Tutoraggio di Algebra 2

Anno accademico 2026–2027

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

Foglio 4

Enunciati e soluzioni commentate

Esercizi 4.1, 4.6, 4.7 e 4.10.

Testo di riferimento: Andrea Loi, *Appunti sulla teoria elementare dei gruppi*, capitolo 4, sezione 4.5, pp. 87–89 dell'edizione fornita.

Esercizio 4.1 Matrici triangolari, centro e normalità

Enunciato

Sia

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbb{Z} \right\}.$$

Dimostrare che:

1. G è un sottogruppo di $\mathrm{GL}_3(\mathbb{Q})$;
2. il centro di G è
$$Z(G) = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \middle| \, b \in \mathbb{Z} \right\};$$
3. l'insieme
$$N = \left\{ \begin{pmatrix} 1 & 2a & 2b \\ 0 & 1 & 2c \\ 0 & 0 & 1 \end{pmatrix} \middle| \, a, b, c \in \mathbb{Z} \right\}$$
è un sottogruppo normale di G.

Soluzione

Idea della soluzione. Scriviamo una matrice di G mediante i suoi tre parametri. La formula del prodotto permette di verificare la proprietà di sottogruppo, riconoscere gli elementi centrali e calcolare i coniugati degli elementi di N.

Per alleggerire la notazione, poniamo

$$M(a, b, c) := \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

I parametri a, b, c individuano univocamente la matrice: due matrici di questa forma sono uguali se e solo se coincidono tutti e tre i parametri.

Esercizio 4.1 Soluzione (continuazione)

1. Verifica che $G \leq \mathrm{GL}_3(\mathbb{Q})$. Ogni $M(a,b,c)$ ha entrate razionali e determinante 1, perché è triangolare con tutti gli elementi diagonali uguali a 1. Pertanto $G \subseteq \mathrm{GL}_3(\mathbb{Q})$.

L'identità è $I_3 = M(0,0,0) \in G$. Calcolando il prodotto, otteniamo

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b+b'+ac' \\ 0 & 1 & c+c' \\ 0 & 0 & 1 \end{pmatrix}.$$

Dunque

$$\boxed{M(a,b,c)M(a',b',c') = M(a+a',\, b+b'+ac',\, c+c').} \tag{1}$$

Se i parametri dei due fattori sono interi, lo sono anche quelli del prodotto. Quindi G è chiuso rispetto alla moltiplicazione.

Per trovare l'inversa, cerchiamo $M(u,v,w)$ tale che $M(a,b,c)M(u,v,w) = I_3$. La formula (1) dà

$$a+u=0, \qquad c+w=0, \qquad b+v+aw=0.$$

Segue che $u=-a$, $w=-c$ e $v=ac-b$. Pertanto

$$\boxed{M(a,b,c)^{-1} = M(-a,\, ac-b,\, -c) \in G.} \tag{2}$$

Abbiamo verificato identità, chiusura e presenza degli inversi: G è un sottogruppo di $\mathrm{GL}_3(\mathbb{Q})$. È anche proprio: la matrice $\mathrm{diag}(2,1,1)$ appartiene a $\mathrm{GL}_3(\mathbb{Q})$ ma non a G.

2. Calcolo del centro. Ricordiamo che

$$Z(G) = \{g \in G \mid gh = hg \text{ per ogni } h \in G\}.$$

Confrontiamo i prodotti nei due ordini:

$$\begin{aligned} M(a,b,c)M(a',b',c') &= M(a+a',\, b+b'+ac',\, c+c'), \\ M(a',b',c')M(a,b,c) &= M(a+a',\, b+b'+a'c,\, c+c'). \end{aligned}$$

Le due matrici coincidono se e solo se

$$ac' = a'c. \tag{3}$$

Affinché $M(a,b,c)$ sia centrale, la (3) deve valere *per ogni* scelta di $a',b',c' \in \mathbb{Z}$.

- Scegliendo $a'=0$ e $c'=1$, otteniamo $a=0$.
- Scegliendo $a'=1$ e $c'=0$, otteniamo $c=0$.

