Tutoraggio di Algebra 2

Anno accademico 2026–2027

Docente del corso: Prof. Andrea Loi
Tutor: Marco Damele

Foglio 3

Enunciati e soluzioni commentate

Esercizi 3.1, 3.7, 3.8, 3.10 e 2.8.

Testo di riferimento: Andrea Loi, *Appunti sulla teoria elementare dei gruppi*, capitolo 3, sezione 3.6, pp. 71–73; per l'esercizio 2.8, capitolo 2, sezione 2.5, p. 49 dell'edizione fornita.

Esercizio 3.1 Riconoscere i sottogruppi

Enunciato

Dire quali dei seguenti insiemi H sono sottogruppi del gruppo G indicato:

1. $G = (\mathbb{R}, +)$, $\quad H = \{\ln a \mid a \in \mathbb{Q},\ a > 0\}$;
2. $G = (\mathbb{R}, +)$, $\quad H = \{\ln n \mid n \in \mathbb{Z},\ n > 0\}$;
3. $G = (\mathbb{R}, +)$, $\quad H = \{x \in \mathbb{R} \mid \tan x \in \mathbb{Q}\}$;
4. $G = (\mathbb{R}^*, \cdot)$, $\quad H = \{2^n 3^m \mid m, n \in \mathbb{Z}\}$;
5. $G = (\mathbb{R} \times \mathbb{R}, +)$, $\quad H = \{(x, y) \mid y = 2x\}$.

Nel punto 3 si intende che $\tan x$ sia definita, oltre che razionale.

Soluzione

Idea della soluzione. Per dimostrare che un insieme è un sottogruppo, verifichiamo un criterio di sottogruppo. Per dimostrare che non lo è, basta trovare un inverso mancante oppure due elementi il cui prodotto non appartiene all'insieme.

Il criterio da usare. Un sottoinsieme non vuoto H di un gruppo è un sottogruppo se $ab^{-1} \in H$ per ogni $a, b \in H$. In notazione additiva la condizione diventa $a - b \in H$.

1. Logaritmi di razionali positivi: sì. Poiché $0 = \ln 1 \in H$, l'insieme è non vuoto. Se $\ln a, \ln b \in H$, allora

$$\ln a - \ln b = \ln\left(\frac{a}{b}\right) \in H,$$

perché a/b è ancora un numero razionale positivo. Il criterio si applica.

2. Logaritmi di interi positivi: no. Abbiamo $\ln 2 \in H$, ma il suo opposto non appartiene a H. Infatti

$$-\ln 2 = \ln(1/2) < 0,$$

mentre $\ln n \geq 0$ per ogni intero $n > 0$. Manca quindi la chiusura rispetto agli opposti.

Esercizio 3.1 Soluzione (continuazione)

3. Argomenti con tangente razionale: no. L'angolo $\pi/4$ appartiene a H, perché $\tan(\pi/4) = 1 \in \mathbb{Q}$. Tuttavia

$$\frac{\pi}{4} + \frac{\pi}{4} = \frac{\pi}{2} \notin H,$$

perché la tangente non è definita in $\pi/2$. Dunque H non è chiuso rispetto alla somma.

Questo esempio spiega anche perché non basta usare formalmente la formula

$$\tan(x+y) = \frac{\tan x + \tan y}{1 - \tan x \tan y}:$$

il denominatore può essere nullo, come accade proprio per $x = y = \pi/4$.

4. Prodotti di potenze intere di 2 e 3: sì. L'elemento neutro appartiene all'insieme, perché $1 = 2^0 3^0$. Se

$$a = 2^n 3^m, \qquad b = 2^p 3^q, \qquad n, m, p, q \in \mathbb{Z},$$

allora

$$ab^{-1} = 2^n 3^m \, 2^{-p} 3^{-q} = 2^{n-p} 3^{m-q} \in H.$$

Gli esponenti $n - p$ e $m - q$ sono ancora interi, quindi $H \leq \mathbb{R}^*$.

5. La retta $y = 2x$: sì. Scriviamo l'insieme nella forma

$$H = \{(t, 2t) \mid t \in \mathbb{R}\}.$$

Esso contiene $(0, 0)$. Inoltre, per ogni $t, u \in \mathbb{R}$,

$$(t, 2t) - (u, 2u) = (t - u, 2(t - u)) \in H.$$

Quindi H è un sottogruppo additivo di $\mathbb{R}^2$.

Riepilogo

Punto	Sottogruppo?	Verifica decisiva
1	Sì	Il rapporto di due razionali positivi è razionale positivo.
2	No	$\ln 2 \in H$, ma $-\ln 2 \notin H$.
3	No	$\pi/4 \in H$, ma $\pi/4 + \pi/4 \notin H$.
4	Sì	Sottrarre gli esponenti conserva la forma $2^n 3^m$.
5	Sì	La differenza di due punti della retta è ancora sulla retta.

