

# Appunti molto belli di Algebra

Floppy Loppy

September 2021

## Contents

<b>1</b>	<b>Insiemi</b>	<b>3</b>
1.1	Proprietà degli insiemi . . . . .	3
1.2	Connettivi Logici . . . . .	4
1.3	Quantificatori universali . . . . .	5
1.4	Ordine dei quantificatori . . . . .	5
1.5	Quantificatori Equivalenti . . . . .	6
1.6	Negazione di un quantificatore . . . . .	6
1.7	Definizioni . . . . .	6
1.8	Insieme delle parti . . . . .	8
1.9	Proprietà degli insiemi . . . . .	8
1.10	Insiemi numerici . . . . .	9
1.11	Insiemi Indiciati . . . . .	9
<b>2</b>	<b>Relazioni e Funzioni</b>	<b>11</b>
2.1	Relazioni . . . . .	11
2.2	Funzioni . . . . .	11
2.3	Immagine e controimmagine . . . . .	12
2.3.1	Immagine . . . . .	12
2.3.2	Controimmagine . . . . .	13
2.4	Il grafico della funzione . . . . .	13
2.5	Iniettività, Surgettività e Bigettività . . . . .	13
2.6	Tipi di funzioni . . . . .	13
2.6.1	Funzione Identità . . . . .	13
2.6.2	Funzione Parte Intera . . . . .	13
2.6.3	Funzione Parte Frazionaria . . . . .	13
2.6.4	Funzione Composta . . . . .	13
2.7	Invertibilità . . . . .	13
<b>3</b>	<b>Assioma della scelta</b>	<b>14</b>

<b>4</b>	<b>Principio di Induzione</b>	<b>15</b>
4.1	Prima forma . . . . .	16
4.2	Seconda forma . . . . .	16
4.3	Terza forma . . . . .	16
<b>5</b>	<b>Esempio</b>	<b>17</b>
<b>6</b>	<b>Numeri Primi</b>	<b>18</b>
6.1	Teoria fondamentale dell'aritmetica . . . . .	18
6.2	Teorema di euclide . . . . .	18
<b>7</b>	<b>Numeri complessi</b>	<b>19</b>
7.1	Piano di Gauss . . . . .	19
7.2	Proprietà dei numeri complessi . . . . .	19
7.3	Forma esponenziale . . . . .	20
7.4	Equazioni di secondo grado complesse . . . . .	20
7.5	Radici complesse . . . . .	21
7.6	Teorema fondamendale dell'Algebra . . . . .	21
<b>8</b>	<b>Relazioni di Equivalenza</b>	<b>22</b>
8.1	Equivalenza modulare . . . . .	22
8.2	Classe di equivalenza . . . . .	22
<b>9</b>	<b>Cardinalità</b>	<b>23</b>
9.1	Teorema di Cantor-Bernstein . . . . .	24
9.2	Impossibilità della surriettività dei numerabili . . . . .	24
9.3	Argomento che il prof si tiene segreto . . . . .	25
9.4	Cardinalità dei $\mathbb{Q}$ . . . . .	26
9.5	Cardinalità di $\mathbb{R}$ . . . . .	26
9.6	Ipotesi del continuo . . . . .	26
<b>10</b>	<b>Calcolo Combinatorio</b>	<b>27</b>
10.1	Mi inventerò un titolo . . . . .	27
10.2	Coefficiente binomiale . . . . .	28
<b>11</b>	<b>Relazioni d'ordine</b>	<b>29</b>
11.1	Esempi di relazioni d'ordine . . . . .	29
11.2	Tipi di ordini . . . . .	30
11.2.1	Ordine lessicografico (LEX) . . . . .	30
11.2.2	Ordine prodotto . . . . .	30
11.2.3	Ordine indotto . . . . .	31
11.3	Minimo e massimo . . . . .	31

# 1 Insiemi

Noi definiamo **insieme** una **collezione** di elementi, questi elementi possono qualsiasi cosa: numeri, oggetti, persone, ecc..

Gli elementi fanno parte di un insieme soltanto se rispettano le proprietà dell'insieme stesso, per esempio gli elementi dell'insieme dei numeri pari dovranno avere come proprietà quella di essere pari appunto.

Perfetto ora che abbiamo una definizione di insieme possiamo iniziare ad introdurre la sintassi e alcune proprietà.

## 1.1 Proprietà degli insiemi

Consideriamo di avere un insieme di nome  $A$  e un elemento che chiamiamo  $x$  che fa parte di  $A$  (perchè rispetta le proprietà dell'insieme), allora si dice che  $x$  **Appartiene** ad  $A$ , ciò in Algebra si scrive:

$$x \in A \quad (1)$$

Mentre l'opposto ovvero che un elemento  $x$  non fa parte di  $A$  (perchè non rispetta le proprietà dell'insieme), allora si dice  $x$  **Non Appartiene** ad  $A$ , e ciò in si scrive (Nella lingua degli algebristi):

$$x \notin A \quad (2)$$

Se un insieme ha più di un elemento, che possono essere  $\{x_1, x_2, \dots, x_n\}$  allora possiamo sintetizzare la scrittura del fatto che ognuno di questi elementi appartiene all'insieme  $A$  scrivendo:

$$x = \{x_1, x_2, \dots, x_n\} \quad (3)$$

Oppure (visto che piace ai matematici) sintetizzare ancora di più scrivendo:

$$A = \{x : P(x)\} \quad (4)$$

Che si legge  $A$  *uguale agli elementi di  $x$  tali che  $P(x)$* , dove:

- $x$  sono gli elementi.
- $P(x)$  la proprietà dell'insieme  $A$  che gli elementi di  $A$  devono rispettare.

La proprietà  $P(x)$  ha l'obbligo di essere **oggettiva** ovvero in grado di dare un valore oggettivamente vero o falso ad un elemento.

Possiamo utilizzare un esempio più concreto come può essere quello dei numeri pari scrivendo:

$$A = \{x : x \text{ è un numero pari}\} \quad (5)$$

In questo caso possiamo dire che:

$$\begin{aligned}2 &\in A \\ 3 &\notin A \\ \text{Alessio} &\notin A\end{aligned}$$

In quanto 2 è pari perciò appartiene ad A, 3 è dispari quindi non appartiene all'insieme e Alessio non è un numero pari quindi non può appartenere all'insieme descritto.

Questo perchè la proprietà di essere pari è **oggettiva** mentre per esempio:

$$B = \{x : x \text{ è un libro interessante}\} \quad (6)$$

Non può essere un insieme in quanto essere un *libro interessante* non è una proprietà oggettiva.

Proseguendo possiamo trovare anche insiemi che contengono un solo elemento, questi insiemi sono detti **singoletti** e sono scritti:

$$\{*\} \quad (7)$$

Dove \* rappresenta il singolo elemento.

Ed infine, l'insieme vuoto che si rappresente con il simbolo:

$$\emptyset \quad (8)$$

Spiegandolo brevemente questo insieme non contiene nessun elemento (infatti si definisce vuoto), e possiede alcune proprietà interessanti come per esempio quello di essere contenuto in qualsiasi insieme.

## 1.2 Connettivi Logici

Attraverso quelli che chiamiamo **connettivi logici** possiamo eseguire delle operazioni tra insiemi, da queste operazioni noi possiamo ricavare due valori: vero o falso, andiamone a vederne alcune.

