(p+d)\cdot d=p\cdot d+d\cdot d$
  $(d+p)\cdot d=d\cdot d+p\cdot d$
  $(d+d)\cdot d=d\cdot d+d\cdot d$
  e in tutte queste espressioni il primo membro e' uguale al secondo: mostriamo come esempio la

dimostrazione della validita' dell'ultima espressione

$(d + d) \cdot d = p \cdot d = p$

$d \cdot (d + d) = d \cdot p = p$

Quindi la struttura (**A, +, ·**) e' un anello

Siccome la moltiplicazione in **A** e' commutativa avremo che l'anello e' commutativo

Poiche' la moltiplicazione in **A** ha come elemento neutro l'elemento **d** l'anello e' unitario: **d** e' l'elemento neutro moltiplicativo perche' moltiplicando **d** per qualunque altro termine l'altro termine non cambia:

$d \cdot d = d \qquad d \cdot p = p$

---

3) Insieme **P(x)** dei polinomi in **x** a coefficienti reali con le operazioni di addizione e moltiplicazione

---

Per insieme dei polinomi in **x** si intende l'insieme dei polinomi della forma

$a_n x^n + a_{n-1}x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0$

con $n = 0,1,2,\dots n,n+1,\dots$ Non ho capito! Aiuto:

Significa che considero tutti i polinomi a cominciare da:
$a_1 x + a_0$
mettendo al posto di a_1 e a_0 qualunque numero reale:
cioe' $3x+2, 4x-3, 5x+0\dots$
passando poi a considerare:
$a_2 x^2 + a_1 x + a_0$
mettendo al posto di a_2, a_1 e a_0 qualunque numero reale:
cioe' $2x^2+3x+2, x^2+4x-3, 6x^2+5x+1\dots$
e cosi' via aumentando i termini.
Inoltre posso anche considerare **3**
come un polinomio in x; infatti considero:
$0x+3$
addirittura **0** sara' considerato un polinomio con tutti i coefficienti nulli
$\dots+0x^2+0x+0$

L'operazione di addizione significa l'addizione fra polinomi per cui sommiamo algebricamente i coefficienti dei termini con x allo stesso grado: cioe', se n e maggiore di m avremo

$(a_n x^n + a_{n-1}x^{n-1} + \dots + a_2 x^2 + a_1 x + a_0) + (b_m x^m + b_{m-1}x^{m-1} + \dots + b_2 x^2 + b_1 x + b_0) =$

$= a_n x^n + a_{n-1}x^{n-1} + \dots + (a_m+b_m)x^m + (a_{m-1}+b_{m-1})x^{m-1} + \dots + (a_2+b_2)x^2 + (a_1+b_1)x + (a_0+b_0)$

Il prodotto fra polinomi e' il normale prodotto fra polinomi gia' visto.

Dimostrazione. Dovremo mostrare:

- la presenza di un gruppo commutativo con la prima operazione
- la presenza di un semigruppo con la seconda operazione
- il fatto che la seconda operazione e' distributiva rispetto alla prima
- Mostriamo che **(P, +)** e' un gruppo; devono valere le proprieta':
  - **+** e' interna infatti avremo sempre che la somma di due polinomi in **x** e' sempre ancora un polinomio in **x**: facciamo un esempio pratico:
    $(2x^3 + 5x^2 -4x + 3) + (3x^2 + 4) = 2x^3 + 8x^2 -4x + 7$

    In pratica la somma nei polinomi si riduce alla somma dei coefficienti numerici di stesso grado e quindi le proprieta' della somma sono le stesse che hanno i numeri reali

    ---

  - **+** e' associativa, infatti chiamati **A(x)**, **B(x)** e **C(x)** tre elementi di **P(x)** abbiamo:
    $[A(x) + B(x)] + C(x) = A(x) + [B(x) + C(x)]$
    facciamo anche qui un esempio pratico:
    $[(2x^3 + 5x^2 -4x + 3) + (3x^2 + 4)] + (2x^2 + 3x -4) =$
    $= (2x^3 + 5x^2 -4x + 3) + [(3x^2 + 4) + (2x^2 + 3x -4)]$
    Per mostrarlo basta che fai i calcoli prima e dopo l'uguale e mostri che i risultati sono uguali: lo sono perche' la somma fra i coefficienti (essendo numeri reali) gode della proprieta' associativa
  - **+** possiede l'elemento neutro: infatti esiste l'elemento **P(0)**, intendendo **P(0)** come il polinomio $0x^n+\dots+0x^2+0x+0$ tale che per ogni elemento **A(x)** di **P(x)** abbiamo
    $A(x) + P(0) = A(x)$

$P(0) + A(x) = A(x)$
cioe' sommando $P(0)$ a qualunque elemento l'altro elemento non cambia
- ogni elemento $A(x)$ di $P(x)$ possiede in $+$ l'elemento simmetrico: infatti preso
$A(x) = a_n x^n + a_{n-1}x^{n-1} \dots a_2 x^2 + a_1 x + a_0$
il simmetrico e'
$A'(x) = -a_n x^n - a_{n-1}x^{n-1} \dots -a_2 x^2 - a_1 x - a_0$
Infatti:
$A(x) + A'(x) = 0$
Quindi $(P, +)$ e' un gruppo; inoltre il gruppo e' commutativo perche' commutativa e' la somma fra i coefficienti numerici (numeri reali)
Mostriamo che $(P(x), \cdot)$ e' un semigruppo

- Basta mostrare che $\cdot$ e' associativa, cioe' chiamati $A(x)$, $B(x)$ e $C(x)$ tre elementi di $P(x)$ abbiamo sempre:
$[A(x) \cdot B(x)] \cdot C(x) = A(x) \cdot [B(x) \cdot C(x)]$
cioe' dati tre polinomi qualunque se moltiplichi il primo per il secondo e poi quello che viene per il terzo ottieni lo stesso risultato che moltiplicando prima il secondo col terzo e poi quello che viene per il primo. Se vuoi puoi costruirti un esempio da solo
- Mostriamo infine che la seconda operazione e' distributiva rispetto alla prima, cioe' dati $A(x)$, $B(x)$ e $C(x)$ appartenenti a $P(x)$ avremo sempre
$A(x) \cdot [B(x) + C(x)] = A(x) \cdot B(x) + A(x) \cdot C(x)$
$[B(x) + C(x)] \cdot A(x) = B(x) \cdot A(x) + C(x) \cdot A(x)$
Anche qui deriva dal fatto che per i coefficienti numerici, che sono numeri reali, vale la proprieta' distributiva della somma rispetto alla moltiplicazione.

Quindi la struttura $(P(x), +, \cdot)$ e' un anello
Siccome la moltiplicazione in $P(x)$ e' commutativa avremo che l'anello e' commutativo
Poiche' la moltiplicazione in A deve avere come elemento neutro l'elemento:
$\dots 1x^n + 1x^{n-1} \dots 1x^2 + 1x + 1$
ma tale elemento non puo' essere definito in modo univoco perche' dovrebbe avere esattamente lo stesso numero di termini (e dello stesso grado) del polinomio con cui si moltiplica, allora non posso parlare di un elemento neutro e l'anello non e' unitario.

4) Insieme r_5 dei resti modulo 5 con le operazioni di addizione e moltiplicazione.

Ripassare l'insieme r_5

Dimostrazione. Dovremo mostrare:
- la presenza di un gruppo commutativo con la prima operazione $\oplus$
- la presenza di un semigruppo con la seconda operazione $\otimes$
- il fatto che la seconda operazione e' distributiva rispetto alla prima

Cominciamo dal primo punto.
La struttura di gruppo additivo $(r_5, \oplus)$ l'abbiamo gia' evidenziata in precedenza ma qui la ripetiamo:

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

- Mostriamo che $(r_5, \oplus)$ e' un gruppo; devono valere le proprieta':
  - $\oplus$ e' interna infatti avremo sempre che la somma di due termini qualunque e' ancora un termine della tabella.
  Esempio: $4 \oplus 2 = (6)_5 = 1$

- $\oplus$ e' associativa, infatti chiamati a_5, b_5 e c_5 tre elementi di r_5 abbiamo:
  $(a_5 \oplus b_5) \oplus c_5 = a_5 \oplus (b_5 \oplus c_5)$
  Facciamo anche qui un esempio pratico:
  $(3 \oplus 2) \oplus 4 = (5)_5 \oplus 4 = 0 \oplus 4 = 4$
  ma vale anche:
  $3 \oplus (2 \oplus 4) = 3 \oplus (6)_5 = 3 \oplus 1 = 4$
- 0 e' l'elemento neutro: infatti sommando qualunque elemento con 0 otteniamo sempre lo stesso elemento
  $0 \oplus 1 = 1 \oplus 0 = 1$
  $0 \oplus 2 = 2 \oplus 0 = 2$
  $0 \oplus 3 = 3 \oplus 0 = 3$
  $0 \oplus 4 = 4 \oplus 0 = 4$
- ogni elemento di r_5 possiede in $\oplus$ l'elemento simmetrico: infatti hai:
  $0 \oplus 0 = 0$
  $1 \oplus 4 = 4 \oplus 1 = (5)_5 = 0$
  $2 \oplus 3 = 3 \oplus 2 = (5)_5 = 0$

- Quindi $(r_5, \oplus)$ e' un gruppo'; la commutativita segue dal fatto che la tabella per l'addizione e' simmetrica rispetto alla diagonale principale;
- Mostriamo che $(r_5, \otimes)$ e' un semigruppo
  - Basta mostrare che $\otimes$e' associativa, cioe' chiamati a_5, b_5 e c_5 tre elementi di r_5 abbiamo sempre:
    $(a_5 \otimes b_5) \otimes c_5 = a_5 \otimes (b_5 \otimes c_5)$
    Questo discende dalla moltiplicazione fra numeri naturali, ma vediamone un esempio pratico:
    $(3 \otimes 2) \otimes 4 = (6)_5 \otimes 4 = 1 \otimes 4 = 4$
    $3 \otimes (2 \otimes 4) = 3 \otimes (8)_5 = 3 \otimes 9 = (9)_5 = 4$
    Per vederlo meglio ti ripeto la tabella di Cayley per la moltiplicazione: se vai sui risultati con il mouse vedi l'operazione svolta.
  -

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

- Mostriamo infine che la seconda operazione e' distributiva rispetto alla prima, cioe' dati a_5, b_5 e c_5 appartenenti a r_5 avremo sempre:
  $a_5 \otimes (b_5 \oplus c_5) = a_5 \otimes b_5 \oplus a_5 \otimes c_5$
  $(b_5 \oplus c_5) \otimes a_5 = b_5 \otimes a_5 \oplus c_5 \otimes a_5$

  Ti faccio un esempio sulla prima; mostro che se eseguo l'operazione oppure se applico la proprieta' distributiva, ottengo lo stesso risultato. Fai un esempio anche tu sulla seconda per esercizio:
  $4 \otimes (1 \oplus 3) =$
  Se eseguo la somma, ottengo:
  $4 \otimes (1 \oplus 3) = 4 \otimes 4 = (16)_5 = 1$
  Se prima applico la proprieta' distributiva e poi faccio la somma, ottengo:
  $4 \otimes (1 \oplus 3) = 4 \otimes 1 \oplus 4 \otimes 3 = 4 \oplus (12)_5 = 4 \oplus 2 = (6)_5 = 1$

Quindi la struttura ($r_5, \oplus, \otimes$) e' un anello.

Inoltre siccome la moltiplicazione in r_5 e' commutativa avremo che l'anello e' **commutativo.**

Poiche' **1** elemento neutro della moltiplicazione in r_5 e' unico l'anello e' **unitario.**

5) L'insieme P(a) potenza dell'insieme A con le operazioni di differenza simmetrica ed intersezione.

Ripassare: L'insieme P(A) La differenza simmetrica L'intersezione

Dimostrazione. Dovremo mostrare:

- la presenza di un gruppo commutativo con la prima operazione
- la presenza di un semigruppo con la seconda operazione
- il fatto che la seconda operazione e' distributiva rispetto alla prima

Cominciamo dal primo punto

- Mostriamo che **(P(A),Δ)** e' un gruppo; devono valere le proprieta':
  - **Δ** e' interna: avremo sempre che la differenza simmetrica di due elementi di **P(A)** e' sempre ancora un elemento di **P(A).**

    Infatti **P(A)** e' costituito da tutti i sottoinsiemi di **A** cioe' gli insiemi che posso costruire con gli elementi di **A**, insieme vuoto compreso, quindi se da due sottoinsiemi tolgo alcuni elementi dell'insieme **A** avremo ancora un sottoinsieme di **A** .

  - **Δ** e' associativa, infatti chiamati A_1, A_2 e A_3 tre elementi di **P(A)** abbiamo:
    $(A_1 \Delta A_2) \Delta A_3 = A_1 \Delta (A_2 \Delta A_3)$
    Infatti, siccome la differenza simmetrica toglie elementi da entrambe gli insiemi che coinvolge, sia che li tolga prima o dopo, quando coinvolge gli stessi insiemi, da' sempre lo stesso risultato.

