

# **Complementi di Algebra 1**

EVAN CHEN

5 ottobre 2022

## Indice

## §1 Insiemi di generatori

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

$$\langle x_1, \dots, x_n \rangle = \bigcap_{\substack{H \leq G \\ \{x_1, \dots, x_n\} \subseteq H}} H$$

**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  $G$  contenente  $x_1, \dots, x_n$ . Inoltre l'intersezione non è vuota in quanto contiene almeno l'identità e gli elementi  $x_1, \dots, x_n$ .

La definizione data non dà informazioni su come sono fatti gli elementi di  $\langle x_1, \dots, x_n \rangle$ , cerchiamo quindi di caratterizzare in modo diverso tale sottogruppo. In quanto sottogruppo,  $\langle x_1, \dots, x_n \rangle$  deve contenere tutti i prodotti finiti, in qualsiasi ordine, delle potenze di  $x_1, \dots, x_n$ , cioè deve contenere l'insieme

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

### Proposizione 1.3

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

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

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

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

## §2 Gruppo diedrale

### §2.1 Elementi del gruppo

**Definizione 2.1.** Dato  $n \geq 2$  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 su se stesso).

**Osservazione 2.2** —  $D_n$  è effettivamente 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  $\text{ord}(r) = n$  e  $\text{ord}(s) = 2$  (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  $-1$  mentre il determinante di una rotazione è  $1$ , per la moltiplicatività del determinante abbiamo quindi  $\det(r^k) = (\det r)^k = 1$  e  $\det(sr^h) = (\det s)(\det r)^h = -1$ , cioè  $r^k \neq sr^h$ .

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

### Proposizione 2.8

Se  $n \geq 3$  allora  $|D_n| = 2n$ .

*Dimostrazione.* Indicando con  $1, \dots, n$  gli  $n$  vertici di un poligono regolare, 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  $g(2)$  determinano due vettori nel piano non allineati, che sono quindi linearmente indipendenti e determinano una base del piano. Una volta determinati 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, abbiamo che  $|D_n| \leq 2n$ . Ricordiamo adesso che  $D_n$  contiene gli elementi della forma  $r^k, sr^h$  per  $h, k \in \mathbb{Z}$ , mostriamo che questi sono infatti  $2n$ : gli elementi  $r^k$  appartengono al gruppo ciclico  $\mathcal{R}$  di ordine  $n$ , pertanto sono  $n$  elementi distinti. Inoltre  $sr^i = sr^j \iff r^i = r^j \iff i \equiv j \pmod{n}$ , pertanto anche questi sono  $n$  elementi distinti. Allora  $|D_n| = 2n$ .  $\square$

**Osservazione 2.9** — Abbiamo mostrato che effettivamente  $D_n = \langle r, s \rangle$ , quindi i suoi elementi sono tutti della forma  $r^k, sr^h$ .

## §2.2 Sottogruppi

Consideriamo un sottogruppo  $H \leq D_n$ , abbiamo due casi distinti:  $H \subseteq \mathcal{R}$  oppure  $H \not\subseteq \mathcal{R}$ . 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  $\langle r^{\frac{n}{d}} \rangle$ , con  $d \mid n$ . Studiamo quindi il caso  $H \not\subseteq \mathcal{R}$ . Osserviamo che  $\mathcal{R} \trianglelefteq D_n$  in quanto  $[D_n : \mathcal{R}] = 2$ , pertanto il gruppo  $D_n/\mathcal{R}$  è ben definito 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  $H \not\subseteq \mathcal{R}$  abbiamo che esiste  $h \in H$  tale che  $h \notin \mathcal{R}$ , pertanto  $\pi_{\mathcal{R}}(h) \notin [\mathcal{R}]$  e in particolare  $\pi_{\mathcal{R}}(H) \not\subseteq [\mathcal{R}]$ . Dato che i sottogruppi di  $D_n/\mathcal{R}$  sono solo  $\{[\mathcal{R}]\}$  e  $D_n/\mathcal{R}$  abbiamo quindi  $\pi_{\mathcal{R}}(H) = D_n/\mathcal{R}$ . Osserviamo 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  $H \cap \mathcal{R} \subseteq \mathcal{R}$ , 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 2.10

Dati  $H \leq D_n$  un sottogruppo tale che  $H \not\subseteq \mathcal{R}$ , se  $r \in \mathcal{R}$  è 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  $|\langle r^k \rangle| = \frac{1}{2}|H|$ , osserviamo inoltre che  $(sr^h)^2 = sr^h sr^h = (srs^{-1})^h r^h = (sr s^{-1})^h r^h = r^{-h} r^h = e$ , pertanto  $\langle sr^h \rangle \cong \mathbb{Z}/2\mathbb{Z}$ . Ricordiamo che, se  $K, N$  sono sottogruppi di un gruppo  $G$ , se vale almeno una delle inclusioni  $K \subseteq N_G(N)$ ,  $N \subseteq N_G(K)$ . 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  $\langle sr^h \rangle \subseteq N_{D_n}(\langle r^k \rangle)$ , 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  $\langle r^k \rangle \cap \langle sr^h \rangle = \{e\}$ , quindi i due sottogruppi coincidono.  $\square$

**Osservazione 2.11** — Per  $k \mid n$  e  $0 \leq h < k$ , 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  $H_{k,h}$  contiene tutti i prodotti finiti delle potenze di  $r^k$  e  $sr^h$ , in particolare gli elementi di  $H$ .

**Osservazione 2.12** — Per  $k \mid n$  e  $0 \leq h < k$ ,  $\langle r^k, sr^h \rangle = \langle r^k, sr^{h+k} \rangle$ , 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 2.13** (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  $k \mid n$ ,  $0 \leq h < k$ ,

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  $\text{ord}(r) = n$ . Consideriamo  $H, K \leq D_n$  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  $0 \leq l < m$ , 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

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

da cui ricaviamo  $h \equiv l \pmod{m}$ . Ma allora  $h = l$  in quanto  $0 \leq h < k$ ,  $0 \leq l < m$ .  $\square$

**Lemma 2.14**

Dati un gruppo  $G$  e  $A, B$  due sottogruppi tali che  $A \leq B \leq G$ , 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

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

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

**Corollario 2.15**

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

*Dimostrazione.* Siano  $\langle r^k \rangle$  un sottogruppo di  $\mathcal{R}$  e  $\varphi \in \text{Aut}(\mathcal{R})$ , allora  $\varphi(\langle r^k \rangle) = \langle r^k \rangle$  in quanto  $\varphi$  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 2.16**

Per  $k \mid n$  e  $0 \leq h < k$ , 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  $H_{k,h} \trianglelefteq D_n$ .

$\square$