Prima di tutto definiamo due **proposizioni/affermazioni** fittizie che chiamiamo *P* e *D* e partendo da questi andiamo a scrivere le operazioni che si possono effettuare su di essi:

- La **Disgiunzione** scritta:  $P \vee D$  ha valore vero quando almeno una delle due proposizioni risulta vera, se entrambe sono false avremo invece un valore falso.
- La **Congiunzione** scritta:  $P \wedge D$  ha valore vero solo quando entrambe sono vere altrimenti otteniamo un valore falso.
- La **Negazione** scritta:  $\neg P$  inverte il valore della proposizione, se infatti *P* è vera  $\neg P$  sarà falsa e viceversa.

- L' **Implicazione** scritta:  $P \Rightarrow D$  ha valore vero solo quando D è vera.
- L' **Equivalenza** scritta:  $P \Leftrightarrow D$  ha valore vero solo quando P e D hanno lo stesso valore logico (vero;vero), (falso;falso).

### 1.3 Quantificatori universali

Abbiamo poi quelli che si chiamano quantificatori universali che servono a descrivere le proposizioni e le andremo a spiegare partendo da una proposizione qualsiasi che chiameremo  $P$ .

Scriviamo:

$$P : \forall x \in A \quad (9)$$

per dire che **per ogni** elemento di  $A$  la proposizione  $P$  vale.

Mentre scriviamo:

$$P : \exists x \in A \quad (10)$$

Per dire che **esiste almeno** un elemento di  $A$  tale per cui la proposizione  $P$  è vera.

Possiamo fare un esempio concreto, prendiamo un insieme  $A = \{2, 4, 6, 8\}$  e  $P(x) = x + 2$  è pari da questo possiamo dire con certezza che:

$$\forall x \in A \quad P(x) \quad \text{è vera in quanto ogni elemento di A è pari} \quad (11)$$

$$\exists x \in A \quad P(x) \quad \text{è vera in quanto almeno un elemento di A è pari} \quad (12)$$

Abbiamo poi l'**esiste unico** che sta ad indicare che esiste un solo elemento in un dato insieme affinché una proposizione risulti vera:

$$\exists! x \in A \quad (13)$$

### 1.4 Ordine dei quantificatori

Come ogni cosa in matematica bisogna rispettare gli ordini delle varie operazioni e questo vale anche per i quantificatori universali, si abbia per esempio:

$$P : x + y = 0 \quad \text{allora:} \quad (14)$$

$$\exists y \forall x P : \exists y \forall x \quad x + y = 0 \quad (15)$$

La proposizione dice che esiste un numero che è opposto di ogni numero (perché appunto un numero sommato al suo opposto è a zero).

Se cambiamo l'ordine dei quantificatori però cambiamo il significato di della proposizione, proviamo:

- $\forall y \exists x P$  che significa che ogni  $y$  esiste almeno un opposto

- $\exists x \forall y$  che significa esiste almeno un  $x$  che è opposto a tutti i numeri

Come abbiamo visto abbiamo radicalmente cambiato il significato della proposizione  $P$ .

Nel caso ci fossero ancora dubbi utilizzerò questo esempio:  
Prendiamo una proposizione  $P$  che dice che  $x$  paga da bere a  $y$ , utilizzando gli esempi di prima avremo che:

- $\forall y \exists x P$  che significa che ogni  $y$  a almeno una persona  $x$  che gli paga da bere.
- $\exists x \forall y$  che significa esiste almeno una persona  $x$  che paga da bere a tutti.

Spero che con questo esempio possa aver chiarito le idee.

## 1.5 Quantificatori Equivalenti

Per indicare un'equivalenza tra proposizioni noi utilizziamo il simbolo  $\equiv$  un esempio di equivalenza tra proposizioni può essere:  $\exists x \exists \equiv \exists y \exists x$ .

## 1.6 Negazione di un quantificatore

Ok la negazione è semplice quindi non mi dilungherò molto: Prendiamo una proposizione  $P$ : lo studente supererà l'esame, avremo:

- $\neg \forall x P(x)$ , che significa che non tutti gli studenti hanno superato l'esame (che non significa che nessuno ha superato l'esame).
- $\neg \exists x P(x)$ , che significa che non esiste alcuno studente che ha superato l'esame.

Se volessimo fare un'equivalenza potremmo dire che:

- $\neg \forall x P \equiv \exists x \neg P$
- $\neg \exists x P \equiv \forall x \neg P$

## 1.7 Definizioni

Ora andiamo ad introdurre alcune definizioni della teoria degli insiemi prendendo due insiemi fittizi  $A$  e  $B$ .

Si dice che  $A$  è contenuto in  $B$  se:

$$\{\forall x \in A : x \in B\} \quad (16)$$

e si legge *per tutti gli elementi di  $A$  sono elementi di  $B$*  e lo scriviamo in questo modo:

$$A \subseteq B \quad (17)$$

ovvero  $A$  sottoinsieme di  $B$  oppure  $A$  contenuto in  $B$ .

Poi abbiamo  $A$  uguale a  $B$  se:

$$x \in A \Leftrightarrow x \in B \quad (18)$$

ovvero ogni elemento  $x$  appartiene sia ad  $A$  che a  $B$ .

Troviamo poi l'**unione** tra due insiemi:

$$A \cup B \quad (19)$$

che sta a significare che ogni elemento di  $A$  appartiene anche a  $B$ , scritto in matematiche:

$$A \cup B = \{x : (x \in A) \vee (x \in B)\} \quad (20)$$

Mentre l'**intersezione** che rappresenta l'insieme degli elementi in comune tra due insiemi si scrive:

$$A \cap B \quad (21)$$

e significa:

$$A \cap B = \{x : (x \in A) \wedge (x \in B)\} \quad (22)$$

Infine abbiamo la **differenza o complementare** che è praticamente una sottrazione tra insiemi si scrive:

$$B \setminus A = \{x : (x \in B) \wedge (x \notin A)\} \quad (23)$$

ovvero tutti gli elementi di  $B$  che non appartengono ad  $A$ , spiegato meglio si tolgono a  $B$  gli elementi che fanno parte di  $A$ .

Ma noi vogliamo esempi pratici giusto?, ok e allora prendiamo due insiemi:  $A = \{1, 2, 4\}$  e  $B = \{1, 2, 3, 4, 5\}$  avremo che:

- $A \subseteq B$  vero
- $A = B$  falso
- $A \cup B = \{1, 2, 3, 4, 5\}$  oppure  $A \cup B = B$
- $A \cap B = \{1, 2, 4\}$  oppure  $A \cap B = A$
- $B \setminus A = \{3, 4, 5\}$

## 1.8 Insieme delle parti

L'insieme delle parti è l'insieme dei sottoinsiemi contenuti in un dato insieme, ok spieghiamolo meglio, l'insieme delle parti di un insieme  $A$  è l'insieme degli elementi che sono sottoinsiemi dell'insieme  $A$ .

Se la cosa vi confonde ancora facciamo un esempio concreto, prendiamo un insieme  $A = \{1, 2, 3\}$  l'insieme delle parti, che si scrive  $P(A)$  è:

$$P(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, A\} \quad (24)$$

Adesso il concetto dovrebbe essere (spero), più chiaro.

