

Complementi di Algebra 1

EVAN CHEN

4 ottobre 2022

Indice

1	Insiemi di generatori	3
2	Gruppo diedrale	3
2.1	Elementi del gruppo	3

§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 r , 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