Appunti molto belli di Algebra

Floppy Loppy

September 2021

Contents

Todo list

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:

$$x \in A \tag{1}$$

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):

$$x \notin A \tag{2}$$

Se un insieme ha più di un elemento, che possono essere $\{x1,x2,\ldots,x_n\}$ allora possiamo sintetizzare la scrittura del fatto che ognuno di questi elementi appartiene all'insieme A scrivendo:

$$x = \{x1, x2, \ldots, x_n\} \tag{3}$$

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

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

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 scriviendo:

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

In questo caso possiamo dire che:

$$2 \in A$$
$$3 \notin A$$
$$Alessio \notin A$$

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:

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

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:

$$\{*\} \tag{7}$$

Dove * rappresenta il singolo elemento.

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

$$\emptyset \tag{8}$$

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** fittizzie che chiamiamo P e D e partendo da questi andiamo a scrivere le operazioi che si possono effettuare su di essi:

- La **Disgiunzione** scritta: $P \vee D$ ha valore vero quando almeno una delle due proposizione 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 propsizione, 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:

$$P : \forall x \in A \tag{9}$$

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

Mentre scriviamo:

$$P : \exists x \in A \tag{10}$$

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:

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

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

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

$$\exists! x \in A \tag{13}$$

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:

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

$$\exists y \forall x P : \exists y \forall x \quad x + y = 0 \tag{15}$$

La proposizione dice che esiste un numero che è opposto di ogni numero (perchè 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 proposizone 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 potremo 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 fittizzi A e B.

Si dice che A è contenuto in B se:

$$\{\forall x \in A : x \in B\} \tag{16}$$

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

$$A \subseteq B \tag{17}$$

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

Poi abbiamo A uguale a B se:

$$x \in A \Leftrightarrow x \in B \tag{18}$$

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

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

$$A \cup B \tag{19}$$

che sta a significare che ogni elemento di A appartene anche a B, scritto in matematichese:

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

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

$$A \cap B \tag{21}$$

e significa:

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

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

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

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:

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

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:

$$\mathcal{P}\{\emptyset\} = \{\emptyset\} \tag{25}$$

1.9 Proprietà degli insiemi

Ora mostriamo alcune proprietà degli insiemi per poi successivamente dimostrarli:

1. $A \cup B = B \cup A$
2. $(A \cup B) = A \cup (B \cup C)$
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 esautivamente al capitolo 6

Per fare un breve riassunto degli insiemi numerici:

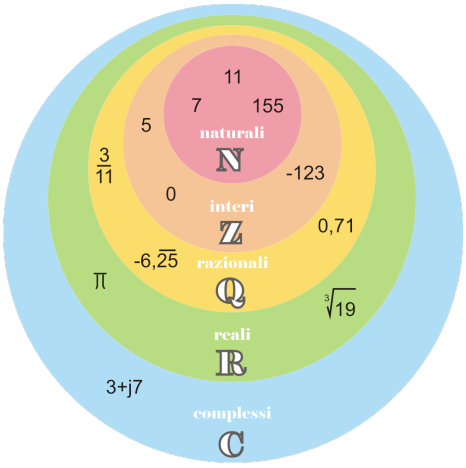

Figure 1: Insiemi numerici

1.11 Insiemi Indiciati

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

Scriviamo un insieme indicato come:

$$\mathcal{F} = \{A_i\}_{i \in I} \tag{26}$$

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 indiciati che contiene:

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

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

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

1.12 Insiemi Indiciati

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 indiciati 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 $a \to b$ 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 $(a, b) \in R$.

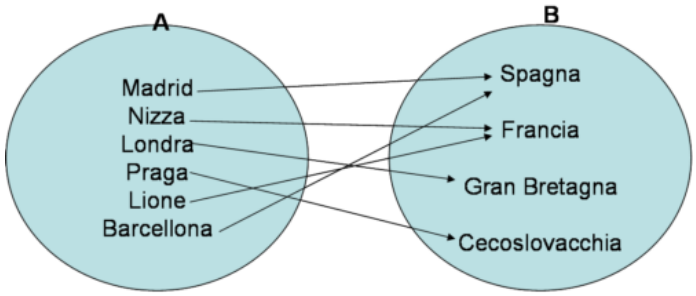

Figure 2: una relazione geografica

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 prorpietà:

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

E si può denotare brevemente con:

$$f : X \to Y$$

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.

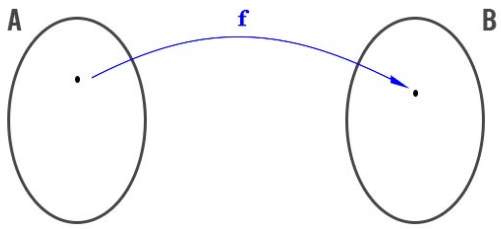

Figure 3: rappresentazione di una funzione

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 $\varphi, \rho \subseteq X * Y$, ipotiziamo che:

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

Da questo possiamo di con certezza che:

- φ non è una funzione in quanto non rispetta 27 infatti troviamo che per $x = 1$ esistono due y differenti.
- ρ è una funzione in quanto rispetta 27, infatti ogni x ha un solo corrispettivo y.

Aggiungo che la funzione ρ 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.

2.3.2 Controimmagine

La controimmagine sono invece gli elementi del **codominio** Y che vengono mandati nel **dominio** X.

Scritto in *matematichese*:

$$f^{-1}(B) = \{x \in X : f(x) \in B\}$$

Prendiamo come esempio un insieme $X = \{1, 2, 3\}$ e un insieme $Y = \{a, b, c, d, e, f\}$ e una funzione che dice:

$$\begin{aligned} \varphi : X &\to Y \\ 1 &\mapsto c \\ 2 &\mapsto c \\ 3 &\mapsto a \end{aligned}$$

E prendiamo tre insiemi che sono *singoletti* 7, $B = \{a\} \quad E = \{c\} \quad F = \{d\}$, avremo che:

- $B = \{a\} \Rightarrow f^{-1}(B) = 3$ in quanto $a \in Y$.
- $E = \{c\} \Rightarrow f^{-1}(E) = 1, 2$ in quanto $c \in Y$.
- $F = \{d\} \Rightarrow f^{-1}(F) = \emptyset$ in quanto $d \notin Y$.

2.4 Iniettività, Surgettività e Bigettività

Una funzione può essere **iniettiva, surriettiva e bigettiva**, ora spieghiamo cosa significa:

- Iniettiva: quando $\forall x_1, x_2 \in X \quad$ per cui $\quad f(x_1) = f(x_2) \Rightarrow x_1 = x_2$.
- Surriettiva: quando $\forall y \in Y \exists x \in X : f(x) = y$.
- Bigettiva: quando la funzione è sia iniettiva che surriettiva.

2.5 Il grafico della funzione

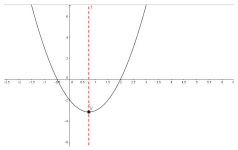

Figure 4: Esempio grafico di una parabola

Il grafico di una funzione f è semplicemente la rappresentazione grafica di una funzione come può essere ad esempio la funzione della parabola.