Prendiamo un esempio particolare dell'insieme delle parti, **l'insieme delle parti dell'insieme vuoto**, come sappiamo infatti l'insieme vuoto non ha nessun elemento, ma l'insieme delle parti è differente è l'insieme dei sotto insiemi di un dato insieme e come sappiamo ogni insieme ha come elemento l'insieme vuoto perciò:

$$P\{\emptyset\} = \{\emptyset\} \quad (25)$$

## 1.9 Proprietà degli insiemi

Ora mostriamo alcune proprietà degli insiemi per poi successivamente dimostrarli:

1.  $A \cup B = B \cup A$
2.  $(A \cup B) \cup C = A \cup (B \cup C)$
3.  $A \cup A = A$  Idempotenza
4.  $(A \cap B) \cap C = A \cap (B \cap C)$
5.  $A \cap A = A$

olte di queste sono facilmente dimostrabili, proviamo ad esempio a dimostrare la 2 che è appunto la proprietà associativa:

Se noi abbiamo che  $x \in (A \cup B) \cup C \Leftrightarrow (x \in A \cup B) \vee (x \in C)$  perchè appunto se  $x$  appartiene all'insieme formato dall'unione di  $A, B, C$  e conoscendo la definizione dell'unione 19 sappiamo che  $x$  deve appartenere almeno ad uno tra  $A, B, C$  e quindi possiamo scrivere che  $(x \in A) \vee (x \in B) \vee (x \in C)$  che può essere riscritta in  $x \in A \vee ((x \in B) \vee (x \in C))$  che sarebbe come scrivere (se seguiamo la definizione di unione)  $x \in A \vee (x \in B \cup C)$  che si può trasformare in  $x \in A \cup (x \in B \cup C)$ . Dimostrando che  $x$  può appartenere all'insieme formato da  $A, B, C$  anche cambiando l'ordine in è scritta l'unione dei tre insiemi, noi abbiamo dimostrato proprio che 2 è vera e anche se non l'ho dimostrato anche 4 è vera.

Se avete capito il meccanismo con il quale ho dimostrato 2 allora potete facilmente dimostrare 1 3 e 5.



## 1.10 Insiemi numerici

Gli insiemi numerici sono appunto gli insiemi formati da numeri.

Non mi dilungherò troppo in questa parte perchè molte nozioni sono già state apprese alle superiori ed alle medie, vi basti sapere che:

- 0 è contenuto in  $\mathbb{N}$
- Di  $\mathbb{C}$  Parleremo esaurientemente al capitolo 7

Per fare un breve riassunto degli insiemi numerici:

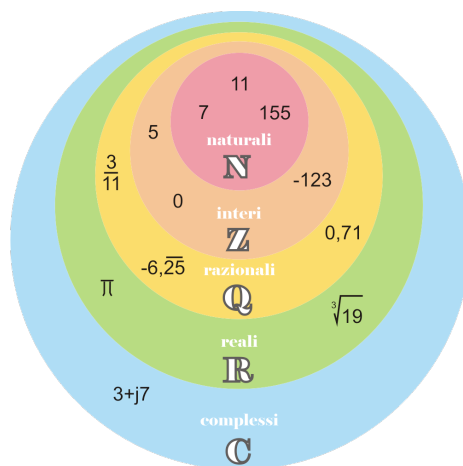


Figure 1: Insiemi numerici

## 1.11 Insiemi Indiciati

Un **Insieme indicato** è una famiglia di insiemi definiti da un indice  $i \in I$  dove  $I \in \mathbb{N}$ , infatti potenzialmente  $I = \{1, 2, 3, \dots, n\}$ .

Scriviamo un insieme indicato come:

$$\mathcal{F} = \{A_i\}_{i \in I} \quad (26)$$

Dove  $\mathcal{F}$  è la famiglia,  $A_i$  è l'insieme e  $i$  l'indice dell'insieme.

Un insieme  $A_i$  ha una certa proprietà che viene ripetuta per tutti gli  $A_i$  presenti nella famiglia, possiamo infatti immaginare la famiglia 26 come l'unione degli insiemi indicati che contiene:

$$\bigcup_{i \in I} A_i = \{P(x)\}$$

Se avessimo  $I = \{1, 2, 3, 4, 5\}$  sarebbe come scrivere:

$$A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$$

Facciamo un esempio, prendiamo  $A_i = \{x \in \mathbb{N} : x \neq 2i\}$  con  $I = \{1, 2, 3\}$ , avremo che:

- $A_1 = \{\mathbb{N} \neq 2\}$
- $A_2 = \{\mathbb{N} \neq 4\}$
- $A_3 = \{\mathbb{N} \neq 6\}$
- $A_1 \cup A_2 \cup A_3 = \mathbb{N}$  oppure  $\mathcal{F} = \{A_i\}_{i \in I} = \mathbb{N}$
- $A_1 \cap A_2 \cap A_3 = \{\mathbb{N} \neq 2, \mathbb{N} \neq 4, \mathbb{N} \neq 6\}$

Prendete con le pinze questa definizione, ma potremo immaginare gli insiemi indicati come array di array che hanno le stesse proprietà.

## 2 Relazioni e Funzioni

Gli elementi appartenenti a uno o più insiemi possono essere collegati attraverso diversi tipi di relazioni, per esempio i membri di una famiglia sono collegati tra loro attraverso una relazione di parentela.

### 2.1 Relazioni

In matematica una relazione può essere espressa attraverso  $a \rightarrow b$  oppure  $aRb$  dove  $a$  e  $b$  sono elementi di un certo insieme ed  $R$  è una relazione.

Questo tipo di relazione tra  $a$  e  $b$  si dice **Relazione binaria** e significa che la coppia  $(a, b) \in R$ .

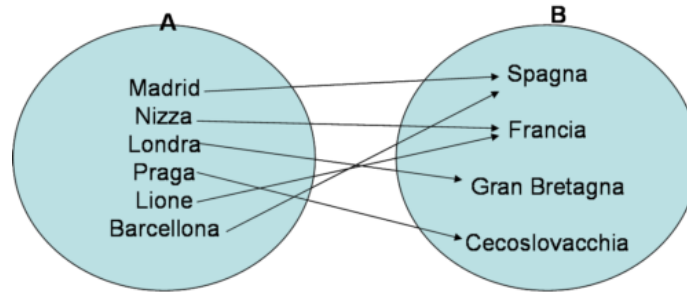


Figure 2: una relazione geografica

Altri tipi di relazioni sono:

- Relazione vuota: se  $R = \emptyset \subseteq X * Y$
- Relazione totale: se  $R = X * Y$
- Relazione diagonale: se  $X = Y$  in particolare viene definita con:  
 $\Delta := \{(x, x) \in X * X\} = \{(x_1, x_2) \in X * X : x_1 = x_2\}$

Facciamo un esempio di relazione diagonale:

Prendiamo un insieme  $X = \{1, 2, 3\}$  avremo  $\Delta = \{(1, 1), (2, 2), (3, 3)\}$  come relazione diagonale su  $X$ .

### 2.2 Funzioni

Una funzione è anch'essa una relazione tra elementi di insiemi ma questo tipo di relazione deve rispettare questa proprietà:

$$f \subseteq X * Y : \forall x \in X \quad \exists! y \in Y : (x, y) \in f \quad (27)$$

E si può denotare brevemente con:

$$f : X \rightarrow Y$$

Dove  $X$  è il detto **Dominio** e  $Y$  è detto **Codominio**.

Inoltre possiamo evitarci la scrittura  $(x, y) \in f$  scrivendo semplicemente  $y = f(x)$  dicendo che  $y$  è l'immagine di  $x$  mediante  $f$ .

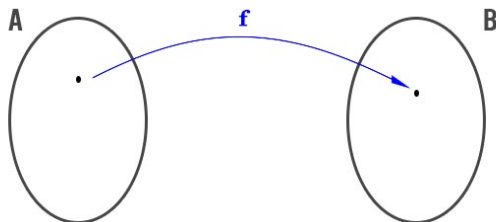


Figure 3: rappresentazione di una funzione

Facciamo un esempio di cosa è una funzione e di cosa non lo è:  
Prendiamo  $X = \{1, 2, 3\}$   $Y = \{a, b, c, d, e, f\}$  e  $\varphi, \rho \subseteq X * Y$ , ipotizziamo che:

- $\varphi = \{(1, a), (1, d), (2, e), (3, a)\}$
- $\rho = \{(1, c), (2, c), (3, a)\}$

Da questo possiamo dire con certezza che:

- $\varphi$  non è una funzione in quanto non rispetta 27 infatti troviamo che per  $x = 1$  esistono due  $y$  differenti.
- $\rho$  è una funzione in quanto rispetta 27, infatti ogni  $x$  ha un solo corrispondente  $y$ .

