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 $\exists x \in G : \mathrm{ord}(x) = p$.

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. □

Facendo uso di quanto affermato dal teorema 1.3, 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 $|N| = 5 = \mathrm{ord}(g)$, 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

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

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

Un modo alternativo di dimostrare il punto (c) dell'esercizio precedente è tramite il seguente lemma.

Lemma 1.2.1. Siano $g_1, g_2 \in G$ tali che $\operatorname{ord}(g_1) = m$ e $\operatorname{ord}(g_2) = n$. Se $g_1 g_2 = g_2 g_1$ e $(m, n) = 1$, allora $\operatorname{ord}(g_1 g_2) = m \cdot n$.

Dimostrazione. Si cerca di capire quando il prodotto $(g_1 g_2)^k = e$, cioè per quali k vale la relazione. Visto che g_1 e g_2 commutano per assunzione, questo si può riformulare più chiaramente come $g_1^k g_2^k = e \iff g_1^k = g_2^{-k}$. Quest'ultima uguaglianza in particolare implica che $g_1^k, g_2^k \in \langle g_1 \rangle \cap \langle g_2 \rangle$, che è un sottogruppo sia di $\langle g_1 \rangle$, che di $\langle g_2 \rangle$. In quanto tale, per Lagrange, deve dividere l'ordine dei due che, essendo coprimi, permette di concludere automaticamente che $|\langle g_1 \rangle \cap \langle g_2 \rangle| = 1$, cioè $\langle g_1 \rangle \cap \langle g_2 \rangle = \{e\}$, quindi $g_1^k = e = g_2^k$. Ma allora $m, n \mid k$, cioè k deve essere un multiplo sia dell'ordine di g_1, che di quello di g_2, quindi il più piccolo fra questi che soddisfa la richiesta è proprio $m \cdot n$, visto che m e n sono coprimi. $\square$

Osservazione 1.2. Il lemma dimostra il punto (c) perché, per Cauchy, si hanno elementi di ordine 3 e di ordine 5; inoltre, avendo dimostrato che $N \subseteq Z(G)$, si ha anche che l'elemento di ordine 5 commuta, in particolare, con quello di ordine 3 e i rispettivi ordini sono coprimi, quindi il prodotto tra i due genera un sottogruppo di ordine 15. Per ragioni di ordine, questo sottogruppo coincide proprio con G, il quale risulta, dunque, ciclico.

Esercizio 1.1. Studiare il gruppo $\operatorname{Aut}((\mathbb{Z}/p\mathbb{Z})^n)$, con p numero primo.

Svolgimento. Si nota che il gruppo $G = (\mathbb{Z}/p\mathbb{Z})^n$ ha una struttura di spazio vettoriale sul campo $\mathbb{F}_p$, dove la somma è quella coordinata per coordinata, mentre il prodotto per scalare è nuovamente quello coordinata per coordinata e deriva direttamente dalla somma: il prodotto per uno scalare $\overline{n} \in \mathbb{F}_p$ consiste nel sommare $\overline{n}$ volte il vettore di G che si sta moltiplicando.

Per il seguito, si farà uso della proposizione 1.2; da questa, segue immediatamente che le mappe di $\operatorname{Aut}(G)$ sono tutte e sole le applicazioni lineari $G \to G$ invertibili. Per caratterizzare questi automorfismi, allora, è sufficiente specificare come agiscono su una base $e_1, \dots, e_n$, richiedendo che $\varphi(e_1), \dots, \varphi(e_n)$ sia ancora una base[1] di G così che φ sia effettivamente un'applicazione lineare suriettiva e iniettiva, quindi invertibile. Seguendo questo ragionamento, si può calcolare la cardinalità di $\operatorname{Aut}(G)$:

- $\varphi(v_1)$ può essere un qualunque vettore di $\mathbb{F}_p^n \setminus \{\underline{0}\}$, quindi si hanno $p^n - 1$ possibilità;

[1] In realtà, è sufficiente che siano linearmente indipendenti, visto che sono già in numero per essere una base.