Noi dicamo che il grafico di una funzione è:

$$\lceil f : \{(x, f(x)) : x \in X\}$$

2.6 Tipi di funzione

Esistono diversi tipi di funzione, di seguite ne mostrerò alcuni tipi.

2.6.1 Funzione Identità

La funzione **Identità (o funzione identica)**, è una funzione che associa ad ogni valore di x se stessa

Per esempio $y = x$ o $y = x + 0$ sono funzioni identità.
Noi scriviamo la funzione identità come:

$$Id_x : X \to X$$
$$x \mapsto x$$

Facciamo un esempio di funzione identità, prendiamo:

$$Id_{\mathbb{N}} : \mathbb{N} \to \mathbb{N}$$
$$n \mapsto n$$

Se prendiamo per esempio $1 \in \mathbb{N}$ avremo $Id(1) = 1$

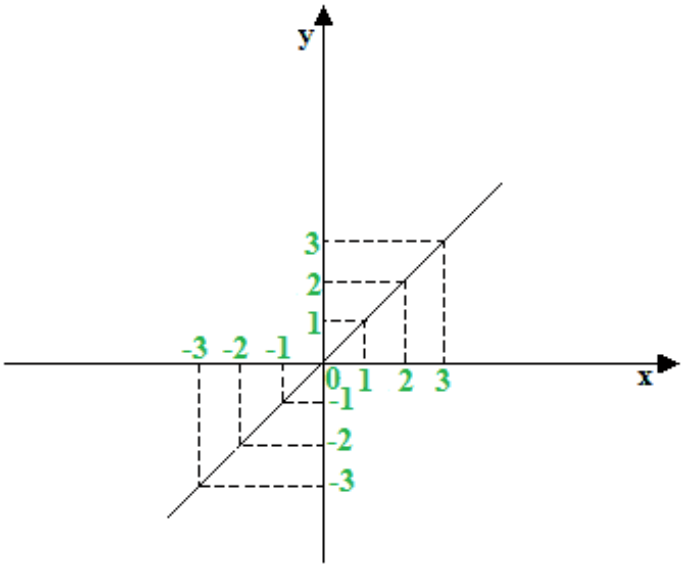

Figure 5: La bisettrice del 1 e 3 quadrante è una funzione identità

La funzione identità è **sempre bigettiva**.

2.6.2 Funzione Parte Intera

La **funzione parte intera (o funzione floor)** è una funzione che si indica con $\lfloor x \rfloor$ che associa ad ogni numero $\mathbb{Z}$ il numero stesso e ad un numero decimale, l'intero precedente.

In matematichese questo si definisce come:

$$\forall x \in \mathbb{R} \forall n \in \mathbb{Z} \quad n \leq n \Rightarrow n \leq P(x)$$

Dove $P(x)$ è il più grande intero $\leq x$.

Facciamo qualche esempio:

- $P(\frac{3}{2}) = 1$ perchè $\frac{3}{2} = 1,5$ dove 1 è la parte intera.
- $P(-\frac{1}{2}) = -1$ perchè $-\frac{1}{2} = -0,5$ dove in questo caso è -1 l'intero più vicino.

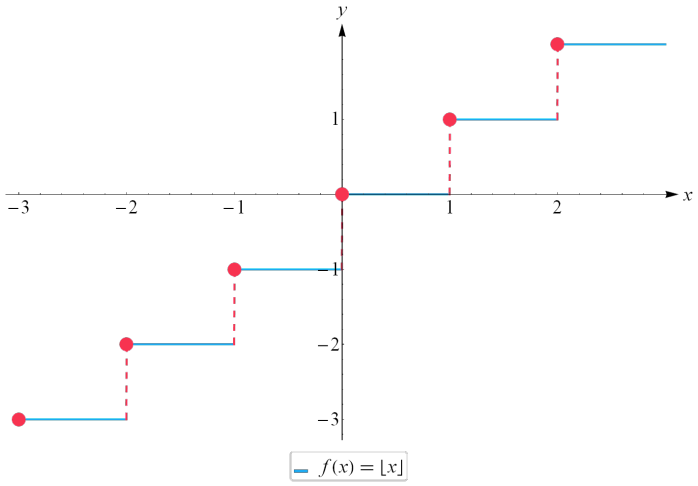

Figure 6: Esempio di funzione parte intera

2.6.3 Funzione Parte Frazionaria

La **funzione parte frazionaria** detta anche **Mantissa** è una funzione che associa ad ogni numero $\mathbb{Z}$ 0, ad un numero decimale positivo la sua parte decimale e ad un numero decimale negativo la sua controparte decimale complementare. La **Mantissa** si denota con:

$$M(x) \quad mant(x) \quad \{x\} \quad frac(x)$$

E in matematichese significa che:

$$M(x) = x - \lfloor x \rfloor \quad \forall x \in \mathbb{R}$$

Facciamo qualche esempio:

- $M(1) = 0$ alla parte intera viene assegnato 0
- $M(1,32) = 0,32$ alla parte intera viene assegnato 0 rimane la parte decimale positiva.
- $M(-0,43) = -0,43 + 1 = 0,57$ si trova il complementare che in questo caso rimane decimale.

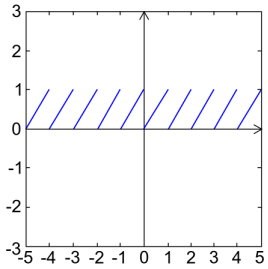

Figure 7: Rappresentazione grafica di una funzione parte frazionaria

2.6.4 Funzione Composta

Una funzione **composta** è una funzione che si ottiene tramite due funzioni g e f e applicando all'immagine della prima funzione la seconda funzione, scritto in formula:

$$g \circ f$$
$$oppure$$
$$g(f)$$

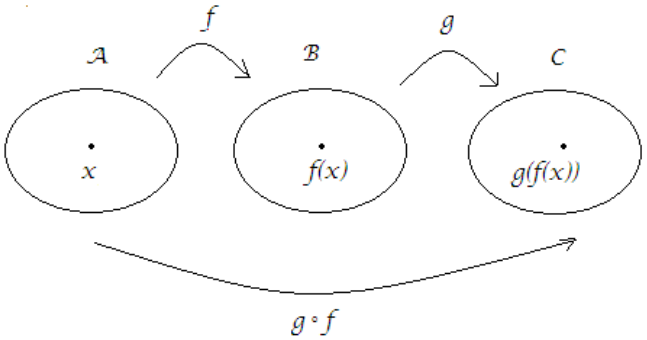

Figure 8: Rappresentazione di una funzione composta

In parole povere noi associamo al dominio X della funzione g il codominio Y della funzione f.

Esempio 2.1. *Prendiamo* $g(x) = x + 2$ *e* $f(x) = 10x + 1$*, noi avremo che:*

$$g \circ f = (10x + 1) + 2$$

Di seguido elencherò alcune proprietà della funzione composta:

- La funzione composta è associativa $h \circ (g \circ f) = (h \circ g) \circ f$.
- Se f, g sono iniettive $\Rightarrow$ $f \circ g$ iniettiva.
- Se f, g sono surriettive $\Rightarrow$ $f \circ g$ surriettiva.
- Se f, g sono bigettive $\Rightarrow$ $f \circ g$ bigettiva.