    Mostriamolo anche su un esempio pratico:
    Considero l'insieme:
    $A = \{ \emptyset, 1, 2, 3, 4 \}$
    Allora l'insieme potenza e' l'insieme composto dagli elementi:
    $\{\emptyset\}$ $\{1\}$ $\{2\}$ $\{3\}$ $\{4\}$
    $\{1,2\}$ $\{1\,3\}$ $\{1\,4\}$ $\{2,3\}$ $\{2,4\}$ $\{3,4\}$
    $\{1,2,3\}$ $\{1,2,4\}$ $\{1,3,4\}$ $\{2,3,4\}$
    $\{1,2,3,4\}$
    Consideriamo:
    $A_1 = \{1,2,4\}$ $A_2 = \{1,3,4\}$ $A_3 = \{1,4\}$
    $(A_1 \Delta A_2) \Delta A_3 = A_1 \Delta (A_2 \Delta A_3)$
    Per mostrarlo facciamo i calcoli prima e dopo l'uguale e mostriamo che i risultati sono uguali:
    $(\{1,2,4\} \Delta \{1,3,4\}) \Delta \{1,4\} = \{3\} \Delta \{1,4\} = \{1,3,4\}$
    $\{1,2,4\} \Delta (\{1,3,4\} \Delta \{1,4\}) = \{1,2,4\} \Delta \{3\} = \{1,3,4\}$

  - **+** possiede l'elemento neutro: infatti esiste l'elemento **Ø**, cioe' il sottoinsieme vuoto e la differenza simmetrica fra l'insieme vuoto e qualsiasi sottoinsieme e' sempre lo stesso sottoinsieme

    $A_n \Delta \emptyset = \emptyset \Delta A_n = A_n$

  - ogni elemento A_n di **P(A)** possiede in **Δ** l'elemento simmetrico: basta considerare l'insieme complementare di A_n rispetto ad **A** perche' la differenza simmetrica dia come risultato l'insieme vuoto

    se ad esempio considero l'insieme **{ 1, 2 }** il suo complementare rispetto ad **A** sara **{ 3, 4 }** e facendo la differenza complementare avremo che spariscono tutti gli elementi e resta il

vuoto:
$\{1,2\} \Delta \{3,4\} = \{3,4\} \Delta \{1,2\} = \emptyset$

Quindi $(P(a),\Delta)$ e' un gruppo; la commutativita' deriva dal fatto che l'operazione restituisce gli elementi non comuni fra due insiemi, quindi e' indifferente l'ordine in cui li considero.
Mostriamo che $(P(A),\cap)$ e' un semigruppo.

- Basta mostrare che $\cap$ e' associativa, cioe' chiamati A_1, A_2 e A_3 tre elementi di $P(x)$, abbiamo sempre:
  $(A_1 \cap A_2) \cap A_3 = A_1 \cap (A_2 \cap A_3)$
  Infatti, poiche' l'operazione intersezione fr insiemi restituisce gli elementi che gli insiemi hanno in comune, in qualunque ordine considereremo i 3 insiemi avremo sempre lo stesso risultato (cioe' gli elementi comuni ai 3 insiemi).
- Mostriamo infine che la seconda operazione e' distributiva rispetto alla prima, cioe' dati A_1, A_2 e A_3 appartenenti a $P(A)$ avremo sempre:
  $A_1 \cap (A_2 \Delta A_3] = A_1 \cap A_2 \Delta A_1 \cap A_3$
  $(A_2 \Delta A_3] \cap A_1 = A_2 \cap A_1 \Delta A_3 \cap A_1$

Questo e' un po' difficile da dimostrare: limitiamoci amostrare che e' vero su un esempio
Consideriamo i tre insiemi:
$A_1 = \{1,2,4\}$ $A_2 = \{1,3,4\}$ $A_3 = \{2,4\}$
Mostriamo che, nella prima uguaglianza, sono uguali i risultati sviluppando prima dell'uguale e dopo l'uguale.
Prima dell'uguale:
$\{1,2,4\} \cap (\{1,3,4\} \Delta \{2,4\}) = \{1,2,4\} \cap \{1,2,3\} = \{1,2\}$
dopo l'uguale:
$\{1,2,4\} \cap \{1,3,4\} \Delta \{1,2,4\} \cap \{2,4\} = \{1,4\} \Delta \{2,4\} \cap \{1,2\}$

Quindi la struttura $(P(A), \Delta, \cap)$ e' un anello.
Siccome l'operazione $\cap$ in $P(A)$ e' commutativa avremo che l'anello e' commutativo.
Poiche' l'intersezione in A ha come elemento neutro l' insieme A stesso e tale elemento e' definito in modo univoco allora posso parlare di un solo elemento neutro e l'anello e' unitario.

6) L'insieme $H(2)$ delle matrici 2x2 con le operazioni di addizione e moltiplicazione riga per colonna.

Ripassare: Le matrici quadrate Addizione Prodotto righe per colonne

---

Il ragionamento fatto per le matrici quadrate 2X2 vale in generale per le matrici quadrate nXn per la parte relativa al gruppo.

Dimostrazione. Dovremo mostrare:

- la presenza di un gruppo commutativo con la prima operazione
- la presenza di un semigruppo con la seconda operazione
- il fatto che la seconda operazione e' distributiva rispetto alla prima

Cominciamo dal primo punto

- Mostriamo che $(H_2,\oplus)$ e' un gruppo; devono valere le proprieta':
  - $\oplus$ e' interna infatti avremo sempre che la somma di due matrici quadrate e' ancora una matrice quadrata dello stesso tipo
    Facciamo un esempio pratico:
    $$\begin{Vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{Vmatrix} \oplus \begin{Vmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{Vmatrix} = \begin{Vmatrix} a_{1,1}+b_{1,1} & a_{1,2}+b_{1,2} \\ a_{2,1}+b_{2,1} & a_{2,2}+b_{2,2} \end{Vmatrix}$$
    essendo la somma di due numeri interi ancora un numero intero, segue quello che cercavamo.

  - $+$ e' associativa, infatti chiamati $H_2(A)$, $H_2(B)$ e $H_2(C)$ tre elementi di H_2 abbiamo:
    $[H_2(A) \oplus H_2(B)] \oplus H_2(C) = H_2(A) \oplus [H_2(B) \oplus H_2(C)]$
    Deriva dal fatto che la somma fra numeri naturali e' commutativa.
  - $\oplus$ possiede l'elemento neutro che e' la matrice:

$$\begin{Vmatrix} 0 & 0 \\ 0 & 0 \end{Vmatrix}$$

Infatti sommando 0 a qualunque elemento tale elemento non cambia.

- ogni elemento $H_2(A)$ di H_2 possiede in $\oplus$ l'elemento simmetrico; infatti basta considerare la matrice formata dagli opposti della matrice di partenza:

$$\begin{Vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{Vmatrix} \oplus \begin{Vmatrix} -a_{1,1} & -a_{1,2} \\ -a_{2,1} & -a_{2,2} \end{Vmatrix} = \begin{Vmatrix} 0 & 0 \\ 0 & 0 \end{Vmatrix}$$

Quindi $(H_2,\oplus)$ e' un gruppo; e' commutativo perche' la somma fra elementi delle matrici discende dalla somma fra numeri interi.

Mostriamo che $(H_2,\otimes)$ e' un semigruppo:

- Basta mostrare che $\otimes$ e' associativa, cioe' chiamate $H_2(A)$, $H_2(B)$ e $H_2(C)$ tre elementi di H_2 abbiamo sempre:
  $[H_2(A) \cdot H_2(B)] \cdot H_2(C) = H_2(A) \cdot [H_2(B) \cdot H_2(C)]$
  Questo deriva dal fatto che nelle matrici quadrate 2x2 il prodotto riga per colonna e' associativo:
  Mostriamolo: siccome la dimostrazione e' piuttosto lunga ti faccio un esempio in una pagina a parte: *Scheda C1*
- Mostriamo infine che la seconda operazione e' distributiva rispetto alla prima, cioe' presi $H_2(A)$, $H_2(B)$ e $H_2(C)$ tre elementi di H_2avremo sempre:
  $H_2(A) \otimes [H_2(B) \oplus H_2(C)] = H_2(A) \otimes H_2(B) \oplus H_2(A) \otimes H_2(C)$
  $[H_2(B) \oplus H_2(C)] \otimes H_2(A) = H_2(B) \otimes H_2(A) \oplus H_2(C) \otimes H_2(A)$
  Anche qui i calcoli sono molto laboriosi, ma intuitivamente epossiamo dire che questo deriva dalle proprieta' dell'operazione somma fra numeri interi; comunque limitiamoci ad un esempio (*Scheda C2*)

Quindi la struttura $(H_2, \oplus,\otimes)$ e' un anello.
Siccome la moltiplicazione in H_2 non e' commutativa avremo che l'anello non e' commutativo
Poiche' la moltiplicazione in H_2 ha come elemento neutro l'elemento:

$$\begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}$$

e tale elemento e' definito in modo univoco posso parlare di un solo elemento neutro e l'anello e' unitario.

Scheda n. C1

E' sufficiente mostrare che il termine prima dell'uguale e' uguale al termine dopo l'uguale per matrici 2x2 con termini generici: $a_{1,1}$ $a_{1,2}$ $a_{2,1}$ $a_{2,2}$
Termine prima dell'uguale:

$$\left(\begin{Vmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{Vmatrix} \oplus \begin{Vmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{Vmatrix}\right) \otimes \begin{Vmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{Vmatrix} =$$

$$= \begin{Vmatrix} a_{1,1}b_{1,1} + a_{1,2}b_{2,1} & a_{1,1}b_{1,2} + a_{1,2}b_{2,2} \\ a_{2,1}b_{1,1} + a_{2,2}b_{1,2} & a_{2,1}b_{2,1} + a_{2,1}b_{1,2} \end{Vmatrix} \otimes \begin{Vmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{Vmatrix} =$$

$= $ eccetera
Questo sarebbe il primo termine della matrice risultato:
$a_{1,1}b_{1,1}c_{1,1}+a_{1,2}b_{2,1}c_{1,1} + a_{1,1}b_{1,1}c_{2,1}+a_{1,2}b_{2,1}c_{2,1}$
Poi dovrei calcolare il termine dopo l'uguale:

$$\begin{Vmatrix} a_{1,1} \\ a_{1,2} \\ a_{2,1} \\ a_{2,2} \end{Vmatrix} \oplus \left(\begin{Vmatrix} b_{1,1} & b_{1,2} \\ b_{2,1} & b_{2,2} \end{Vmatrix} \otimes \begin{Vmatrix} c_{1,1} & c_{1,2} \\ c_{2,1} & c_{2,2} \end{Vmatrix}\right) =$$

$= $ eccetera

Come vedi i calcoli sono chilometrici; io non ho pazienza, quindi ti mostro che la regola e' valida su delle matrici 2x2 con termini numerici.
Questa quindi non e' una dimostrazione ma un esempio.

Mostriamo, come esempio, che vale:

$$\left(\begin{Vmatrix} 1 & 2 \\ 0 & 1 \end{Vmatrix} \otimes \begin{Vmatrix} 2 & 4 \\ 3 & 5 \end{Vmatrix}\right) \otimes \begin{Vmatrix} 6 & 7 \\ 8 & 9 \end{Vmatrix} = \begin{Vmatrix} 1 & 2 \\ 0 & 1 \end{Vmatrix} \otimes \left(\begin{Vmatrix} 2 & 4 \\ 3 & 5 \end{Vmatrix} \otimes \begin{Vmatrix} 6 & 7 \\ 8 & 9 \end{Vmatrix}\right) =$$

Calcoliamo la prima:

$$\left(\begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\begin{Vmatrix}2 & 4\\ 3 & 5\end{Vmatrix}\right)\otimes\begin{Vmatrix}6 & 7\\ 8 & 9\end{Vmatrix} = \begin{Vmatrix}1\cdot 2+2\cdot 3 & 1\cdot 4+2\cdot 5\\ 0\cdot 2+1\cdot 3 & 0\cdot 4+1\cdot 5\end{Vmatrix}\otimes\begin{Vmatrix}6 & 7\\ 8 & 9\end{Vmatrix} =$$

$$= \begin{Vmatrix}8 & 14\\ 3 & 5\end{Vmatrix}\otimes\begin{Vmatrix}6 & 7\\ 8 & 9\end{Vmatrix} = \begin{Vmatrix}8\cdot 6+14\cdot 8 & 8\cdot 7+14\cdot 9\\ 3\cdot 6+5\cdot 8 & 3\cdot 7+5\cdot 9\end{Vmatrix} = \begin{Vmatrix}160 & 182\\ 58 & 66\end{Vmatrix}$$

Calcoliamo la seconda:

$$\begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\left(\begin{Vmatrix}2 & 4\\ 3 & 5\end{Vmatrix}\otimes\begin{Vmatrix}6 & 7\\ 8 & 9\end{Vmatrix}\right) = \begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\begin{Vmatrix}2\cdot 6+4\cdot 8 & 2\cdot 7+4\cdot 9\\ 3\cdot 6+5\cdot 8 & 3\cdot 7+5\cdot 9\end{Vmatrix} =$$

$$\begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\begin{Vmatrix}44 & 50\\ 58 & 66\end{Vmatrix} = \begin{Vmatrix}1\cdot 44+2\cdot 58 & 1\cdot 50+2\cdot 66\\ 0\cdot 44+1\cdot 58 & 0\cdot 50+1\cdot 66\end{Vmatrix} = \begin{Vmatrix}160 & 182\\ 58 & 66\end{Vmatrix}$$

Come volevamo.