Viceversa, se $a=c=0$, la (3) diventa $0=0$ per ogni a',c', senza imporre alcuna condizione su b. Quindi

$$\boxed{Z(G) = \{M(0,b,0) \mid b \in \mathbb{Z}\}.}$$

Esercizio 4.1 Soluzione (continuazione)

3. Il sottogruppo N è normale in G. Con la notazione introdotta,

$$N = \{M(2u, 2v, 2w) \mid u, v, w \in \mathbb{Z}\}.$$

Verifichiamo prima che N sia un sottogruppo, poi che sia normale.

Proprietà di sottogruppo. L'identità appartiene a N. Per la formula (1),

$$\begin{aligned} &M(2u, 2v, 2w)M(2u', 2v', 2w') \\ &\quad = M\big(2(u+u'),\, 2(v+v'+2uw'),\, 2(w+w')\big) \in N. \end{aligned}$$

Anche l'inversa appartiene a N: infatti, per la (2),

$$M(2u, 2v, 2w)^{-1} = M\big(-2u,\, 4uw - 2v,\, -2w\big) = M\big(2(-u),\, 2(2uw - v),\, 2(-w)\big) \in N.$$

I tre parametri restano pari sia nel prodotto sia nell'inversa. Quindi $N \leq G$.

Normalità. Dobbiamo mostrare che $gng^{-1} \in N$ per ogni $g \in G$ e ogni $n \in N$. Prendiamo

$$g = M(a, b, c), \qquad n = M(2u, 2v, 2w).$$

Usando ancora le formule (1) e (2), abbiamo

$$\begin{aligned} gn &= M(a + 2u,\, b + 2v + 2aw,\, c + 2w), \\ g^{-1} &= M(-a,\, ac - b,\, -c). \end{aligned}$$

Pertanto

$$\begin{aligned} gng^{-1} &= M\big(2u,\, b + 2v + 2aw + ac - b - (a + 2u)c,\, 2w\big) \\ &= M\big(2u,\, 2v + 2aw - 2uc,\, 2w\big) \\ &= M\big(2u,\, 2(v + aw - uc),\, 2w\big) \in N. \end{aligned}$$

L'intero $v + aw - uc$ può cambiare, ma il secondo parametro resta pari; il primo e il terzo restano invariati. Dunque $gNg^{-1} \subseteq N$ per ogni $g \in G$, e il criterio di normalità dà

$$\boxed{N \trianglelefteq G.}$$

Da ricordare. Essere normale non significa essere contenuto nel centro. Ad esempio $M(2, 0, 0) \in N$ ma $M(2, 0, 0) \notin Z(G)$, perché il suo primo parametro non è nullo. La normalità richiede che il coniugio conservi il sottogruppo nel suo insieme, non che fissi ogni suo elemento.

Esercizio 4.6 Il centro di un sottogruppo

Enunciato

Sia $Z(G)$ il centro di un gruppo G e sia $H \leq G$. Dimostrare che

$$Z(G) \cap H \subseteq Z(H)$$

e che l'inclusione può essere stretta.

Soluzione

Idea della soluzione. Un elemento che commuta con tutto G commuta anche con gli elementi di H. Il viceversa può fallire: un elemento centrale in H deve commutare soltanto con gli elementi di H.

1. Dimostrazione dell'inclusione. Prendiamo $z \in Z(G) \cap H$. Per appartenenza all'intersezione,

$$z \in H \qquad \text{e} \qquad zg = gz \quad \text{per ogni } g \in G.$$

Poiché $H \leq G$, la seconda condizione vale in particolare per ogni $h \in H$:

$$zh = hz \quad \text{per ogni } h \in H.$$

Quindi z appartiene a H e commuta con tutti gli elementi di H, cioè $z \in Z(H)$. Abbiamo così provato che