2.7 Invertibilità di una funzione

Definizione 2.1. Una funzione si dice **invertibile** quando da un $f : X \to Y$ è possibile avere la funzione $f^{-1} : Y \to X$

Una funzione può essere invertibile a **destra, sinistra, o in entrambi i lati (invertibile e basta)**, ora andremo a vedere come.

2.7.1 Invertibile a sinistra

Definizione 2.2. Una funzione f è invertibile a **sinistra** quando:

$$\exists g : Y \to X, g \circ f = Id_x$$

E si dice che g è l'inversa sinistra di f.

2.7.2 Invertibile a destra

Definizione 2.3. Una funzione f è invertibile a **destra** quando:

$$\exists h : Y \to X, f \circ h = Id_y$$

E si dice che h è l'inversa destra di f.

2.7.3 Invertibile a destra e sinistra

Definizione 2.4. Una funzione f è invertibile a **destra e sinistra** quando:

$$\exists t : Y \to X, t \circ f = Id_x \wedge f \circ t = Id_y$$

E si dice che t è l'inversa di f e si denota con f^{-1}.

2.7.4 Teorema dell'invertibilità

Teorema 2.1. *Se $f : X \to Y$ funzione allora:*

$$f \quad \text{è iniettiva} \quad \Leftrightarrow \quad f \quad \text{è invertibile a sinistra}$$

Proof. $\leftarrow$ assiumiamo che $\exists g : Y \to X \quad g \circ f = Id_x$
Per essere iniettiva $x_1 = x_2$ ma quindi possiamo dire che $g(f(x_1)) = g(f(x_2))$
Ma ciò significa fare $Id_x(x_1) = Id_x(x_2)$ che è come dire $x_1 = x_2$. □

Proof. $\rightarrow$ assiumiamo che f sia iniettiva
Costruiamo quindi un $g : Y \to X$ un'inversa sinistra di f e prendiamo un elemento $x_0 \in X$ e andiamo a definire un $g(y)$ tale che:

$$g(y) \begin{cases} x & \text{se} \quad y \in f(x) \Rightarrow \exists! x \in X \quad f(x) = y \\ x_0 & (se) y \notin f(x) \end{cases}$$

□

2.8 Assioma della scelta

Definizione 2.5. Sia $\{A_i\}_{i \in I}$ una famiglia di insiemi dove $A_1 \neq \emptyset$ allora:

$$\psi : I \to \bigcup_{i \in I} A_i \quad : \quad \varphi(i) \in A_i$$

φ viene detta **funzione di scelta**.

Esempio 2.2. *Se vogliamo un esempio per analogia immaginiamo i cassetti come una famiglia di insiemi, abbiamo:*

- *un cassetto* $A_1 = \{calzini\}$
- *un cassetto* $A_2 = \{pantaloni\}$
- *un cassetto* $A_3 = \{maglietta\}$

L'assioma della scelta dice che attraverso questi insiemi tu puoi vestirti, ovvero esiste un modo per scegliere un elemento per ognuno di questi insiemi per creare un nuovo insieme contenente **i rappresentanti** (calzini, pantaloni, maglietta) degli elementi degli insiemi scelti.

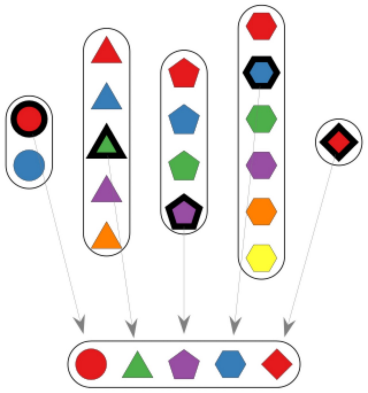

Figure 9: Esempio grafico dell'assioma della scelta

Come possiamo vedere nella figura 9 da 5 insiemi prendiamo un elemento rappresentante a scelta e andiamo a formare un insieme contenente questi rappresentanti (in questo caso: cerchio, triangolo, pentagono, esagono, rombo).

2.8.1 Dimostrazioni attraverso l'assioma della scelta

Teorema 2.2. *Avendo $f : X \to Y$ applicazione, allora f surriettiva $\Leftrightarrow$ f è invertibile a destra.*

Possiamo dimostrare questo teorema attraverso l'assioma della scelta sia da destra che da sinistra:

Proof. '$\to$' Assumiamo f surriettiva e costruiamo un'inversa a destra:

$$\forall y \in Y \quad f^{-1}(y) = \emptyset$$
$$A_y = f^{-1}(y) \quad \text{famiglia di insiemi} \quad I = Y$$

Secondo questi *assunti*, per l'assioma della scelta:

$$\exists \varphi : Y \to \bigcup_{y \in Y} f^{-1}(y) = X$$

Perchè ogni elemento di X ha un corrispettivo in Y perciò se prendo tutti gli elementi di $f^{-1}(y)$ e come se stessi prendendo X stessa $\square$

RIP:Aggiungere la *proof* '$\leftarrow$'

Esempio 2.3. *Prendiamo due insiemi* $X = \{1, 2, 3\}$ *e* $Y = \{a, b, c, d\}$ *con:*

$$\eta : Y \to X \quad \textit{surriettiva} \quad \Rightarrow \exists \quad \textit{Inversa dx}$$
$$a \mapsto 1$$
$$b \mapsto 1$$
$$c \mapsto 2$$
$$d \mapsto 3$$

Con l'assioma della scelta noi avremo un insieme $u_1 : X \to Y$ *che:*

$1 \mapsto ? \in \eta^{-1}(1) = \{a, b\}$ *Posso scegliere tra a e b ed in base alla scelta si formerà un diverso insieme*

$2 \mapsto ? \in \eta^{-1}(2) = \{c\}$

$3 \mapsto ? \in \eta^{-1}(3) = \{d\}$

RIP:Funzione da ri-allineare

3 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 matematichese diciamo che se abbiamo una proposizione P e:

$$\begin{aligned} P(n_0) &\quad \text{vera} \\ P(n) &\quad \text{vera} \end{aligned}$$

Allora $P(n)$ è vera.

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

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

Esempio 3.1. *Utiliziamo un esempio, dimostramo che $\forall n \geq 0$ la somma che denotiamo con $S(n)$ dei primi numeri naturali:*

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

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.

3.1 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 $\Rightarrow P(n)$ vera allora $P(n)$ vera $\forall n \in \mathbb{N}$.

Un esempio di ciò è 28 e 29.

3.2 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 $\forall n \geq n_0$.

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

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

4 Approfondimenti sui numeri interi

In questo capitolo andremo a vedere più in profondità alcune delle proprietà e dei teoremi dei numeri $\mathbb{N}$ e $\mathbb{Z}$.

4.1 Divisione Euclidea

Definizione 4.1. Una **divisione euclidea** è il processo di dividere un numero $\mathbb{Z}$ (**il dividendo**) per un altro numero $\mathbb{Z}$ (**divisore**).

