Complementi di Algebra 1

APPUNTI DEL CORSO DI ALGEBRA 1 TENUTO
DALLA PROF. DEL CORSO E DAL PROF. LOMBARDO

Leonardo Migliorini
l.migliorini@studenti.unipi.it

Anno Accademico 2022-23

Indice

§1 Insiemi di generatori

Definizione 1.1. Dati un gruppo G e $x_1, \ldots, x_n$ elementi di G, chiamiamo **sottogruppo generato** da $x_1, \ldots, x_n$ il più piccolo sottogruppo $\langle x_1, \ldots x_n \rangle$ di G contenente $x_1, \ldots, x_n$, cioè

$$\langle x_1, \ldots, x_n \rangle = \bigcap_{\substack{H \leqslant G \\ \{x_1, \ldots, x_n\} \subseteq H}} H$$

Osservazione 1.2 — La definizione è ben posta, infatti l'intersezione avviene su una famiglia non vuota di insiemi dal momento che G è un sottogruppo di se stesso contenente $x_1, \ldots, x_n$. Inoltre l'intersezione non è vuota in quanto contiene almeno l'identità e gli elementi $x_1, \ldots, x_n$.

La definizione data non dà informazioni su come sono fatti gli elementi di $\langle x_1, \ldots, x_n \rangle$, cerchiamo quindi di caratterizzare in modo diverso tale sottogruppo. Poiché chiuso per l'operazione indotta da G, $\langle x_1, \ldots, x_n \rangle$ deve contenere tutti i prodotti finiti, in qualsiasi ordine, delle potenze di $x_1, \ldots, x_n$, cioè deve contenere l'insieme

$$\{g_1^{\pm 1}, \ldots, g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \ldots, x_n\} \ \forall i \in \{1, \ldots, r\}\}$$

Proposizione 1.3

Dati un gruppo G e $x_1, \ldots, x_n$ elementi di G, allora

$$\langle x_1, \ldots, x_n \rangle = \{g_1^{\pm 1}, \ldots, g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \ldots, x_n\} \ \forall i \in \{1, \ldots, r\}\}.$$

Dimostrazione. Poniamo $S = \{g_1^{\pm 1}, \ldots, g_r^{\pm 1} \mid r \in \mathbb{N}, g_i \in \{x_1, \ldots, x_n\} \ \forall i \in \{1, \ldots, r\}\}$, mostriamo che S è un sottogruppo di G. Effettivamente $e \in S$ in quanto è prodotto nessuna potenza di $x_1, \ldots, x_n$, il prodotto di due elementi di S è ancora un elemento di S in quanto prodotto finito di potenze di $x_1, \ldots, x_n$ e l'inverso di un elemento $g_1^{\pm 1} \ldots g_r^{\pm 1} \in S$ è $(g_1^{\pm 1} \ldots g_r^{\pm 1})^{-1} = g_r^{\mp 1} \ldots g_1^{\mp 1}$, che è un elemento di S. Abbiamo quindi che S è un sottogruppo di G contenente $x_1, \ldots, x_n$, pertanto $\langle x_1, \ldots, x_n \rangle \subseteq S$ per minimalità di $\langle x_1, \ldots, x_n \rangle$. D'altra parte, per quanto osservato sopra abbiamo che tutti gli elementi della forma $g_1^{\pm 1} \ldots g_r^{\pm 1}$ con $r \in \mathbb{N}$, $g_i \in \{x_1, \ldots, x_n\}$ per ogni $i \in \{1, \ldots, r\}$ devono essere contenuti in $\langle x_1, \ldots, x_n \rangle$, pertanto i due sottogruppi coincidono. □

Osservazione 1.4 — Se G è un gruppo ciclico abbiamo che esiste $x \in G$ tale che $\langle x \rangle = G$, cioè tutti gli elementi di G sono potenze di x.

Diciamo che $x_1, \ldots, x_n \in G$ sono **generatori** per G, o che l'insieme $\{x_1, \ldots, x_n\}$ **genera** G se $\langle x_1, \ldots, x_n \rangle = G$.

