PARTE PRIMA
Complementi sui gruppi

Lezione 1

Prerequisiti: Gruppi simmetrici, gruppi diedrali, gruppi ciclici.

Sottogruppo generato da un sottoinsieme.

Dato un poligono regolare avente n lati, il gruppo delle sue simmetrie (detto gruppo diedrale D_n, che è un sottogruppo del gruppo G delle isometrie del piano) è univocamente determinato una volta assegnate la rotazione antioraria r di un angolo $\frac{2\pi}{n}$ intorno al centro, ed una delle sue simmetrie assiali, che denoteremo con s. Precisamente

$$D_n = \{\mathrm{id}, r, r^2, ..., r^{n-1}, s, rs, r^2 s, ..., r^{n-1}s\}.$$

A questa conclusione si può arrivare con le seguenti considerazioni. Poiché D_n è un gruppo a cui appartengono r ed s, a D_n devono appartenere anche:

a) tutte le potenze intere di r: r^n, con $n \in \mathbf{Z}$;
b) tutte le potenze intere di s: s^n, con $n \in \mathbf{Z}$;
c) tutti i prodotti di potenze intere di r e di s:

$$r^{h_1} s^{k_1} r^{h_2} s^{k_2} \cdots r^{h_u} s^{k_u}, \tag{*}$$

ove $u \in \mathbf{N}$, e $h_i, k_i \in \mathbf{Z}$ per ogni $i = 1,2,...,u$.

Osserviamo che la (*) è la forma più generale degli elementi di D_n: essa comprende, in particolare, anche le forme a) e b), poiché alcuni degli esponenti h_i, k_i possono essere nulli.

Inoltre, sappiamo che:

a) $o(r) = n$, cioè $r^h = \mathrm{id} \Leftrightarrow n \mid h$;
b) $o(s) = 2$, cioè $s^k = \mathrm{id} \Leftrightarrow 2 \mid k$;
c) $sr = r^{-1}s$.

Ciò ci permette di concludere che:

a) le potenze distinte di r sono, oltre all'identità, $r, r^2, ..., r^{n-1}$;
b) l'unica potenza di s distinta dall'identità è s;
c) per ogni $h \in \mathbf{Z}$, $sr^h = r^{-h}s$.

Pertanto, ogni prodotto del tipo $s^k r^h$ coincide con id, r^h, con s, oppure con $r^{-h}s$, quindi ogni elemento (*) è del tipo

$$\text{id}, \ r^i, \ s \ \text{ oppure } \ r^i s, \qquad \text{con} \qquad 1 \le i \le n-1.$$

Questo esempio si può generalizzare. Anzitutto osserviamo che, dati due elementi *r* e *s* di un gruppo moltiplicativo *G,* ogni sottogruppo di *G* a cui essi appartengono comprende gli elementi del tipo (*). È facile vedere che gli elementi del tipo (*), a loro volta, formano un gruppo, che, ovviamente, è il "più piccolo" sottogruppo di *G* a cui essi appartengono. Si ha la seguente:

Proposizione 1.1 Dato un gruppo moltiplicativo *G* ed un suo sottoinsieme non vuoto *S*, l'insieme

$$\langle S \rangle = \left\{ s_1^{h_1} s_2^{h_2} \cdots s_r^{h_r} \,\middle|\, s_i \in S, \, h_i \in \mathbf{Z} \text{ per ogni } i = 1, \dots, r \right\}$$

è un sottogruppo di *G*, ed è il più piccolo sottogruppo contenente *S*. Lo si dice *sottogruppo generato da S*.

Dimostrazione: Per la prima parte dell'enunciato, basta osservare che:

- $\langle S \rangle$ è non vuoto perché, non essendo *S* l'insieme vuoto, esiste $s \in S$, e dunque $s \in \langle S \rangle$;
- per ogni $s_1^{h_1} s_2^{h_2} \cdots s_r^{h_r}, \overline{s}_1^{k_1} \overline{s}_2^{k_2} \cdots \overline{s}_t^{k_t} \in \langle S \rangle$, si ha che
$$(s_1^{h_1} s_2^{h_2} \cdots s_r^{h_r})(\overline{s}_1^{k_1} \overline{s}_2^{k_2} \cdots \overline{s}_t^{k_t})^{-1} = s_1^{h_1} s_2^{h_2} \cdots s_r^{h_r} \overline{s}_t^{-k_t} \cdots \overline{s}_2^{-k_2} \overline{s}_1^{-k_1} \in \langle S \rangle.$$

La seconda parte dell'enunciato è ovvia. □

Osservazione 1.2 Se S è ridotto ad un solo elemento *g* di *G*, allora $\langle S \rangle$ è il sottogruppo ciclico generato da *g*.