Se prendiamo $a, b \in \mathbb{Z}$ diciamo che a è il divisore di b oppure che b è il multiplo di a oppure che a divide b

Se prendiamo $b = ak$ con $k \in \mathbb{Z}$ scriviamo:

$$a \mid b \quad \text{Se a è divisore}$$
$$a \nmid b \quad \text{Se a } \textbf{NON} \text{ è divisore}$$

Esempio 4.1. *Facciamo qualche esempio con qualche numero intero:*

$$2 \mid 4 \quad 3 \nmid 5 \quad 3 \mid 9 \quad 3 \nmid 2$$

Osservazione 4.1. Possiamo dire che un numero è pari $\Leftrightarrow 2|a \wedge a \in \mathbb{Z}$

Teorema 4.1. *$a, b \in \mathbb{Z}, a > 0$ allora $\exists! q, r \in \mathbb{Z}$ tali che:*

- *r è un numero $0 < r < a$.*
- *$b = aq + r$.*

Esempio 4.2. *$b = 24$ e $a = 13$:*

$$24 = 1 * 13 + 11$$
$$b = q * a + r$$
$$0 < 11 < a$$

Proof. Dimostramo l'esistenza attraverso l'induzione (terza forma 3.3):

Esempio 4.3. *Con $b \geq 0$ supponiamo che la tesi $\forall n \leq b$ e proviamola per $b + 1$,*
se $b + 1 < a$ scelgo $q = 0 \quad r = b + 1 < a$

□

4.2 Minimo comune multiplo

4.3 Massimo comune divisore

4.4 Algoritmo Euclideo

4.5 Identità di Bezòut

4.6 Equazioni Diofantee lineari

4.6.1 Esempio

Se considero la funzione:

$$f : \mathbb{Z}^2 \to \mathbb{Z} \tag{30}$$

$$(x, y) \to 21x - 15y \tag{31}$$

Dobbiamo dimostrare che la funzione è **iniettiva** o **surriettiva**. Prendiamo quindi $f(1,1) = 21 - 15 = 6$ possiamo dire che
$f$surriettiva $\Leftrightarrow f(\mathbb{Z}^2) = 2$ 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 $n \in 3Z$

5 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 matematichese:

$$a \in \mathbb{Z}, a > 1 \tag{32}$$

Lemma 5.1.

$$a, b \in Z, p \in Z \quad \text{Primo} \tag{33}$$

$$p|a \quad op|a * b \tag{34}$$

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

DIM:Possiamo dimostrarlo utilizzando anche **Bezout**

5.1 Teoria fondamentale dell'aritmetica

Ok prepariamoci a scrivere un pò di formule.
si dice che: $a \in Z, a \neq 0, 1, -1$ allora a si scrive in un modo unico come prodotto di primi:

$$a = \tag{35}$$

5.2 Teorema di euclide

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

Perfetto ora consideriamo un numero $N = p_1 * \ldots * p_n$. La divisione euclidea di N per p_1 da resto 1. Analogamente N diviso per $N = p_1 * \ldots * p_n$ da resto 1

$p_1 \dagger N \ldots p_n \dagger N$ 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.

6 Numeri complessi

Noi definiamo numeri complessi quei numeri che

$\mathbb{C} = \mathbb{R} \times \mathbb{R}$ denotiamo che $(x, y) \in \mathbb{R}^2$ 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 $x, y, u, v \in \mathbb{R}$
- **Prodotto** $(x + iy) * (u + iv) := (xu - yv) + i(xv + yu)$ con $x, y, u, v \in \mathbb{R}$

Utiiziamo un esempio numerico:

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

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

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

$$i * i = (0 * 0 - 1 * 1) + i(0 + 1 + 0 + 1) = -1 + i0 = -1$$
$$i^2 = -1 \quad i^3 = i * i^2 = -i = i^2 * i^2 = \dots$$

Osservazione 6.1. $\boxed{i^1 = i \quad i^2 = -1 \quad i^3 = -i \quad i^4 = i}$

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

6.1 Piano di Gauss

Con $\mathbb{C} = \mathbb{R}^2$ 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 $z \in \mathbb{R}$ allora $|z| = \sqrt{x^2}$

6.2 Proprietà dei numeri complessi

- $\overline{zw} = z * \overline{w}$
- $\overline{z} = z$
- $\overline{z + w} = \overline{z} + \overline{w}$

- $z + \overline{z} = 2Re(z)$
- $z - \overline{z} = 2Im(z)$

TEO:Cercare le dimostrazioni

Altre proprietà però con il modulo:

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

DEF:disugiaglainza triangolare

$\theta = \arg(z)$ argomento di z angolo formato da z e l'asse Re θ è definito a meno di Re multipli di 2π abbiamo la **forma trigonometrica di z**.

FIG:grafico con il modulo

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

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

FIG:forma trigonometrica $\mathbb{Z}$

6.3 Forma esponenziale

REM:Re sta per parte reale

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

TEO:formula di De Mouire

6.4 Radici di un numero $\mathbb{C}$

6.5 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:

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

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

$$z_1 = \frac{-b + \delta_1}{2a} \tag{38}$$

$$z_1 = \frac{-b + \delta_2}{2a} \tag{39}$$

Mentre:

$$\text{Se} \quad \Delta = 0, \delta_1 = \delta_2 \quad \text{quindi} \quad z_1 = z_2 \tag{40}$$

$$\text{Se} \quad \Delta < 0, \delta_1 \neq \delta_2 \quad \text{quindi} \quad z_1 \neq z_2 \tag{41}$$

6.6 Radici complesse (di secondo grado)

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, $\quad |z| = \sqrt{Re(z^2) + In(z^2)} = \sqrt{-8^2 + 0^2} = \sqrt{(-8^2)} = 8.$

6.7 Teorema fondametale dell'Algebra

Il teorema fondamentale dell'algebra dice che ogni polinomio in $\mathbb{R}$ o $\mathbb{C}$ di grado ≥ 1 ha soluzioni nei $\mathbb{C}$
Ovvero sia $p(x) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ un polinomio, $p(x) = a_n + a_{n-1} + \cdots + a_1 + a_0 \in \mathbb{C} a_n \neq 0$ di grado n

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

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

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

7 Relazioni di Equivalenza

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

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

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

7.1 Equivalenza modulare

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

$x \backsim_n y \Leftrightarrow \exists k \in \mathbb{Z}$ tale che $x - y = Kn$ si diche che x è congruo a y mmodulo n e si scrive $x \equiv yMODn$. $\forall x \in \mathbb{Z}$vale $x \equiv x \mod n$ perchè $\exists K \in \mathbb{Z}$ tale che $x - x = K * n$

7.2 Classe di equivalenza

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

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

8 Cardinalità

RIP:recuperare lezione sulla 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 $\exists f : A \to B$ bigettiva, in tal caso scriviamo $|A| = |B|$.

Ok detto questo mostriamo alcune proprietà:

1. **Riflessiva** A è equipotente con A tramite $id_A A \to A$ bigettiva.
2. **Simmetrica** A è equipotente a $B \Rightarrow \exists f : A \to B$ 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. $\exists f : X \to X$ iniettiva, ma non suriettiva.