$$\boxed{Z(G) \cap H \subseteq Z(H).}$$

2. Un esempio di inclusione stretta. Consideriamo

$$G = S_3, \qquad H = \langle (1\ 2) \rangle = \{\mathrm{id}, (1\ 2)\}.$$

Il sottogruppo H è ciclico, dunque abeliano. Pertanto ogni suo elemento è centrale in H:

$$Z(H) = H.$$

La trasposizione $(1\ 2)$, però, non appartiene a $Z(S_3)$. Infatti, applicando prima il fattore a destra, si ha

$$(1\ 2)(2\ 3) = (1\ 2\ 3), \qquad (2\ 3)(1\ 2) = (1\ 3\ 2).$$

I due prodotti sono diversi, quindi $(1\ 2)$ non commuta con $(2\ 3) \in S_3$. Dato che H contiene soltanto l'identità e $(1\ 2)$, ne segue che

$$Z(S_3) \cap H = \{\mathrm{id}\}.$$

Concludiamo che in questo caso

$$\boxed{Z(G) \cap H = \{\mathrm{id}\} \subsetneq H = Z(H).}$$

Da ricordare. La condizione $z \in Z(H)$ richiede che $z \in H$ e che z commuti con ogni elemento di H. Non impone che commuti con gli elementi di G esterni a H. È questa la ragione dell'inclusione stretta nell'esempio.

Esercizio 4.7 Ordine dei prodotti e coniugio

Enunciato

Dimostrare che

$$o(xy) = o(yx) \qquad \text{per ogni } x, y \in G,$$

dove G è un gruppo. Inoltre, se x è l'unico elemento di G che ha ordine k, dimostrare che $x \in Z(G)$.

Soluzione

Idea della soluzione. Gli elementi xy e yx sono coniugati. Il coniugio conserva l'ordine; quindi, se un elemento è l'unico del suo ordine, tutti i suoi coniugati devono coincidere con esso.

1. I prodotti xy e yx hanno lo stesso ordine. Osserviamo che

$$yx = x^{-1}(xy)x.$$

Per ogni intero $m \geq 1$, le coppie adiacenti xx^{-1} si cancellano nel prodotto di m fattori, e otteniamo

$$(yx)^m = \big(x^{-1}(xy)x\big)^m = x^{-1}(xy)^m x. \tag{4}$$

Ad esempio, per $m = 2$,

$$\big(x^{-1}(xy)x\big)\big(x^{-1}(xy)x\big) = x^{-1}(xy)^2 x.$$

Dalla (4) segue l'equivalenza

$$(yx)^m = 1 \quad \Longleftrightarrow \quad (xy)^m = 1.$$

Dunque i due elementi hanno esattamente gli stessi esponenti positivi che danno l'identità. Se tali esponenti esistono, il più piccolo è il medesimo per entrambi; se non esistono, entrambi hanno ordine infinito. In ogni caso

$$\boxed{o(xy) = o(yx).}$$

2. Un elemento unico del suo ordine è centrale. Sia ora x l'unico elemento di G di ordine k e prendiamo un qualsiasi $g \in G$. Applichiamo la prima parte ai due elementi

$$u = g, \qquad v = xg^{-1}.$$

Poiché $uv = gxg^{-1}$ e $vu = x$, otteniamo

$$o(gxg^{-1}) = o(x) = k.$$

Per l'unicità dell'elemento di ordine k, necessariamente

$$gxg^{-1} = x.$$

Moltiplicando a destra per g, ricaviamo $gx = xg$. Questo vale per ogni $g \in G$; quindi

$$\boxed{x \in Z(G).}$$

Da ricordare. L'uguaglianza degli ordini non implica $xy = yx$: nell'esempio con $x = (1\ 2)$ e $y = (2\ 3)$ dell'esercizio 4.6, i due prodotti sono diversi ma hanno entrambi ordine 3. La dimostrazione non richiede che G sia finito.

