Appunti del corso di Aritmetica

tenutosi sotto la supervisione dei proff. Gaiffi e D'Adderio

Gabriel Antonio Videtta
g.videtta1@studenti.unipi.it

A.A. 2022/2023

Università di Pisa

Premessa

Affinché possano chiamarsi queste dispense, voglio mettere alcuni punti in chiaro. Non sono un professore, né ho mai insegnato nella mia vita, per quanto punti a farlo, pertanto queste dispense non forniscono né coprono l'esperienza che un professore potrebbe condividere durante un vero e proprio corso universitario.

Piuttosto queste dispense hanno lo scopo di immagazzinare e incapsulare le nozioni che un normale corso di Aritmetica – o Algebra 1 che sia – potrebbe fornire, e non hanno quindi la pretesa di sostituirsi a uno studio più approfondito e personale.

Naturalmente sono accettati a braccia aperte suggerimenti e correzioni (che potete inviare alla mia mail, `g.videtta1@studenti.unipi.it`).

Ringraziamenti

Chiaramente ci sono alcuni ringraziamenti che ho piacere a fare. Innanzitutto vorrei ringraziare il mio caro amico **Diego Monaco** (`d.monaco2@studenti.unipi.it`), da cui ho preso pesante ispirazione per lo stile e il contenuto di queste dispense (trovate difatti i suoi appunti su GitHub).

In secondo luogo, voglio ringraziare **Evan Chen**, dal quale ho reperito già pronti i fogli di stile per queste dispense (e che anche voi potete trovare sul suo sito personale).

Indice

§1 Gruppi

§1.1 Definizione e motivazione

Innanzitutto, prima di dare una definizione formale, un **gruppo** è una struttura algebrica, ossia un insieme di oggetti di varia natura che rispettano alcune determinate regole.

Il motivo (con ogni probabilità l'unico) per cui la teoria dei gruppi risulta interessante è la facilità con cui un'astrazione come la struttura di gruppo permette di desumere teoremi universali per oggetti matematici apparentemente scollegati.

Infatti, dimostrato un teorema in modo astratto per un gruppo generico, esso è valido per ogni gruppo. Per quanto questo fatto risulti di una banalità assoluta, esso è di fondamentale aiuto nello studio della matematica. Si pensi ad esempio all' aritmetica modulare, o alle funzioni bigettive, o ancora alle trasformazioni del piano: tutte queste nozioni condividono teoremi e metodi che si fondano su una stessa logica. Come vedremo, esse condividono la natura di gruppo.

Definizione 1.1. Dato un insieme non vuoto G, $(G, \cdot)$ si dice **gruppo** se data un'operazione ben definita $\cdot : G \times G \to G$ essa è t.c:

- (**associatività**) $\forall\, a, b, c \in G,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- (**esistenza dell'elem. neutro**) $\exists\, e \in G \mid a \cdot e = a = e \cdot a\ \ \forall\, a \in G$
- (**esistenza dell'elem. inverso**) $\forall\, a \in G,\ \exists\, a^{-1} \in G \mid a \cdot a^{-1} = e$

Osservazione 1.2 — Nella definizione di gruppo si è chiaramente specificato che l'operazione dev'essere ben definita e, soprattutto, che l'insieme G dev'essere chiuso rispetto ad esso.

Pertanto, non è sufficiente aver verificato le tre proprietà sopraelencate senza aver prima verificato che l'operazione sia effettivamente un'operazione di gruppo.