Scheda n. C2

Anche qui sarebbe sufficiente mostrare che il termine prima dell'uguale e' uguale al termine dopo l'uguale per matrici 2x2 con termini generici.
Come ho detto lo sviluppo richiede molta pazienza; limitiamoci ad un esempio che coinvolga la prima parte della proprieta' (solo la prima riga):

$$H_2(A)\otimes[H_2(B)\oplus H_2(C)] = H_2(A)\otimes H_2(B)\oplus H_2(A)\otimes H_2(C)$$

$$\begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\left(\begin{Vmatrix}2 & 4\\ 3 & 5\end{Vmatrix}\oplus\begin{Vmatrix}6 & 7\\ 8 & 9\end{Vmatrix}\right) = \begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\begin{Vmatrix}2 & 4\\ 3 & 5\end{Vmatrix}\oplus\begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\begin{Vmatrix}6 & 7\\ 8 & 9\end{Vmatrix} =$$

Calcoliamo il termine prima dell'uguale: prima eseguiamo la somma $\oplus$ poi il prodotto $\otimes$:

$$\begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\left(\begin{Vmatrix}2 & 4\\ 3 & 5\end{Vmatrix}\oplus\begin{Vmatrix}6 & 7\\ 8 & 9\end{Vmatrix}\right) = \begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\begin{Vmatrix}2+6 & 4+7\\ 3+8 & 5+9\end{Vmatrix} =$$

$$= \begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\begin{Vmatrix}8 & 11\\ 11 & 14\end{Vmatrix} = \begin{Vmatrix}1\cdot 8+2\cdot 11 & 1\cdot 11+2\cdot 14\\ 0\cdot 8+1\cdot 11 & 0\cdot 11+1\cdot 14\end{Vmatrix} = \begin{Vmatrix}30 & 39\\ 11 & 14\end{Vmatrix}$$

Calcoliamo il termine dopo l'uguale Prima esguiamo i prodotti poi la somma:

$$\begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\begin{Vmatrix}2 & 4\\ 3 & 5\end{Vmatrix}\oplus\begin{Vmatrix}1 & 2\\ 0 & 1\end{Vmatrix}\otimes\begin{Vmatrix}6 & 7\\ 8 & 9\end{Vmatrix} = \begin{Vmatrix}1\cdot 2+2\cdot 3 & 1\cdot 4+2\cdot 5\\ 0\cdot 2+1\cdot 3 & 0\cdot 4+1\cdot 5\end{Vmatrix}\oplus\begin{Vmatrix}1\cdot 6+2\cdot 8 & 1\cdot 7+2\cdot 9\\ 0\cdot 6+1\cdot 8 & 0\cdot 7+1\cdot 9\end{Vmatrix} =$$

$$= \begin{Vmatrix}8 & 14\\ 3 & 5\end{Vmatrix}\oplus\begin{Vmatrix}22 & 25\\ 8 & 9\end{Vmatrix} = \begin{Vmatrix}8+22 & 14+25\\ 3+8 & 14\end{Vmatrix} = \begin{Vmatrix}30 & 39\\ 11 & 14\end{Vmatrix}$$

Come volevamo.

6. Corpo

Continuiamo a evidenziare le proprieta' che ci permettono di definire i vari tipi di numeri e cerchiamo di esplicitare quali di esse sono significative, nel senso che si possano applicare ad alcuni tipi di oggetti oppure no.
Finora abbiamo trovato la struttura ad anello, tipica dell'insieme dei numeri interi **Z**. Ora dobbiamo enucleare la proprieta' che trasforma un anello in qualcos'altro, proprieta' che ci permette di passare dagli interi ai razionali **Q**. Quello che contraddistingue l'insieme dei razionali dall'insieme degli interi e' il fatto che, mentre negli interi la moltiplicazione non ha un elemento inverso, nei razionali possiamo definire l'elemento inverso per la moltiplicazione per ogni elemento dell'insieme eccetto lo zero (che non ha inverso):

1. Definizione
2. Campo
3. Esempi

a) Definizione

Diamo ora la definizione di corpo: bastera' aggiungere alla struttura di anello il fatto che esista per la seconda operazione un elemento neutro e che per ogni elemento sia presente un elemento opposto (con l'eccezione dell'elemento neutro della prima operazione).

Al solito consideriamo la prima operazione come "addizione" e la seconda come "moltiplicazione", naturalmente dovremo adattare tale termini ed ogni insieme su cui studieremo le nostre strutture: parleremo comunque di moltiplicazione mentre, ad esempio, tra matrici quadrate considereremo il prodotto righe per colonne e negli insiemi considereremo l'operazione di intersezione.

Si definisce **Corpo** $(K;\oplus,\otimes)$ un insieme di enti K formato da almeno due oggetti, su cui siano definite due operazioni, una che chiameremo di addizione $\oplus$ e una che chiameremo di moltiplicazione $\otimes$ che godano delle seguenti proprieta':

1) $(K;\oplus)$ e' un gruppo abeliano (commutativo)
2) l'operazione $\otimes$ e' distributiva rispetto all'operazione $\oplus$, sia a destra che a sinistra, cioe':

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$
$$(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$$

E fin qui siamo ancora alla struttura ad anello.

3) Gli elementi di K ad eccezione delle'elemento neutro rispetto all'addizione formano un gruppo rispetto alla moltiplicazione: $(K-\{0\};\otimes)$ e' un gruppo
Sarebbe a dire che, oltre la struttura di semigruppo, esiste l'elemento neutro per la moltiplicazione e per ogni elemento (eccetto lo 0) esiste l'inverso moltiplicativo.

Attenzione: per la seconda operazione $\otimes$ non e' richiesta ' la proprieta' commutativa, cioe' che:

$$a \otimes b = b \otimes a$$

b) Campo

Abbiamo detto che nel concetto di corpo non abbiamo la commutativita' per la seconda operazione (vedremo sugli esempi che il corpo delle matrici quadrate non e' commutativo); siccome pero' l'insieme Q, che ci guida nell'enucleare le strutture, e' commutativo ci conviene introdurre la commutativita' e quindi individuare una nuova struttura il **campo,** il cui rappresentante tipico sara' appunto l'insieme Q, che per questo sara' anche chiamato ***campo dei numeri razionali.***

Quindi per la nuova struttura di campo bastera' aggiungere che la seconda operazione (moltiplicazione) e' commutativa.

Si definisce **Campo** $(K;\oplus,\otimes)$ un insieme di enti tali che:

1) $(K;\oplus,\otimes)$ e' un corpo
2) l'operazione $\otimes$ e' commutativa, cioe' per ogni coppia di elementi a e b di K vale la relazione:
$a \otimes b = b \otimes a$

c) Esempi di struttura di corpo e campo

Consideriamo i seguenti esempi e mostriamo per ciascuno la presenza della struttura di corpo e/o di campo, oppure mostriamo che tale struttura non esiste: per ognuno dovremo mostrare:

Per la struttura di corpo:

- la presenza di un gruppo commutativo con la prima operazione
- la presenza di un gruppo con la seconda operazione (escludendo l'elemento neutro addittivo)
- la distributivita' della seconda operazione rispetto alla prima

per la struttura di campo aggiungeremo

- la proprieta' commutativa per la seconda operazione

---

1) Insieme Q dei numeri razionali con le operazioni di addizione e moltiplicazione

---

E' l'esempio piu' semplice perche' e' quello da cui abbiamo ricavato la struttura di campo; ma questo esempio ci servira' soprattutto per mostrare come bisogna procedere per mostrare la struttura di campo su un qualunque altro insieme.

Dimostrazione:
Dovremo mostrare per il corpo:

- la presenza di un gruppo commutativo con la somma
- la presenza di un gruppo con il prodotto escludendo l'elemento neutro per l'addizione (lo zero)
- il fatto che la seconda operazione e' distributiva rispetto alla prima
- per il campo aggiungeremo la dimostrazione della commutativita' della seconda operazione

Cominciamo dal primo punto

- Mostriamo che **(Q, +)** e' un gruppo; devono valere le proprieta':
  - **+** e' interna infatti chiamati **a** e **b** due elementi di **Q** allora anche **c = a+b** appartiene a **Q**
  - **+** e' associativa, infatti chiamati **a**, **b** e **c** tre elementi di **Q** abbiamo:
    $(a + b) + c = a + (b + c)$
  - **+** possiede l'elemento neutro: infatti esiste l'elemento **0** tale che per ogni elemento **a** di **Q** abbiamo
    $a + 0 = 0 + a = a$
  - ogni elemento **a** di **q** possiede in **+** l'elemento simmetrico **-a** tale che:
    $a + (-a) = (-a) + a = 0$
    Infatti dato un numero basta considerare lo stesso numero con segno contrario.
    Quindi **(Q, +)** e' un gruppo; inoltre tale gruppo e' commutativo perche', presi comunque due elementi **a** e **b** di **Q**, vale sempre:
    $a + b = b + a$
- Mostriamo che **(Q-{0}, ·)** e' un gruppo; devono valere le proprieta':
  - **·** e' interna infatti chiamati **a** e **b** due elementi di **Q** allora anche il prodotto **c = a·b** appartiene a **Q**
  - **·** e' associativa, infatti chiamati **a**, **b** e **c** tre elementi di **q** abbiamo:
    $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
  - **·** possiede l'elemento neutro: infatti esiste l'elemento **1** tale che per ogni elemento **a** di **Q** abbiamo
    $a \cdot 1 = 1 \cdot a = a$
  - ogni elemento **a** di **q** possiede in **·** l'elemento simmetrico **1/a** tale che:
    $a \cdot (1/a) = (1/a) \cdot a = 1$
    Infatti dato un numero basta considerarne l'inverso.
    Quindi **(Q, ·)** e' un gruppo.
- La seconda operazione e' distributiva rispetto alla prima, cioe' dati **a**, **b** e **c** appartenenti a **Z,** avremo sempre:
  $a \cdot (b + c) = a \cdot b + a \cdot c$
  $(b + c) \cdot a = b \cdot a + c \cdot a$
- Mostriamo infine che la seconda operazione e' commutativa; infatti, dati comunque due elementi **a** e **b** appartenenti a **Q**, avremo sempre:
  $a \cdot b = b \cdot a$
  Quindi la struttura (**Q, +, ·**) e' un campo (qualche testo lo chiama anche **dominio d'integrita'**).

2) Insieme R dei numeri reali con le operazioni di addizione e moltiplicazione.

In pratica, l'insieme **R** dal punto di vista della struttura e' identico all'insieme **Q**; quindi lo sviluppo e' lo stesso dell' esercizio precedente sostituendo il simbolo **R** al simbolo **Q.**

Ti ricordo che **R** si ottiene da **Q** aggiungendovi i valori dati dai numeri decimali illimitati e non periodici, pensati come elementi separatori di classi contigue di numeri razionali, cioe' mediante le sezioni di Dedekind: tale aggiunta non altera la struttura dell'insieme che resta sempre un campo: il **campo dei numeri reali**

Se non hai capito quello che ho detto e' meglio che ripassi la teoria della misura fino alla retta reale compresa.

3) Insieme $\mathbf{r_2}$ dei resti modulo 2 con le operazioni di addizione e moltiplicazione.

Verificare la presenza delle strutture di corpo e di campo sull' insieme $\mathbf{r_2}$ dei resti modulo 2 con le operazioni di addizione e moltiplicazione.

Sara' il campo piu' semplice che possiamo pensare: composto da due soli elementi.

Dimostrazione. Dovremo mostrare per il corpo:

- la presenza di un gruppo commutativo con la somma
- la presenza di un gruppo con il prodotto escludendo l'elemento neutro per l'addizione (lo zero)
- il fatto che la seconda operazione e' distributiva rispetto alla prima
- per il campo aggiungeremo la dimostrazione della commutativita' della seconda operazione

Cominciamo dal primo punto

- Mostriamo che $(\mathbf{r_2}, +)$ e' un gruppo; devono valere le proprieta':
  - $+$ e' interna infatti avremo sempre che
    $0+0=0 \qquad 0+1=1+0=1 \qquad 1+1=(2)_2=0$
    Tutti i risultati appartengono ad $\mathbf{A}$; inoltre l'operazione e' commutativa perche' scambiando l'ordine dei fattori il risultato e' lo stesso.
  - $+$ e' associativa; infatti, chiamati $\mathbf{a}$, $\mathbf{b}$ e $\mathbf{c}$ tre elementi di $\mathbf{A}$, abbiamo:
    $(a+b)+c=a+(b+c)$
    Per mostrarlo posso considerare le 8 possibilita'.