§2 Gruppo diedrale

§2.1 Elementi del gruppo

Definizione 2.1. Dato $n \geqslant 2$ un naturale, consideriamo un poligono regolare di n vertici, definiamo il **gruppo diedrale** su n vertici D_n come l'insieme delle isometrie del piano che mandano i vertici in se stessi, cioè che fissano il poligono (per $n = 2$ consideriamo le isometrie che mandano un segmento in se stesso).

Osservazione 2.2 — D_n è un gruppo, in quanto l'applicazione identità che fissa tutti i vertici è un'isometria dal poligono in se stesso, la composizione di isometrie è un'isometria e un'isometria ammette sempre un'inversa, che è anch'essa un'isometria.

Osservazione 2.3 — Una rotazione di angolo $\frac{2\pi}{n}$ è un elemento di D_n, così come una simmetria rispetto a un asse.

Proseguendo con questa intuizione geometrica, indicheremo con r una rotazione di angolo $\frac{2\pi}{n}$ e con s una simmetria rispetto a un qualsiasi asse. Notiamo che $\mathrm{ord}(r) = n$ e $\mathrm{ord}(s) = 2$ (per convenzione, indichiamo con un angolo positivo una rotazione in senso antiorario e con un angolo negativo una rotazione in senso orario).

Definizione 2.4. Data $r \in D_n$ una rotazione di ordine n, indichiamo con $\mathcal{R}$ il **sottogruppo delle rotazioni** $\langle r \rangle$.

Osservazione 2.5 — Il sottogruppo $\mathcal{R}$ contiene tutte le rotazioni di D_n, infatti se r' è una rotazione di angolo $\frac{2k\pi}{n}$, $k \in \mathbb{Z}$, allora $r^k = r'$ in quanto anche r^k è una rotazione di angolo $\frac{2k\pi}{n}$.

Per determinare come sono fatti gli elementi di D_n, studiamo il sottogruppo $\langle r, s \rangle$. Sicuramente $\langle r, s \rangle$ contiene il sottogruppo $\mathcal{R}$ e tutti gli elementi della forma sr^k, $sr^k s$, $sr^k sr^h$ e così via, vogliamo mostrare che in effetti D_n è generato da r e s.

Osservazione 2.6 — Gli elementi della forma r^k e sr^h sono distinti per ogni $h, k \in \mathbb{Z}$. Infatti sappiamo dall'algebra lineare che il determinante di una simmetria è -1 e che il determinante di una rotazione è 1, per la moltiplicatività del determinante quindi $\det(r^k) = (\det r)^k = 1$ e $\det(sr^h) = (\det s)(\det r)^h = -1$, da cui $r^k \neq sr^h$.

Lemma 2.7

Per ogni rotazione $r \in D_n$ e per ogni simmetria $s \in D_n$ vale

$$srs^{-1} = r^{-1}.$$

Dimostrazione.

$$srs^{-1} = r^{-1} \iff sr = r^{-1}s = (s^{-1}r)^{-1}.$$

Si conclude osservando che $s^2 = 1$, pertanto $s^{-1} = s$ e

$$(s^{-1}r)^{-1} = (sr)^{-1} = r^{-1}s^{-1} = r^{-1}s.$$

□

Proposizione 2.8
Se $n \geqslant 3$ allora $|D_n| = 2n$.

Dimostrazione. Indicando con $1, \dots, n$ gli n vertici di un poligono regolare di n lati, notiamo che un elemento $g \in D_n$ è univocamente determinato da $g(1), \dots, g(n)$. In particolare, fissato $g(1)$, per il quale abbiamo n possibili scelte, abbiamo al massimo due valori per $g(2)$, cioè $g(2) \in \{g(1)+1, g(1)-1\}$ (a meno di sommare n se uno dei due elementi è negativo). Poiché $g(1)$ e $g(2)$ individuano due vettori nel piano non allineati, cioè linearmente indipendenti, ne costituiscono una base: fissati i valori di $g(1)$ e $g(2)$ abbiamo quindi determinato ogni elemento di D_n in modo unico e, poiché possiamo farlo in al più $2n$ modi, $|D_n| \leqslant 2n$. Ricordiamo adesso che D_n contiene gli elementi della forma r^k, sr^h al variare di $h, k \in \mathbb{Z}$, mostriamo che questi sono infatti $2n$. Gli elementi r^k appartengono al gruppo ciclico $\mathcal{R}$ di ordine r, pertanto sono n elementi distinti, inoltre

$$sr^i = sr^j \iff r^i = r^j \iff i \equiv j \mod n,$$

pertanto anche questi sono n elementi distinti. Allora $|D_n| = 2n$. □

Osservazione 2.9 — Abbiamo mostrato che effettivamente $D_n = \langle r, s \rangle$, quindi i suoi elementi sono tutti della forma r^k, sr^h al variare di $h, k \in \mathbb{Z}$.