- $\varphi(v_2)$ può essere mappato in un qualunque elemento di $\mathbb{F}_p^n$ che non sia linearmente indipendente con $\varphi(v_1)$, cioè $\varphi(v_2) \in \mathbb{F}_p^n \setminus \text{Span}(v_1)$, da cui si hanno $p^n - p$ possibilità;
- $\varphi(v_k)$ deve essere mappato in un qualunque elemento di $\mathbb{F}_p^n \setminus \text{Span}(v_1, \dots, v_{k-1})$, per un totale di $p^n - p^{k-1}$.

Per questo ragionamento, si ha la seguente formula:

$$|\text{Aut}(G)| = (p^n - 1)(p^n - p) \dots (p^n - p^{n-1}) \tag{1.1.1}$$

Visto che gli automorfismi di $\mathbb{F}_p^n$ sono tutte e sole le applicazioni lineari $n \times n$ a coefficienti in $\mathbb{F}_p$ e invertibili, si individua con $\text{GL}_n(\mathbb{F}_p)$. ■

Proposizione 1.2. Sia $G = (\mathbb{Z}/p\mathbb{Z})^n$, con p numero primo; una mappa $\varphi : G \to G$ è un omomorfismo di gruppi se e solo se è un'applicazione lineare.

Dimostrazione. Sia $\varphi : G \to G$ un omomorfismo di gruppi; si dimostra che un'applicazione lineare. Per farlo, bisogna far vedere che $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$, $\forall v_1, v_2 \in G$, ma questo deriva direttamente dall'assunzione di φ omomorfismo di gruppi, e che $\varphi(\lambda v) = \lambda\varphi(v)$, $\forall \lambda \in \mathbb{F}_p$, $\forall v \in G$. Per dimostrare quest'ultima, si usa che $\lambda v = v + v + \dots + v$ per λ volte, quindi, per la proprietà di omomorfismo, si conclude che $\varphi(\lambda v) = \lambda\varphi(v)$.

L'implicazione opposta è diretta conseguenza della proprietà $\varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$ che deriva dall'assunzione di φ applicazione lineare. □

Osservazione 1.3. Come diretta conseguenza dell'esercizio precedente, si può dimostrare facilmente che $\text{Aut}\big((\mathbb{Z}/2\mathbb{Z})^2\big) \cong S_3$. Infatti, gli elementi di $(\mathbb{Z}/2\mathbb{Z})^2$ sono

$$(0,0) \qquad (1,0) \qquad (0,1) \qquad (1,1)$$

Per $\varphi \in \text{Aut}\big((\mathbb{Z}/2\mathbb{Z})^2\big)$, si deve necessariamente avere $\varphi(0,0) = (0,0)$, altrimenti si perderebbe la suriettività. Quindi, un automorfismo è fondamentalmente individuato a seconda di come permuta i tre elementi rimanenti; per esempio, se $(1,0) \mapsto (1,1)$ e $(1,1) \mapsto (1,0)$, allora $(0,1) \mapsto (0,1)$.

Esercizio 1.2. Si considerano $\sigma = (12345), \tau = (2,5)(3,4) \in S_5$; si vuole studiare il gruppo $G = \langle \sigma, \tau \rangle$.

Svolgimento. Per cominciare, si vuole capire come si comportano le potenze di σ e τ, nel senso che se i due commutassero, capire cosa rappresenta $(\sigma\tau)^k$ sarebbe molto più semplice. Tuttavia, piuttosto che calcolare il commutatore, in questo caso, ci si può limitare al seguente (usando la proposizione 1.3):

$$\tau\sigma\tau^{-1} = (1, 5, 4, 3, 2) = \sigma^{-1}$$

Ma quindi σ e τ soddisfano la presentazione di D_5, da cui $G \cong D_5$. ■

Osservazione 1.4. L'idea geometria alla base di questo è che τ è la riflessione rispetto all'asse passante per il centro del pentagono; infatti, numerandone i vertici in senso antiorario, si vede che $2 \leftrightarrow 5$ e $3 \leftrightarrow 4$ corrisponde proprio a tale riflessione. Inoltre, ovviamente, σ rappresenta una rotazione di angolo $2\pi/5$, che manda un vertice nel successivo (sempre in verso antiorario).