    $(0+0)+0=0+(0+0)=0$
    $(0+0)+1=0+(0+1)=1$
    $(0+1)+0=0+(1+0)=1$
    $(1+0)+0=1+(0+0)=1$
    $(0+1)+1=0+(1+1)=(2)_2=0$
    $(1+0)+1=1+(0+1)=(2)_2=0$
    $(1+1)+0=1+(1+0)=(2)_2=0$
    $(1+1)+1=1+(1+1)=(3)_2=1$
  - $+$ possiede l'elemento neutro: infatti esiste l'elemento $\mathbf{0}$ tale che per ogni elemento di $\mathbf{r_2}$ abbiamo
    $0+0=0$
    $0+1=1+0=1$
    cioe' sommando $\mathbf{0}$ a qualunque elemento l'altro elemento non cambia
  - ogni elemento di $\mathbf{r_2}$ possiede in $+$ l'elemento simmetrico: infatti
    $0+0=0$ e 0 e' simmetrico di se' stesso
    $1+1=0$ e $\mathbf{1}$ e' simmetrico di se' stesso
    Quindi $(\mathbf{r_2}, +)$ e' un gruppo commutativo;
- Mostriamo che $(\mathbf{r_2}, \cdot)$ e' un gruppo; devono valere le proprieta':
  - $\cdot$ e' interna infatti avremo sempre che:
    $0\cdot 0=0 \qquad 0\cdot 1=1\cdot 0=1 \qquad 1\cdot 1=1$
    Tutti i risultati appartengono ad $\mathbf{r_2}$; inoltre l'operazione e' commutativa (scambiando i posti il risultato del prodotto e' lo stesso)
  - $\cdot$ e' associativa; infatti, chiamati $\mathbf{a}$, $\mathbf{b}$ e $\mathbf{c}$ tre elementi di $\mathbf{A}$, abbiamo:
    $(a\cdot b)\cdot c=a\cdot(b\cdot c)$
    Per mostrarlo posso considerare le 8 possibilita'.

    $(0\cdot 0)\cdot 0=0\cdot(0\cdot 0)=0$
    $(0\cdot 0)\cdot 1=0\cdot(0\cdot 1)=0$
    $(0\cdot 1)\cdot 0=0\cdot(1\cdot 0)=0$
    $(1\cdot 0)\cdot 0=1\cdot(0\cdot 0)=0$
    $(0\cdot 1)\cdot 1=0\cdot(1\cdot 1)=0$
    $(1\cdot 0)\cdot 1=1\cdot(0\cdot 1)=0$
    $(1\cdot 1)\cdot 0=1\cdot(1\cdot 0)=0$
    $(1\cdot 1)\cdot 1=1\cdot(1\cdot 1)=1$
  - $+$ possiede l'elemento neutro; infatti, esiste l'elemento $\mathbf{1}$ tale che per ogni elemento di $\mathbf{r_2}$ abbiamo:
    $1\cdot 1=1$
    $0\cdot 1=1\cdot 0=0$
    cioe' moltiplicando $\mathbf{1}$ a qualunque elemento l'altro elemento non cambia.

- ogni elemento di r_2 ad eccezione di **0** possiede in $\cdot$ l'elemento simmetrico; infatti, togliendo **0** ci resta solo **1** e poiche':
  $1 \cdot 1 = 1$
  allora **1** e' elemento simmetrico di se' stesso rispetto alla moltiplicazione.

- Mostriamo infine che la seconda operazione e' distributiva rispetto alla prima, cioe' dati **a**, **b** e **c** appartenenti a r_2 avremo sempre:
  $a \cdot (b + c) = a \cdot b + a \cdot c$
  $(b + c) \cdot a = b \cdot a + c \cdot a$
  Per mostrarlo dovrei considerare le 16 possibilita', ma preferisco dire che deriva dalla distributivita' del prodotto rispetto alla somma che vale nell'insieme dei numeri naturali
  Quindi la struttura ($r_2, +, \cdot$) e' un campo
  Infatti abbiamo visto che la moltiplicazione in r_2 e' commutativa.

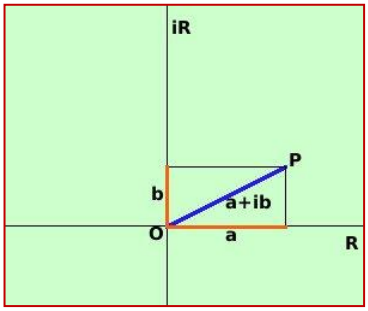
7. Spazi vettoriali

Il prossimo passo e' di evidenziare le struttura dei numeri Complessi. Sia i numeri razionali **Q** sia i numeri Reali **R** hanno la struttura di Campo. Per proseguire nel nostro ragionamento vediamo in cosa i numeri complessi differiscono per struttura dai numeri razionali e reali. Questo ci portera' a definire una nuova struttura: gli spazi vettoriali.

1. Caratteristiche di un numero complesso
2. I vettori in fisica
3. La moltiplicazione nei numeri complessi
4. Spazio vettoriale
5. Esempi di spazi vettoriali

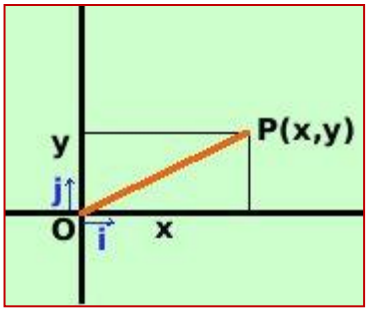
a) Caratteristiche vettoriali di un numero complesso

Consideriamo un numero complesso, cioe' $a + ib$, formato da una parte reale piu' una parte immaginaria e consideriamolo come segmento nel piano complesso. La prima cosa che e' evidente e' che si tratta di un numero composto di due parti fra loro indipendenti, nel senso che una parte e' un normale numero reale e l'altra ha una parte **i** che la rende diversa dalla prima.

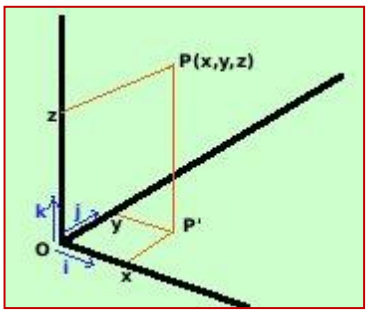


Quindi potrei anche rappresentare il numero complesso $OP = a + ib$ come la coppia:
$P = (a, b)$
considerando che il numero **a** si trova sulla retta reale **R**, mentre il numero **b** si trova sulla retta immaginaria **iR**, cioe' considerare il numero complesso come una coppia di numeri in cui il primo appartiene ad **R** ed il secondo ad **iR** .

Questo modo di pensare un punto e' abbastanza comune in matematica; basta pensare al piano cartesiano ed alla rappresentazione di un punto mediante le coordinate; pero' invece di considerare il punto **P** consideriamo il segmento **OP** (vettore):
$P = (x, y)$
ma posso anche pensare:
$OP = xi + yj$
con **i** e **j** segmenti unitari il primo sull'asse x ed il secondo sull'asse y.



Come l'abbiamo fatto per il piano, possiamo farlo per lo spazio. Rappresentiamo un punto **P** mediante le cooordinate **P(x,y,z)** e consideriamo il segmento **OP**:



$P = (x, y, z)$

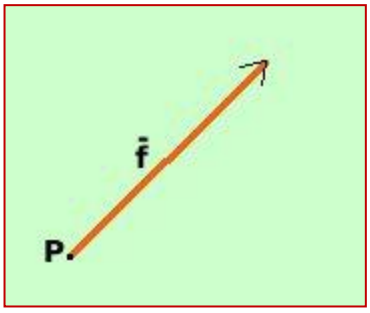
ma posso anche pensare:

$OP = xi + yj + zk$

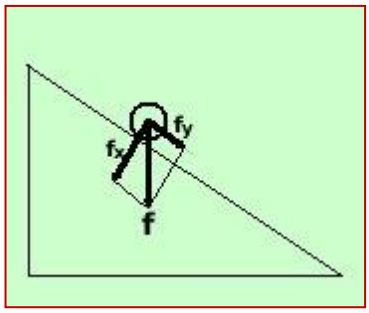
con **i**, **j** e **k** segmenti unitari il primo sull'asse x, il secondo sull'asse y ed il terzo sull'asse z.

I vari segmenti **OP**, qui sopra considerati, sono dei **vettori.**

b) I vettori in fisica



Se pensiamo alla fisica noi abbiamo trovato spesso il concetto di vettore e delle sue componenti.
In fisica un vettore, e' un ente caratterizzato da un *modulo* (lunghezza del segmento) un *verso* (la freccia) ed *un punto di applicazione* (se consideriamo il punto di applicazione diremo che il vettore e' applicato).
Se, ad esempio, consideriamo una forza, il modulo e' il valore della forza, il verso e' verso dove tira la forza, ed il punto di applicazione e' il punto **P** dove tale forza e' applicata.

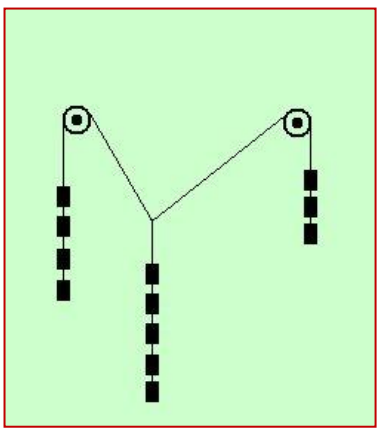


L'importante in fisica e' pensare un vettore come somma di due o piu' componenti. Ad esempio, consideriamo un piano inclinato; sul corpo agisce la forza peso **f**. Posso pensare tale forza come composta di due parti:

- la prima f_x, perpendicolare al piano inclinato che viene annullata dal piano stesso per il terzo principio della dinamica (e' la forza che ti piega la tavola che forma il piano inclinato, ma noi pensiamo tale piano non flessibile).
- la seconda f_y, parallela al piano e' quella responsabile del moto del corpo, cioe' quella che fa scendere il corpo lungo il piano.

Quindi, anche qui, come nella pagina precedente, posso scrivere:

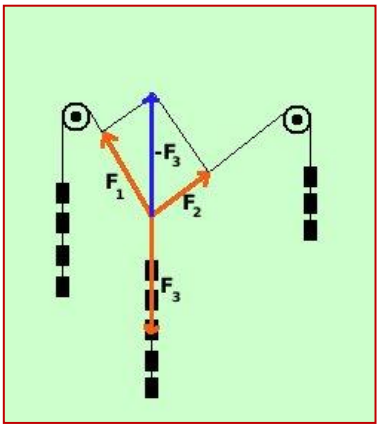
$$f = f_x + f_y$$



Uno degli esperimenti che preferivo era quello di mostrare la scomposizione di una forza nelle sue componenti; te lo descrivo.
Occorrente:
- un filo di nylon tipo da pesca, circa 1 metro
- 2 carrucole fissate su un supporto
- un insieme di 12 pesi uguali con gancetti

Facciamo un cappio agli estremi del filo, facciamolo passare per le carrucole e poi colleghiamo ad un estremo 4 pesi ed all'altro estremo 3 pesi.
Attacchiamo con un gancetto 5 pesi al filo teso tra le due

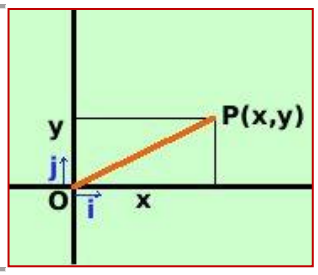
carrucole: allora i pesi si disporranno come in figura.