Aggiungo che la funzione  $\rho$  ha una  $y$  a cui corrispondono due  $x$   $((1, c), (2, c))$  questo però non viola 27 in quanto è  $x$  che deve rispettare quella proprietà non  $y$ .

## 2.3 Immagine e controimmagine

Definiamo ora cosa sono l'immagine e la controimmagine di una funzione

### 2.3.1 Immagine

L'immagine della funzione è semplicemente la funzione stessa  $y = f(x)$  scritto anche:

$$f(A) := \{y \in Y, \exists x \in A : y = f(x)\}$$

Dove  $A \subseteq X$  ovvero  $A$  sottoinsieme del dominio.

Ovvero gli elementi del **dominio**  $X$  che vengono mandati in un solo **codominio**  $Y$

### 2.3.2 Controimmagine

La controimmagine sono invece gli elementi del **codominio**  $Y$  che vengono mandati n

## 2.4 Il grafico della funzione

## 2.5 Iniettività, Surgettività e Bigettività

## 2.6 Tipi di funzioni

### 2.6.1 Funzione Identità

### 2.6.2 Funzione Parte Intera

### 2.6.3 Funzione Parte Frazionaria

### 2.6.4 Funzione Composta

## 2.7 Invertibilità

### 3 Assioma della scelta

## 4 Principio di Induzione

Il Principio di induzione detto anche procedimento induttivo è un procedimento matematico per dimostrare la validità di una tesi attraverso la verifica della veridicità di due condizioni:

- passo zero:  $(n_0)$
- passo induttivo:  $(n)$

Se lo scriviamo in matematica diciamo che se abbiamo una proposizione  $P$  e:

$$\begin{array}{ll} P(n_0) & \text{vera} \\ P(n) & \text{vera} \end{array}$$

Allora  $P(n)$  è vera.

Ne consegue quindi che anche  $P(n+1)$  è vera, potremo dire semplicemente che se:

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

Utilizziamo un esempio, dimostriamo che  $\forall n \geq 0$  la somma che denotiamo con  $S(n)$  dei primi numeri naturali:

$$S(n) = 0 + 1 + 2 + 3 + 4 + 5 + \dots + n$$

è data da:

$$S(n) = \frac{n(n+1)}{2} \quad \forall n \geq 1$$

La nostra proposizione sarà quindi:

$$P(n) : S(n) = \frac{n(n+1)}{2}$$

Il nostro compito sarà quindi quello di dimostrare che  $P(n_0)$  e  $P(n)$  è vero  $\forall n \geq 1$ .

Quindi dimostriamo  $S(n)$  con  $n = 1$ :

$$S(1) = \frac{0 * (0 + 1)}{2} = 0 \tag{28}$$

A questo punto secondo la proprietà dell'induzione anche  $P(n+1)$  sarà vera ovvero  $S(1)$ :

$$S(1) = \frac{1 * (1 + 1)}{2} = 1 \tag{29}$$

Esistono tre tipi di induzione che spiegheremo di seguito.

## 4.1 Prima forma

Il Principio di induzione prima forma dice che con  $P$  proposizione sui numeri naturali:

1.  $P(0)$  è vera.
2.  $P(n)$  è vera  $\Rightarrow P(n+1)$  vera allora  $P(n)$  vera  $\forall n \in \mathbb{N}$ .

Un esempio di ciò è 28 e 29.

## 4.2 Seconda forma

Il Principio di induzione seconda forma dice che con  $P$  proposizione sui numeri naturali e  $n_0 \in \mathbb{N}$  dove  $n_0$  è il **passo zero**, se vale:

1.  $P(n_0)$  vera.
2.  $P(n)$  vera  $\Rightarrow P(n+1)$  vera.

Allora  $P(n)$  è vera  $\forall n \geq n_0$ .

## 4.3 Terza forma

Il Principio di induzione terza forma dice che con  $P$  proposizione su  $\mathbb{Z}$  e  $n_0 \in \mathbb{Z}$  dove  $n_0$  è il **passo zero**, se vale:

1.  $P(n_0)$  vera.
2.  $P(n)$  vera  $\forall m \in \mathbb{Z} \quad n_0 \leq m < n \Rightarrow P(m)$  vera.

Allora diciamo che  $P(n)$  vera  $\forall n \geq n_0$ .



## 5 Esempio

Se considero la funzione:

$$f : \mathbb{Z}^2 \rightarrow \mathbb{Z} \quad (30)$$

$$(x, y) \rightarrow 21x - 15y \quad (31)$$

Dobbiamo dimostrare che la funzione è **iniettiva** o **surriettiva**. Prendiamo

quindi  $f(1, 1) = 21 - 15 = 6$  possiamo dire che

$f$  surriettiva  $\Leftrightarrow f(\mathbb{Z}^2) = \mathbb{Z}$  e che quindi:  $f(\mathbb{Z}^2) = n \in \mathbb{Z} : \exists (x, y) \in \mathbb{Z}^2 n = f(x, y) = 21x - 15y$

Quella che abbiamo appena scritto è una funzione **Diofantea** ovvero  $MCD(21, 15) :$   
 $n \Leftrightarrow f(\mathbb{Z}^2) = 3k : k \in \mathbb{Z}$ .

E quindi possiamo dire con certezza che la funzione non è né surriettiva e né iniettiva perchè:

$$1 \notin f(\mathbb{Z}^2)$$

Perchè fissato  $n \in 3\mathbb{Z}$

## 6 Numeri Primi

I numeri primi sono quei **numeri interi maggiori di 1 che sono divisibili solo per 1 e se stessi**, se questa proprietà non viene rispettata allora il numero è invece **composto** che scritto in matematiche:

$$a \in \mathbb{Z}, a > 1 \quad (32)$$

Dimostriamo ora un **Lemma** dei numeri primi:

$$a, b \in \mathbb{Z}, p \in \mathbb{Z} \quad \text{Primo} \quad (33)$$

$$p|a \quad \text{oppo} \quad p|a * b \quad (34)$$

Quindi supponiamo di avere  $p|a$ , dimostriamo che  $p|b \quad p|a * b \Rightarrow \exists k \in \mathbb{Z}$  tale che  $a * b = k * p$

Possiamo dimostrarlo utilizzando anche **Bezout** (DA FARE A CASA).

### 6.1 Teoria fondamentale dell'aritmetica

Ok prepariamoci a scrivere un pò di formule.

si dice che:  $a \in \mathbb{Z}, a \neq 0, 1, -1$  allora  $a$  si scrive in un modo unico come prodotto di primi:

$$a = \quad (35)$$

### 6.2 Teorema di euclide

Esistono infiniti numeri primi e lo possiamo dimostrare attraverso una dimostrazione per assurdo. Supponiamo infatti per assurdo che esistano soltanto  $p_1, \dots, p_n$  numeri primi.

Perfetto ora consideriamo un numero  $N = p_1 * \dots * p_n$ . La divisione euclidea di  $N$  per  $p_1$  da resto 1. Analogamente  $N$  diviso per  $N = p_1 * \dots * p_n$  da resto 1  $p_1 \nmid N \dots p_n \nmid N$  contraddice il teorema precedente e perciò abbiamo dimostrato che ci sono infiniti numeri primi, ok può non essere chiarissimo quindi vado ad utilizzare i numeri per fare un esempio:

$$N = 2 * 7 + 1 = 14 + 1 = 15 \quad \text{Non è primo} \\ 3|15, 5|15$$

Abbiamo infatti trovato due nuovi numeri primi 3 e 5 quindi ci sono infiniti numeri primi.

