Spunti di matematica pura per l'orientamento nelle scuole superiori

Matteo Misurati

Università di Ferrara
Laurea triennale in matematica

Seminario Fermat
24 Novembre 2020

Introduzione

Obiettivo della presentazione: fornire a studenti della triennale spunti e materiale per parlare di matematica pura a ragazzi delle scuole superiori.

- L'idea nasce da esperienze personali di orientamento.
- Lo stage offerto dal dipartimento.
- Orientamento presso il liceo Ariosto di Ferrara.
- In tale occasione ci si era concentrati sulla matematica applicata.
- Ciò ha presentato dei vantaggi.

Introduzione

Tuttavia ritengo che affiancare alle applicazioni argomenti di matematica pura introduca, oltre ad alcune problematiche, diversi benefici.

- Risulta complesso presentare argomenti teorici senza spaventare gli studenti.
- Tuttavia mette in mostra le peculiarità del corso di studi.
- Offre un'idea di cosa ci si possa aspettare da un corso della triennale di Matematica.
- Incuriosisce i ragazzi riguardo ad oggetti e argomenti non trattati dai programmi scolastici.

Introduzione

Il materiale è organizzato in tre percorsi, descritti integralmente nelle note della presentazione:

1. Il concetto di gruppo
2. Il concetto di omeomorfismo
3. Principio di induzione e teorema fondamentale dell'aritmetica

Introduzione

- Contengono argomenti scelti all'interno dei corsi di matematica pura della triennale.
- Puntano a descrivere formalmente un oggetto o raggiungere un risultato partendo da conoscenze base.
- Strutturati come una successione di definizioni, esempi e proposizioni.
- Integralmente, adatti a ragazzi molto motivati.
- Tuttavia parti di essi possono essere utilizzate indipendentemente per trattare con studenti a vari livelli di interesse per la matematica.

Il concetto di gruppo

Il primo percorso è un'introduzione al concetto di gruppo.

1. Inizia con una brevissima premessa storica, citando Galois e il problema delle formule risolutive per equazioni di quinto grado,
2. fornisce esempi di gruppo,
3. ne da una definizione formale,
4. dimostra l'equivalenza tra essa e altre definizioni.

Il concetto di gruppo

I primi due esempi vogliono essere familiari allo studente delle superiori.

Esempio

- L'insieme $\mathbb{Z}$ dei numeri interi e la mappa

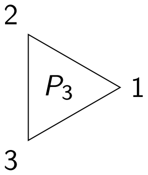
$$\begin{aligned} + : \mathbb{Z} \times \mathbb{Z} &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto x + y \end{aligned}$$

- $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$ associato all'applicazione di moltiplicazione:

$$\begin{aligned} \cdot : \mathbb{Q}^* \times \mathbb{Q}^* &\longrightarrow \mathbb{Q}^* \\ (x, y) &\longmapsto x \cdot y \end{aligned}$$

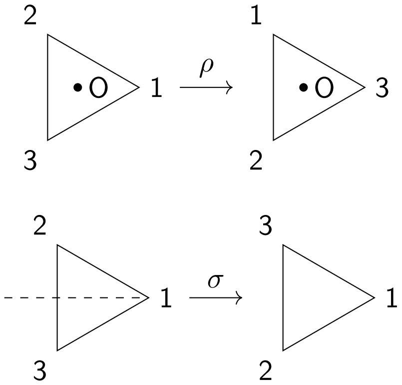
Vengono ricordate per entrambi le proprietà di associatività, di esistenza del elemento neutro e dell'inverso.

Si porta l'esempio delle isometrie di un piano che fissano un triangolo equilatero P_3.



Il concetto di gruppo

Sono quindi mostrate due isometrie di D_3, la rotazione di $\frac{\pi}{3}$ ρ e la simmetria σ:

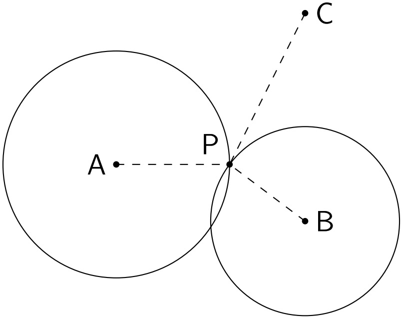


Il concetto di gruppo

Si mostra che ogni isometria del piano è univocamente determinata dal valore che assume in tre punti non allineati, come conseguenza di:

Osservazione

Conoscendo la posizione nel piano di tre punti non allineati e la distanza tra ciascuno di questi e un quarto punto P, la posizione di P è univocamente determinata.