X si dice **numerabile** (o di cardinalità numerabile) se $|X| = |\mathbb{N}|$ e scriviamo $|X| = X_0$ e lo si chiama **Aleph Zero**.

Se X è numerabile $\Rightarrow X$ infinito.

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

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

$$f : \mathbb{N} \to \mathbb{Z} \tag{42}$$

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 $f^{-1} : \mathbb{Z} \to \mathbb{N}$

$\mathbb{N}x\mathbb{N}$ è numerabile dimostriamo che $f : \mathbb{N}x\mathbb{N} \to \mathbb{N}$.

ES:aggiungere esempi

.

Definiamo A, B insiemi e scriviamo:

8.1 Teorema di Cantor-Bernstein

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

In formule questo ci dice che se:

$$|A| \leq |B| \quad |B| \leq |A| \Rightarrow |A| = |B| \tag{43}$$

Se A, B finiti, $|A| = n, \quad |B| = m \quad n, m \in \mathbb{N}$ 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 $|X| > |\mathbb{N}|$

8.2 Impossibilità della surriettività dei numerabili

Prendiamo la proposizione che prende X insieme con $X \neq \not{0}$ allora non esite alcuna mappa surriettiva $X \to P(x)$

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

La proposione 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.

8.3 Argomento che il prof si tiene segreto

Definiamo A, B insiemi.

$$B^A := f : A \to B \quad \text{funzione} \tag{44}$$

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:

$$\phi : 0, 1^x \to P(x)$$
$$f \mapsto f(1)^{-1} = \{x \in X : f(x) = 1\} \subseteq X$$

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

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

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

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

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

$$\varphi : B^A \to B^n = Bx, \ldots, xB$$
$$f \mapsto (f(a_1), \ldots, f(a_n))$$

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

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

8.4 Cardinalità dei $\mathbb{Q}$

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

$$\varphi : \mathbb{Q}\{0\} \to \mathbb{N}*$$
$$\frac{p}{q} \mapsto |p| + |q|$$

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 $\neq 0$ e disgiunti $\Rightarrow Q$ numerabile.

FIG:cardinalità di Cantor

Lemma 8.1. prendiamo $\{X_m : m \in \mathbb{N}\}, |X_n| \leq \aleph_0, X_m \neq \emptyset \forall n \in \mathbb{N}$ se $|Xm| < \aleph_0 \forall n \in \mathbb{N}$ allora $X_n \cap X_m = \emptyset$ se $n \neq m$ allora $|\bigcup_{n \in \mathbb{N}}^{1} X_n| = \aleph_0$

8.5 Cardinalità di $\mathbb{R}$

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

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

8.6 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 verrano trattati nel corso ma sono good to know.*

9 Calcolo Combinatorico

Iniziamo con una definizione, se abbiamo X insieme infinito,

ovvero: $\{X \to X \quad \text{Bigettiva}\}$ 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:

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

Lemma 9.1. X, Y insiemi finiti, $|X| = n \leq m = |Y|$ Il numero delle applicazioni iniettive $X \to Y$ è uguale:

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

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

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

- $x_1 \mapsto ?$ 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 $X \to Y$ 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:

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

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

$$n, k \in \mathbb{N}, n \geq 1, 0 \leq k \leq n, \quad \text{il coefficiente binomiale}$$
$$(nk) := \frac{n!}{k!(n-k)!}$$

9.1 Mi inventerò un titolo

RIP:trovare il titolo di questa subsection

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 cotruire 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:

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

Lemma $(nsuk) = (n-1suk) + (m-1k-1)$

9.2 Coefficiente binomiale

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

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

Dimostriamolo attraverso l'induzione:

ES:Dimostrare il coefficiente binomiale attraverso l'induzione

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 su k).

Il numero di sottoinsiemi di X è:

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

10 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 $(x, \triangle) \quad POSET \quad x, y \in X$, 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.

10.1 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
- $x \leq y, y \leq x \Rightarrow x = y \mathbb{R}$ 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 $P(x) A, B \in P(x) \quad A \triangle B \Leftrightarrow A \subseteq B$

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 $X \neq \{*\}$

10.2 Tipi di ordini

Definiamo $(A_1, \triangle_1), \ldots, (A_n, \triangle_n) \quad POSET$ definimo ordini parziali su $A_1 x, \ldots, x A_n$.

Esistono diversi tipi di ordini che ora andremo a spiegare nel dettaglio.

10.2.1 Ordine lessicografico (LEX)

Ordine lessicografico (LEX):

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

10.2.2 Ordine prodotto

Ordine prodotto $\triangle_1 x, \ldots, \triangle_n$:

$$(a_1, \ldots, a_n) \triangle_1 x, \ldots, x \triangle_n (b_1, \ldots, b_n) \Leftrightarrow a_i \triangle_i b_i \forall i = 1, \ldots, n$$

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

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

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:

$$(A_1, \triangle_1), \ldots, (A_n, \triangle_n) \Rightarrow (A_1 x, \ldots, x A_n, \triangle_{LEX})$$

Esempio:

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

10.2.3 Ordine indotto

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

$$y_1 \triangle_y, y_2 \Leftrightarrow y_1 \triangle y_2 \quad \forall y_1, y_2 \in Y \subseteq X$$

Diciamo che Y è una **catena** se $(Y, \triangle y)$ 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)

10.3 Minimo e massimo

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

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

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 $\triangle$ è totale, esiste un elemento minimale $\Leftrightarrow$ esiste il minimo.
- Se $\triangle$ 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**.

10.4 Maggioranti e minoranti

Definiamo $(X, \triangle)$ POSET, $Y \subseteq X, Y \neq \emptyset, z \in X$:

- z è un <u>minorante</u> di Y se $\forall y \in Y \quad z \triangle y$
- z è un <u>maggiorante</u> di Y se $\forall y \in Y \quad y \triangle z$
- Se l'insieme dei minoranti di Y è non vuoto ed ha un massimo M allora diciamo che M è l'estremo inferiore di Y e lo denotiamo con $\inf \quad Y = M$

- Se l'insieme dei maggioranti di Y è non vuoto ed ha un minimo m allora diciamo che m è l'estremo superiore di Y e lo denotiamo con sup $\quad Y = M$

Esempio prendiamo $(\mathbb{R}, \leq) \quad Y = (0,1)$ intervallo aperto $= \{x \in \mathbb{R} : 0 < x < 1\}$:

- 2 è maggiorante per y in quanto $2 \geq y \forall y \in Y$

Per esempio prendiamo $(\mathbb{R}, \leq) \quad Y = (0,1)$ intervallo aperto dove $= \{x \in \mathbb{R} : 0 < x < 1\}$ in qunto 2 è maggiorante per $y \quad$ visto che $2 \geq y \quad \forall Y$.

Definiamo $(X, \triangle)$ POSET, diciamo che X è Bene ordinato se ogni sottoinsieme $\neq \emptyset$ ammette minimo.

Ad esempio se prendiamo $(\mathbb{N}, \leq)$ è bene ordinato Ad esempio se prendiamo $(\mathbb{Z}, \leq)$ non è bene ordinato.