Proposizione 1.3. Siano $c, \tau \in S_n$ due permutazioni, con $c = (a_1, \dots, a_k)$ ciclo; allora $\tau c \tau^{-1} = (\tau(a_1), \dots, \tau(a_k))$.

Dimostrazione. Per dimostrarlo, è sufficiente osservare che:

$$(\tau c \tau^{-1})\tau(a_j) = \tau c(a_j) = \tau(a_{j+1})$$

quindi $\tau c \tau^{-1}$ consiste nel ciclo $(\tau(a_1), \tau(a_2), \dots, \tau(a_k))$. □

Osservazione 1.5. Chiaramente, se $\sigma \in S_n$ è decomposta in cicli $\sigma = c_1 \dots c_m$, allora:

$$\tau\sigma\tau^{-1} = \tau c_1 \dots c_m \tau^{-1} = \tau c_1 \tau^{-1} \dots \tau c_m \tau^{-1}$$

semplicemente moltiplicando per $\tau^{-1}\tau$ in mezzo ad ogni ciclo, quindi si può applicare la formula sopra.

1.1.1 Studiare l'esistenza di sottogruppi normali

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 $\mathrm{Ker}(\phi) \subseteq N \implies \mathrm{Ker}(\phi) = N$. □

Esercizio 1.3. Studiare l'azione considerata sopra, cioè definita da $\phi(g) = \phi_g : g'H \mapsto gg'H$, nel caso in cui $H < G$ non è normale.

Svolgimento. Si nota anzitutto che, come prima $\phi : G \to S(G/H) \cong S_{|G/H|}$ e, per definizione, $\mathrm{Ker}(\phi) \lhd G$. Inoltre, analogamente al caso precedente, si conclude che $\mathrm{Ker}(\phi) \subseteq H$ perché $\forall g \in \mathrm{Ker}(\phi)$ si ha, in particolare, che $g \cdot H = gH = H \iff g \in H$, pertanto si ha la catena

$$\mathrm{Ker}(\phi) \subseteq H \subseteq G$$

Ora, se $[G : H] = n$, si vuole capire cosa è possibile affermare riguardo a $[G : \mathrm{Ker}(\phi)]$. Per il primo teorema di omomorfismo, si ha

$$[G : \mathrm{Ker}(\phi)] = |G/\mathrm{Ker}(\phi)| = |\mathrm{Im}(\phi)| \mid n! = |S_{|G/H|}|$$

Per la stessa relazione, si sa anche che

$$[G : \mathrm{Ker}(\phi)] \mid |G|$$

Inoltre, per un corollario del teorema di Lagrange, si può anche affermare che

$$[G : \mathrm{Ker}(\phi)] = [G : H][H : \mathrm{Ker}(\phi)] = n[H : \mathrm{Ker}(\phi)] \implies n \mid [G : \mathrm{Ker}(\phi)]$$

■

Esercizio 1.4. Usando i risultati dell'esercizio precedente, studiare l'esistenza di sottogruppi normali di un gruppo G di ordine $3 \cdot 5 \cdot 7$, con l'assunzione che $\exists H < G$ di ordine 21.

Svolgimento. Si assume che N sia un potenziale sottogruppo normale di G; allora $[G : N] \mid |G/H|! = 5!$. Unito al fatto che $[G : N] \mid |G|$, si ha che $[G : N] \in \{1, 3, 5, 15\}$. Infine, usando anche la condizione per cui $[G : H] = 5 \mid [G : N]$, quindi le possibilità si riducono a $[G : N] = \{5, 15\}$; in particolare, N non può essere banale, quindi G ammette almeno un sottogruppo normale non-banale. ■