Da ricordare. Il fatto che H sia chiuso rispetto all'operazione non basta, da solo, a renderlo un sottogruppo. Nel punto 2 la somma di due elementi di H è ancora in H, perché $\ln n + \ln m = \ln(nm)$; sono gli opposti a mancare.

Esercizio 3.7 Elementi di ordine due nel gruppo diedrale

Enunciato

Sia $G = D_n$, $n \geq 3$, il gruppo diedrale. Dimostrare che G ha esattamente n elementi di ordine 2 se e solo se n è dispari. Nel caso in cui n sia dispari, dimostrare che gli n elementi di G che non hanno ordine 2 formano un sottogruppo abeliano di G.

Soluzione

Idea della soluzione. Separiamo le simmetrie del poligono in rotazioni e riflessioni. Tutte le riflessioni hanno ordine 2; tra le rotazioni, soltanto il mezzo giro può avere ordine 2.

Usiamo la convenzione del testo: D_n è il gruppo delle simmetrie del poligono regolare con n lati e ha ordine $2n$. Siano r la rotazione di angolo $2\pi/n$ e s una riflessione. Allora

$$D_n = \{1, r, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}, \qquad r^n = 1, \quad s^2 = 1, \quad srs = r^{-1}.$$

1. Le n riflessioni hanno ordine 2. La relazione $sr^k s = r^{-k}$ dà

$$(sr^k)^2 = sr^k sr^k = r^{-k} r^k = 1 \qquad (0 \leq k < n).$$

Poiché una riflessione non è l'identità, ciascuno degli n elementi sr^k ha ordine esattamente 2.

2. Quando una rotazione ha ordine 2? Una rotazione r^k ha ordine 2 se e solo se

$$r^{2k} = 1 \quad \text{e} \quad r^k \neq 1.$$

Per $0 \leq k < n$, queste condizioni equivalgono a $n \mid 2k$ e $k \neq 0$.

- Se n è dispari, $n \mid 2k$ implica $n \mid k$: nessuna rotazione ha ordine 2.
- Se n è pari, l'unica possibilità non nulla è $k = n/2$. Compare quindi un ulteriore elemento di ordine 2, la rotazione $r^{n/2}$ di angolo π.

Pertanto

$$\boxed{\#\{g \in D_n \mid o(g) = 2\} = \begin{cases} n, & n \text{ dispari}, \\ n+1, & n \text{ pari}. \end{cases}}$$

Questo dimostra l'equivalenza richiesta.

3. Gli elementi che non hanno ordine 2, per n dispari. Sono esattamente le rotazioni, quindi formano il sottogruppo

$$\langle r \rangle = \{1, r, \dots, r^{n-1}\}.$$

Esso ha ordine n ed è ciclico; in particolare è abeliano, perché $r^i r^j = r^{i+j} = r^{j+i} = r^j r^i$.

Da ricordare. L'identità ha ordine 1: appartiene dunque all'insieme degli elementi che *non* hanno ordine 2.

Esercizio 3.8 Permutazioni che conservano un sottoinsieme

Enunciato

Sia X un insieme finito e sia $A \subseteq X$. Sia H il sottoinsieme di S_X costituito dalle permutazioni f tali che $f(x) \in A$ per ogni $x \in A$.

1. Dimostrare che H è un sottogruppo di S_X.
2. Fornire un esempio in cui la conclusione del punto precedente non vale se X è infinito.

Soluzione

Idea della soluzione. La condizione data è $f(A) \subseteq A$. Se A è finito, l'iniettività di f forza $f(A) = A$, e quindi anche l'inversa conserva A. Per un insieme infinito l'inclusione può invece essere stretta.

1. Il caso finito. Scriviamo

$$H = \{f \in S_X \mid f(A) \subseteq A\}.$$

Verifichiamo le proprietà di sottogruppo, con operazione la composizione.

- **Identità.** $\mathrm{id}_X(A) = A$, quindi $\mathrm{id}_X \in H$.
- **Composizione.** Se $f, g \in H$ e $x \in A$, allora $g(x) \in A$ e dunque $f(g(x)) \in A$. Pertanto $f \circ g \in H$.
- **Inverse.** Se $f \in H$, la restrizione $f|_A$ è iniettiva, perché f è una permutazione di X. Quindi $|f(A)| = |A|$. Dato che A è finito e $f(A) \subseteq A$, otteniamo $f(A) = A$. Applicando f^{-1} ai due insiemi,

  $$f^{-1}(A) = A.$$

  In particolare $f^{-1}(A) \subseteq A$, perciò $f^{-1} \in H$.

Concludiamo che $H \leq S_X$. Questo gruppo è lo *stabilizzatore insiemistico* di A: i suoi elementi possono permutare i punti di A, senza doverli fissare uno per uno.