Esempio 1.3 (Gruppo ciclico elementare)

L'insieme $\mathbb{Z}/n\mathbb{Z}$ (che talvolta indicheremo semplicemente come $\mathbb{Z}_n$) degli interi modulo n è un gruppo con l'operazione di somma $+$. Infatti:

- $\forall\, [a]_n, [b]_n \in \mathbb{Z}/n\mathbb{Z},\ [a]_n + [b]_n = [a+b]_n \in \mathbb{Z}/n\mathbb{Z}$ (*chiusura rispetto all'operazione*)
- $\forall\, [a]_n, [b]_n, [c]_n \in \mathbb{Z}/n\mathbb{Z},\ ([a]_n + [b]_n) + [c]_n = [a+b]_n + [c]_n = [a+b+c]_n = [a]_n + [b+c]_n = [a]_n + ([b]_n + [c]_n)$ (*associatività*)
- $\forall\, [a]_n \in \mathbb{Z}/n\mathbb{Z},\ [a]_n + 0 = [a]_n$ (*esistenza dell'elem. neutro*)
- $\forall\, [a]_n \in \mathbb{Z}/n\mathbb{Z},\ \exists\, [-a]_n \in \mathbb{Z}/n\mathbb{Z} \mid [a]_n + [-a]_n = 0$ (*esistenza dell'elem. inverso*)

Esempio 1.4 (Gruppo simmetrico)
L'insieme S_n delle funzioni bigettive da $X_n = \{1, 2, \dots, n\}$ in sé stesso è un gruppo rispetto all'operazione di composizione, detto **gruppo simmetrico**. Infatti:

- $\forall\, f, g \in S_n,\ f \circ g \in S_n$ (*chiusura rispetto all'operazione*)
- $\forall\, f, g, h \in S_n,\ (f \circ g) \circ h = f \circ (g \circ h)$ (*associatività*)
- $\exists\, e = \mathrm{Id} \in S_n \mid f \circ e = f = e \circ f\ \forall\, f \in S_n$ (*esistenza dell'elem. neutro*)
- $\forall\, f \in S_n,\ \exists\, f^{-1} \in S_n \mid f \circ f^{-1} = e$ (*esistenza dell'elem. inverso*)

Le proprietà date dalla definizione di un gruppo ci permettono immediatamente di desumere altre proprietà fondamentali, e che sulle quali faremo affidamento d'ora in poi.

Teorema 1.5
L'inverso a^{-1} di un elemento a di un gruppo G è unico.

Dimostrazione. Supponiamo che b e c siano due elementi inversi distinti di a. Allora $b = b \cdot e = b \cdot \underbrace{(a \cdot c)}_{=e} = \underbrace{(b \cdot a)}_{=e} \cdot c = c$, ↯. Pertanto l'inverso è unico. □

Teorema 1.6
L'inverso dell'inverso $\left(a^{-1}\right)^{-1}$ è pari a a.

Dimostrazione. Dal momento che l'inverso è unico (per il **Teorema 1.5**), $\left(a^{-1}\right)^{-1} a^{-1} = e \implies \left(a^{-1}\right)^{-1} = a$. □

Teorema 1.7
L'inverso di ab è $b^{-1}a^{-1}$.

Dimostrazione. Si verifica facilmente che $abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$. Poiché l'inverso è unico (per il **Teorema 1.5**), allora $(ab)^{-1} = b^{-1}a^{-1}$. □

Osservazione 1.8 — In realtà, sebbene a prima vista potrebbe sembrare inusuale l'inversione dei due fattori nell'ultima identità, essa è una conseguenza del modo in cui operiamo naturalmente. Si prenda per esempio la composizione $f \circ g$, per ottenere l'identità è necessario prima decomporre f, l'ultima funzione aggiunta, ed infine g, ossia seguendo l'ordine da sinistra a destra.

Nel corso di Geometria vi sarà spiegato come anche la matrici si comportano in questo modo (non è un caso, dal momento che anch'esse, sotto talune condizioni, formano un gruppo, il cosiddetto **gruppo lineare** $\mathrm{GL}_n(\mathbb{K})$).

Teorema 1.9

Un'equazione della forma $ax = bx$ è vera se e solo se $a = b$.

Dimostrazione. Infatti, moltiplicando per l'inverso di x, $ax = bx \iff axx^{-1} = bxx^{-1} \iff a = b$. □