## 7 Numeri complessi

Noi definiamo numeri complessi quei numeri che

$C = RxR$  denotiamo che  $(x, y) \in R^2$  come  $x + iy$  e consideriamo  $i$  come unità immaginaria, definiamo due operazioni su  $C$

- **Somma**  $(x + iy) + (u + iv) := (x + u) + i(y + v)$  con  $x, y, u, v \in R$
- **Prodotto**  $(x + iy) * (u + iv) := (xu - yv) + i(xv + yu)$  con  $x, y, u, v \in R$

Utilizziamo un esempio numerico:

$$\text{Somma: } (2 + 3i) + (4 + 5i) = (2 + 4) + i(3 + 5) = 6 + 8i \quad (36)$$

$$\text{Prodotto: } (2 + 3i) * (4 + 5i) = (2 * 4) + i(2 * 5 + 3 * 4) = (8 - 15 + i(10 + 12)) = 7 + 22i \quad (37)$$

Anche se i calcoli possono sembrare complessi possiamo semplificare il tutto con questo ragionamento:

$$i + i = (0 * 0 - 1 * 1) + i(0 + 1 + 0 + 1) = -1 + i0 = -1 \quad (38)$$

L'inverso di  $x + iy$  rispetto al punto si denota con  $(x + iy)^{-1}$  oppure  $\frac{1}{x+iy}$

### 7.1 Piano di Gauss

Con  $C = R^2$  consideriamo un piano cartesiano possiamo rappresentare tutti i numeri complessi utilizzando però delle coordinate dette **Polari**. Da un punto  $x$  e un punto  $y$  troviamo un punto  $z$  possiamo infatti dire che  $z = x + iy$  dove il  $|z|$  rappresenta la distanza del punto  $z$  dall'origine (l'intersezione dell'asse  $x$  e  $y$ ) e lo si può calcolare attraverso **Pitagora** con  $|z| := \sqrt{x^2 + y^2}$ .

E quindi se  $z \in R$  allora  $|z| = \sqrt{x^2}$

### 7.2 Proprietà dei numeri complessi

- $\overline{zw} = z * \overline{w}$
- $\overline{\overline{z}} = z$
- $\overline{z + w} = \overline{z} + \overline{w}$
- $z + \overline{z} = 2\text{Re}(z)$
- $z - \overline{z} = 2i\text{Im}(z)$

Cercare le dimostrazioni su internet perchè oggi il prof ha deciso di fare il cosplay di Flash.

Altre proprietà però con il modulo:

- $z * \bar{z} = |z|^2$
- $|zw| = |z||w|$
- $|z + w| \leq |z| + |w|$
- $z \neq 0 \quad z^{-1} = \frac{\bar{z}}{|z|^2}$

## **CERCARE SU INTERNET DISUGUAGLIANZA TRIANGOLARE E GRAFICO CON IL MODULO**

$\theta = \arg(z)$  argomento di  $z$  angolo formato da  $z$  e l'asse  $Re$   $\theta$  è definito a meno di  $Re$  multipli di  $2\pi$

## **CERCARE SU INTERNET FORMA TRIGONOMETRICA Z**

Ok facciamo un esempio, prendiamo  $z = 2$ , avremo quindi  $|z| = \sqrt{2^2} = 2$  e  $\arg z = 0$ .

A questo punto possiamo dire che  $z = 2(\cos(0) + i \sin(0))$

## **RICORDARSI CHE Re STA PER PARTE REALE (GRAZIE GABRIEL DEL PASSATO)**

### **7.3 Forma esponenziale**

Avendo  $z \in \mathbb{C}, z \neq 0$

$\theta = \arg z$  e  $z = |z|e^{i * \arg(z)}$

$w \in \mathbb{C}, w \neq 0 := |z|(\cos(\theta) + i \sin(\theta))$

## **CERCARE FORMULA DI DE MOIURE**

### **7.4 Equazioni di secondo grado complesse**

Una radice semplice si calcola quando si hanno equazioni di grado inferiore al terzo, nello specifico ogni equazione di secondo grado  $ax^2 + bx + c = 0$  con  $a, b, c \in \mathbb{C}$  ha due soluzioni in  $\mathbb{C}$ .

Si trovano così  $\Delta := b^2 - 4ac$  dove:

- $\Delta = 0$  prendo  $\delta_1 = \delta_2 = 0$
- $\Delta \neq 0$  per il teorema  $\exists \delta_1, \delta_2 \in \mathbb{C}$  distinti, tali che  $\delta_1^2 = \delta_2^2 = \Delta$

Le soluzioni dell'equazione di secondo grado si trovano facendo:

$$z_1 = \frac{-b + \delta_1}{2a} \quad (39)$$

$$z_2 = \frac{-b + \delta_2}{2a} \quad (40)$$

Mentre:

$$\text{Se } \Delta = 0, \delta_1 = \delta_2 \quad \text{quindi } z_1 = z_2 \quad (41)$$

$$\text{Se } \Delta < 0, \delta_1 \neq \delta_2 \quad \text{quindi } z_1 \neq z_2 \quad (42)$$

## 7.5 Radici complesse

le  $Zk$  sono chiamate radici complesse che se le andassimo a disegnare sul piano di Gauss formerebbero i su

Facciamo un esempio, le radici cubiche ( $n = 3$ ) di  $z = -8 + i * 0$  del modulo di  $z$ ,  $|z| = \sqrt{Re(z^2) + Im(z^2)} = \sqrt{-8^2 + 0^2} = \sqrt{(-8^2)} = 8$ .

## 7.6 Teorema fondamentale dell'Algebra

Il teorema fondamentale dell'algebra dice che ogni polinomio in  $\mathbb{R}$  o  $\mathbb{C}$  di grado  $\geq 1$  ha soluzioni nei  $\mathbb{C}$

Ovvero sia  $p(x) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$  un polinomio,  $p(x) = a_n + a_{n-1} + \dots + a_1 + a_0 \in \mathbb{C} a_n \neq 0$  di grado  $n$

Allora  $p(x)$  ha  $n$  soluzioni in  $\mathbb{C}$  contate con la loro molteplicità.

Cioè  $p(x)$  si può decomporre come  $p(x) = a(x - w_1)^{m_1} \dots (x - w_r)^{m_r}$

(a detta del prof è troppo complesso dimostrarlo e se lo dice lui io mi fido)

## 8 Relazioni di Equivalenza

Prima di tutto definiamo un insieme  $A$ , una relazione  $R \subseteq A \times A$  si dice di equivalenza se soddisfa:

1. Riflessiva ( $\forall a \in A (a, a) \in R$ )
2. Simmetrica ( $((a, b) \in R \Rightarrow (b, a) \in R)$ )
3. Transitiva ( $((a, b) \in R, (b, c) \in R \Rightarrow (a, c) \in R)$ )

Generalmente indichiamo una relazione d'equivalenza con un simbolo  $\sim$  oppure  $\equiv$  e scriviamo  $a \sim b$  oppure  $a \equiv b$  oppure  $aRb$  per indicare  $(a, b) \in R$

### 8.1 Equivalenza modulare

Sia  $A = \mathbb{Z}$  fissiamo  $n \in \mathbb{Z}, n \geq 1$  definiamo  $\sim_n$

$x \sim_n y \Leftrightarrow \exists k \in \mathbb{Z}$  tale che  $x - y = Kn$  si dice che  $x$  è congruo a  $y$  modulo  $n$  e si scrive  $x \equiv y \text{ MOD } n$ .