Ci piacciono gli esempi quindi prendiamo anche $\mathbb{N} * \mathbb{N}, \leq * \leq$ non è bene ordintato

Se invece utilizziamo l'ordine **LEX** con una coppia ordinata $((x_1, \triangle_1))\ (x_2, \triangle_2)$ POSET.

10.5 Assioma del buon ordinamento

Se prendiamo X insieme, $X \neq \emptyset$ allora $\exists \triangle$ ordine prziale tale ce $(x, \triangle)$ bene ordinato.

Lemma 10.1. Citando il **Lemma di Zorn** $(x, \triangle)$ POSET, $X \neq \emptyset$ tale che ogni catena in X possiede almeno un maggiorante, Allora X possiede elementi massimali.

(Assioma della scelta) $\Leftrightarrow$ (Assioma B.O.) $\Leftrightarrow$ (Lemma di Zorn).

11 Principio di Induzione Strutturale

DEF:dare una definizione non matematica

Prendiamo $(x, \triangle)$ POSET ben definito, $\mathcal{P}$ affermazione sugli elementi di X se vale:

1. $\mathcal{P}(x)$ vera $\forall x \in X$ minimale
2. $\forall y, z \in X$ tale che $y \triangle z$ se $\mathcal{P}(y)$ vera allora $\mathcal{P}(z)$ vera

Allora $\mathcal{P}(x)$ vera $\forall x \in X$.

12 Aritmetica modulare

DEF:Aggiungere una definizione non matematica

Definiamo un insieme A, operazione (binaria) su A è una funzione che:

$$* : A * A \to A$$

Denotiamo $*(x, y) = x * y$ con $x, y \in A$.

Per esempio quando eseguiamo una somma noi stiamo facendo:

$$+ : \mathbb{N} * \mathbb{N} \to \mathbb{N}$$
$$(n, m) \mapsto n + m$$

Con i numeri:

$$(2, 3) \mapsto 2 + 3 = 5$$

12.1 Proprietà dell'aritmentica modulare

Se abbiamo $* : A * A \to A$ operazione possiamo avere:

- $*$ commutativa $\quad x * y = y * x \quad \forall x, y \in A$
- $*$ associativa $\quad x * (y * z) = (x * y) * z \quad \forall x, y, z \in A$
- $*$ un elemento neutro $\quad \exists e \in A$ tale che $e * x = x * e = x \quad \forall x \in A$.

Funzione $\mathbb{Z}_n = \overline{0}, \overline{1}, \ldots, \overline{n+1}$ classi di resto n.

12.2 Operazioni in $\mathbb{Z}_n$

$$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$
$$(\overline{a}, \overline{b}) \mapsto a + b$$
$$\overline{a} * \overline{b} := \overline{a * b}$$

$$* : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$$
$$(\overline{a}, \overline{b}) \mapsto a * b$$
$$\overline{a} * \overline{b} := \overline{a * b}$$

Verifichiamo che le operazioni sono ben definite:

$$a, b, r, s \in \mathbb{Z} \quad \overline{a} = \overline{r} \quad , \overline{b} = \overline{s}$$

Dobbiamo quindi verificare che:

1. $\overline{a} + \overline{b} = \overline{r} + \overline{s}$
2. $\overline{a} * \overline{b} = \overline{r} * \overline{s}$

Supponiamo che: $\overline{a} = \overline{r} \Rightarrow a - r = Kn \quad k \in \mathbb{Z}$
$\overline{b} = \overline{s} \Rightarrow b - s = hn \quad h \in \mathbb{Z}$

Proof. (1) Viene verificato con:

$$a + b = r + Kn + s + hn = r + s + (K + h)n \Rightarrow \overline{a + b} = \overline{r + s}$$

□

Proof. (2) Viene verificato con:

$$a * b = (r + Kn) * (s + hn) = r * +s + (rh + sK + Khn)n \Rightarrow \overline{a * b} = \overline{r * s}$$

□

Definizione 12.1. Abbiamo quindi che le operazioni $+, *$ sono commutativi e associativi.

Definizione 12.2. La funzione $+$ e $*$ hanno un elemento neutro:

- $+$ ha come elemento neutro lo $\overline{0}$
- $*$ ha come elemento neutro l' $\overline{1}$

Osservazione 12.1. Se $\overline{a} \in \mathbb{Z}$ allora:

$$\exists \overline{b} \in \mathbb{Z}_n : \overline{a} + \overline{b} = \overline{0}.$$

Ovvero quando $\overline{b}$ è opposto di $\overline{a}$.

Esempio 12.1. $\mathbb{Z}_6 \quad \overline{2}$ *ha un opposto:* $\overline{-2} = \overline{4}$ *perchè:*

$$-2 \equiv 4 \mod 6$$

ES:Riguardare gli esempi della classe inversa 9:55

12.3 Inversionedella classe

Definizione 12.3. La classe di $\overline{a} \in \mathbb{Z}_n$ è invertibile in $\mathbb{Z}_n$ (Rispetto al $*$) se:

$$\exists \overline{b} \in \mathbb{Z}_n : \overline{a} * \overline{b} = \overline{1}$$

In tal caso $\overline{b}$ si dice inverso di $\overline{a}$ e si denota con:

$$\overline{a}^{-1}, \overline{b}^{-1}$$

Altrimenti $\overline{a}$ si dice non invertibile in $\mathbb{Z}_n$:

$$\bigcup(\mathbb{Z}_n) := \{\overline{a} \in \mathbb{Z}_n : \overline{a} \quad \text{è invertibile}\}$$

Esempio 12.2.

$$\bigcup(\mathbb{Z}_4) = \{\overline{1}, \overline{3}\}$$

Osservazione 12.2. Per ogni $n \geq 2$:

$$\overline{0} \notin \bigcup(\mathbb{Z}_n), \overline{1} \in \bigcup(\mathbb{Z}_n)$$

Teorema 12.1. *con $x \in \mathbb{Z}_n$ allora si ha che:*
$\overline{x}$ è invertibile $\Leftrightarrow MCD(x,n) = 1$

Proof. Possiamo dimostrare **??** osservando che se $y \in \mathbb{Z}$ tale che $\overline{x} = \overline{y}$ allora:

$$x = y + hn, \quad h \in \mathbb{Z}$$

Quindi $MCD(x,n) = 1 \Leftrightarrow MCD(y,n) = 1$ Pertanto la condizione $MCD(x,n) = 1$ non dipende dalla scelta del rappresentante per $\overline{x}$
'$\Rightarrow$' sia $\overline{x} \in \mathbb{Z}_n$ invertibile $\Rightarrow \exists \overline{z} \in \mathbb{Z}_n : \overline{x} * \overline{z} = \overline{1} \Rightarrow xz = 1 + Kn \in \mathbb{Z}, K \in \mathbb{Z}$ □

Osservazione 12.3. Possiamo osservare che $xz - nk = 1$ non è altro che un'equazione Diofantea lineare 4.6.