Osservazione 2.10 — Il risultato è valido anche per D_2, ma con motivazioni diverse. Se consideriamo un segmento nel piano $\mathbb{R}^2$ giacente sulla retta $y = 0$, le isometrie che possiamo applicare sono l'identità, la rotazione di angolo π, la simmetria lungo la retta $y = 0$ e la simmetria lungo l'asse passante per il suo punto medio. D_2 contiene quindi quattro elementi, l'identità e tre elementi di ordine due, pertanto è isomorfo a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

§2.2 Sottogruppi

Consideriamo un sottogruppo $H \leqslant D_n$, distinguiamo due possibilità: $H \subseteq \mathcal{R}$ oppure $H \nsubseteq \mathcal{R}$. Nel primo caso abbiamo che $|H| \mid n$, ed è l'unico sottogruppo di $\mathcal{R}$ con questa proprietà in quanto $\mathcal{R}$ è ciclico, in particolare H è ciclico della forma $\left\langle \frac{n}{d} \right\rangle$, con $d \mid n$. Studiamo quindi il caso $H \nsubseteq \mathcal{R}$: notiamo che $\mathcal{R} \trianglelefteq D_n$ in quanto $[D_n : \mathcal{R}] = 2$, pertanto $D_n/\mathcal{R}$ è un gruppo con l'operazione indotta da D_n e risulta essere isomorfo a $\mathbb{Z}/2\mathbb{Z}$. Consideriamo la proiezione al quoziente

$$\pi_{\mathcal{R}} : D_n \longrightarrow D_n/\mathcal{R} : g \mapsto [g],$$

poiché $H \nsubseteq \mathcal{R}$ abbiamo che esiste $h \in H$ tale che $h \notin \mathcal{R}$, pertanto $\pi_{\mathcal{R}}(h) \notin [\mathcal{R}]$ e in particolare $\pi_{\mathcal{R}}(H) \nsubseteq [\mathcal{R}]$. Dato che i sottogruppi di $D_n/\mathcal{R}$ sono solo $\{[\mathcal{R}]\}$ e $D_n/\mathcal{R}$ abbiamo $\pi_{\mathcal{R}}(H) = D_n/\mathcal{R}$. Osserviamo inoltre che $\ker \pi_{|H} = \ker \pi \cap H = \mathcal{R} \cap H$, per il Primo Teorema di Omomorfismo allora $H/H \cap \mathcal{R} \cong \mathbb{Z}/2\mathbb{Z}$, quindi $|H \cap \mathcal{R}| = \frac{1}{2}|H|$. Dato che $R \cap H \subseteq \mathcal{R}$, esiste $k \in \mathbb{Z}$ tale che $H \cap \mathcal{R} = \langle r^k \rangle$ in particolare $\langle r^k \rangle$ e $\langle sr^h \rangle$, $h \in \mathbb{Z}$, sono contenuti in H.

Proposizione 2.11

Dati $H \leqslant D_n$ un sottogruppo tale che $H \nsubseteq \mathcal{R}$, se r è un generatore di $\mathcal{R}$ tale che $H \cap \mathcal{R} = \langle r^k \rangle$ e s è una simmetria allora

$$H = \langle r^k \rangle \cdot \langle sr^h \rangle = \{xy \mid x \in \langle r^k \rangle, y \in \langle sr^h \rangle\}, h, k \in \mathbb{Z}.$$