Siccome il sistema e' in equilibrio, allora le forze che esistono (i pesi) si annullano fra loro.
Andiamo a disegnare tali forze. Le forze che agiscono sono i pesi (te li evidenzio in rosso); il gruppo di 5 pesi tira verso il basso, mentre i gruppi di 3 e 4 pesi tendono nella direzione dei fili per colpa delle carrucole.
Se il sistema e' in equilibrio allora la forza F_3 che tende verso il basso e' bilanciata da una forza uguale e contraria $-F_3$ che tende verso l'alto; tale forza e' la somma vettoriale delle due forze che agiscono lungo il filo verso le carrucole, cioe' F_1 e F_2 sono le componenti di $-F_3$ lungo le direzioni del filo.
La figura che si forma e' un rettangolo con i lati proporzionali a 3 e 4 e la diagonale a 5 (il semirettangolo e' un triangolo rettangolo speciale di lati 3, 4 e 5). Quindi:

$$-F_3 = F_1 + F_2$$

In matematica possiamo pensare un vettore sempre con origine in **O** e quindi semplicemente come formato da modulo e verso; ad esempio, vedendo la figura a fianco puoi considerare il vettore **PO**; il modulo e' la lunghezza del segmento ed il verso e' da **O** a **P.**



Se considero il vettore unitario (cioe' di modulo 1) esso viene detto **versore.**
Il vettore **OP** sara' la somma:

$$OP = xi + yj$$

ove **x** ed **y** sono numeri ed **i** e **j** sono i versori sull'asse **x** e sull'asse **y.**

c) La moltiplicazione nei numeri complessi

Consideriamo un numero complesso, cioe' $a + ib$ formato da una parte reale piu' una parte immaginaria e consideriamo l'operazione di moltiplicazione.
Se moltiplico un numero complesso per un numero reale, tale numero si trasforma in modo che la parte reale resta reale e le parte immaginaria resta immaginaria:

$$4\cdot(2 + 3i) = 8 + 12i$$

Mentre se moltiplico un numero complesso per un numero immaginario, tale numero si trasforma trasformando la parte reale nella parte immaginaria e viceversa:

$$4i\cdot(2 + 3i) = 8i + 12i^2 = 8i - 12\ .$$

Cio' ci porta a considerare l'esistenza di due operazioni di tipo moltiplicazione:

- una esterna (numero reale per numero complesso) che pur modificando il numero ne lascia inalterata la struttura: numero reale + numero immaginario nelle stesse proporzioni (se una parte raddoppia allora raddoppia anche l'altra):
  $2\cdot(2 - 3i) = 4 - 6i$
- una interna (numero complesso per numero complesso) che puo' trasformare il numero anche nella sua struttura trasformando in alcuni casi il risultato anche nella sola parte reale:
  $(3 + 4i)\cdot(2 - 3i) = 6 - 9i + 8i - 12i^2 = 6 - 9i + 8i + 12 = 18 - i$
  $(2 + 3i)\cdot(2 - 3i) = 4 - 9i^2 = 4 + 9 = 13$

Da notare che, nell'insieme dei numeri complessi, la moltiplicazione esterna fa solo ingrandire o rimpicciolire il vettore che rappresenta il numero complesso stesso, mentre la moltiplicazione interna, oltre ad ingrandire o rimpicciolire il vettore, lo fa anche ruotare (ampliare l'argomento in futuro).

d) Spazio vettoriale

Ora possiamo finalmente evidenziare una struttura, lo **spazio vettoriale** che e' quella suggerita dai numeri complessi **C** e quindi completare, per ora, le strutture basate sui numeri.
Tale struttura (**spazio**) sara' detta **vettoriale** perche' ogni elemento di essa potra' essere posto in corrispondenza con un determinato vettore.

Consideriamo un Insieme di enti **V** ed un corpo commutativo **K.**

Indicheremo con **x**, **y**, **t**,... gli elementi di **V** (vettori) e con **a, b, c,...** gli elementi di **K** (scalari).
Indichiamo sugli elementi di **V** l' operazione di addizione vettoriale con il simbolo **+**
Indichiamo sugli elementi di **k** le operazioni di addizione e moltiplicazione con i simboli $\oplus$ e $\otimes$
l' operazione $\otimes$ opera oltre che in **K** anche come moltiplicazione (scalare) fra gli elementi di **K** e **V**.

Diremo che **V** e' uno **spazio vettoriale** sul campo **K** se abbiamo:

- L'insieme **(V, +)** e' un gruppo commutativo
- La moltiplicazione scalare $K \otimes V$ ha come codominio una porzione di **V**
- La moltiplicazione scalare e' commutativa:
  $a \otimes x = x \otimes a$ per ogni elemento di **V** e **K**
- Vale la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale:
  $a \otimes (x + y) = a \otimes x + a \otimes y$
- Vale la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari:
  $(a \oplus b) \otimes x = a \otimes x + b \otimes x$
  Dopo l'uguale devo usare il simbolo **+** perche' $a \otimes \mathbf{x}$ e $b \otimes \mathbf{x}$ sono vettori e quindi devo sommare due vettori.
- Vale la proprieta' associativa fra gli scalari:
  $a \otimes b\ (\otimes x) = (a \otimes b) \otimes x$
- Inoltre se 1 e' l'elemento neutro moltiplicativo di **K** allora vale:
  $1 \otimes x = x$

Lo spazio vettoriale e' una di quelle strutture che meglio si prestera' a studiare vari enti matematici, dai polinomi, alle matrici, agli spazi ad n dimensioni fino alle applicazioni lineari, quindi andrebbe sviluppata nei particolari (dimensione, sottospazi, basi, somma di spazi vettoriali,....).
Lasciando, per ora, lo sviluppo di questi argomenti a studi universitari, vediamo nella prossima pagina alcuni semplici esempi di spazi vettoriali .

e) Esempi di struttura di spazi vettoriali

Consideriamo i seguenti esempi e mostriamo per ciascuno la presenza della struttura di spazio vettoriale, oppure mostriamo che tale struttura non esiste. Per ognuno, supponendo presente la struttura di corpo su **K,** dovremo mostrare:

- la presenza di un gruppo commutativo su **V** con la somma

- la commutativita' del prodotto scalare $\otimes$
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari
- la proprieta' associativa fra gli scalari.

---

1) Insieme **C** dei numeri complessi sul corpo **R** con le normali operazioni di addizione e moltiplicazione in **C** e con la moltiplicazione scalare $\mathbf{R} \otimes \mathbf{C}$ numero reale per numero complesso.

Individuare la struttura di spazio vettoriale per l'insieme **C** dei numeri complessi sul corpo **R** con le normali operazioni di addizione e moltiplicazione in **C** e con la moltiplicazione scalare $\mathbf{R} \otimes \mathbf{C}$ numero reale per numero complesso.

E' l'esempio piu' semplice perche' e' quello da cui abbiamo ricavato la struttura di spazio: questo esempio ci servira' soprattutto per mostrare come bisogna procedere per mostrare la struttura di spazio vettor iale su un qualunque altro insieme.

Dimostrazione. Dovremo mostrare che abbiamo:

- la presenza di un gruppo commutativo su **C** con la somma fra complessi
- la commutativita' del prodotto scalare (che coincide col prodotto ordinario in R) $\mathbf{R} \cdot \mathbf{C}$
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari
- la proprieta' associativa fra gli scalari.

Cominciamo dal primo punto.

- Mostriamo che **(C, +)** e' un gruppo commutativo; devono valere le proprieta':
  - **+** e' interna; infatti chiamati **a+ib** e **c+id** due elementi di **C,** allora anche $e + if = (a + ib) + (c + id)$ appartiene a **C.**
    Infatti:
    $(a + ib) + (c + id) = a + ib + c + id = (a + c) + i(b + d) = e + if$
    essendo:
    $e = a + c$ ed $f = b + d$
  - **+** e' associativa; infatti chiamati **a+ib**, **c+id** e **e+if** tre elementi di **C** abbiamo:
    $(a + ib + c + id) + e + if = a + ib + (c + id + e + if)$
    Siccome dobbiamo sommare le parti reali con le parti reali e, per le parti immaginarie, dobbiamo mettere in evidenza la **i** per poi sommare i numeri reali entro parentesi, allora l'associativita' deriva dal fatto che la somma in **R** e' associativa.
  - **+** possiede l'elemento neutro: infatti esiste l'elemento **0+i0** tale che per ogni elemento **a+ib** di **C** abbiamo:
    $a + ib + 0 + i0 = 0 + i0 + a + ib = a + ib$
  - ogni elemento **a+ib** di **C** possiede in **+** l'elemento simmetrico **-a-ib** tale che:
    $a + ib + (-a - ib) = (-a - ib) + a + ib = 0 + i0$
    Infatti dato un numero complesso basta considerare lo stesso numero con segni opposti;

  Quindi **(C, +)** e' un gruppo; inoltre tale gruppo e' commutativo perche' presi comunque due elementi **a+ib** e **c+id** di **C** vale sempre:
  $a + ib + c + id = (a + c) + i\,(b + d) = (c + a) + i\,(d + b) = c + id + a + ib$
  Siccome dobbiamo sommare le parti reali con le parti reali e, per le parti immaginarie, dobbiamo mettere in evidenza la **i** per poi sommare i numeri reali entro parentesi, allora la commutativita' deriva dalla commutativita' della somma fra numeri reali.

- Mostriamo la commutativita' del prodotto scalare (che coincide col prodotto ordinario in R):
  $x \cdot (a + ib) = x \cdot a + x \cdot ib = ax + i\,bx = (a + ib) \cdot x$
  Il prodotto ordinario in R e' commutativo, quindi...
- Mostriamo la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale:
  $x \cdot [(a + ib) + (c + id)] = x \cdot (a + ib + c + id) = x \cdot a + x \cdot ib + x \cdot c + x \cdot id =$
  $= ax + i\,bx + cx + i\,dx = x \cdot (a + ib) + x \cdot (c + id)$

- Mostriamola proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari:
  $x \cdot (y + z) = x \cdot y + x \cdot z$
  siamo in **R** e quindi la proprieta' e' valida.
- Mostriamo la proprieta' associativa fra gli scalari:
  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
  Siamo sempre in **R** e quindi la proprieta' e' valida.
  Quindi **C** e' uno spazio vettoriale sul campo **R.**

2) Ogni corpo **K** e'uno spazio vettoriale su se' stesso; in tal caso vettori e scalari coincidono.

Individuare la struttura di spazio vettoriale per un generico corpo **K** su se' stesso.
Dimostrazione. Dovremo mostrare che abbiamo:

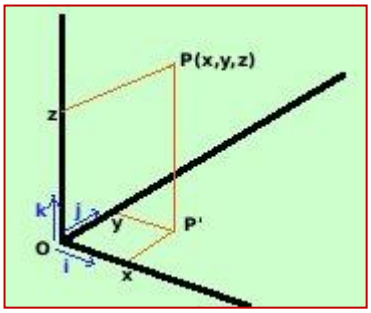
- la presenza di un gruppo commutativo su **K** con la somma fra elementi di **K**
- la commutativita' del prodotto scalare (che coincide col prodotto ordinario in **K**)
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari
- la proprieta' associativa fra gli scalari

Cominciamo dal primo punto:

- **(K, +)** e' un gruppo commutativo; infatti e' un corpo quindi la proprieta' di essere gruppo commutativo fa parte delle proprieta' di un corpo
- la commutativita' del prodotto scalare (che coincide col prodotto ordinario in K) deriva sempre dalla definizione di corpo
- La proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale deriva dalla definizione di corpo
- La proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari deriva dalla definizione di corpo
- La proprieta' associativa fra gli scalari deriva dalla definizione di corpo

Quindi **K**) e' uno spazio vettoriale sul corpo **K.**

3) Insieme R^3 dello spazio ordinario con le normali operazioni di addizione e moltiplicazione e con la moltiplicazione scalare $R \otimes R^3$



Individuare la struttura di spazio vettoriale sullo spazio ordinario R^3 con le normali operazioni di addizione e moltiplicazione e con moltiplicazione scalare la normale moltiplicazione $R \cdot R^3$
Dimostrazione. Dovremo mostrare che abbiamo:

- la presenza di un gruppo commutativo su R^3 con l'operazione somma (nelle componenti si riduce a somma fra elementi di **R**)
- la commutativita' del prodotto scalare (che coincide col prodotto ordinario in **R**)
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari
- la proprieta' associativa fra gli scalari

Cominciamo dal primo punto.

- Mostriamo che **(R^3, +)** e' un gruppo commutativo; devono valere le proprieta':
  - **+** e' interna infatti chiamati **(a, b, c)** e **(d,e,f)** due elementi di R^3 allora anche
    $(a + d, b + e, c + f)$ appartiene a R^3
    infatti abbiamo che sulle varie componenti vale l'addizione in **R**
  - **+** e' associativa, infatti chiamati **(a, b, c)**, **(d, e, f)** e **(g, h, i)** tre elementi di R^3 abbiamo:
    $[(a, b, c) + (d, e,f)] + (g,h,i) = (a + d, b + e, c + f) + (g, h, i) =$
    $= (a + d + g,\ b + e + h,\ c + f + i) = (a, b, c) + (d + g,\ e + h,\ f + i) =$
    $= (a, b, c) + [(d, e, f) + (g, h, i)]$
    Infatti proiettandoci sulle varie componenti, l'addizione in **R** e' associativa.
  - **+** possiede l'elemento neutro; infatti esiste l'elemento **(0, 0, 0)** tale che per ogni elemento **(a, b, c)** di R^3 abbiamo:
    $(0, 0, 0) + (a, b, c) = (0 + a,\ 0 + b,\ 0 + c) = (a + 0,\ b + 0,\ c + 0) = (a, b, c) + (0, 0, 0)$
    sulle componenti l'addizione e' commutativa.

- ogni elemento **(a, b, c)** di $\mathbf{R^3}$ possiede in **+** l'elemento simmetrico **(-a, -b, -c)** tale che:
  $(a, b, c) + (-a, -b, -c) = (a-a, b-b, c-c) = (0, 0, 0)$
  Infatti, dato su una componente un numero reale basta considerare lo stesso numero con segno opposto.

