

## laterali di un sottogruppo

Siano  $G$  un gruppo e  $H$  un suo sottogruppo.

**DEFINIZIONE 1** Le due relazioni  $\mathfrak{R}'_H$  e  $\mathfrak{R}''_H$  sugli elementi di  $G$  definite da

$$a, b \in G, a\mathfrak{R}'_H b \Leftrightarrow a^{-1}b \in H, \quad (1)$$

$$a, b \in G, a\mathfrak{R}''_H b \Leftrightarrow ab^{-1} \in H, \quad (2)$$

si chiamano *congruenze*, rispettivamente *sinistra* e *destra*, *modulo*  $H$  ed é un esercizio provare che risultano d'equivalenza.

**OSSERVAZIONE 2** Nel caso  $G$  sia un gruppo additivo, le relazioni  $\mathfrak{R}'_H$  e  $\mathfrak{R}''_H$  sono definite rispettivamente da

$$a, b \in G, a\mathfrak{R}'_H b \Leftrightarrow -a + b \in H$$

e

$$a, b \in G, a\mathfrak{R}''_H b \Leftrightarrow a - b \in H.$$

**OSSERVAZIONE 3** Se  $G$  é abeliano, le relazioni  $\mathfrak{R}'_H$  e  $\mathfrak{R}''_H$  coincidono.

**DEFINIZIONE 4** La classe di  $\mathfrak{R}'_H$ -equivalenza di un elemento  $a$ , che si vede facilmente essere data da

$$[a]_{\mathfrak{R}'_H} = aH = \{ah : h \in H\}, \quad (3)$$

si chiama *laterale sinistro di  $H$  in  $G$  relativo ad  $a$* .

La classe di  $\mathfrak{R}''_H$ -equivalenza di un elemento  $a$ , data da

$$[a]_{\mathfrak{R}''_H} = Ha = \{ha : h \in H\}, \quad (4)$$

si chiama *laterale destro di  $H$  in  $G$  relativo ad  $a$* .

**OSSERVAZIONE 5**  $H$  stesso é un suo laterale sinistro, essendo  $[1]_{\mathfrak{R}'_H} = 1H = H$ . Analogamente  $H$  é un suo laterale destro, essendo  $[1]_{\mathfrak{R}''_H} = H1 = H$ .

## laterali di un sottogruppo

**OSSERVAZIONE 6** I laterali sinistri (risp. destri) di  $H$  in  $G$  formano una partizione degli elementi di  $G$ .

**ESEMPIO 7** Nel gruppo additivo degli interi  $(\mathbb{Z}, +)$  si consideri il sottogruppo  $H = m\mathbb{Z}$ , con  $m$  intero maggiore di 1. Allora le relazioni  $\mathcal{R}'_H$  e  $\mathcal{R}''_H$  coincidono con la congruenza modulo  $m$ .

**ESERCIZIO 8** Siano  $H, K$  due sottogruppi di un gruppo  $G$ . Provare che

$$aH \cap aK = a(H \cap K) \quad e \quad Ha \cap Ka = (H \cap K)a,$$

per ogni elemento  $a \in G$ .

**PROPOSIZIONE 9** Per ogni  $a \in G$ , le funzioni (traslazioni ristrette ad  $H$ )

$$h \in H \rightarrow ah \in aH \quad e \quad h \in H \rightarrow ha \in Ha$$

sono biunivoche, ne segue che  $|H| = |aH| = |Ha|$ .

**PROPOSIZIONE 10** Gli insiemi quoziente  $G/\mathcal{R}'_H$  e  $G/\mathcal{R}''_H$ , cioè gli insiemi dei laterali di  $H$  rispettivamente sinistri e destri, sono equipotenti.

**DIM.** Osserviamo che risulta:

$$\begin{aligned} aH = bH &\Leftrightarrow a \equiv b \pmod{\mathcal{R}'_H} \Leftrightarrow a^{-1}b \in H \\ \Leftrightarrow a^{-1}b &= (a^{-1})(b^{-1})^{-1} \in H \Leftrightarrow a^{-1} \equiv b^{-1} \pmod{\mathcal{R}''_H} \\ &\Leftrightarrow Ha^{-1} = Hb^{-1}. \end{aligned}$$

Ne segue che é ben definita la funzione

$$aH \in G/\mathcal{R}'_H \rightarrow Ha^{-1} \in G/\mathcal{R}''_H,$$

la quale é biunivoca.

## lateralali di un sottogruppo

**DEFINIZIONE 11** Se l'insieme quoziente  $G/\mathcal{R}'_H$  (o equivalentemente  $G/\mathcal{R}''_H$ ) é finito ed ha ordine  $n$ , l'intero  $n$  si chiama *indice di  $H$  in  $G$*  e si denota con  $|G : H|$  o con  $[G : H]$ . Se  $G/\mathcal{R}'_H$  (o equivalentemente  $G/\mathcal{R}''_H$ ) é infinito, si dice che  $H$  ha *indice infinito in  $G$* .

**OSSERVAZIONE 12** Risulta  $|G : G| = 1$ . Inoltre,  $|G : 1|$  é uguale a  $|G|$  se  $G$  é finito ed é infinito se  $G$  é infinito.