Dimostrazione. Per quanto visto sopra abbiamo che $|\langle r^k \rangle| = \dfrac{1}{2}|H|$, inoltre osserviamo che $\operatorname{ord}(sr^h) = 2$ in quanto

$$(sr^h)^2 = sr^h sr^h = (srs)^h r^h = (srs^{-1})^h r^h = r^{-h} r^h = e,$$

pertanto $\langle sr^h \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Ricordiamo che, dati K, N sottogruppi di un gruppo G, se vale almeno una delle inclusioni $K \subseteq N_G(N)$, $N \subseteq N_G(K)$ allora $HK = KH$ e quindi HK è un sottogruppo di G. Nel nostro caso abbiamo che $\langle sr^h \rangle \subseteq N_{D_n}(\langle r^k \rangle)$, infatti per ogni $m \in \mathbb{Z}$ abbiamo

$$(sr^h) r^{mk} (sr^h)^{-1} = sr^{h+mk} sr^h = r^{-h-mk} r^h = r^{-mk} \in \langle r^k \rangle,$$

cioè $\langle sr^h \rangle \subseteq N_{D_n}(\langle r^k \rangle)$ e quindi $\langle r^k \rangle \cdot \langle sr^h \rangle$ è un sottogruppo di D_n. Poiché $\langle r^k \rangle$ e $\langle sr^h \rangle$ sono contenuti in H abbiamo che $\langle r^k \rangle \cdot \langle sr^h \rangle \subseteq H$, inoltre

$$|\langle r^k \rangle \cdot \langle sr^h \rangle| = \frac{1}{2}|H| \cdot 2 = |H|$$

in quanto $\langle r^k \rangle \cap \langle sr^h \rangle = \{e\}$, pertanto i due sottogruppi coincidono. $\square$

Osservazione 2.12 — Per $k \mid n$ e $0 \leqslant h < k$, i sottogruppi $H_{k,h} = \langle r^k, sr^h \rangle$ e $H = \langle r^k \rangle \cdot \langle sr^h \rangle$ coincidono. Infatti $H_{k,h} \subseteq H$ in quanto r^k, sr^h sono elementi di H, d'altra parte $H \subseteq H_{k,h}$ in quanto $H_{h,k}$ contiene tutti i prodotti finiti delle potenze di r^k e sr^h, in particolare gli elementi di H.

Osservazione 2.13 — Per $k \mid n$ e $0 \leqslant h < k$, $\langle r^k, sr^h \rangle = \langle r^k, sr^{h+k} \rangle$, infatti $\langle r^k, sr^h \rangle \subseteq \langle r^k, sr^{h+k} \rangle$ in quanto $sr^h = (sr^{h+k})r^{-k}$ è un elemento del secondo gruppo, simmetricamente $\langle r^k, sr^{h+k} \rangle \subseteq \langle r^k, sr^h \rangle$ in quanto $sr^{h+k} = (sr^h)r^k$ è un elemento del primo gruppo.

Abbiamo quindi finito la classificazione dei sottogruppi di D_n.

Teorema 2.14 (Classificazione dei sottogruppi di D_n)

I sottogruppi di D_n sono della forma

(1) $\langle r^k \rangle$ con $k \mid n$;

(2) $\langle r^k, sr^h \rangle$ con $k \mid n$, $0 \leqslant h < k$,

con $r \in \mathcal{R}$ e s una simmetria. Inoltre tali sottogruppi sono tutti distinti.

Dimostrazione. Abbiamo già visto che i sottogruppi di D_n hanno una di queste forme, mostriamo quindi che sono tutti distinti. A meno di cambiare k, possiamo supporre che r generi $\mathcal{R}$, cioè $\operatorname{ord}(r) = n$. Consideriamo $H, K \leqslant D_n$ due sottogruppi, distinguiamo tre casi

- se $H = \langle r^k \rangle$ e $K = \langle r^m \rangle$, $m \in \mathbb{Z}$, allora $H = K \iff k = m$ in quanto entrambi sottogruppi di un gruppo ciclico, pertanto esiste un unico sottogruppo della forma $\langle r^k \rangle$ per ogni $k \mid n$;
- se $H = \langle r^k \rangle$ e $K = \langle sr^h \rangle$ allora $H \neq K$ in quanto H è ciclico e K no;
- se $H = \langle r^k, sr^h \rangle$ e $K = \langle r^m, sr^l \rangle$, con $m \mid n$ e $0 \leqslant l < m$, considerando le intersezioni con $\mathcal{R}$ $H \cap \mathcal{R} = \langle r^k \rangle$ e $K \cap \mathcal{R} = \langle r^m \rangle$ abbiamo

$$H \cap \mathcal{R} = K \cap \mathcal{R} \iff \langle r^k \rangle = \langle r^m \rangle \iff k = m.$$