$\forall x \in \mathbb{Z}$  vale  $x \equiv x \text{ mod } n$  perchè  $\exists K \in \mathbb{Z}$  tale che  $x - x = K * n$

### 8.2 Classe di equivalenza

Sia  $A$  un insieme e sia  $\sim$  una relazione di equivalenza su  $A$ . La classe di equivalenza di un elemento  $a \in A$  con  $\bar{a} = [a] := \{b \in A : b \sim a\}$  è un insieme.

$a$  si chiama rappresentante della classe  $[a]$  e notare bene che  $a \in [a]$  perchè  $a \sim a$ .

## 9 Cardinalità

Con **cardinalità** noi intendiamo definire quali e quanti elementi fanno parte di un certo insieme utilizzando il linguaggio matematico.

Supponiamo per esempio che  $A, B$  sono insiemi, possiamo dire che  $A, B$  sono **equipotenti** se  $\exists f : A \rightarrow B$  bigettiva, in tal caso scriviamo  $|A| = |B|$ .

Ok detto questo mostriamo alcune proprietà:

1. **Riflessiva**  $A$  è equipotente con  $A$  tramite  $id_A A \rightarrow A$  bigettiva.
2. **Simmetrica**  $A$  è equipotente a  $B \Rightarrow \exists f : A \rightarrow B$  bigettiva.
3. **Transitiva**  $A$  equipotente a  $B$ ,  $B$  equipotente a  $C$ .

Con  $X$  insieme diciamo che:

- $X$  è finito se  $X = \emptyset$  oppure  $\exists n \in \mathbb{N}$  tale che  $X$  è equivalente a  $\{1, 2, 3, 4, n\}$  e in tal caso diciamo che  $X$  ha cardinalità  $n$  scrivendo  $|X| = n$ .
- $X$  è **infinito** se  $X$  non è finito (ovviamente), si dice che  $X$  insieme è  $= \emptyset$  allora sono equivalenti e si dice anche che:
  1.  $X$  è infinito
  2.  $\exists Y \subsetneq X$  tale che  $|Y| = |X|$ .
  3.  $\exists f : X \rightarrow X$  iniettiva, ma non suriettiva.

$X$  si dice **numerabile** (o di cardinalità numerabile) se  $|X| = |\mathbb{N}|$  e scriviamo  $|X| = \aleph_0$  e lo si chiama **Aleph Zero**.

Se  $X$  è numerabile  $\Rightarrow X$  infinito.

$f \circ s \circ f^{-1} X \rightarrow X$  iniettiva, ma non suriettiva.

Esempio proviamo a vedere se  $\mathbb{Z}$  che contiene  $\mathbb{N}$ .

$$f : \mathbb{N} \rightarrow \mathbb{Z} \tag{43}$$

ok ora vediamo che:

$$f(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari} \\ \frac{n+1}{2} & \text{se } n \text{ è dispari} \end{cases}$$

se invece  $f$  è bigettiva, l'inversa è  $f^{-1} : \mathbb{Z} \rightarrow \mathbb{N}$

$\mathbb{N} \times \mathbb{N}$  è numerabile dimostriamo che  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ .

**AGGIUNGERE ESEMPLI.**

Definiamo  $A, B$  insiemi e scriviamo:

**Altra parte di lezione mancante**

## 9.1 Teorema di Cantor-Bernstein

$A, B$  insiemi,  $\exists f : A \rightarrow B$  iniettiva,  $g : B \rightarrow A$  iniettiva, allora esiste una funzione  $h : A \rightarrow B$  bigettiva.

In formule questo ci dice che se:

$$|A| \leq |B| \quad |B| \leq |A| \Rightarrow |A| = |B| \quad (44)$$

Se  $A, B$  finiti,  $|A| = n$ ,  $|B| = m$   $n, m \in \mathbb{N}$  allora:

$$n = m : \begin{cases} |A| \leq |B| \Rightarrow n \leq m \\ |B| \leq |A| \Rightarrow m \leq n \end{cases}$$

Definiamo  $X$  insieme, diciamo che:

- $X$  è al più numerabile se  $|X| \leq |\mathbb{N}|$
- $X$  è più che numerabile se  $|X| > |\mathbb{N}|$

**PROBABILMENTE C'È TROPPIA ROBA CHE NON HO SCRITTO**

## 9.2 Impossibilità della surriettività dei numerabili

Prendiamo la proposizione che prende  $X$  insieme con  $X \neq \emptyset$  allora non esiste alcuna mappa surriettiva  $X \rightarrow P(x)$

In particolare questo ci dice che  $|X| \neq |P(x)|$  e quindi  $X$  e  $P(x)$  non sono equipotenti.

Bene proviamo a dimostrare quello che abbiamo appena detto per assurdo, supponiamo infatti per assurdo che  $\exists f : X \rightarrow P(x)$  surriettiva e prendiamo un insieme  $S = \{x \in X : x \notin f(x)\}$ .

Abbiamo che:

- $S \subseteq X$ , Eventualmente  $S$  può essere  $\emptyset$ .
- $S \in P(x)$  ed essendo  $f$  surgettiva  $\exists s \in X$  tale che  $f(s) = S$

Quindi la domanda è  $s \in S$  o  $s \notin S$ , andiamo a trovare la contraddizione:

1. Se  $s \in S$  allora  $s \notin f(s) = S$  che è una **CONTRADDIZIONE**.
2. Se  $s \notin S$  allora  $s \in f(s) = S$  che è anch'essa una **CONTRADDIZIONE**.

Da tutto questo osserviamo che  $X \neq \emptyset \exists f : X \rightarrow P(x)$  iniettiva e cioè  $f(x) = x$  (il singoletto composto da  $x$ ) e ciò implica che  $\Rightarrow |X| \leq |P(x)|$ .

La proposizione precedente ci dice che  $|X| < |P(x)|$  ad esempio per  $X = \mathbb{N}$  si ha:

$|P(\mathbb{N})| > |\mathbb{N}| = \aleph_0$  dove  $P(\mathbb{N})$  è più che numerabile.



### 9.3 Argomento che il prof si tiene segreto

Definiamo  $A, B$  insiemi.

$$B^A := f : A \rightarrow B \text{ funzione} \quad (45)$$

E nel caso in cui  $B = 0, 1$  si usa indicare  $0, 1^A$  con  $2^A$ .

Vogliamo  $X$  insieme dove  $X \neq \emptyset$  allora  $P(x)$  è equipotente a  $0, 1^x$ .  
 $|P(x)| = |0, 1^x|$ .

