ESERCIZI DI ALGEBRA 1

MANUEL DEODATO

Indice

1 Gruppi

1.1 Lezione 3 [10-10-2023]

Si inizia col dimostrare il teorema di Cauchy e il piccolo teorema di Fermat usando le azioni di gruppo.

Teorema 1.1 (Teorema di Cauchy). Sia G un gruppo finito, con p primo tale che $p \mid |G|$; allora $\exists x \in G : \text{ord}(x) = p$.

Dimostrazione. Si considera l'azione di $\mathbb{Z}/p\mathbb{Z}$ sull'insieme

$$X = \left\{ (g_1, \dots, g_p) \in G^p \;\middle|\; \prod_{i=1}^{p} g_i = e_G \right\}$$

dove l'elemento $i \in \mathbb{Z}/p\mathbb{Z}$ agisce mandando

$$(g_1, \dots, g_p) \longmapsto (g_{1+i}, g_{2+i}, \dots, g_{p+i})$$

dove l'indice di ciascun g_i è letto modulo p. Ad esempio, l'elemento $1 \in \mathbb{Z}/p\mathbb{Z}$ agisce come

$$(g_1, \dots, g_p) \longmapsto (g_2, g_3, \dots, g_{p+1})$$

Da questa definizione, è facile convincersi un'azione corrisponde ad una rotazione delle componenti di ogni p-upla di X, pertanto il prodotto restituisce sempre e_G, quindi è ben definita come biezione di X.

Osservazione 1.1. Si può osservare che se $i \in \mathbb{Z}/p\mathbb{Z}$ agisce su una p-upla, essendo che

$$e_G = g_1 \cdots g_p = (g_1 g_2 \cdots g_i) g_{i+1} \cdots g_p \implies g_1 g_2 \cdots g_i = (g_{i+1} \cdots g_p)^{-1}$$

quindi, a seguito della rotazione tramite i, si ha il prodotto

$$(g_{i+1} \cdots g_p)(g_1 g_2 \cdots g_i) = e_G$$

Si nota immediatamente che $|X| = n^{p-1}$ perché ogni componente della p-upla può essere scelta arbitrariamente tra gli n elementi di G, mentre l'ultima, la p-esima, è fissata dalla condizione che sia l'inverso del prodotto delle $p-1$ componenti precedenti.

Ora si studiano le orbite dell'azione. Per il teorema di orbita-stabilizzatore

$$|\mathrm{Orb}(x)| \mid |\mathbb{Z}/p\mathbb{Z}| \implies |\mathrm{Orb}(x)| = \{1, p\}$$

Le orbite di lunghezza 1 sono date da tutti gli elementi di X che hanno ogni componente uguale perché sotto rotazione di ogni $i \in \mathbb{Z}/p\mathbb{Z}$ non devono cambiare. Un elemento $g \in G$ che ha un corrispondente vettore in X con tutte le componenti uguali deve necessariamente soddisfare

$$e_G = \underbrace{gg\cdots g}_{p \text{ volte}} = g^p \implies \mathrm{ord}(g) \in \{1, p\}$$

Un'orbita del genere esiste sicuramente ed è data proprio dall'elemento neutro di G, e_G ed è corrispondente proprio a $\mathrm{ord}(g) = 1$; poi le altre eventuali orbite del genere sono date dagli elementi di G che hanno ordine p. L'idea è dimostrare che ne esiste almeno uno. Ora, visto che le orbite partizionano l'insieme, si ha:

$$|X| = \bigsqcup_{x \in X} \mathrm{Orb}(x) \implies |X| = \sum_{x \in \mathcal{R}} |\mathrm{Orb}(x)|$$

dove $\mathcal{R}$ è l'insieme dei rappresentanti delle orbite. La somma si può spezzare separando le orbite che hanno lunghezza 1, da quelle che hanno lunghezza p:

$$|X| = 1 + \#\left\{\begin{matrix}\text{elementi di} \\ \text{ordine } p\end{matrix}\right\} + p \cdot \#\left\{\begin{matrix}\text{elementi con} \\ \text{orbita lunga } p\end{matrix}\right\}$$

da cui, passando in modulo p, si ottiene che

$$n^{p-1} - 1 \equiv \#\left\{\begin{matrix}\text{elementi di} \\ \text{ordine } p\end{matrix}\right\} \pmod{p}$$

Per assunzione, però, $p \mid n$, per cui $n^{p-1} - 1 \equiv -1 \pmod{p}$ e, pertanto

$$\#\left\{\begin{matrix}\text{elementi di} \\ \text{ordine } p\end{matrix}\right\} \equiv -1 \pmod{p}$$

Ma questo significa che il numero di elementi di ordine p non è nullo perché $0 \not\equiv -1 \pmod{p}$. □

In maniera del tutto analoga si dimostra il piccolo teorema di Fermat.

Teorema 1.2 (Piccolo teorema di Fermat). Sia $n \in \mathbb{Z}$ un intero non divisibile per p; allora $n^{p-1} \equiv 1 \pmod{p}$.

