Appunti di Algebra 2

Github Repository: `0xke/appunti/Algebra2`

Secondo semestre, 2024 - 2025, prof. Paola Frediani

I testi preferiti sono

- *Algebra*, di Michael Artin
- *Algebra*, di Herstein

1 Azioni di gruppi su insiemi

Chiameremo G un gruppo e S un insieme

Definizione 1.1: Azione di gruppo

Un'azione (sinistra) di G su S e un'applicazione

$$F : G \times S \to S$$

tale che

i) $F(e, s) = s$ per ogni $s \in S$

ii) $\forall g, h \in G$ e $\forall s \in S$ vale $F(g, F(h, s)) = F(gh, s)$

Si usa anche la notazione $F(g, s) =: g(s)$ che permette la scrittura più concisa

$$e(s) = s \quad \text{e} \quad g(h(s)) = (gh)(s) \quad \forall s \in S, \quad \forall g, h \in G$$

Proposizione 1.1. *Per ogni $g \in G$, l'applicazione $F_g : S \to S$ definita da $F_g(s) = F(g, s) = g(s)$ è una biiezione e in particolare*

$$F_g^{-1} = F_{g^{-1}} \tag{1.1}$$

Dimostrazione.

$$F_g \circ F_{g^{-1}}(s) = g(g^{-1}(s)) \overset{(ii)}{=} e(s) \overset{(i)}{=} s$$

e analogamente per l'altra composizione □

Proposizione 1.2. *L'applicazione $\psi : G \to S(S) = \{f : S \to S \text{ biunivoche}\}$ dove $S(S)$ il gruppo delle permutazioni di S è un omomorfismo di gruppi.*

Dimostrazione.

$$\psi(gh) = F_{gh} \overset{(ii)}{=} F_g \circ F_h = \psi(g) \circ \psi(h)$$

□

Definizione 1.2: Azione fedele

Un'azione $F : G \times S \to S$ si dice **fedele** se ψ è iniettivo

Osservazione. Ovvero se e solo se $\text{Ker}\psi = \{e\} \iff (\psi(g) = \text{Id}_S \iff g = e)$

Esempio 1.1. Se $S = G$ il gruppo stesso e sia

$$m : G \times G \to G \quad \text{con} \quad m(g,h) = gh$$

la moltiplicazione a sinistra. Allora m è un'azione sinistra, infatti

i) $m(e,h) = eh = h$ per ogni $h \in G$

ii) $m(gg',h) = (gg')h = g(g'h) = m(g,g'h)$ per ogni $g,g',h \in G$

Inoltre m è un'azione fedele, infatti

$$\psi(g)(h) = h \quad \forall h \in G \iff gh = h \implies g = e$$

Osservazione. Se G è un gruppo finito, con $\#G = n$ allora $S(G) \cong S_n$ e poiché ψ è iniettivo, $G \cong \psi(G) < S(G) \cong S_n$ il teorema di Cayley.

Esempio 1.2. Sempre con $G = S$ possiamo considerare l'azione di coniugio

$$\varphi : G \times G \to G \quad \text{con} \quad \varphi(g,h) = ghg^{-1}$$

i) $\varphi(e,h) = ehe^{-1} = h$ per ogni $h \in G$

ii) $\varphi(gg',h) = (gg')h(gg')^{-1} = gg'hg'^{-1}g^{-1} = g(\varphi(g',h))g^{-1} = \varphi(g,\varphi(g',h))$

$\psi : G \to S(G)$ e $\text{Im}\psi = \text{Inn}(G) < \text{Aut}(G)$. Non è necessariamente un'azione fedele, infatti

$$\text{Ker}(\psi) = \{g \in G : \forall h \in G \quad ghg^{-1} = h\} = Z(G)$$

da cui per il primo teorema di isomorfismo

$$G/Z(G) = \text{Inn}(G)$$

Esempio 1.3. Con $G = S_n$ e $S = \{1,\dots,n\}$ allora la funzione

$$(\sigma,i) \mapsto \sigma(i)$$

è ovviamente un'azione

Esempio 1.4. Preso $G \cong \mathbb{Z}/2\mathbb{Z} \cong \{1,\sigma\}$ con $\sigma^2 = 1$ e $S = \mathbb{C}$ allora la funzione

$$F : G \times \mathbb{C} \to \mathbb{C} \quad \text{con} \quad F(1,z) = z \quad \text{e} \quad F(\sigma,z) = \overline{z} \quad \forall z \in \mathbb{C}$$

è un'azione.