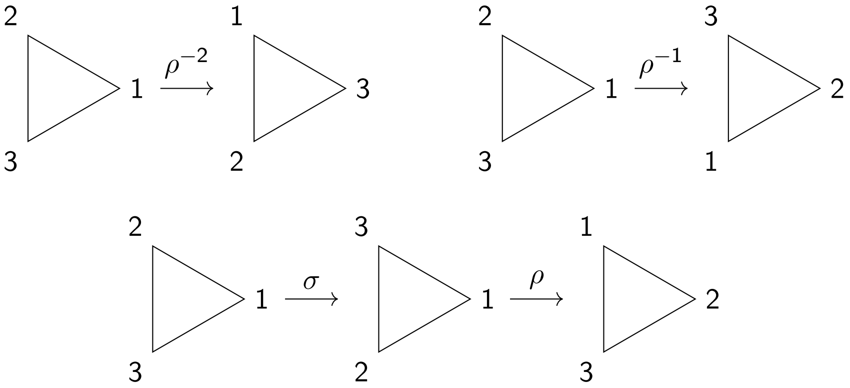


Il concetto di gruppo

Si dimostra:

Proposizione

$D_3 = \{1, \rho, \rho^2, \sigma, \rho\sigma, \rho^2\sigma\}$



È quindi veloce mostrare che:

Esempio

La funzione composizione su D_3:

$$\begin{aligned} \circ : D_3 \times D_3 &\longrightarrow D_3 \\ (f,g) &\longmapsto fg := f \circ g \end{aligned}$$

è associativa ed ammette elemento neutro e inversi bilateri in D_3.

Il concetto di gruppo

- Avendo dato allo studente tre esempi di oggetti in contesti molto diversi con le stesse proprietà, è spiegata la necessità di definire i gruppi.
- Dopo aver spiegato il significato di notazione additiva e moltiplicativa, si procede con la definizione.

Definizione

Un gruppo $(G, +)$ è un insieme non vuoto G munito di un'operazione associativa $+ : G \times G \to G$ (in notazione moltiplicativa: $\times : G \times G \to G$) tale che esista un elemento neutro $0 \in G$ (rispettivamente, in notazione moltiplicativa, $1 \in G$) e per ogni elemento x in G esista in G l'inverso bilatero x', tale che $x + x' = x' + x = 0$. Si nota $-x := x'$ (in notazione moltiplicativa $x^{-1} := x'$, se $xx' = x'x = 1$).

Il concetto di gruppo

Proposizione

Sia G un insieme non vuoto e sia $+ : G \times G \to G$ un'operazione associativa. Se $u \in G$ è zero destro, ossia $x + u = x$ per ogni $x \in G$, e per ogni $x \in G$ esiste $x' \in G$ inverso destro rispetto a u, ossia $x + x' = u$, allora $(G, +)$ è un gruppo.

Dim.

1. Siano x, x' e x'' in G.
2. u è zero bilatero:

$$\begin{aligned} u + x &= (u + x) + u = u + (x + u) = u + (x + (x' + x'')) \\ &= u + ((x + x') + x'') = u + (u + x'') = (u + u) + x'' \\ &\overset{\Diamond}{=} u + x'' = (x + x') + x'' = x + (x' + x'') \\ &= x + u = x. \end{aligned}$$

3. Rileggendo da $\Diamond$, si ottiene $u + x'' = x$, quindi $x'' = x$.
4. $x' + x = x' + x'' = 0 = x + x'$, ovvero x' è inverso bilatero di x.

$\square$

Si conclude dimostrando una terza definizione di gruppo.

Proposizione

Sia G un insieme non vuoto e sia $+ : G \times G \to G$ un'operazione associativa, tale che, per ogni $a, b \in G$, esistono $x, y \in G$ soluzioni delle equazioni $a + X = b$ e $Y + a = b$. Allora esiste uno zero u in G e $(G, +)$ è un gruppo.

Il concetto di gruppo: conclusioni

Riassumendo:

1. Esempi: $(\mathbb{Z}, +)$ e $(\mathbb{Q}^*, \cdot)$.
2. Introduzione di D_3.
3. Isometrie determinate da tre punti.
4. $D_3 = \{1, \rho, \rho^2, \sigma, \rho\sigma, \rho^2\sigma\}$.
5. Esempio: $(D_3, \circ)$.
6. Definizione di gruppo.
7. Definizione: zero e inversi destri.
8. Definizione: equazioni.

Il concetto di gruppo: conclusioni

È possibile accorciare il percorso in vari modi, per ovviarne alla lunghezza.
I seguenti hanno diversi pro e contro.