Inoltre, se $sr^h \in \langle r^m, sr^l \rangle = \langle r^m \rangle \cdot \langle sr^l \rangle$, allora esiste $t \in \mathbb{Z}$ tale che

$$sr^h = (r^m)^t sr^l \iff sr^h = s^2 r^{mt} sr^l \iff r^h = r^{-mt+l} \iff h \equiv l - mt \mod n,$$

da cui ricaviamo $h \equiv l \mod m$. Ma allora $h = l$ in quanto $0 \leqslant h < k$, $0 \leqslant l < m$.

$\square$

Lemma 2.15

Dati un gruppo G e A, B due sottogruppi tali che $A \leqslant B \leqslant G$, se $B \trianglelefteq G$ e A è caratteristico in B allora $A \trianglelefteq G$.

Dimostrazione. Fissato $g \in G$, consideriamo l'omomorfismo di coniugio

$$\varphi_g : G \longrightarrow G : x \longmapsto gxg^{-1},$$

poiché $B \trianglelefteq G$ è ben definita la restrizione

$$\varphi_{g|B} : B \longrightarrow B : b \longmapsto gbg^{-1},$$

in particolare $\varphi_{g|B} \in Aut(G)$. Dal momento che A è un sottogruppo caratteristico di B abbiamo che $\varphi_{g|B}(A) = A$, pertanto $A \trianglelefteq G$. $\square$

Corollario 2.16

Ogni sottogruppo di $\mathcal{R}$ è normale in D_n.

Dimostrazione. Siano $\langle r^k \rangle$ un sottogruppo di $\mathcal{R}$ e $\varphi \in Aut(\mathcal{R})$, allora $\varphi(\langle r^k \rangle) = \langle r^k \rangle$ in quanto φ preserva l'ordine del sottogruppo e $\langle r^k \rangle$ è l'unico sottogruppo di $\mathcal{R}$ di tale ordine, pertanto $\langle r^k \rangle$ è caratteristico in $\mathcal{R}$. Allora per il Lemma 2.14 abbiamo che $\langle r^k \rangle \trianglelefteq D_n$. $\square$

Corollario 2.17

Per $k \mid n$ e $0 \leqslant h < k$, il sottogruppo $H_{k,h} = \langle r^k, sr^h \rangle$ è normale in D_n se e solo se $r, s \in N_{D_n}(H_{k,h})$.

Dimostrazione.

- Se $H_{k,h} \trianglelefteq D_n$ allora $N_{D_n}(H_{k,h}) = D_n$, in particolare $r, s \in N_{D_n}(H_{k,h})$;

- se $r, s \in N_{D_n}(H_{k,h})$, poiché il normalizzatore è un sottogruppo di D_n abbiamo che $D_n = \langle r, s\rangle \subseteq N_{D_n}(H_{k,h})$, pertanto $H_{k,h} \trianglelefteq D_n$.

$\square$

Vediamo effettivamente quali sono i sottogruppi normali della forma $\langle r^k, sr^h\rangle$. Consideriamo gli automorfismi di coniugio

$$\varphi_s : D_n \longrightarrow D_n : x \longmapsto sxs^{-1} \qquad \varphi_r : D_n \longrightarrow D_n : x \longmapsto rxr^{-1}$$

e sia $x_1^{\pm 1} \dots x_m^{\pm 1} \in H_{k,h} = \langle r^k, sr^h\rangle$, allora

$$\varphi_s(x_1^{\pm 1} \dots x_m^{\pm 1}) = \varphi_s(x_1)^{\pm 1} \dots \varphi_s(x_m)^{\pm 1} \in \langle srs, r^h s^{-1}\rangle = \langle sr^k s, r^h s^{-1}\rangle = \langle r^k, sr^{-h}\rangle,$$

$$\varphi_r(x_1^{\pm 1} \dots x_m^{\pm 1}) = \varphi_r(x_1)^{\pm 1} \dots \varphi_r(x_m)^{\pm 1} \in \langle r^k, rsr^{h-1}\rangle = \langle r^k, sr^{h-2}\rangle.$$

Pertanto $H_{k,h} \trianglelefteq D_n$ se e solo se $\langle r^k, sr^{h-2}\rangle = \langle r^k, sr^{-h}\rangle = \langle r^k, sr^h\rangle$, se e solo se $h \equiv h-2 \mod k$, cioè $k \in \{1, 2\}$.