Definizione 1.3: Orbita e Stabilizzatore

Sia $F : G \times S \to S$ un'azione di un gruppo G su S. Allora per ogni $s \in S$ si definisce **orbita** di s l'insieme

$$O_s = \{g(s) : g \in G\}$$

e si definisce **stabilizzatore** di s l'insieme

$$\text{stab}_s = \{g \in G : g(s) = s\}$$

Esempio 1.5. Nell'esempio dell'azione di coniugio lo stabilizzatore di h è

$$\mathrm{stab}_h = \{g \in G : ghg^{-1} = h\} = \{g \in G : gh = hg\} = C_G(h)$$

Proposizione 1.3. *Le orbite O_s per un'azione di G sono classi di equivalenza per la relazione di equivalenza su S seguente:*

$$S \sim S' \iff \exists g \in G : s' = g(s) = F(g,s)$$

Dimostrazione. $\sim$ è in effetti una relazione di equivalenza, infatti:

- *riflessiva*: $s = e(s)$
- *simmetrica*: se $s' = g(s)$ allora $s = g^{-1}(s')$ per la proposizione 1.1
- *transitiva*: se $s' = g(s)$ e $s'' = h(s')$ allora $s'' = h(s') = h(g(s)) \overset{(ii)}{=} (hg)(s)$

Ne segue chiaramente che $O_s = [s]_\sim$ e allora $S = \coprod_{s \in S} O_s$ □

Proposizione 1.4. $\mathrm{stab}_s < G$

Dimostrazione. Supponiamo $g, h \in \mathrm{stab}_s$. Allora $g(s) = h(s) = s$, ne consegue che

$$F_{gh^{-1}}(s) = F_g(F_{h^{-1}}(s)) \overset{(1.1)}{=} F_g(F_h^{-1}(s)) = F_g(s) = s$$

□

Definizione 1.4: Azione transitiva

Un'azione $F : G \times S \to S$ si dice **transitiva** se per ogni $s, s' \in S$ esiste $g \in G$ tale che $s' = g(s)$

Proposizione 1.5. *Sia $F : G \times S \to S$ un'azione di gruppo. Allora fissato un $s \in S$, consideriamo $O_s \subseteq S$ e $H := \mathrm{stab}_s < G$. Allora esiste un'applicazione naturale biettiva*

$$\begin{aligned} \Phi : G/H &\longrightarrow O_s \\ gH &\longmapsto \Phi(gH) = g(s) = F(g,s) \end{aligned}$$

Inoltre per ogni $C \in G/H$, $g(\Phi(C)) = \Phi(g(C))$ dove la prima azione è quella di G su O_s e la seconda è quella di G su G/H

Dimostrazione.

- *Ben definita*: se $aH = bH$ allora $b^{-1}a \in H$ e quindi esiste un $h \in H$ tale che $b^{-1}a = h$ e quindi $a = bh$. Allora $F(a,s) = F(bh,s) = F(b, F(h,s)) = F(b,s)$
- *Iniettiva*: supponiamo che esistano $a, b \in G$ tali che $\Phi(aH) = \Phi(bH)$, allora $F(a,s) = F(b,s)$ ma allora

  $$F(b^{-1}a, s) = F(b^{-1}, F(a,s)) = F(b^{-1}, F(b,s)) = F(b^{-1}b, s) = F(e,s) = s$$

  e quindi $b^{-1}a \in H \iff aH = bH$
- *Suriettiva*: per ogni $s' \in O_s$ esiste $g \in G$ tale che $s' = g(s)$ e quindi $s' = g(s) = \Phi(gH)$