- Uno si concentra sull'esempio dato da $(D_3, \circ)$:

$$\text{Esempi numerici} \to \text{Dimostrazioni su } D_3 \to \text{Definizione di gruppo},$$

- l'altro sulle definizioni alternative di gruppo:

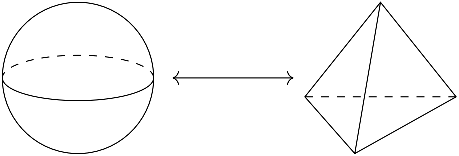
$$\mathbb{Z}, \mathbb{Q}^* \text{ e } D_3 \text{ (no dim.)} \to \text{Def. gruppo} \to \text{Dim. def. altern. di gruppo.}$$

Il concetto di omeomorfismo

L'obbiettivo del percorso è fornire un'idea di cosa sia la topologia, definendo i concetti di spazio topologico e omeomorfismo.

Il concetto di omeomorfismo

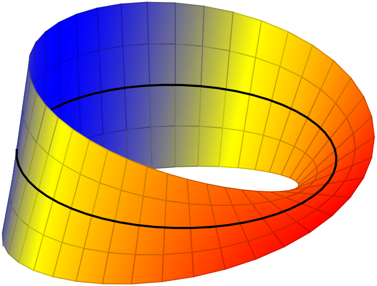
- Si inizia dando una spiegazione informale di cosa sia un omeomorfismo.
- Viene dato l'esempio di due superfici omeomorfe apparentemente molto diverse, tetraedro e sfera;
- ne vengono messe in evidenza le proprietà comuni.
- Attraverso queste è spiegata l'utilità di considerare, in certi problemi, la sfera e il tetraedro come se fossero lo stesso tipo di oggetto.



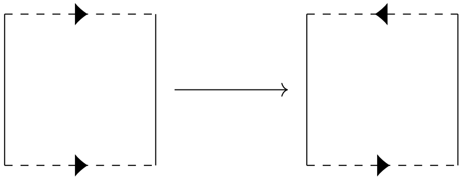
Il concetto di omeomorfismo

Esempio di oggetti non omeomorfi: superficie laterale cilindrica e nastro di Möbius.

- Si introduce brevemente il nastro di Möbius.



- Si mostra come, secondo la definizione intuitiva data, non sia omeomorfo ad una superficie laterale cilindrica.



Il concetto di omeomorfismo

Definiamo gli spazi metrici (X, d_X), in modo da poterli usare come esempio nel parlare di spazi topologici.
Ne vengono quindi descritti due, dimostrando la loro aderenza alla definizione:

- la retta $(\mathbb{R}, d_\mathbb{R})$, con

$$\begin{aligned} d_\mathbb{R} : \mathbb{R} \times \mathbb{R} &\longrightarrow \mathbb{R}^+ \\ (x, y) &\longmapsto |x - y|, \end{aligned}$$

- la metrica discreta (X, d_X), con

$$\begin{aligned} d_X : X \times X &\longrightarrow \mathbb{R}^+ \\ (x, y) &\longmapsto d_X(x, y) := \begin{cases} 0 & \text{for } x = y \\ 1 & \text{for } x \neq y \end{cases}. \end{aligned}$$

Il concetto di omeomorfismo

Definiamo:

- le bolle

$$B_\epsilon(x_0) := \{x \in X \mid d_X(x, x_0) < \epsilon\},$$

- la controimmagine

$$f^{\leftarrow}(S) = \{x \in X \mid f(x) \in S\},$$

- e la continuità per mappe $f : X \to Y$ tra spazi metrici, sfruttando le bolle.

$$f^{\leftarrow}(B_\epsilon(f(x_0))) \supseteq B_\delta(x_0)$$

Si mostra come, con $(X, d_X) = (Y, d_Y) = (\mathbb{R}, d_\mathbb{R})$, questa equivalga alla continuità nota ai ragazzi.

Il concetto di omeomorfismo

Dopo aver dato la definizione di aperti e chiusi in spazi metrici (X, d_X):

- si fa notare come $\varnothing$ e X siano chiusi e aperti,
- si dimostra la seguente proposizione:

Proposizione

Siano (X, d_X) e (Y, d_Y) spazi metrici, sia $f : X \to Y$ un'applicazione. f è continua se e solo se, per ogni $V \subseteq Y$ aperto, $f^{\leftarrow}(V)$ è aperto in X.

La definizione di continuità può essere quindi data usano gli aperti.