12.4 Elementi in $\bigcup(\mathbb{Z}_n)$

Definizione 12.4. notazione $m \in \mathbb{N}*, \underline{a} \in \mathbb{Z}_n$ definiamo:

$$\underline{a}^m := \underbrace{\overline{a} * \overline{a} * \ldots * \overline{a}}_{m \text{ volte}}$$

Se $m \in \mathbb{Z}, m < 0$ e $\overline{a}$ è invertibile:

$$\overline{a}^m := (\overline{a}^{-1})^{-1}$$
$$m = 0, \overline{a} \neq \overline{0} \quad DEF \quad \overline{a}^0 := \overline{1}$$

12.5 Teorema di Eulero

Definizione 12.5. Definiamo φ di **Eulero** $\varphi : \mathbb{N}* \to \mathbb{N}*$ come:

$$\varphi(n) = \#\{m \in \mathbb{N}* : m \leq n, MCD(m,n) = 1\} = \#\bigcup(\mathbb{Z}_n)$$

TEO:Approfondire il teorema di Eulero φ

é computazionalmente difficile fattorizzare n se $n \gg 0$

Teorema 12.2. *(Eulero) se $n, x \in \mathbb{Z}, n \geq 2$ tali che $MCD(x,n) = 1$ allora:*

$$x^{\varphi(n)} \equiv 1 \mod n$$
$$\text{cioè} \quad \overline{x}^{\varphi(n)} = \overline{1} \in \mathbb{Z}_n$$
$$\overline{x} * \overline{x}^{\varphi(n)-1} = \overline{1} \quad \text{quindi} \quad \overline{x}^{\varphi(n)-1} \quad \text{è l'inverso di} \quad \overline{x}$$

Ovvero conta quanti interi $\varphi(n)$ ci sono.

12.6 Teorema di Fermart

Definizione 12.6. Se $p \in \mathbb{Z}$ primo, $x \in \mathbb{Z}$ pTx allora:

$$x^{\varphi-1} \equiv 1 \mod p$$

Che è come dire che:

$$\overline{x}^{\varphi-1} \in \mathbb{Z}$$

E ne consegue che:

$$\overline{x}^{-1} = \overline{x}^{\varphi(n)-1} \in \mathbb{Z}$$

Osservazione 12.4. Se dimostriamo il teorema di Eulero 12.5 allora dimostriamo anche il teorema di Fermart 12.6

Proof.

$$\begin{aligned} \bigcup(\mathbb{Z}_n) &= \{\overline{a} \in \mathbb{Z} : MCD(a,n) = 1\} \\ &= \{\overline{a} \in \mathbb{Z} : 1 \leq a \leq n, MCD(a,n) = 1\} \\ &= \{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{\varphi(n)}}\} \end{aligned}$$

□

TEO:Approfondire teorema di Fermart a casa

12.7 Crittosistema

Definizione 12.7. Un crittosistema consiste di:

- Un alfabeto A, un insieme finito ($A = \mathbb{Z}_n$).
- Un insieme dei messaggi in chiaro $m \subseteq \bigcup_{n\in\mathbb{N}*} A^n$.
- Un insieme dei messaggi cifrati $c \subseteq \bigcup_{n\in\mathbb{N}*} A^n$.
- Un insieme di chiavi k
- funzione di cifratura (encryption function).
- funzione di decifratura (decryption function).
- Insieme di chiavi ammissibili $S \subseteq K \times K : \forall(k, k^1) \in S$ avrò che $D(k^1, E(k,x)) = x \quad \forall x \in M$.

Per esempio una funzione che cifra si mostra come:

$$\begin{aligned} E : K \times M &\to C \\ (k,x) &\mapsto E(h,x) \end{aligned}$$

Per esempio una funzione che decifra si mostra come:

$$\begin{aligned} D : K \times C &\to M \\ (k^1, y) &\mapsto D(h,y) \end{aligned}$$

Esempio 12.3. *Alice e Bob vogliono comunicare in modo sicuro, per farlo:*

- *Si mettono d'accordo su un crittoistema e scelgono preventivamente una coppia di chiavi* $(k, k^1) \in S$
- *Se Alice vuole mandare il messaggio* $x \in M$ *a Bob, calcola* $y = E(k, x)$.
- *Quindi Alice manda* y *a Bob.*
- *Bob riceve* $y \in C$ *e calcola* $D(k^1, y) = D(k^1, E(k, x)) = x$.

12.7.1 Tipi di crittosistemi

Esistono due tipi di crittosistemi:

- a chiave private o simmetrico se $S = \{(k, k) \in K^2\}$
- a chiave pubblica o asimmetrico se non è possibile ottenere (in tempo ragionevole) la chiave di decifratura conoscendo la chiave di cifratura

12.7.2 Crittosistema RSA

Definizione 12.8. Il crittosistema **RSA** è un tipo di crittosistema a chiave pubblica creato nel 1977 da (Rivest, Shamir, dleman).

Esempio 12.4. *Bob sceglie due* $p, q \in \mathbb{Z}$, *numeri primi grandi:*

$$p, q \approx 2^{512} \approx 10^{154}$$

Bob deve:

- *Calcolare* $n = p * q$.
- *Calcolare* $\varphi(n) = (p-1) * (q-1) = pq - p - q + 1$.
- *Scegliere* $e \in \mathbb{Z}$ *invertibile modulo* $\varphi(n)$.
- *Calcolare* $d \in \mathbb{Z}$ *inverso di* e *modulo* $\varphi(n)$.

12.7.3 Cifrario di Cesare

Prendiamo un tipo di crittosistema, il **cifrario di Cesare** dove:

$$A = M = C = \mathbb{Z}_n, K = \mathbb{Z}_n^1\overline{0}$$
$$S = \{(k, k) \in k^2 : k \in K\} \quad E : \mathbb{Z}_n^1\overline{0} \times \mathbb{Z}_n \to \mathbb{Z}_n$$
$$E(k, x) = x + k \quad D(k, y) = y - ki \quad D : \mathbb{Z}_n^1\overline{0} \times \mathbb{Z}_n \to \mathbb{Z}_n$$

Esempio 12.5.

$$\overline{k} = \overline{3} \quad x = C|A|E|S|A|R = \overline{3}|\overline{1}|\overline{5}|\overline{19}|\overline{1}|\overline{18}.$$

Che cifrato diventa:

$$E(\overline{3}, \overline{3}) = \overline{3} + \overline{3} = \overline{6}$$

TEO:guardarsi la lezione sul RSA

13 Monoidi e Gruppi

In questo capitolo finale andremo a spiegare quelli che sono i **Monoidi** e i **Gruppi**

13.1 Monoidi

Definizione 13.1. Un **semigruppo** è una coppia $(M, *)$ dove M è un insieme e $*$ è un operazione su M tale che $* : M \times M$.

Definizione 13.2. Un **monoide** è una tripla $(M, *, \lambda)$ dove $(M, *)$ è un semigruppo e λ è un elemento neutro per *.

Esempio 13.1. $(\mathbb{N}, +, 0)$ *Monoide:*

- $(\mathbb{N}*, +)$ *semigruppo, ma non monoide.*

Lemma 13.1. L'elemento neutro di un monoide è unico.