- Se $k = 1$ allora $H_{k,h} = \langle r, s\rangle = D_n$;
- se $k = 2$ (e n pari) allora $H_{k,h} = \langle r^2, sr\rangle$ oppure $H_{k,h} = \langle r^2, s\rangle$.

Osservazione 2.18 — Il secondo caso si presenta solo se n è pari, questo corrisponde al fatto che in un poligono con un numero pari di lati gli assi di simmetria sono per metà passanti per i lati e metà passanti per i vertici opposti. In un poligono con un numero dispari di lati gli assi di simmetria sono tutti sui lati.

§2.3 Classi di coniugio

Per quanto visto fino a ora, possiamo scrivere ogni elemento di D_n nella forma $s^h r^k$, dove s è una simmetria e r è una rotazione che genera il sottogruppo $\mathcal{R}$, con $h \in \{0, 1\}$ e $k \in \{0, \dots, n-1\}$ in quanto $\mathrm{ord}(s) = 2$ e $\mathrm{ord}(r) = n$. Inoltre tutti gli elementi della forma sr^h hanno ordine 2.

Consideriamo la classe di coniugio di r, $C_r = \{grg^{-1} \mid g \in D_n\}$, fissato $g \in D_n$ abbiamo due possibili valori per grg^{-1}:

- se $g \in \mathcal{R}$ allora g è una potenza di r, pertanto i due elementi commutano e si ha $grg^{-1} = r$;
- se $g \notin \mathcal{R}$ allora $g = sr^h$ con $h \in \mathbb{Z}$, quindi

$$(sr^h)r(sr^h)^{-1} = (sr^h)r(sr^h) = sr^{h+1}sr^h = s^2 r^{-1-h} r^h = r^{-1},$$

cioè $C_r = \{r, r^{-1}\}$. In modo analogo si mostra che $C_{r^k} = \{r^k, r^{-k}\}$ per ogni $k \in \mathbb{Z}$.

Osservazione 2.19 — Se n è pari, scriviamo $n = 2m$ e consideriamo la classe di coniugio di r^m. Poiché $r^m \neq e$ e $r^{2m} = (r^m)^2 = e$ abbiamo che $\mathrm{ord}(r^m) = 2$, cioè $(r^m)^{-1} = r^m$. Allora $C_{r^m} = \{r^m\}$, pertanto abbiamo trovato un elemento del centro di D_n (infatti se G è un gruppo e $x \in G$, allora $x \in Z(G)$ se e solo se $C_x = \{x\}$).

Consideriamo adesso la classe di coniugio di sr^h, $C_{sr^h} = \{g(sr^h)g^{-1} \mid g \in D_n\}$, fissato $g \in D_n$ abbiamo due possibili valori per $g(sr^h)g^{-1}$:

- se $g \in \mathcal{R}$ allora $g = r^k$ con $k \in \mathbb{Z}$, pertanto

$$r^k(sr^h)r^{-k} = sr^{-k}r^hr^{-k} = sr^{h-2k};$$

- se $g \notin \mathcal{R}$ allora $g = sr^k$ con $k \in \mathbb{Z}$, pertanto

$$(sr^k)(sr^h)(sr^k)^{-1} = (sr^k)(sr^h)(sr^k) = sr^{2k-h},$$

cioè $C_{sr^k} = \{sr^{h-2k}, sr^{2k-h} \mid k \in \mathbb{Z}\}$.

Osservazione 2.20 — La classe di coniugio di sr^h contiene tutte le simmetrie in cui l'esponente di r ha la stessa parità di h. Se n è dispari tutte le simmetrie appartengono alla stessa classe, mentre se n è pari abbiamo due classi distinte: quella delle simmetrie rispetto agli assi passanti per i vertici opposti e quella delle simmetrie rispetto agli assi passanti per i lati.