Il concetto di omeomorfismo

- Vengono esposte le seguenti proprietà dell'insieme degli aperti di (X, d_X), $\mathcal{U}_X \subseteq \mathcal{P}(X)$:
  1. $X, \varnothing \subseteq \mathcal{U}_X$,
  2. $A_1, A_2 \in \mathcal{U}_X \Rightarrow A_1 \cap A_2 \in \mathcal{U}_X$,
  3. $\{A_j\}_{j \in J} \subseteq \mathcal{U}_X \Rightarrow \bigcup_{j \in J} A_j \in \mathcal{U}_X$.
- Viene quindi motivato e definito il concetto di spazio topologico.
- Viene data l'ultima definizione:

Definizione

Siano $(X,\mathcal{U}_X)$ e $(Y,\mathcal{U}_Y)$ due spazi topologici. Si ha $X \approx Y$ (X è omeomorfo a Y) se esistono $f : X \to Y$ e $g : Y \to X$ continue, tali che $f \circ g = Id_Y$ e $g \circ f = Id_X$.

Il concetto di omeomorfismo

Esempio finale: Raccogliamo le lettere dell'alfabeto latino rispetto alla relazione di omeomorfismo.

$$\{C, G, I, J, L, M, N, S, U, V, W, Z\}$$

$$\{D, O\},\ \{P, Q\} \text{ e } \{A, R\}$$

$$\{H, K\}$$

$$\{E, F, Y, T\} \text{ e } \{X\}$$

$$\{B\}$$

Il concetto di omeomorfismo: conclusioni

Riassumendo:

1. Introduzione informale: omeomorfismo.
2. Esempi: sfera e tetraedro.
3. Esempi: sup. laterale cilindrica e nastro di Möbius.
4. Definizione: spazi metrici.
5. Esempi: la retta e la metrica discreta.
6. Definizione di bolle e continuità.
7. Definizione di aperti e chiusi, esempio $\varnothing$, X.
8. Proposizione: continuità per aperti.
9. Insieme degli aperti di sp. metrico e spazio topologico.
10. Definizione di omeomorfismo ed esempio alfabeto.

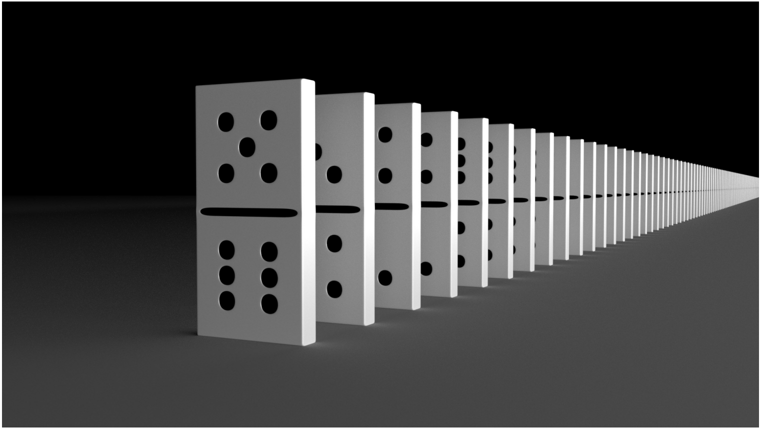
Principio di induzione e teorema fondamentale dell'aritmetica

Obiettivi:

- dimostrare il teorema fondamentale dell'aritmetica,
- fornire esempi di vari tipi di dimostrazione.

Induzione e teorema fondamentale dell'aritmetica

Dopo una breve introduzione (citati Gauss e Euclide), viene descritto il primo principio di induzione, attraverso un paragone con tessere del domino.



Vengono quindi dimostrati il primo principio di induzione e il secondo:

Teorema

Sia $P(n)$ una proprietà dipendente da $n \in \mathbb{Z}$ e sia dato $n_0 \in \mathbb{Z}$. Se valgono le seguenti condizioni:

- *$P(n_0)$ è vera;*
- *per ogni $n \in \mathbb{Z}$ tale che $n \geq n_0$ e che $P(k)$ sia verificata per ogni $n_0 \leq k \leq n$, si ha che $P(k+1)$ è vera;*

allora $P(n)$ è vera per ogni $n \in \mathbb{Z}$ maggiore di n_0.

Induzione e teorema fondamentale dell'aritmetica

- Si dimostra per induzione:

Proposizione

Ogni intero $n > 1$ *è rappresentabile come prodotto di numeri primi.*

- Si definisce:

Definizione

Dati due interi $a, b \in \mathbb{N}$, *il massimo comune divisore tra* a *e* b *è un intero* $d > 0$ *che divide sia* a *che* b *e tale che, se* $c \mid a$ *e* $c \mid b$, *allora* $c \mid d$. *In tal caso si scrive* $(a, b) := d$. *Se* $(a, b) = 1$, a *e* b *sono detti primi fra loro.*

Si dimostrano:

- l'identità di Bezout,

Teorema

Siano $a, b \in \mathbb{N}$ due interi positivi non nulli, allora il loro massimo comune divisore esiste. Esistono inoltre $u, v \in \mathbb{Z}$ tali che $(a, b) = au + bv$.