**TEOREMA 13 (teorema di Lagrange)** *Se  $G$  é un gruppo finito e  $H$  un suo sottogruppo, allora*

$$|G : H| = \frac{|G|}{|H|} \quad (5)$$

e quindi  $|H|$  é un divisore di  $|G|$ .

**OSSERVAZIONE 14** Il teorema di Lagrange dice che l'ordine di un sottogruppo di un gruppo finito  $G$  é un divisore dell'ordine di  $G$  ma, si faccia bene attenzione, non garantisce che un divisore positivo di  $|G|$  é l'ordine di un sottogruppo di  $G$ . Quest'ultima affermazione é in generale falsa. Essa é, però, vera per il gruppo additivo  $(\mathbb{Z}_n, +)$  degli interi modulo  $n$ .

**ESERCIZIO 15** *Provare che ogni gruppo finito d'ordine primo é ciclico.*

**ESERCIZIO 16** *Provare che un gruppo finito d'ordine dispari non possiede elementi d'ordine pari.*

**PROPOSIZIONE 17** *Se  $G$  é finito d'ordine  $m$ , allora il periodo di ogni elemento di  $G$  divide  $m$ . Inoltre risulta  $a^m = 1$ , per ogni  $a \in G$ .*

## ordine di una permutazione

Nel seguito, quando parleremo di *fattorizzazione di una permutazione in cicli disgiunti*, sottointenderemo sempre che tali cicli sono non banali. La scrittura di una permutazione  $\sigma$  come prodotto di cicli disgiunti prende il nome di *notazione ciclica* di  $\sigma$  ed é chiaro che, se un elemento  $j \in N_n$  non compare in nessuno dei cicli che fattorizzano  $\sigma$ , allora  $j$  é unito in  $\sigma$ .

**PROPOSIZIONE 18** *L'ordine di un elemento  $\sigma$  di  $S_n$  é uguale al minimo comune multiplo delle lunghezze dei cicli che fattorizzano  $\sigma$ .*

**DIM.** Sia  $\sigma_1\sigma_2\cdots\sigma_k$  la fattorizzazione di  $\sigma$  in cicli disgiunti, sia  $s_j$  l'ordine di  $\sigma_j$  e poniamo

$$m = \text{mcm}(s_1, s_2, \dots, s_k), \quad m = s_j m_j,$$

per ogni  $j = 1, 2, \dots, k$ . I cicli  $\sigma_1, \sigma_2, \dots, \sigma_k$  sono a due a due disgiunti e quindi a due a due permutabili; ne segue che

$$\sigma^t = \sigma_1^t \sigma_2^t \cdots \sigma_k^t,$$

per ogni intero  $t$ . Allora risulta

$$\sigma^m = \sigma_1^m \sigma_2^m \cdots \sigma_k^m = (\sigma_1^{s_1})^{m_1} (\sigma_2^{s_2})^{m_2} \cdots (\sigma_k^{s_k})^{m_k} = 1.$$

Inoltre, se  $t$  é un intero positivo minore di  $m$ , esiste un indice  $j$  tale che  $t$  non é multiplo di  $s_j$ . Ne segue che

$$\sigma_j^t \neq 1$$

e

$$\sigma^t = \sigma_1^t \sigma_2^t \cdots \sigma_k^t \neq 1.$$

L'asserto é cosí provato.

## Il gruppo alterno $A_n$

Sia  $S_n$  il gruppo simmetrico su  $n$  oggetti, cioè il gruppo di tutte le permutazioni sull'insieme  $N_n = \{1, 2, \dots, n\}$ . I cicli di lunghezza 2 prendono il nome di *trasposizioni* ed è chiaro che, per ogni trasposizione  $\sigma$ , risulta  $\sigma = \sigma^{-1}$ . Ogni trasposizione ha dunque periodo due in  $S_n$ .

Osserviamo che ogni ciclo, e quindi ogni permutazione, può scriversi come prodotto di trasposizioni; infatti si ha

$$(j_1, j_2, \dots, j_k) = (j_1, j_2)(j_1, j_3) \cdots (j_1, j_{k-1})(j_1, j_k).$$

Una permutazione  $\sigma$  può in generale fattorizzarsi in modi diversi mediante trasposizioni, nel senso che le trasposizioni di una sua fattorizzazione e il loro numero non sono degli invarianti di  $\sigma$ ; in altre parole possiamo dire che per le trasposizioni non vale un teorema analogo a quello dimostrato per la decomposizione di una permutazione in cicli.

**DEFINIZIONE 19** Allo scopo di trovare un invariante delle possibili fattorizzazioni di una permutazione in trasposizioni diamo le seguenti definizioni per una permutazione  $\sigma$  :

- Considerata una coppia  $(i, j)$ , ove  $i, j$  sono elementi di  $N_n$  con  $i < j$ , si dice che  $\sigma$  presenta un'*inversione* su  $(i, j)$  se risulta  $\sigma(i) > \sigma(j)$ .
- Si dice che  $\sigma$  è una permutazione *pari* se presenta un numero pari di inversioni, *dispari* nel caso contrario.
- si definisce *segno* di  $\sigma$ , e si denota con  $sgn(\sigma)$ , l'intero 1 o  $-1$  a seconda che  $\sigma$  sia rispettivamente pari o dispari.

**ESEMPIO 20** Ogni trasposizione è una permutazione dispari e il suo segno è  $-1$ . La permutazione identica è ovviamente pari.