□

Corollario 1.5.1. *Se G è un gruppo finito e ho un'azione $F : G \times S \to S$, allora per ogni $s \in S$ vale $\#O_s = [G : stab_s]$ o equivalentemente*

$$\#G = \#O_s \cdot \#\text{stab}_s$$

e inoltre

$$\#G = \sum_{[s] \in S} \#O_s$$

Corollario 1.5.2. *Sia $F : G \times G \to G$ l'azione di coniugio $(g, h) \mapsto ghg^{-1}$. Ricordiamo che* $\text{stab}_a = C(a)$ *e la formula delle classi si traduce in*

$$\#G = \#C(a) \cdot \#O_a = \sum_{[g] \in G} \#O_g = \sum_{[g] \in G} \frac{\#G}{\#C(g)}$$

inoltre se $g \in Z(G)$ allora $C(g) = G$ e dunque

$$\#G = \#Z + \sum_{[g] \in G \setminus Z} \#O_g$$

Teorema 1.6

Sia G un gruppo tale che $\#G = p^n$ con p primo. Allora $Z(G) \neq \{e\}$

Dimostrazione. Se $a \notin Z$ allora $C(a) = p^{n_a}$ con $n_a < n$ e quindi da

$$p^n = \#G = \#Z + \sum_{[g] \in G \setminus Z} \# \frac{p^n}{p^{n_a}}$$

ne deduciamo che $p | \#Z$ □

Corollario 1.6.1. *Sia G un gruppo di cardinalità p^2, con p primo. Allora G è abeliano.*

Dimostrazione. Per il teorema sappiamo che $Z \neq \{e\}$ e quindi $\#Z = p$ oppure $\#Z = p^2$. Nel secondo caso $G = Z$ e quindi è abeliano. Nel primo caso invece esiste un $a \in G \setminus Z$ e dunque $C(a) \neq G$. Ma

$$\{e\} < Z < C(a) < G$$

e quindi $C(a) = Z$ per cardinalità che è assurdo perché $a \in C(a)$ e $a \notin Z$. □

Esempio 1.6. Riprendendo l'esempio della moltiplicazione a sinistra $m : G \times G \to G$. Allora m è un'azione transitiva. Infatti per ogni $g', g'' \in G$ se prendo $h = (g')^{-1} g''$ allora $m(g', h) = g'(g'^{-1} g'') = g''$

Esempio 1.7. Se prendo $GL(V)$ il gruppo lineare delle trasformazioni invertibili su uno spazio vettoriale V, allora l'azione $(T, v) \mapsto Tv$ è transitiva su $V \setminus \{0\}$

Teorema 1.7: Cauchy per gruppi abeliani

Sia G un gruppo abeliano finito e p un primo tale che $p | \#G$. Allora

$$\exists e \neq a \in G \text{ tale che } a^p = e$$

Dimostrazione. Procediamo per induzione su $n = \#G$. Se $2 = \#G$ allora $G = \{e, a\}$ e dunque $a^2 = e$. Supponiamo ora $\#G \geq 3$.

Se G non ha sottogruppi $e \neq H \neq G$ allora G è ciclico di ordine primo. Infatti se G non è ciclico allora esistono due elementi $e \neq g_1, g_2$ e $g_2 \notin \langle g_1 \rangle$. Ma allora $\{e\} \neq \langle g_1 \rangle \neq G$ è un sottogruppo. Dunque G è ciclico, inoltre è di ordine primo perché se così non fosse (ad esempio $n = ab$) allora $\{e\} \neq \langle g^a \rangle \neq G$ è un sottogruppo, con g tale che $< g >= G$.

Allora se G non ha sottogruppi propri esistono $p - 1$ elementi in G di ordine p.