- il Lemma di Euclide.

Teorema

p è primo se e solo se, per ogni $a, b \in \mathbb{N}$, $p \mid ab$ implica $p \mid a$ o $p \mid b$.

Induzione e teorema fondamentale dell'aritmetica

- Spiegato come il Lemma di Euclide fornisca la definizione di primo usata in matematica moderna,
- si mostra come non sia equivalente alla definizione "usuale" in alcuni contesti:

Esempio

$$\mathbb{Z}[\sqrt{-5}] := \{n + m\sqrt{-5} \mid n, m \in \mathbb{Z}\}.$$

Per $2 \in \mathbb{Z}[\sqrt{-5}]$, si ha che 2 è divisibile solo per 1 e se stesso. Ma, nonostante $2 \mid (1+\sqrt{-5})(1-\sqrt{-5}) = 1 - (-5) = 6$, 2 non divide ne $(1+\sqrt{-5})$ ne $(1-\sqrt{-5})$.

Siamo ora pronti per la dimostrazione del teorema fondamentale dell'aritmetica. Ci limitiamo a dimostrare l'unicità della fattorizzazione.

Teorema

Per ogni intero positivo $n > 1$, esiste ed è unica la fattorizzazione in numeri primi, a meno dell'ordine dei fattori.

Dim. (per induzione su n)

1. Per $n = 2$ ✓
2. Supponiamo unica la fattorizzazione in primi per ogni k intero, $1 < k < n$.
3. Siano $p_1 \cdot \ldots \cdot p_l = q_1 \cdot \ldots \cdot q_r$ due fattorizzazioni di n.
4. Poiché $p_1 \mid n = q_1 \cdot \ldots \cdot q_r$ ed è primo, esiste $\lambda \in \{1, \ldots, r\}$ tale che $p_1 \mid q_\lambda$; tuttavia, essendo q_λ primo, $p_1 = q_\lambda$.

5. L'intero positivo $\frac{n}{q_\lambda} < n$ ammette due fattorizzazioni in primi:

$$p_2 \cdot \ldots \cdot p_l = q_1 \cdot \ldots \cdot q_{\lambda-1} q_{\lambda+1} \cdot \ldots \cdot q_r = \frac{n}{p_\lambda}.$$

6. Ipotesi induttiva: la fattorizzazione di tale numero è unica.Allora, per ogni indice $i \in \{2, \ldots, l\}$, esiste un unico indice $j \in \{1, \ldots, r\} \setminus \{\lambda\}$ tale che $p_i = q_j$.
7. Conseguenza di ciò è l'uguaglianza fra le fattorizzazioni in primi di n (per ogni indice $i \in \{1, 2, \ldots, l\}$ esiste un unico indice $j \in \{1, \ldots, r\}$ tale che $p_i = q_j$, dove, in particolare, $p_1 = q_\lambda$).
8. Abbiamo quindi dimostrato per induzione che la fattorizzazione in primi è unica per ogni intero $n > 1$. $\square$

Induzione e TFA: conclusioni

Riassumendo:

1. Descrizione e dimostrazione del primo principio di induzione.
2. Dimostrazione del secondo principio di induzione.
3. Prima parte del teorema fondamentale
4. Definizione MCD.
5. Identità di Bezout.
6. Lemma di Euclide.
7. Esempio $\mathbb{Z}[\sqrt{-5}]$.
8. Teorema fondamentale.

Bibliografia

Nella redazione delle note sono state consultate le seguenti fonti:

- Richard Courant e Herbert Robbins, "What Is Mathematics?", Oxford University Press (1941)
- Gerardo con Diaz, "Mathematical Induction", Harvard University (2013)
- G.H.Miller, "The evolution of group theory", The Mathematics Teacher, National Council of Teachers of Mathematics (1964)

Dimostrazioni e idee sono inoltre state tratte dai seguenti corsi della laurea triennale in Matematica di Unife:

- Algebra (2017/2018), C.Menini e F.Stumbo
- Analisi matematica I (2017/2018), C.Boiti
- Geometria II (2018/2019), M.Mella
- Number theory (2019/2020), F.A.Ellia
- Teoria dei numeri e fondamenti di crittografia (2018/2019), P.Codecà