Esercizio 1.3 Dati $m_1, \dots, m_r \in \mathbf{Z}$, determinare il sottogruppo di $\mathbf{Z}$ generato da $S = \{m_1, \dots, m_r\}$ (diremo, più semplicemente: il sottogruppo generato da $m_1, \dots, m_r$, e scriveremo $\langle m_1, \dots, m_r \rangle$).

Svolgimento: Per definizione

$$\langle m_1, \dots, m_r \rangle = \{a_1 m_1 + \dots + a_r m_r \,|\, a_i \in \mathbf{Z}\},$$

che è uguale a $\langle \text{MCD}(m_1, \dots, m_r) \rangle$.

Esercizio 1.4 Determinare il sottogruppo di $\mathbf{Z}_7^*$ generato da $[2]_7$ e $[6]_7$.

Svolgimento: A causa della commutatività del prodotto, il più generale elemento di $\langle [2]_7, [6]_7 \rangle$ è $[2]_7^h [6]_7^k$, con $h, k \in \mathbf{Z}$. Ora, però, $o([2]_7) = 3, o([6]_7) = 2$, essendo

$$[2]_7^2 = [4]_7, [2]_7^3 = [1]_7, \quad [6]_7^2 = [1]_7$$

Dunque

$$\langle [2]_7, [6]_7 \rangle = \{[1]_7, [2]_7, [6]_7, [2]_7[6]_7, [2]_7^2, [2]_7^2[6]_7\} =$$
$$\{[1]_7, [2]_7, [6]_7, [5]_7, [4]_7, [3]_7\} = \mathbf{Z}_7^*$$

Alla stessa conclusione si può giungere anche utilizzando opportunamente il Teorema di Lagrange. (vedi Algebra 2, Teorema 4.2). Come?

Esercizio 1.5 Determinare il sottogruppo di S_4 generato da
a) (12) e (34);
b) (12) e (13);
c) (12), (13) e (14).

Svolgimento:
a) $\langle(12),(34)\rangle = \{\mathrm{id},(12),(34),(12)(34)\}$.
b) Non possiamo più avvalerci della commutatività per semplificare la forma (*). Possiamo però aiutarci con le seguenti considerazioni. Il sottogruppo $\langle(12),(13)\rangle$ è formato da elementi che lasciano fisso 4, quindi è contenuto in $S_3 = \{\mathrm{id},(12),(13),(23),(123),(132)\}$. D'altra parte l'unico sottogruppo di S_3 a cui appartengono (12) e (13) è S_3 stesso (in virtù del Teorema di Lagrange, un sottogruppo siffatto ha come ordine un divisore di 6 che è pari ed è maggiore di 2). Dunque $\langle(12),(13)\rangle = S_3$.
c) In base a quanto visto al punto b), il sottogruppo cercato contiene $\langle(12),(13)\rangle = \{\mathrm{id},(12),(13),(23),(123),(132)\}$ e, analogamente, contiene $\langle(13),(14)\rangle = \{\mathrm{id},(13),(14),(34),(134),(143)\}$. Quindi esso ha almeno 10 elementi. A questi si aggiungono (123)(134) = (234), il suo inverso (243) e la trasposizione $(24) = (34)(23)(34)$. Quindi $\langle(12),(13),(14)\rangle$ ha almeno 13 elementi. Ma il suo ordine, per il Teorema di Lagrange, è un divisore di 24. Quindi il suo ordine è necessariamente 24, cioè
$$\langle(12),(13),(14)\rangle = S_4.$$

Esercizio 1.6
a) Provare che $S_n = \langle(12),(13),\ldots,(1n)\rangle$.
b) Provare che, per ogni $n \geq 3$, A_n è generato dai 3-cicli.

Svolgimento:
a) Poiché, come noto, ogni permutazione è prodotto di trasposizioni, è sufficiente provare che ogni trasposizione si scrive come prodotto di permutazioni scelte tra (12), (13), ... , $(1n)$. In effetti, per ogni coppia di indici i, j diversi da 1 e tali che $i \neq j$, si ha che

$$(ij) = (1i)(1j)(1i).$$

b) Poiché ogni elemento di A_n è prodotto di un numero pari di trasposizioni, è sufficiente provare che il prodotto di due trasposizioni è sempre rappresentabile come prodotto di 3-cicli. Ciò è banalmente vero se le due trasposizioni sono uguali, poiché in tal caso il prodotto è l'identità. Altrimenti, a meno di ridenominare gli elementi, si ha uno dei seguenti due casi:
- (12)(13) = (132)
- (12)(34) = (123)(234).

Omettiamo la facile dimostrazione della

Proposizione 1.7 Sia G un gruppo moltiplicativo, sia S un suo sottoinsieme non vuoto. Allora il sottogruppo $\langle S \rangle$ è normale se e solo se, per ogni $g \in G$, $gSg^{-1} \subset \langle S \rangle$.

Osservazione 1.8 Siano S, T sottoinsiemi di G. Se $S \subset T$, allora $\langle S \rangle \subset \langle T \rangle$.