Proof. Siano μ e λ due elementi neutri, possiamo scrivere:

$$\mu = \mu * \lambda = \lambda$$

□

Definizione 13.3. Se $*$ è commutativa, il monoide (i semigruppo) si dice commutativo o Abeliano

Esempio 13.2. $(\mathbb{N}, *, 1)$ *monoide commutativo, allora:*

$$(\mathbb{Z}, +, 0), (\mathbb{Z}, *, 1) \quad \textit{Monoidi commutativi}$$

Ma anche $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$ *sono monoidi*
$\mathbb{R}$ $\mathbb{Q}$ ***non è un monoide né con*** $+$ ***né con*** $*$.

Inoltre se abbiamo X insieme, con $X \neq \emptyset$ allora:

$$X^x = \{f : X \to X \text{Funzione}\}$$

13.1.1 Invertibilità di un monoide

Definizione 13.4. $(M, *, \lambda)$ monoide con $a \in M$ si dice che:

1. a si dice invertibile a sinistra se $\exists b \in M : b * a = \lambda$, b viene detto **inverso sinistro** di a.
2. a si dice invertibile a sinistra se $\exists b \in M : b * a = \lambda$, c viene detto **inverso sinistro** di a.
3. a si dice invertibile a destra se $\exists d \in M : a * d = d * a = \lambda$, d viene detto **inverso** di a e si denota con a^{-1}.

Proprietà 13.1. $(M, *, \lambda)$ monoide allora:

1. λ è inverso di se stesso $(\lambda * \lambda = \lambda)$
2. $a \in M$, b inverso sinistro di a, c inverso destro di a allora $b = c$.
3. Se $(M, *, \lambda)$ è commutativo allora $a \in M$ ha inverso dx $\Leftrightarrow$ ha inverso sx.

Proof. (2)

$$b = b * \lambda = b * (a * c) = (b * a) * c = \lambda * c = c$$

□

Esempio 13.3.

$$\begin{aligned}(\mathbb{Z}, +, 0) &\quad \textit{tutti gli elementi sono invertibili}\\ (\mathbb{Z}, *, 1) &\quad \textit{Gli unici eleenti invertibili sono } 1 - 1\\ (\mathbb{Z}_n, *, \overline{1}) &\quad \overline{x} \textit{invertibile} \Leftrightarrow MCD(x, n) = 1\\ (X^x, \circ, Id_x) &\quad f \in X^x \textit{ invertibile} \Leftrightarrow f \textit{ bigettiva}\end{aligned}$$

Definizione 13.5. Un monoide $(M, *, \lambda)$ tale che ogni elemento è invertibile si dice gruppo

Definizione 13.6. $(M, *, \lambda)$ monoide, $m \in \mathbb{N}*, g \in M$:

$$g^m = g * \ldots * g$$

Esempio 13.4.

$$\begin{aligned}(\mathbb{Z}, *, 1) &\quad g = 3 \quad m = 4 \quad g^m = g * g * g * g\\ (\mathbb{Z}, +, 0) &\quad g = 3 \quad m = 4 \quad g^m = g + g + g + g\end{aligned}$$

Quindi l'ordine di g è il più piccolo intero positivo m tale che $g^m = \lambda$. Scriviamo che l'ordine di $g = m$

Se tale insieme non esiste scriviamo $ord_m(g) = infinito$

TEO:Aggiungere ultima lezione 15:30 09/12/2021

13.2 Gruppi

Definizione 13.7. Un **gruppo** $(G, *, \lambda)$ ci chiediamo cos'è un sottogruppo di G ovvero un sottinsieme $H \subseteq G$ tale che:

1. $lambda \in H$,
2. $a, b \in H \Rightarrow a * b \in H$.
3. $a \in H \Rightarrow a^{-1} \in H$.

Esempio 13.5.

$$\begin{aligned} * : G \to G \\ \textit{Si restringe a} \\ (H, *, \lambda) \quad \textit{è un gruppo} \end{aligned}$$

Esempio 13.6.

$$\begin{aligned} (\mathbb{Z}, +, 0) &\subseteq (\mathbb{Q}, +, 0) \\ &\subseteq (\mathbb{R}, +, 0) \\ &\subseteq (\mathbb{C}, +, 0) \end{aligned}$$

Osservazione 13.1. Si può verificare che tutti i sottogruppi di $(\mathbb{Z}, +, 0)$ sono di questa forma.

13.2.1 Relazione di equivalenza tra gruppi

Definizione 13.8. $(G, *, \lambda)$ gruppo, relazione d'equivalenza $\sim$ su G è compatibile con $*$ se vale $\forall a, b, c, d \in G$:

$$(a \sim b) \wedge (c \sim d) \Rightarrow (a * c) \sim (b * d)$$

definiamo un'operazione $[*]$ sul quoziente $\frac{G}{\sim}$:

$$[x][*][y] := [x * y] \quad \forall x, y \in G$$

$(\frac{G}{\sim}, [*], [\lambda])$ è un gruppo detto gruppo quiziente.

Esempio 13.7. $(\mathbb{Z}, +, 0)$ $n \in \mathbb{N}^*$ *relazione di equivalenza modulare, cioè* $x \sim y \Leftrightarrow x \equiv y \mod n$*:*

$$\frac{\mathbb{Z}}{\sim_n} = \mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$$

$\sim_n$ *è compatibile con la somma su* $\mathbb{Z}$

Definizione 13.9. $(G, *, \lambda)$ gruppo, $H \subseteq G$ sottogruppo induce la relazione:

$$g, g^1 \in G \quad g \sim_s g^i \Leftrightarrow g^{-1} * g^i \in H$$

Verifichiamo che $\sim_s$ è relazione di equivalenza:

1. Riflessiva $g \sim_s g^i \Leftrightarrow g^{-1} * g \in H$ **?**.
2. Simmetrica $g \sim_s g^i \Rightarrow g^i \sim_s g \in H$ **?**.
3. Transitiva $g \sim_s g^i \Rightarrow g^i \sim_s g^{ii}$ **?**.

TEO:dimostrazioni lezione 15/12/2021 10:20

Definizione 13.10. Le classi di equivalenza sono classi laterali destre:

$$H * g := [g] = \{x \in G : x \sim_\Delta g\} = \{x = K * g : K \in H\}$$

Nota Bene 13.1. ! $\frac{G}{H}$ e $\frac{H}{G}$ sono equipotenti, ma sono in generali diversi.

Esempio 13.8. *S_3 $H = \{Id, \phi\}$ sottogruppo, le classi laterali sinistre: $g \circ H$ $g \in S_3$:*

$$\begin{aligned} Id \circ H &= \{Id \circ h : h \in H\} = \{Id \circ Id, Id \circ \phi\} = \{Id, \phi\} = H \\ \phi \circ H &= \{\phi \circ h : h \in H\} = \{\phi \circ Id, \phi \circ \phi\} = \{\phi, Id\} \\ \varphi \circ H &= \{\varphi \circ h : h \in H\} = \{\varphi \circ Id, \varphi \circ \phi\} = \{\varphi, \varphi \circ \phi\} \\ \varphi^2 \circ H &= \{\varphi^2 : \varphi^2 \circ \phi\} = \{\varphi^2, \varphi \circ \phi\} = (\phi \circ \varphi) \circ H \end{aligned}$$