Dimostrazione. Si considera $G = \mathbb{Z}/n\mathbb{Z}$, con $p \nmid n$ e

$$X = \left\{(g_1, \dots, g_p) \in G^p \mid g_1 + \dots + g_p = 0\right\}$$

Allora si considera l'azione di $\mathbb{Z}/p\mathbb{Z}$ su X come sopra e, analogamente, si ha $|X| = n^{p-1}$. Visto che $p \nmid n$, non ci possono essere elementi di ordine p in G e, quindi, vi è un'unica orbita di ordine 1 data dall'elemento neutro 0. Ne segue che:

$$n^{p-1} = |X| = 1 + p \cdot \# \left\{ \begin{matrix} \text{elementi con} \\ \text{orbita lunga } p \end{matrix} \right\} \equiv 1 \pmod{p}$$

da cui la tesi. □

Il seguente teorema ha come conseguenza il fatto che se un sottogruppo di un gruppo finito ha indice 2, allora è normale.

Teorema 1.3. Sia G un gruppo finito di ordine n e sia $N < G$. Se $[G : N] = p$, con p il più piccolo primo che divide n, allora $N \lhd G$.

Dimostrazione. Si considera l'azione di G sul quoziente G/N data da

$$g' \cdot (gN) = g'gN$$

Si può dimostrare facilmente che questa è una buona azione e, quindi, si ha un omomorfismo $G \xrightarrow{\phi} S(G/N) \cong S_p$, visto che $|G/N| = p$ per assunzione. Si vuole dimostrare che il suo nucleo coincide con N, da cui $N \lhd G$.

Si inizia col notare che $|\mathrm{Im}(\phi)| \mid |S(G/N)| = |S_p| = p!$; allo stesso tempo, per il primo teorema di omomorfismo, si ha

$$\frac{G}{\mathrm{Ker}(\phi)} \cong \mathrm{Im}(\phi) \implies |\mathrm{Im}(\phi)| \mid \frac{|G|}{|\mathrm{Ker}(\phi)|} \implies |\mathrm{Im}(\phi)| \mid |G|$$

Visto che $|\mathrm{Im}(\phi)|$ deve dividere $p!$, che contiene tutti primi minori o pari a p, e deve dividere anche $|G|$, che contiene tutti primi maggiori o uguali a p, significa che $|\mathrm{Im}(\phi)| = \{1, p\}$. Però non può essere $|\mathrm{Im}(\phi)| = 1$ perché, prendendo $g \in G \setminus N$ e prendendo $n \in N$, si ottengono due mappe $\phi_g, \phi_n \in S(G/N)$ diverse fra loro: $\phi_g(N) = gN \neq N = nN = \phi_n(N)$. Allora $|\mathrm{Im}(\phi)| = p = [G : \mathrm{Ker}(\phi)] = [G : N]$, quindi $\mathrm{Ker}(\phi)$ e N hanno stessa cardinalità in un gruppo finito G. Per concludere che $\mathrm{Ker}(\phi) = N$, quindi che $N \lhd G$, è sufficiente mostrare un'inclusione; a questo proposito, si nota che se $g \in \mathrm{Ker}(\phi)$, allora $g \cdot N = gN = N \iff g \in N$, cioè $\mathrm{Ker}(\phi) \subseteq N \implies \mathrm{Ker}(\phi) = N$. □

Facendo uso di questo risultato, è possibile dimostrare che ogni gruppo di ordine 15 è ciclico.

Proposizione 1.1. Ogni gruppo G di ordine 15 è ciclico.

Dimostrazione. Si dimostra tramite i seguenti punti.

(a). $\exists N \lhd G$ tale che $|N| = 5$.

(b). $N \subseteq Z(G)$.

(c). G abeliano $\Rightarrow G$ ciclico.

Il punto (a) si dimostra direttamente applicando il teorema di Cauchy e il teorema appena visto; dal primo, si conclude che $\exists g \in G : \langle g \rangle = N < G$ tale che $|N| = 5 = \text{ord}(g)$, mentre dal teorema precedente, visto che $|G|/|N| = 3$, che è il più piccolo primo che divide $|G|$, si conclude che N è normale in G.

Per il punto (b), N è normale in G, quindi la mappa

$$\phi : \begin{array}{ccc} \text{Int}(G) & \longrightarrow & \text{Aut}(N) \\ \varphi_x & \longmapsto & \varphi_x|_N \end{array}$$

è ben definita. Allora basta mostrare che che $\text{Im}(\phi) = \{\text{Id}\}$ per far vedere che N è normale. Intanto si ricorda che $\text{Int}(G) \cong G/Z(G)$, quindi $|\text{Int}(G)| \mid 15$; inoltre $\text{Aut}(N) \cong \text{Aut}(\mathbb{Z}/5\mathbb{Z}) \cong (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/4\mathbb{Z}$. Ma allora $|\text{Im}(\phi)| \mid (4, 15) \mid 1$, da cui $\text{Im}(\phi) = \{\text{Id}\}$ e, quindi, $N \subseteq Z(G)$.

Infine, per il punto (c), si può osservare che $|G/Z(G)| = \{1, 3\}$ perché $N \subseteq Z(G) \implies |Z(G)| \geq 5$, da cui $G/Z(G)$ è ciclico in entrambi i casi; ricordando che $G/Z(G)$ ciclico $\Rightarrow G$ abeliano, si conclude la dimostrazione. □

Continuare 56:00…