Dimostriamo (quello che ho scritto senza sapere cosa stavo scrivendo) con:

$$\begin{aligned} \phi : 0, 1^x &\rightarrow P(x) \\ f &\mapsto f(1)^{-1} = \{x \in X : f(x) = 1\} \subseteq X \end{aligned}$$

Iniziamo con le dimostrazioni:  $\phi$  surriettiva sia  $A \in P(x), A \subseteq X$  sottoinsieme e considero  $X_A : X \rightarrow 0, 1$ .

$$x \mapsto \begin{cases} 1 & \text{se } x \in A \\ 0 & \text{se } x \notin A \end{cases}$$

$$\begin{aligned} X_A &\in 0, 1^X \\ \varphi(X_A) &= X_A - 1(1) = \{x \in X : X_A(x) = 1\} = \{x \in X : x \in A\} = A. \end{aligned}$$

Ora che non so che cazzo ho scritto prendiamo  $\phi$  iniettiva e  $f, g \in 0, 1^x, f \neq g$   
 tesi  $\phi(f) \neq \phi(g)$ .  $f, g : X \rightarrow 0, 1$   
 $f \neq g \Rightarrow \exists x \in X$  tale che  $f(x) \neq g(x)$ . Supponiamo che  $f(x) = 1 \Rightarrow g(x) = 0$   
 $\Rightarrow x \in f - 1 = \varphi(f)x \notin g - 1(1) = \varphi(g) \Rightarrow \varphi(f) \neq \varphi(g)$

**MA CHE CAZZO HO APPENA SCRITTO**

Prendiamo il lemma  $A = a_1, \dots, a_n$  insieme finito,  $B$  insieme finito,  $|B^A| = |B^n|$  che (a quanto dice il prof) è facilmente dimostrabile:

$$\begin{aligned} \varphi : B^A &\rightarrow B^n = Bx, \dots, xB \\ f &\mapsto (f(a_1), \dots, f(a_n)) \end{aligned}$$

Corollario  $A, B$  insiemi finiti, allora  $AxB, B^A, P(A)$  sono insiemi finiti di cardinalità:

- $|A * B| = |A| * |B|$
- $|B^A| = |B|^{|A|}$
- $P(A) = |0, 1^A| = |\{0, 1\}|^{|A|} = 2^{|A|}$

## 9.4 Cardinalità dei $\mathbb{Q}$

Prima di tutto diciamo che  $\mathbb{Q}$  è numerabile, e lo possiamo dimostrare con:

$$\begin{aligned} \varphi : \mathbb{Q} \setminus \{0\} &\rightarrow \mathbb{N}^* \\ \frac{p}{q} &\mapsto |p| + |q| \end{aligned}$$

Avendo  $p, q \in \mathbb{Z}, p, q \neq 0, MCD(p, q) = 1$  e quindi,  $Q = 0 \cup \bigcup_{n \in \mathbb{N}} \varphi^{-1}(n)$ .

Si dice quindi che unione numerabile di insiemi finiti  $\neq \emptyset$  e disgiunti  $\Rightarrow Q$  numerabile.

### Cercare la diagonale di Cantor

Lemma prendiamo  $\{X_m : m \in \mathbb{N}\}, |X_n| \leq \aleph_0, X_m \neq \emptyset \forall n \in \mathbb{N}$  se  $|X_m| < \aleph_0 \forall n \in \mathbb{N}$  allora  $X_n \cap X_m = \emptyset$  se  $n \neq m$  allora  $|\bigcup_{n \in \mathbb{N}} X_n| = \aleph_0$

## 9.5 Cardinalità di $\mathbb{R}$

$\mathbb{R}$  è equipotente a  $P(\mathbb{N})$ , in particolare è più che numerabile.

$$\begin{array}{ll} \text{Cardinalità} & 0, 1, 2, \dots, n, \dots, \aleph_0 \\ \text{Insiemi} & \emptyset, *, 1, 2, \dots, 1, \dots, n, \dots, \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \dots \end{array}$$

## 9.6 Ipotesi del continuo

Questa ipotesi, formulata da Cantor chiede se  $\exists A$  insieme tale che  $\aleph_0 < |A| < 2^{\aleph_0}$ ??

*BTW questi problemi non verranno trattati nel corso ma sono good to know.*

## 10 Calcolo Combinatorio

Iniziamo con una definizione, se abbiamo  $X$  insieme infinito,

ovvero:  $\{X \rightarrow X \text{ Bigettiva}\}$  è l'insieme delle permutazioni di  $X$ , nel caso in cui  $X = \{1, \dots, n\}$ , l'insieme è detto **Insieme delle permutazioni** si denota con:

$$S_n = \{\{1, \dots, n\} \rightarrow \{1, \dots, n\} \text{ Bigettiva}\}.$$

E con il *lemma*  $X, Y$  insiemi finiti,  $|X| = n \leq m = |Y|$  Il numero delle applicazioni iniettive  $X \rightarrow Y$  è uguale:

$$m * (m - 1) * \dots * (m - n + 1)$$

Osserviamo che se  $n > m$ ,  $\nexists X \rightarrow Y$  iniettiva, facilmente dimostrabile con  $|X| = n \Rightarrow X = \{x_1, x_2, \dots, x_n\}$ .

Possiamo vedere in quanti modi possiamo definire  $f : X \rightarrow Y$  iniettiva. Prendiamo  $X = \{x_1, \dots, x_n\} \rightarrow Y = \{y_1, \dots, y_n\}$ :

- $x_1 \mapsto ?$  ho  $m$  possibili scelte.
- $x_2 \mapsto ?$  ho  $m - 1$  possibili scelte.
- $x_3 \mapsto ?$  ho  $m - 2$  possibili scelte.
- $x_n \mapsto ?$  ho  $m - (n - 1)$  possibili scelte.

In tutto quindi avremo  $m(m - 1), \dots, (m - n + 1)$  possibili funzioni  $X \rightarrow Y$  iniettive  $\square$ .

Corollario  $|X| = |Y| = n$  ci sono  $n(n - 1), \dots, (n - n + 1) = n(n - 1), \dots, (2)$  funzioni bigettive da  $X$  a  $Y$ .

Definiamo  $n \in \mathbb{N}$ , il fattoriale di  $n$ :

$$n! = \begin{cases} n * (n - 1) * \dots * 2 * 1 & \text{se } n > 0 \\ 1 & \text{se } n = 0 \end{cases}$$

Un altro corollario,  $|S_n| = n!$  che definiamo con:

$$n, k \in \mathbb{N}, n \geq 1, 0 \leq k \leq n, \quad \text{il coefficiente binomiale}$$

$$(nk) := \frac{n!}{k!(n - k)!}$$

### 10.1 Mi inventerò un titolo

$X$  insieme finito,  $|X| = n$  per ogni intero  $0 \leq k \leq n$  il numero di sottoinsiemi di  $X$  con  $k$  elementi è  $(nsuk)$ .

Dimostrimolo:

- $k = 0$ , c'è solo un insieme con 0 elementi:  $\emptyset$
- $k = n$ , c'è solo un insieme con  $n$  elementi:  $(nsun) = (nsu0) = 1$

Ora proviamo a costruire un  $Y \subseteq X$  con  $\#Y = k$  e  $0 < k < n$

- Scegliamo il 1° elemento di  $y:n$  possibilità
- Scegliamo il 2° elemento di  $y:n - (k - 1)$  possibilità

Devo dividere per il numero di permutazioni di una stringa con  $k$  elementi:

$$\frac{n(n-1)\dots(n-k+1)}{k!} = (nsk) \square$$

Lemma  $(nsk) = (n-1sk) + (n-k-1)$

## 10.2 Coefficiente binomiale

Il coefficiente binomiale è  $x, y \in \mathbb{C}, n \in \mathbb{N}^*$  allora:

$$(x+y)^n = \sum_{k=0}^n (nsk) x^{n-k} y^k$$

Dimostriamolo attraverso l'induzione:

**CHE SEGUIRÒ E POI SCRIVERÒ IN FUTURO QUANDO RIFINISCO GLI APPUNTI VERO GABRIEL???**

Corollario  $X$  insieme finito,  $|X| = n$  allora  $|P(x)| = 2^n$  dimostrabile  $\forall 0 \leq k \leq n$  il numero di sottoinsiemi di  $k$  elementi di  $X$  è  $(n \text{ su } k)$ .

Il numero di sottoinsiemi di  $X$  è:

$$\sum_{k=0}^n (nsk) = 2^n$$

## 11 Relazioni d'ordine

Le relazioni d'ordine sono un tipo di relazione che hanno come modello la disuguaglianza per esempio tra insiemi di diverso tipo oppure oggetti che non necessariamente sono numeri.