2. Un controesempio infinito. Prendiamo

$$X = \mathbb{Z}, \qquad A = \{0, 1, 2, \ldots\}, \qquad f(k) = k + 1.$$

La funzione f è una permutazione di $\mathbb{Z}$, con inversa $f^{-1}(k) = k - 1$. Inoltre

$$f(A) = \{1, 2, 3, \ldots\} \subsetneq A,$$

quindi $f \in H$. L'inversa, invece, manda $0 \in A$ in $-1 \notin A$: dunque $f^{-1} \notin H$. L'insieme H non è un sottogruppo di $S_{\mathbb{Z}}$.

Da ricordare. Nel primo punto basta in realtà che sia finito A, anche se X è infinito. Per un qualsiasi A, finito o infinito, la condizione più forte $f(A) = A$ definisce sempre un sottogruppo di S_X.

Esercizio 3.10 Moltiplicatività dell'indice

Enunciato

Siano H e K sottogruppi di un gruppo finito G, con

$$H \leq K \leq G.$$

Dimostrare che

$$[G : H] = [G : K]\,[K : H].$$

Soluzione

Idea della soluzione. L'indice di un sottogruppo in un gruppo finito è il rapporto dei loro ordini. Inserendo $|K|$ tra $|G|$ e $|H|$, la formula segue immediatamente.

1. La dimostrazione con il teorema di Lagrange. Le classi laterali di H in G hanno tutte $|H|$ elementi e costituiscono una partizione di G. Quindi

$$[G : H] = \frac{|G|}{|H|}.$$

Applicando la stessa formula a $K \leq G$ e a $H \leq K$, otteniamo

$$[G : K] = \frac{|G|}{|K|}, \qquad [K : H] = \frac{|K|}{|H|}.$$

Moltiplicando membro a membro,

$$\boxed{[G : K]\,[K : H] = \frac{|G|}{|K|}\frac{|K|}{|H|} = \frac{|G|}{|H|} = [G : H].}$$

2. Come leggere la formula attraverso le classi laterali. Ogni classe laterale sinistra gK è unione disgiunta di $[K : H]$ classi laterali di H: se

$$K = k_1 H \sqcup \cdots \sqcup k_t H, \qquad t = [K : H],$$

allora, moltiplicando a sinistra per g,

$$gK = gk_1 H \sqcup \cdots \sqcup gk_t H.$$

Le $[G : K]$ classi di K in G si dividono dunque ciascuna in $[K : H]$ classi di H. In totale, le classi di H sono $[G : K][K : H]$.

3. Un esempio in $\mathbb{Z}_{12}$. Con la somma modulo 12, consideriamo

$$G = \mathbb{Z}_{12}, \quad K = \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\}, \quad H = \{\overline{0}, \overline{6}\}.$$

Sono sottogruppi e $H \leq K \leq G$. I loro ordini sono rispettivamente 12, 4 e 2, perciò

$$[G : H] = 6, \qquad [G : K] = 3, \qquad [K : H] = 2, \qquad 6 = 3 \cdot 2.$$

Da ricordare. Non occorre che H o K siano normali: stiamo contando classi laterali, senza attribuire loro una struttura di gruppo quoziente.

Esercizio 2.8 Generare il gruppo simmetrico con l'alterno

Enunciato

Dimostrare che S_n è generato da A_n e da una trasposizione arbitraria τ:

$$S_n = \langle A_n, \tau \rangle.$$

Qui $n \geq 2$, in modo che esistano trasposizioni in S_n.

Soluzione

Idea della soluzione. Ogni permutazione è pari oppure dispari. Quelle pari appartengono già ad A_n; una permutazione dispari diventa pari se la componiamo con una trasposizione.

Ricordiamo che

$$A_n = \{\sigma \in S_n \mid \operatorname{sign}(\sigma) = 1\},$$

mentre una trasposizione ha segno -1 e soddisfa $\tau^2 = \mathrm{id}$. Poniamo

$$L = \langle A_n, \tau \rangle \leq S_n.$$

Per definizione, $A_n \subseteq L$ e $\tau \in L$. Dimostriamo che ogni $\sigma \in S_n$ appartiene a L.

Caso 1: σ è pari. Allora $\sigma \in A_n \subseteq L$.

Caso 2: σ è dispari. La composizione $\sigma \circ \tau$ è pari, perché

$$\operatorname{sign}(\sigma \circ \tau) = \operatorname{sign}(\sigma)\operatorname{sign}(\tau) = (-1)(-1) = 1.$$

Quindi $\alpha := \sigma \circ \tau \in A_n$. Usando $\tau^2 = \mathrm{id}$, ricaviamo

$$\sigma = (\sigma \circ \tau) \circ \tau = \alpha \circ \tau \in L.$$

In entrambi i casi $\sigma \in L$. Pertanto

$$\boxed{S_n = \langle A_n, \tau \rangle.}$$