Quindi **($\mathbf{R^3}$, +)** e' un gruppo; inoltre tale gruppo e' commutativo perche' presi comunque due elementi **(a, b, c)** e **(d, e, f)** di $\mathbf{R^3}$ vale sempre:
$(a, b, c) + (d, e, f) = (a + d,\ b + e,\ c + f) = (d + a,\ e + b,\ f + c) = (d, e, f) + (a, b, c)$
Infatti, su una componente posso applicare la legge commutativa valida in **R.**

- Mostriamo la commutativita' del prodotto scalare (che coincide col prodotto ordinario in R):
  $x \cdot (a, b, c) = (x \cdot a,\ x \cdot b,\ x \cdot c) = (a \cdot x,\ b \cdot x,\ c \cdot x) = (a, b, c) \cdot x$
  Il prodotto ordinario in R e' commutativo, quindi...
- Mostriamo la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale:
  $x \cdot [(a, b, c) + (d, e, f)] = x \cdot (a + d,\ b + e,\ c + f) = [x \cdot (a + d),\ x \cdot (b + e),\ x \cdot (c + f)] =$
  $(xa + xd,\ xb + xe,\ xc + xf) = (ax + dx,\ bx + ex,\ cx + fx) = (dx + ax,\ ex + bx,\ fx + cx) =$
  $= (dx, ex, fx) + (ax, bx, cx) = (xd, xe, xf) + (xa, xb, xc) = x\,(d, e, f) + x\,(a, b, c)$
- Mostriamola proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari
  $x \cdot (y + z) = x \cdot y + x \cdot z$
  Siamo in **R** e quindi la proprieta' e' valida.
- Mostriamo la proprieta' associativa fra gli scalari
  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
  Siamo sempre in **R** e quindi la proprieta' e' valida.
  Quindi $\mathbf{R^3}$) e' uno spazio vettoriale sul corpo **R.**

---

4) Insieme $\mathbf{R^n}$ dello spazio ad n dimensioni con le normali operazioni di addizione e moltiplicazione e con la moltiplicazione scalare $\mathbf{R \otimes R^n}$.

Individuare la struttura di spazio vettoriale sullo spazio ordinario $\mathbf{R^n}$ con le normali operazioni di addizione e moltiplicazione e con moltiplicazione scalare la normale moltiplicazione $\mathbf{R \cdot R^n}$.

E' la stessa dimostrazione fatta nella pagina precedente, solamente consideriamo n componenti invece delle tre ordinarie; quindi procede nello stesso modo; se hai fatto quella puoi non fare questa.

Dimostrazione. Dovremo mostrare che abbiamo:

- la presenza di un gruppo commutativo su $\mathbf{R^n}$ con l'oprazione somma (nelle componenti si riduce a somma fra elementi di **R**)
- la commutativita' del prodotto scalare (che coincide col prodotto ordinario in **R**)
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari
- la proprieta' associativa fra gli scalari.

Cominciamo dal primo punto.

- Mostriamo che **($\mathbf{R^3}$, +)** e' un gruppo commutativo; devono valere le proprieta':
  - **+** e' interna infatti chiamati $(a_1, a_2, a_3, \ldots, a_n)$ e $(b_1, b_2, b_3, \ldots, b_n)$ due elementi di $\mathbf{R^n}$ allora anche:
    $(a_1 + b_1,\ a_2 + b_2,\ a_3 + b_3,\ \ldots,\ a_n + b_n)$ appartiene a $\mathbf{R^n}$
    Infatti abbiamo che sulle varie componenti vale l'addizione in **R**
  - **+** e' associativa, infatti chiamati:
    $(a_1, a_2, a_3, \ldots, a_n)$, $(b_1, b_2, b_3, \ldots, b_n)$ e $(c_1, c_2, c_3, \ldots, c_n)$ tre elementi di $\mathbf{R^3}$, abbiamo:
    $[(a_1, a_2, a_3, \ldots, a_n) + (b_1, b_2, b_3, \ldots, b_n)] + (c_1, c_2, c_3, \ldots, c_n) =$
    $= (a_1 + b_1,\ a_2 + b_2,\ a_3 + b_3,\ \ldots,\ a_n + b_n) + (c_1, c_2, c_3, \ldots, c_n) =$
    $= (a_1 + b_1 + c_1,\ a_2 + b_2 + c_2,\ a_3 + b_3 + c_3,\ \ldots,\ a_n + b_n + c_n) =$
    $= [a_1 + (b_1 + c_1),\ a_2 + (b_2 + c_2),\ a_3 + (b_3 + c_3),\ \ldots,\ a_n + (b_n + c_n)] =$
    $= (a_1, a_2, a_3, \ldots, a_n) + (b_1 + c_1,\ b_2 + c_2,\ b_3 + c_3,\ \ldots,\ b_n + c_n) =$
    $= (a_1, a_2, a_3, \ldots, a_n) + [(b_1, b_2, b_3, \ldots, b_n) + (c_1, c_2, c_3, \ldots, c_n)]$
    Infatti sulle varie componenti (in **R**) vale le proprieta' associativa dell'addizione.
  - **+** possiede l'elemento neutro; infatti esiste l'elemento $(0, 0, 0, \ldots\ldots, 0)$ tale che per ogni elemento $(a_1, a_2, a_3, \ldots, a_n)$ di $\mathbf{R^3}$ abbiamo:
    $(0, 0, 0, \ldots\ldots, 0) + (a_1, a_2, a_3, \ldots, a_n) = (0 + a_1,\ 0 + a_2,\ 0 + a_3,\ \ldots,\ 0 + a_n) =$
    $= (a_1 + 0,\ a_2 + 0,\ a_3 + 0,\ \ldots,\ a_n + 0) = (a_1, a_2, a_3, \ldots, a_n) + (0, 0, 0, \ldots\ldots, 0)$
    Questo perche' sulle componenti l'addizione e' commutativa.

- ogni elemento $(a_1, a_2, a_3, ..., a_n)$ di R^n possiede in $+$ l'elemento simmetrico:
  $(-a_1, -a_2, -a_3, ..., -a_n)$
  tale che:
  $(a_1, a_2, a_3, ..., a_n) + (-a_1, -a_2, -a_3, ..., -a_n) = (a_1-a_1, a_2-a_2, a_3-a_3, ... a_n-a_n) = (0, 0,0,.....,0)$
  Infatti dato su una componente un numero reale basta considerare lo stesso numero con segno opposto.

Quindi $(R^n, +)$ e' un gruppo.
Inoltre tale gruppo e' commutativo perche' presi comunque due elementi:
$(a_1, a_2, a_3, ..., a_n)$ e $(b_1, b_2, b_3, ..., n_n)$ di R^n vale sempre:
$(a_1, a_2, a_3, ..., a_n)+(b_1, b_2, b_3, ..., b_n) = (a_1+b_1, a_2+b_2+a_3+b_3, ... a_n+b_n) =$
$= (b_1 + a_1,\ b_2 + a_2,\ b_3 + a_3,\ .....\ b_n + a_n) = (b_1, b_2, b_3, ..., b_n) + (a_1, a_2, a_3, ..., a_n)$
infatti su una componente posso applicare la legge commutativa valida in R

- Mostriamo la commutativita' del prodotto scalare (che coincide col prodotto ordinario in R)
  $x \cdot (a_1, a_2, a_3, ..., a_n) = (x \cdot a_1, x \cdot a_2, x \cdot a_1, ..., x \cdot a_n) = (a_1 \cdot x, a_2 \cdot x, a_3 \cdot x, ..., a_n \cdot x) = (a_1, a_2, a_3, ..., a_n) \cdot x$
  Il prodotto ordinario in R e' commutativo, quindi...
- Mostro la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale:
  $x\cdot[(a_1, a_2, a_3, ..., a_n)+(b_1, b_2, b_3, ..., b_n)] = x\cdot(a_1+b_1, a_2+b_2, a_3+b_3, ..., a_n+b_n) =$
  $= [x\cdot(a_1+b_1, x\cdot(a_2+b_2), x\cdot(a_3+b_3), ..., x\cdot(a_n+b_n)] = (xa_1+xb_1, xa_2+xb_2, xa_3+xb_3, ..., xa_n+xb_n) =$
  $= (a_1x+b_1x, a_2x+b_2x, a_3x+b_3x, ..., a_nx+b_nx) = (b_1x+a_1x, b_2x+a_2x, b_3x+a_3x, ..., b_nx+a_nx) =$
  $=(b_1x, b_2x, b_3x, ..., b_nx)+(a_1x, a_2x, a_3x, ..., a_nx) = (xb_1, xb_2, xb_3, ..., xb_n)+(xa_1, xa_2, xa_3, ..., xa_n) =$
  $= x(b_1, b_2, b_3, ..., b_n) + x(a_1, a_2, a_3, ..., a_n)$
- Mostriamola proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari:
  $x \cdot (y + z) = x \cdot y + x \cdot z$
  Siamo in R e quindi la proprieta' e' valida.
- Mostriamo la proprieta' associativa fra gli scalari:
  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
  Siamo sempre in R e quindi la proprieta' e' valida.
  Quindi R^n) e' uno spazio vettoriale sul corpo R.

---

5) Uno spazio funzionale $F(x)$ i cui elementi sono funzioni $y=f(x)$ in cui e' definita la somma vettoriale come $f(x)+g(x)$ ed il prodotto scalare come $a\cdot f(x)$ con a appartenete ad R.

Individuare la struttura di spazio vettoriale sullo spazio funzionale $F(x)$ i cui elementi sono funzioni $y=f(x)$ (definite su tutto R)?, in cui e' definita la somma vettoriale come la nuova funzione $y = f(x)+g(x)$ ed il prodotto scalare come $a\cdot f(x)$ con a appartenete ad R.
Dimostrazione. Dovremo mostrare che abbiamo:

- la presenza di un gruppo commutativo su $F(x)$ con l'operazione somma
- la commutativita' del prodotto scalare (che coincide col prodotto ordinario)
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari
- la proprieta' associativa fra gli scalari

Cominciamo dal primo punto

- Mostriamo che $(F(x), +)$ e' un gruppo commutativo; devono valere le proprieta':
  - $+$ e' interna infatti chiamati $y=f_1(x)$ e $y = f_2(x)$ due elementi di $F(x)$ allora anche
    $f_3(x) = f_1(x) + f_2(x)$ appartiene a $F(x)$
    infatti una somma di funzioni e' ancora una funzione
  - $+$ e' associativa
    infatti chiamati $f_1(x)$, $f_2(x)$ e $f_3(x)$ tre elementi di $F(x)$ abbiamo:
    $[f_1(x) + f_2(x)] + f_3(x) = f_1(x) + [f_2(x) + f_3(x)]$
    Al solito le proprieta' della somma in R si applicano anche alla somma dei termini delle funzioni: te lo mostro su un esempio
    Consideriamo le funzioni

$y_1 = x^2 + \log x$
$y_2 = x^2 + 3x + 4$
$y_1 = e^x + x$
Devo mostrare che vale:
$[x^2 + \log x + x^2 + 3x + 4] + e^x + x = x^2 + \log x + [x^2 + 3x + 4 + e^x + x]$

Basta applicare la proprieta' associativa e dissociativa della somma:
$[x^2 + \log x + x^2 + 3x + 4] + e^x + x = x^2 + \log x + x^2 + 3x + 4 + e^x + x =$
$= x^2 + \log x + [x^2 + 3x + 4 + e^x + x]$

- **+** possiede l'elemento neutro: infatti esiste la funzione $\mathbf{y = 0}$ tale che per ogni elemento:
  $(f_1(x) + 0 = 0 + f_1(x) = f_1(x)$
- ogni elemento $\mathbf{f_1(x)}$ di $\mathbf{F(x)}$ possiede in **+** l'elemento simmetrico $\mathbf{-f_1(x)}$ tale che:
  $f_1(x) - f_1(x) = 0$
  Infatti bastera' considerare la funzione i cui termini hanno segno opposto.

Esempio: se
$f_1(x) = x^2 + \log x$
considero come simmetrica:
$-f_1(x) = -x^2 - \log x$

Quindi $\mathbf{(F(x), +)}$ e' un gruppo;
inoltre tale gruppo e' commutativo perche' presi comunque due elementi:
$f_1(x)$ e $f_2(x)$ di $\mathbf{F(x)}$ vale sempre:
$f_1(x) + f_2(x) = f_2(x) + f_1(x)$
Infatti la somma dei termini di una funzione e' commutativa.