Supponiamo ora che G abbia qualche sottogruppo non banale. Sia $N < G$ con $\{e\} \neq N \neq G$. Allora se $p | \#N$ per ipotesi induttiva si conclude. Se invece $p \not| \#N$ allora G/N è un gruppo abeliano con $\#G/N < \#G$ e quindi per ipotesi induttiva (infatti G/N ha ordine multiplo di p poiché N non lo è) esiste $bN \in G/N$, $b \notin N$ e tale che $b^p \in N$. Allora $b^{p\#N} = e$ e ci resta solo da dimostrare che $c := b^{\#N} \neq e$.

Supponiamo che $c = b^{\#N} = e$. Sappiamo che $MCD(p, \#N) = 1$ e dunque per il teorema di Bézout esistono $\alpha, \beta \in \mathbb{Z}$ tali che $\alpha p + \beta \#N = 1$. Allora

$$bN = (bN)^{\alpha p + \beta \#N} = (bN)^{\alpha p} \cdot (bN)^{\beta \#N}$$

e poiché $b^p \in N$ e $b^{\#N} = e$ otteniamo che $bN = N$ che è assurdo perché $b \notin N$. $\square$

Teorema 1.8: Cauchy

Sia G è un gruppo finito e p è un primo tale che $p | \#G$. Allora

$$\exists a \in G \text{ tale che } \#\langle a \rangle = p$$

Dimostrazione. Vogliamo procedere per induzione su $\#G$. Se $\#G = 2$ è già dimostrato. Se esiste $H < G$ tale che $p | \#H$ concludo per ipotesi induttiva.

Supponiamo dunque che p non divide l'ordine di nessun sottogruppo proprio di G. Dalla formula delle classi

$$\#G = \#Z(G) + \sum_{[a] \in G \setminus Z(G)} \frac{\#G}{\#C(a)}$$

tutti i termini della serie sono divisibili per p, infatti se $a \notin Z$, $C(a) \neq G$ è un sottogruppo proprio e quindi $p \not| \#C(a)$. Allora $p | \#Z$ ma quindi $Z = G$ e quindi G è abeliano. Concludiamo con il teorema di Cauchy per gruppi abeliani. $\square$

Teorema 1.9: Sylow (prima parte)

Sia G un gruppo finito e p un primo tale che esiste $\mathbb{Z} \ni m \geq 1$ tale che $p^m | \#G$ ma $p^{m+1} \not| G$. Allora

$$\exists H < G \text{ tale che } \#H = p^m$$

Dimostrazione. Procediamo per induzione su $\#G$ e su m. Se $\#G = 2$ allora $H = G$. Supponiamo ora $\#G > 2$ e il risultato vero per ogni gruppo di cardinalità minore di G. Se $m = 1$ allora ci si riduce al teorema di Cauchy. Supponiamo ora che $m \geq 2$ e $\#G \geq 3$.

Se esiste $H < G$ proprio con $p^m | \#G$ allora concludo per ipotesi induttiva.

Supponiamo dunque che $p^m \not| \#K$ per ogni $K < G$ proprio.

$$\#G = \#Z(G) + \sum_{[a] \in G \setminus Z(G)} \frac{\#G}{\#C(a)}$$

nuovamente come nel teorema di Cauchy, otteniamo che $p | \#Z$ e quindi per il teorema di Cauchy abbiamo che esiste $e \neq b \in Z$ tale che $b^p = e$. Allora $\langle b \rangle \trianglelefteq G$.

Ma allora poiché $\#(G/\langle b\rangle) = \#G/p$ abbiamo che $p^{m-1}|\#(G/\langle b\rangle)$ e dunque per ipotesi induttiva esiste $\overline{S} < G/\langle b\rangle$ tale che $\#\overline{S} = p^{m-1}$. Allora $S = \pi^{-1}(\overline{S})$ è un sottogruppo di G e $\overline{S} = S/B$. Ne consegue infine che $\#S = p^m$. $\square$

Osservazione. Il sottogruppo H viene detto p-sottogruppo di Sylow di G.