Se vogliamo dare una definizione più precisa possiamo dire che se  $X$  insieme,  $R \subseteq X * X$  relazione  $R$  è un preordine se:

- Riflessiva:  $\forall x \in X \quad (x, x) \in R$
- Transitiva:  $(x, y) \in R \quad (y, z) \in R \Rightarrow (x, z) \in R$
- Antisimmetrica:  $((x, y) \in R) \wedge ((y, x) \in R) \Rightarrow x = y$

si dice che  $R$  è un ordine parziale.

In questo caso  $X$  si dice parzialmente ordinato (POSET)

Scriviamo  $(x, y) \in R$  come  $x \triangle y$  oppure  $x \leq y$  ( $x, \triangle$ ) dove  $x$  è un insieme e  $\triangle$  è un **ordine parziale** su  $X$

Definiamo meglio  $(x, \triangle)$  *POSET*  $x, y \in X$ , si dicono confrontabili se vale  $(x \triangle y) \vee (y \triangle x)$ , altrimenti si dicono non confrontabili se tutti gli elementi di  $X$  sono confrontabili,  $\triangle$  si dice ordine totale.

### 11.1 Esempi di relazioni d'ordine

Prendiamo come adesso alcuni esempi:

$\mathbb{R}, \leq$  è totalmente ordinato ( $\leq$  è un ordine totale su  $\mathbb{R}$ ) 1.:

- $x \leq x \forall x \in \mathbb{R}$  Riflessiva
- $x \leq y, y \leq z \Rightarrow x \leq z$  Transitiva
- $x \leq y, y \leq x \Rightarrow x = y$  Antisimmetrica

è totale perchè dati  $x$

2.  $<$  minore stretto non è un ordine parziale su  $\mathbb{R}$  non soddisfa la riflessiva

3.  $\triangle = \{(x, y) \in X : x = y\}$  ordine parziale.

4.  $\mathbb{C} z \triangle w \Leftrightarrow |z| \leq |w|$  dove  $z, w \in \mathbb{C}$  è un preordine ma, ma non un ordine parziale perchè:

- Riflessiva  $z \triangle z$  si perchè  $|z| \leq |z|$
- Transitiva  $x \triangle y, y \triangle z \Rightarrow x \triangle z$  si perchè  $|x| \leq |y|$
- Antisimmetrico no perchè prendiamo per esempio  
 $x = i, |i| = 1 \leq 1 = |1| \quad i \triangle 1$  ma  $i \neq 1$   
 $y = 1 \quad |1| = 1 \leq 1 = |i| \quad 1 \triangle i$

5.  $X$  insieme,  $X \neq \emptyset$ , definiamo una relazione d'ordine su  $P(x)A, B \in P(x)$   $A \triangle B \Leftrightarrow A \subseteq B$   
 In particolare  $(P(x), \subseteq)$  è un POSET:

- $A \subseteq A$
- $A \subseteq B, B \subseteq C \Rightarrow A \subseteq C$
- $A \subseteq B, A \subseteq B \Rightarrow A = B$

$\subseteq$  non è totale, esempio  $X = \{1, 2, 5\}, A = \{1, 2\}, B = \{2, 3\}$  e se  $X \neq \{*\}$

## 11.2 Tipi di ordini

Definiamo  $(A_1, \triangle_1), \dots, (A_n, \triangle_n)$  *POSET* definimo ordini parziali su  $A_1x, \dots, xA_n$ .

### 11.2.1 Ordine lessicografico (LEX)

Ordine lessicografico (LEX):

$$(a_1, a_2, \dots, a_n) \triangle_{lex} (b_1, b_2, \dots, b_n) \Leftrightarrow \begin{cases} a_1 \triangle_1 b_1 & \text{se } a_1 \neq b_1 \\ a_{k+1} \triangle_{k+1} b_{k+1} & \text{se } a_j = b_j \forall j = 1, \dots, k \end{cases}$$

### 11.2.2 Ordine prodotto

Ordine prodotto  $\triangle_1x, \dots, \triangle_n$ :

$$(a_1, \dots, a_n) \triangle_1x, \dots, x\triangle_n (b_1, \dots, b_n) \Leftrightarrow a_i \triangle_i b_i \forall i = 1, \dots, n$$

Facciamo un esempio numerico, prendiamo  $(\mathbb{R}, \leq)$  consideriamo  $\mathbb{R}^2, \mathbb{R} * \mathbb{R}$ , possiamo dire che:

$$(1, 0) \text{ e } (0, 1) \text{ non sono confrontabili con } \leq x \leq$$

Mentre utilizzando il **LEX** possiamo facilmente dire che:

$$(1, 0) \geq_{LEX} (0, 1)$$

Facciamo un altro esempio, prendiamo  $(2, 3) \leq x \leq (2, 5)$  perchè  $2 \leq 2$  e  $3 \leq 5$ .

Facciamo un ultimo esempio, prendiamo  $(2, 3) \leq_{LEX} x \leq (2, 5)$  perchè  $2 = 2$  e  $3 \leq 5$ .

Se tutti i *POSET* sono totalmente ordinati allora anche l'ordine *LEX* è totalmente ordinato, scriviamo quindi:

$$(A_1, \triangle_1), \dots, (A_n, \triangle_n) \Rightarrow (A_1x, \dots, xA_n, \triangle_{LEX})$$

Esempio:

$$(\mathbb{R}^2, \leq_{LEX}) \text{ TOTALMENTE ORDINATO } (\mathbb{R}^2, \leq x \leq) \text{ non è competamente ordintato.}$$

### 11.2.3 Ordine indotto

Diciamo ordine indotto  $(X, \Delta)$  *POSET*,  $Y \subseteq X$  con:

$$y_1 \Delta y, y_2 \Leftrightarrow y_1 \Delta y_2 \quad \forall y_1, y_2 \in Y \subseteq X$$

Diciamo che  $Y$  è una catena se  $(Y, \Delta y)$  è totalmente ordinato.

Esempio prendiamo  $(\mathbb{N}^*, I)$  *POSET* non è totalmente ordinato perchè se prendiamo 2 e 3 **non sono confrontabili**.

**Aggiungere l'esempio (MIN 0:40)**

### 11.3 Minimo e massimo

Definiamo con  $(X, \Delta), Y \subseteq X, Y \neq \emptyset$ :

- $y$  è minimo di  $Y$  se  $\forall x \in Y$  vale  $y \Delta x$  scriviamo  $y = \min Y$
- $y$  è massimo di  $Y$  se  $\forall x \in Y$  vale  $x \Delta y$  scriviamo  $y = \max Y$
- $y$  è elemento minimale di  $Y$  se  $\forall x \in Y$  vale  $(x \Delta y \Rightarrow x = y)$
- $y$  è elemento massimale di  $Y$  se  $\forall x \in Y$  vale  $(y \Delta x \Rightarrow x = y)$

Ad esempio se prendiamo come *POSET*  $(\mathbb{N}, \leq), Y = \mathbb{N}$  possiamo dire che:

- $Y$  ha un minimo, 0, che è anche elemento minimale.
- $Y$  non ha un massimo, e non ci sono elementi massimali.

*Osserviamo che se esistono massimo e minimo, sono unici:*

- Se il minimo esiste, ogni elemento minimale coincide con il minimo.
- Se il massimo esiste, ogni elemento massimale coincide con il massimo.
- Se  $\Delta$  è totale, esiste un elemento minimale  $\Leftrightarrow$  esiste il minimo.
- Se  $\Delta$  è totale, esiste un elemento massimale  $\Leftrightarrow$  esiste il massimo.

Un ottimo metodo per trovare i minimali e i massimali è il **Diagramma di Hasse**.