- Mostriamo, su un esempio la commutativita' del prodotto scalare (che coincide col prodotto ordinario):
  $x \cdot f_1(x) = f_1(x) \cdot x$

$3 \cdot (x^2 + \log x) = 3 \cdot x^2 + 3 \cdot \log x = x^2 \cdot 3 + \log x \cdot 3 = (x^2 + \log x) \cdot 3$

- Proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale:
  $x \cdot [f_1(x) + f_2(x)] = x \cdot f_1(x) + x \cdot f_2(x)$

Anche qui te la mostro su un esempio:
$f_1(x) = e^x + x$
$f_2(x) = x^2 + x + 3$
$4 \cdot [(e^x + x) + (x^2 + x + 3)] = 4 \cdot [e^x + x + x^2 + x + 3] =$
$= 4 \cdot e^x + 4 \cdot x + 4 \cdot x^2 + 4 \cdot x + 4 \cdot 3 = (4 \cdot e^x + 4 \cdot x) + (4 \cdot x^2 + 4 \cdot x + 4 \cdot 3) =$
$= 4 \cdot (e^x + x) + 4 \cdot (x^2 + x + 3)$

- Mostriamola proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari:
  $x \cdot (y + z) = x \cdot y + x \cdot z$
  Siamo in $\mathbf{R}$ e quindi la proprieta' e' valida.
- Mostriamo la proprieta' associativa fra gli scalari
  $x \cdot (y \cdot z) = (x \cdot y) \cdot z$
  Siamo sempre in $\mathbf{R}$ e quindi la proprieta' e' valida.
  Quindi $\mathbf{F(x)}$) e' uno spazio vettoriale sul corpo $\mathbf{R}$.

6) Insieme $\mathbf{P(x)}$ dei polinomi in $\mathbf{x}$ a coefficienti reali con le normali operazioni di addizione (+) e moltiplicazione (·) fra polinomi sul corpo $\mathbf{R}$ e con la normale moltiplicazione · come prodotto scalare.

Individuare la struttura di spazio vettoriale sull' insieme $\mathbf{P(x)}$ dei polinomi in $\mathbf{x}$ a coefficienti reali con le normali operazioni di addizione (+) e moltiplicazione (·) fra polinomi sul corpo $\mathbf{R}$ e con la normale moltiplicazione · come prodotto scalare.

Per insieme dei polinomi $\mathbf{P(x)}$ si intende l'insieme dei polinomi della forma:
$a_n x^n + a_{n-1} x^{n-1} \ldots a_2 x^2 + a_1 x + a_0$
con $\mathbf{n = 0,1,2,\ldots,n,n+1,\ldots}$ Non ho capito:

L'operazione di addizione significa l'addizione fra polinomi per cui sommiamo algebricamente i coefficienti dei termini con x allo stesso grado: cioe', se n e maggiore di m avremo
$(a_n x^n + a_{n-1} x^{n-1} \ldots a_2 x^2 + a_1 x + a_0) + (b_m x^m + b_{m-1} x^{m-1} \ldots b_2 x^2 + b_1 x + b_0) =$

$= a_n x^n + a_{n-1}x^{n-1} .... + (a_m+b_m)x^m + (a_{m-1}+b_{m-1})x^{m-1} .... + (a_2+b_2)x^2 + (a_1+b_1)x + (a_0+b_0)$
Il prodotto fra polinomi e' il normale prodotto fra polinomi gia' visto.

Dimostrazione. Dovremo mostrare che abbiamo:

- la presenza di un gruppo commutativo su **P(x)** con l'operazione somma
- la commutativita' del prodotto scalare (che coincide col prodotto ordinario su ogni termine)
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale
- la proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari
- la proprieta' associativa fra gli scalari

Cominciamo dal primo punto: ti ripeto la dimostrazione gia' fatta nell'esercizio sugli anelli

- Mostriamo che **(P(x), +)** e' un gruppo commutativo; devono valere le proprieta':
  - **+** e' interna infatti avremo sempre che la somma di due polinomi in **x** e' sempre ancora un polinomio in **x**: facciamo un esempio pratico:
    $(2x^3 + 5x^2 -4x + 3) + (3x^2 + 4) = 2x^3 + 8x^2 -4x + 7$

    In pratica la somma nei polinomi si riduce alla somma dei coefficienti numerici di stesso grado e quindi le proprieta' della somma sono le stesse che hanno i numeri reali.

  - **+** e' associativa, infatti chiamati **A(x)**, **B(x)** e **C(x)** tre elementi di **P(x)** abbiamo:
    $[A(x) + B(x)] + C(x) = A(x) + [B(x) + C(x)]$
    facciamo anche qui un esempio pratico:
    $[(2x^3 + 5x^2 -4x + 3) + (3x^2 + 4)] + (2x^2 + 3x -4) =$
    $= (2x^3 + 5x^2 -4x + 3) + [(3x^2 + 4) + (2x^2 + 3x -4)]$
    Per mostrarlo basta che fai i calcoli prima e dopo l'uguale e mostri che i risultati sono uguali; lo sono perche' la somma fra i coefficienti (essendo numeri reali) gode della proprieta' associativa.
  - **+** possiede l'elemento neutro: infatti esiste l'elemento **P(0)**, intendendo **P(0)** come il polinomio $0x^n+....+0x^2+0x+0$ tale che per ogni elemento **A(x)** di **P(x)** abbiamo:
    $A(x) + P(0) = A(x)$
    $P(0) + A(x) = A(x)$
    cioe' sommando **P(0)** a qualunque elemento l'altro elemento non cambia.
  - ogni elemento **A(x)** di **P(x)** possiede in **+** l'elemento simmetrico; infatti preso:
    $A(x) = a_n x^n + a_{n-1}x^{n-1} .... a_2x^2 + a_1x + a_0$
    il simmetrico e':
    $A'(x)= -a_n x^n - a_{n-1}x^{n-1} .... -a_2x^2 - a_1x - a_0$
    Infatti:
    $A(x) + A'(x) = 0$

  Quindi **(P(x), +)** e' un gruppo. Inoltre il gruppo e' commutativo perche' commutativa e' la somma fra i coefficienti numerici.
  Cioe' presi comunque due elementi: $P_1(x)$ e $P_2(x)$ di **P(x)** , vale sempre:
  $P_1(x) + P_2(x) = P_2(x) + P_1(x)$
- La commutativita' del prodotto scalare deriva dalla commutativita' del prodotto ordinario fra numeri rali dovendo moltiplicare il numero dato per ogni coefficiente numerico
  $h \cdot (a_n x^n + a_{n-1}x^{n-1} .... a_2x^2 + a_1x + a_0) = ha_n x^n + ha_{n-1}x^{n-1} .... ha_2x^2 + ha_1x + ha_0 =$
  $= a_n h\, x^n + a_{n-1}hx^{n-1} .... a_2hx^2 + a_1hx + a_0h = (a_n x^n + a_{n-1}x^{n-1} .... a_2x^2 + a_1x + a_0) \cdot h$

- Proprieta' distributiva della moltiplicazione scalare rispetto all'addizione vettoriale:
  $h \cdot [P_1(x) + P_2(x)] = h \cdot P_1(x) + h \cdot P_2(x)$
  Dimostriamolo. Supponiamo **m > n.**
  Supponiamo sia $P_1(x)$ un generico polinomio di grado **n** e $P_2(x)$ un polinomio generico di grado **m** ed inoltre supponiamo **m > n:**
  $h\cdot [(a_n x^n + a_{n-1}x^{n-1} .... a_2x^2 + a_1x + a_0) + (b_m x^m + b_{m-1}x^{m-1} ....+b_n x^n + b_{n-1}x^{n-1}+..... +b_2x^2 + b_1x + b_0)] =$

  $= h\cdot (a_n x^n + a_{n-1}x^{n-1} .... a_2x^2 + a_1x + a_0 + b_m x^m + b_{m-1}x^{m-1} ....+b_n x^n + b_{n-1}x^{n-1}+..... +b_2x^2 + b_1x + b_0) =$

  $= ha_n x^n + ha_{n-1}x^{n-1} .... ha_2x^2 + ha_1x + ha_0 + hb_m x^m + hb_{m-1}x^{m-1} ....+hb_n x^n + hb_{n-1}x^{n-1}\, hb_2x^2 + hb_1x + hb_0 =$

  $= (ha_n x^n + ha_{n-1}x^{n-1} .... ha_2x^2 + ha_1x + ha_0) + (hb_n x^n + hb_{n-1}x^{n-1}+ ...+hb_n x^n + hb_{n-1}x^{n-1}+... +hb_2x^2 + hb_1x + hb_0) =$
  $= h\cdot (a_n x^n + a_{n-1}x^{n-1} .... a_2x^2 + a_1x + a_0) + h\cdot (b_n x^n + b_{n-1}x^{n-1}+ ....+b_n x^n + b_{n-1}x^{n-1}+..... +b_2x^2 + b_1x + b_0)$

- Mostriamola proprieta' distributiva della moltiplicazione scalare rispetto all'addizione di scalari
  $h \cdot (p + q) = h \cdot p + h \cdot q$
  Siamo in **R** e quindi la proprieta' e' valida,
- Mostriamo la proprieta' associativa fra gli scalari:
  $h \cdot (p \cdot q) = (h \cdot p) \cdot q$
  Siamo sempre in **R** e quindi la proprieta' e' valida.
  Quindi **F(x)**) e' uno spazio vettoriale sul corpo **R**

D. *Morfismi*

Spesso, anche fra parti molto diverse della matematica, si notano delle somiglianze, delle operazioni che si comportano nello stesso modo, delle strutture equivalenti; vediamo in questo capitolo di formalizzare tali fatti con la nozione di **morfismo**.
Naturalmente lo faremo a livello molto, molto elementare.

In alcuni testi ho visto utilizzare la stessa definizione per morfismo ed omomorfismo, siccome ogni docente ha un suo "gergo matematico" ti conviene sempre seguire le definizioni che ti da' il tuo docente.

1. Un esempio di morfismo

In pratica, dobbiamo vedere se un'operazione si "mantiene" quando trasformiamo mediante funzioni gli oggetti di un dominio su cui tale operazione lavora. Naturalmente, se gli oggetti sono trasformati, anche l'operazione sul codominio potra' essere diversa, pero' talvolta l'operazione valida nel primo insieme trova corrispondenza in un'operazione nel secondo insieme nel senso che, operando sui trasformati dei singoli termini oppure sul trasformato del risultato, otteniamo gli stessi valori; in questo caso diciamo che abbiamo un morfismo.
Per capire bene il concetto partiamo da degli esempi e vedrai che e' piu' difficile da dire che da fare, poi, nella pagina successiva, diamo la definizione matematica.

Consideriamo due insiemi e costruiamo una funzione che ci trasformi gli elementi del primo insieme negli elementi del secondo insieme.
Consideriamo come insieme di partenza l'insieme **N** dei numeri Naturali e come secondo insieme l'insieme dei quadrati $\mathbf{N^2}$ dei numeri naturali:

N = {	1	2	3	4	5	6	7	8	9	10	...	}
f	|	|	|	|	|	|	|	|	|	|		
N^2 = {	1	4	9	16	25	36	49	64	81	100	...	}

e consideriamo la funzione **f** tale che ad ogni numero faccia corrispondere il suo quadrato:
$f: n \to n^2$
cioe':
$f(1) = 1$
$f(2) = 4$
$f(3) = 9$
.....
$f(n) = n^2$
.....
Consideriamo ora il prodotto; per distinguere chiamiamo:
x il prodotto nel primo insieme
$\otimes$ il prodotto nel secondo insieme.
Facciamo un prodotto nel primo insieme:
$3 \times 2 = 6$
Se consideriamo i corrispondenti nel secondo insieme abbiamo:
$9 \otimes 4 = 36$
e l'uguaglianza e' valida.
Quindi abbiamo che sull'insieme **N** dotato dell'operazione di moltiplicazione **x** la funzione **f** e' un morfismo; cioe' intuitivamente una funzione e' un morfismo se conserva l'operazione:

	3	x	2	=	6
f	|		|		|
	9	$\otimes$	4	=	36

Sullo stesso esempio vediamo che, se dotiamo l'insieme **N** dell'operazione somma, allora **f** non e' piu' un morfismo.
Per distinguere chiamiamo:
$+$ la somma nel primo insieme
$\oplus$ la somma nel secondo insieme
Facciamo una somma nel primo insieme
$3 + 2 = 5$
Se consideriamo i corrispondenti nel secondo insieme abbiamo:
$9 \oplus 4 = 13$
e l'uguaglianza non e' valida
quindi abbiamo che sull'insieme **N** dotato dell'operazione di addizione $+$ la funzione **f** non e' un morfismo;

	3	+	2	=	5
f	|		|		|
	9	$\oplus$	4	=	13

Deriva da cio' che il concetto di morfismo e' strettamente legato al concetto di operazione: cioe' il morfismo e' un'applicazione che trasporta un'operazione da un insieme ad un altro.

2. Definizione di morfismo

Per dare la definizione matematica partiamo dall'esempio della pagina precedente:

	3	x	2	=	6
f	|		|		|
	9	⊗	4	=	36

Ti ho evidenziato in blu la parte che conta; conta il fatto che trasformare mediante f due termini e fare il prodotto ⊗ oppure trasformare il risultato dopo aver fatto il loro prodotto **x** da' sempre lo stesso risultato.
Cioe' essendo $9 = f(3)$ e $4 = f(2)$ ed inoltre $6 = 3 \text{ x } 2$ abbiamo:
$f(3) \otimes f(2) = f(6) = f(3 \text{ x } 2)$
Tolgo il termine al centro ed ottengo:
$f(3) \otimes f(2) = f(3 \text{ x } 2)$
Applichiamo adesso quanto visto al caso generale e diamo la definizione:

Date due strutture (A, x) e (B,⊗) dotate di due operazioni diverse x e ⊗ sugli insiemi A e B e data l'applicazione
$f: A \to B$
diremo che f e' un morfismo fra le due strutture, se indicati con a e b due elementi qualunque dell'insieme A e con f(a) ed f(b) gli elementi corrispondenti nell'insieme B, vale sempre:

$$f(a) \otimes f(b) = f(a \text{ x } b)$$

cioe', in breve, chiamando prodotto l'operazione generica:
Il prodotto dei trasformati e' uguale al trasformato del prodotto.