Esercizio 4.10 Il centro del gruppo diedrale

Enunciato

Sia

$$D_n = \{1, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}, \qquad n \geq 3,$$

il gruppo diedrale. Dimostrare che

$$Z(D_n) = \begin{cases} \{1\}, & \text{se } n \text{ è dispari,} \\ \{1, r^{n/2}\}, & \text{se } n \text{ è pari.} \end{cases}$$

Suggerimento: mostrare preliminarmente che ogni elemento centrale è una potenza r^k e dedurre che $r^{2k} = 1$.

Soluzione

Idea della soluzione. Un elemento centrale deve commutare sia con r sia con s. Le riflessioni non commutano con r; una rotazione r^k commuta con s esattamente quando n divide $2k$.

Usiamo la convenzione del corso: D_n è il gruppo delle simmetrie del poligono regolare con n lati e ha ordine $2n$. I generatori r e s soddisfano

$$r^n = 1, \qquad o(r) = n, \qquad s^2 = 1, \qquad srs = r^{-1}.$$

In particolare,

$$sr = r^{-1}s, \qquad sr^k = r^{-k}s \quad \text{per ogni } k \in \mathbb{Z}. \tag{5}$$

Ogni elemento di D_n si scrive in modo unico come r^k oppure $r^k s$, con $0 \leq k < n$.

1. Nessuna riflessione è centrale. Sia $x = r^k s$. Per la (5),

$$xr = (r^k s)r = r^{k-1}s, \qquad rx = r(r^k s) = r^{k+1}s.$$

Se x fosse centrale, avremmo $xr = rx$, quindi, cancellando s a destra,

$$r^{k-1} = r^{k+1}.$$

Ne seguirebbe $r^2 = 1$, impossibile perché $o(r) = n \geq 3$. Pertanto

$$Z(D_n) \subseteq \langle r \rangle.$$

2. Quali rotazioni sono centrali? Ogni r^k commuta con r. Per la (5), commuta anche con s se e solo se

$$r^k s = sr^k = r^{-k}s \quad \iff \quad r^k = r^{-k} \quad \iff \quad r^{2k} = 1.$$

Commutare con entrambi i generatori r, s basta per commutare con ogni elemento di D_n. Quindi questa condizione è anche sufficiente e

$$r^k \in Z(D_n) \quad \iff \quad n \mid 2k.$$

Esercizio 4.10 Soluzione (continuazione)

3. Distinguiamo il caso dispari dal caso pari. Ricordiamo che abbiamo scelto $0 \leq k < n$.

- **Se n è dispari**, allora $\gcd(n, 2) = 1$. Dalla divisibilità $n \mid 2k$ segue $n \mid k$, dunque $k = 0$. L'unica rotazione centrale è $r^0 = 1$:

$$\boxed{Z(D_n) = \{1\} \qquad (n \text{ dispari}).}$$

- **Se n è pari**, scriviamo $n = 2m$. Allora

$$n \mid 2k \iff 2m \mid 2k \iff m \mid k.$$

Nell'intervallo $0 \leq k < 2m$ le sole possibilità sono $k = 0$ e $k = m = n/2$. Entrambe soddisfano la condizione trovata, perciò

$$\boxed{Z(D_n) = \{1, r^{n/2}\} \qquad (n \text{ pari}).}$$

Interpretazione geometrica. Se n è pari, $r^{n/2}$ è la rotazione di angolo

$$\frac{n}{2} \cdot \frac{2\pi}{n} = \pi,$$

cioè il mezzo giro. La relazione $sr^k s = r^{-k}$ dice che coniugare una rotazione mediante una riflessione ne inverte il verso. Il mezzo giro coincide con la propria inversa, e per questo commuta anche con le riflessioni.

Se n è dispari, nessuna potenza di r, tranne l'identità, coincide con la propria inversa.

Due esempi.

Gruppo	Simmetrie del poligono	Centro
D_3	Triangolo equilatero	$\{1\}$
D_4	Quadrato	$\{1, r^2\}$

Da ricordare. Tutte le riflessioni hanno ordine 2, ma nessuna è centrale per $n \geq 3$. Avere ordine 2 non basta per appartenere al centro: occorre commutare con tutti gli elementi del gruppo.