Naturalmente **x** e ⊗ sono simboli per due operazioni qualunque; sotto ti faccio un esempio usando la somma ed il prodotto.

Esempio:
Consideriamo le due strutture:
$(N, +)$ cioe' l'insieme dei numeri naturali con l'operazione di addizione
$(2^N, \cdot)$ cioe' l'insieme delle potenze del 2 con esponente naturale con l'operazione di prodotto
e consideriamo l'applicazione:
$f: N \to 2^n \quad f(a) = 2^a$
Applichiamo la definizione per due elementi **a** e **b** di **N:**
$f(a) \cdot f(b) = f(a + b)$
$2^a \cdot 2^b = 2^{a+b}$
l'uguaglianza e' valida, (vedi le regole per il prodotto di potenze con la stessa base)
Quindi **f** e' un morfismo fra le due strutture.
(vedremo poi, su un esempio con base diversa, che e' addirittura un isomorfismo).

In alcuni testi ho visto utilizzare la stessa definizione per morfismo ed omomorfismo, siccome ogni docente ha un suo "gergo matematico" ti conviene sempre seguire le definizioni che ti da' il tuo docente.

3. Endomorfismo

L'**endomorfismo** e' un caso particolare di morfismo; si ha quando le strutture agiscono sullo stesso dominio, cioe' gli insiemi su cui si opera sono identici (morfismo di **A** su se' stesso).
Definizione:

Date due strutture (A, x) e (A,⊗) e data l'applicazione univoca:
f: A → A
diremo che f e' un endomorfismo fra le due strutture se, indicati con a e b due elementi qualunque dell'insieme A e con f(a) ed f(b) gli elementi corrispondenti sempre nell'insieme A, vale:

$$f(a) \otimes f(b) = f(a \otimes b)$$

4. Omomorfismo

L'**omomorfismo** e' un caso speciale di morfismo; si ha quando l'operazione si conserva, cioe' le due strutture:
(A,⊗) e **(B,⊗)**
sono dotate della stessa operazione (chiamiamola prodotto), ed al prodotto di due elementi in **A** corrisponde in **B** il prodotto degli elementi corrispondenti.

Quindi un omomorfismo e' sempre un morfismo.

Definizione:

Date due strutture (A,⊗) e (B,⊗) dotate della stessa operazione ⊗sugli insiemi A e B e data l'applicazione univoca:
f: A → B
diremo che f e' un omomorfismo fra le due strutture se indicati con a e b due elementi qualunque dell'insieme A e con f(a) ed f(b) gli elementi corrispondenti nell'insieme B vale:

$$f(a) \otimes f(b) = f(a \otimes b)$$

Esempio:
Consideriamo le due strutture:
(N, +) cioe' l'insieme dei numeri naturali con l'operazione di addizione
(2N, +) cioe' l'insieme dei numeri pari sempre con l'operazione di addizione
e consideriamo l'applicazione:
$f: N \to 2N \quad f(a) = 2a$ che trasforma ogni numero nel suo doppio
Applichiamo la definizione per due elementi **a** e **b** di **N:**

$$f(a) + f(b) = f(a + b)$$
$$2a + 2b = 2(a + b)$$

Per mostrare la validita' dell'uguaglianza basta applicare al secondo membro la proprieta' distributiva del prodotto rispetto alla somma:

$$2(a + b) = 2a + 2b$$

Quindi **f** e' un omomorfismo fra le due strutture.

Invece, nell'esempio della pagina precedente, non si tratta di morfismo essendo le due operazioni diverse
Vedi anche la nota finale della pagina precedente.

5. Monomorfismo

Diciamo che si ha un **monomorfismo** se abbiamo un morfismo e l'applicazione **f** e' iniettiva, cioe' ad ogni elemento diverso della prima struttura corrisponde un solo elemento della seconda struttura.
Definizione:

Date due strutture (A, x) e (B,⊗) dotate dell' operazione x sull'insieme A e ⊗sull' insieme B se l'applicazione:
f: A → B
e' un morfismo ed e' iniettiva, allora f e' un monomorfismo fra le due strutture.

Vediamo un esempio di monomorfismo:
Consideriamo le due strutture:
(Z, +) cioe' l'insieme dei numeri interi con l'operazione di somma
(R,⊕) cioe' l'insieme dei numeri Reali con l'operazione di addizione
Per farti capire meglio ti lascio le addizioni con simboli diversi.
Consideriamo l'applicazione:
f: z → R **f(a) = -a** che trasforma ogni numero intero nel suo opposto.
Applichiamo la definizione di morfismo per due elementi **a** e **b** di **Z**
f(a) ⊕ f(b) = f(a + b)
-a ⊕ (-b) = - (a + b)
Per mostrare la validita' dell'uguaglianza basta far cadere le parentesi:
-(a+b) = -a -b = -a + (-b)
Quindi **f** e' un omomorfismo fra le due strutture (l'operazione e' la stessa), e, siccome ad ogni elemento diverso in **Z** corrisponde un solo elemento in **R** l'applicazione e' iniettiva e si tratta di un monomorfismo.

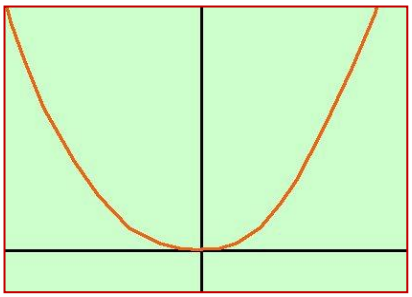
Vediamo ora un esempio che non sia un monomorfismo.
Consideriamo le due strutture:
(Q, x) cioe' l'insieme dei numeri razionali con l'operazione di moltiplicazione
(R,⊗) cioe' l'insieme dei numeri Reali con l'operazione di moltiplicazione
Per farti capire meglio anche qui ti lascio le moltiplicazioni con simboli diversi.
Consideriamo l'applicazione:
f: Q → R **$f(a) = \pm\sqrt{a}$** che trasforma ogni numero nel suo radicale algebrico.
Applichiamo la definizione di morfismo per due elementi **a** e **b** di **Q:**
f(a) ⊗ f(b) = f(a x b)
$\pm\sqrt{a} \otimes (\pm\sqrt{b}) = \pm\sqrt{(a \times b)}$
Per mostrare la validita' dell'uguaglianza basta ricordare la regola del prodotto fra due radicali con lo stesso indice.
Quindi **f** e' un omomorfismo fra le due strutture (l'operazione e' la stessa); ma, siccome ad ogni elemento in **Q** corrispondono due elementi in **R** l'applicazione **f** non e' univoca, quindi non si tratta di un monomorfismo.

6. Epimorfismo

Diciamo che si ha un **epimorfismo** se abbiamo un morfismo e l'applicazione **f** e' suriettiva, cioe' la seconda struttura viene tutta coperta.
Definizione:

Date due strutture (A, x) e (B,⊗) dotate dell' operazione x sull'insieme A e ⊗ sull' insieme B, se l'applicazione:
f: A → B
e' un morfismo ed e' suriettiva, allora f e' un epimorfismo fra le due strutture.

Vediamo un esempio di epimorfismo.
Consideriamo le due strutture:
(R, x) cioe' l'insieme dei numeri razionali con l'operazione di moltiplicazione
(R^+,⊗) cioe' l'insieme dei numeri Reali positivi o nulli con l'operazione di moltiplicazione
Per farti capire meglio ti lascio le moltiplicazioni con simboli diversi.
Consideriamo l'applicazione



$f: R \to R^+$ $f(a) = a^2$ che trasforma ogni numero nel suo quadrato.
Applichiamo la definizione di morfismo per due elementi **a** e **b** di **Q:**
$f(a) \otimes f(b) = f(a \times b)$
$a^2 \otimes b^2 = (a \times b)^2$
Per mostrare la validita' dell'uguaglianza basta ricordare la regola del prodotto fra due potenze con lo stesso esponente ma con basi diverse.
Quindi **f** e' un omomorfismo fra le due strutture (l'operazione e' la stessa), e, siccome ogni elemento in R^+ deriva da elementi di **R** e l'insieme R^+ viene esaurito, (si tratta della funzione tipo parabola con vertice nell'origine) **f** e' suriettiva, quindi si tratta di un epimorfismo.ò
Non si tratta invece di monomorfismo perche', a parte lo zero, un elemento di R^+ e' ottenuto sempre da due elementi di **R.**

7. Isomorfismo

Veniamo adesso all'applicazione che prende una struttura e la trasforma in una struttura equivalente; quindi ci servira' per individuare sottostrutture simili in strutture diverse, tipo la struttura dei numeri reali all'interno della struttura dei numeri complessi, oppure la struttura di **Z** all'interno di **Q** e cosi' via di seguito.
Naturalmente questo lo sapevamo gia', ma potremo applicare il metodo anche ad altri insiemi di enti per trovare relazioni che non conosciamo.
In pratica corrispondera' a trovare la corrispondenza biunivoca fra strutture o fra parti di strutture.

Abbiamo un **isomorfismo** se abbiamo un morfismo che sia contemporaneamente monomorfismo ed epimorfismo, cioe' tale che l'applicazione **f** sia iniettiva ed anche suriettiva.
Definizione:

Date due strutture (A, x) e (B,⊗) dotate dell' operazione x sull'insieme A e ⊗ sull' insieme B, se l'applicazione:
f: A -> B
e' un morfismo ed e' contemporaneamente iniettiva e suriettiva, allora f e' un isomorfismo fra le due strutture.

Esempio:
Consideriamo le due strutture:
(N, +) cioe' l'insieme dei numeri naturali con l'operazione di addizione
(10^N, ·) cioe' l'insieme delle potenze del 10 con esponente naturale con l'operazione di prodotto
e consideriamo l'applicazione:
$f: N \to 10^n$ $f(a) = 10^a$
Applichiamo la definizione per due elementi **a** e **b** di **N:**
$f(a) \cdot f(b) = f(a + b)$
$10^a \cdot 10^b = 10^{a+b}$
L'uguaglianza e' valida, (vedi le regole per il prodotto di potenze con la stessa base)
Quindi **f** e' un morfismo fra le due strutture.
L'applicazione e' iniettiva perche' ogni elemento diverso di **N** viene trasformato in un solo elemento di 10^N.
L'applicazione e' suriettiva perche' ogni elemento di 10^N deriva da un elemento di **N.**

8. Automorfismo

L'automorfismo e' l'equivalente per l'isomorfismo dell'endomorfismo per il morfismo

Si ha un **automorfismo** se si ha un isomorfismo e coincidono i due insiemi su cui sono definite le strutture.
Definizione:

Date due strutture (A, ·) e (A,⊗) dotate delle operazioni · e ⊗ sull' insieme A, se l'applicazione:
f: A → A
e' un isomorfismo. allora f e' un automorfismo fra le due strutture.

Esempio:
Consideriamo le due strutture:
(R-{0}, ·) cioe' l'insieme dei numeri reali privati dello zero con l'operazione di moltiplicazione
(R-{0},⊗) sempre l'insieme dei numeri reali privati dello zero con l'operazione di moltiplicazione
(le due operazioni possono essere diverse: te le indico quindi in modo diverso anche se in questo esempio particolare sono uguali).
Consideriamo l'applicazione:
$f: R-\{0\} \to R-\{0\} \quad f(a) = 1/a$

Ho tolto lo zero perche' **0** non ha inverso. Avrei potuto lasciare lo zero introducendo il simbolo ∞, ma perche' complicarci la vita?

Applichiamo la definizione per due elementi **a** e **b** di **R- {0}**
$f(a) \otimes f(b) = f(a \cdot b)$
$1/a \otimes 1/b = 1/(a \cdot b)$
L'uguaglianza e' valida, (regole per il prodotto di frazioni).
Quindi **f** e' un morfismo fra le due strutture.
L'applicazione e' iniettiva perche' ogni elemento diverso di **R-{0}** viene trasformato in un solo elemento di **R-{0}.**
L'applicazione e' suriettiva perche' ogni elemento di **R-{0}** deriva da un elemento di **R-{0}.**
Coincidendo gli insiemi di partenza abbiamo un automorfismo.

Ora si puo' sviluppare quanto qui appreso ed applicarlo ai vari enti matematici per evidenziarne e studiarne le proprieta' e le leggi, ma questo e' ormai un compito che spetta all'Universita'.

Fine capitolo di algebra astratta (almeno per ora)