Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 07-04-2020

Testi di riferimento

Per la parte di teoria dei gruppi potranno essere utili soprattutto i seguenti testi.

- J.S. Milne, *Group Theory*, disponibile all'indirizzo `http://www.jmilne.org/math/CourseNotes/gt.html`
  Parti dei capitoli 3 (prodotti semidiretti), 4 (azioni e gruppi di permutazioni), 5 (teorema di Sylow) e 6 (gruppi risolubili).
- I.N. Herstein, *Algebra*
  Sezioni 2.9, 2.11 (alcuni risultati sulle azioni), 2.12 (teorema di Sylow) e 5.7 (gruppi risolubili).

Azioni di gruppi

Definizione

Un'azione di un gruppo G su un insieme X è una funzione

$$G \times X \to X \qquad (g, x) \mapsto gx$$

tale che $\forall\, g, h \in G$ e $\forall\, x \in X$ si ha:

(A1) $(gh)x = g(hx)$;

(A2) $1x = x$.

Si dice anche che X è un G-insieme.

Azioni di gruppi

Definizione

Un'azione di un gruppo G su un insieme X è una funzione

$$G \times X \to X \qquad (g, x) \mapsto gx$$

tale che $\forall\, g, h \in G$ e $\forall\, x \in X$ si ha:

(A1) $(gh)x = g(hx)$;

(A2) $1x = x$.

Si dice anche che X è un G-insieme.

Osservazione

La condizione (A2) non è ridondante: fissato $x_0 \in X$, la funzione

$$G \times X \to X \qquad (g, x) \mapsto x_0$$

soddisfa (A1), ma non (A2) se $\#X > 1$.

Azioni come omomorfismi

Proposizione

Se X è un G-insieme, $\forall\, g \in G$ la funzione

$$\varphi(g) \colon X \to X \qquad x \mapsto gx$$

è biunivoca. Inoltre $\varphi \colon G \to S(X)$ (dove $S(X)$ indica il gruppo delle permutazioni di X) è un omomorfismo di gruppi.

Viceversa, dato un omomorfismo di gruppi $\varphi \colon G \to S(X)$, la funzione

$$G \times X \to X \qquad (g, x) \mapsto \varphi(g)(x)$$

definisce un'azione del gruppo G sull'insieme X.

Dimostrazione

Se X è un G-insieme, per (A1) $\forall\, g, h \in G$ e $\forall\, x \in X$

$$\varphi(gh)(x) = (gh)x = g(hx) = \varphi(g)(\varphi(h)(x)) = (\varphi(g) \circ \varphi(h))(x),$$

quindi $\varphi(gh) = \varphi(g) \circ \varphi(h)$, e resta da vedere che $\varphi(g) \in S(X)$.
Per (A2) $\varphi(1)(x) = 1x = x = \mathrm{id}_X(x)$, per cui $\varphi(1) = \mathrm{id}_X$. Allora

$$\varphi(g)\circ\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = \mathrm{id}_X = \varphi(g^{-1}g) = \varphi(g^{-1})\circ\varphi(g),$$

il che dimostra che $\varphi(g)$ è biunivoca (con inversa $\varphi(g^{-1})$).

Dimostrazione

Se X è un G-insieme, per (A1) $\forall\, g, h \in G$ e $\forall\, x \in X$

$$\varphi(gh)(x) = (gh)x = g(hx) = \varphi(g)(\varphi(h)(x)) = (\varphi(g) \circ \varphi(h))(x),$$

quindi $\varphi(gh) = \varphi(g) \circ \varphi(h)$, e resta da vedere che $\varphi(g) \in S(X)$.
Per (A2) $\varphi(1)(x) = 1x = x = \mathrm{id}_X(x)$, per cui $\varphi(1) = \mathrm{id}_X$. Allora

$$\varphi(g)\circ\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = \mathrm{id}_X = \varphi(g^{-1}g) = \varphi(g^{-1})\circ\varphi(g),$$

il che dimostra che $\varphi(g)$ è biunivoca (con inversa $\varphi(g^{-1})$).

Viceversa, se $\varphi\colon G \to S(X)$ è un omomorfismo di gruppi,
$\forall\, g, h \in G$ e $\forall\, x \in X$

$$(gh)x = \varphi(gh)(x) = (\varphi(g) \circ \varphi(h))(x) = \varphi(g)(\varphi(h)(x)) = g(hx),$$

cioè vale (A1). Inoltre $\varphi(1) = \mathrm{id}_X$, per cui
$1x = \varphi(1)(x) = \mathrm{id}_X(x) = x$, cioè vale (A2).

Esempi

- $gx = x\ \forall\, g \in G$ e $\forall\, x \in X$ (azione banale), corrispondente all'omomorfismo banale $G \to S(X)$.
- $G < S(X) \implies X$ è un G-insieme con l'omomorfismo di inclusione $G \to S(X)$.
- $H < G \implies$ un G-insieme X definito da un omomorfismo $\varphi\colon G \to S(X)$ è anche un H-insieme con $\varphi|_H\colon H \to S(X)$. Più in generale, dato un omomorfismo di gruppi $f\colon G' \to G$, X è anche un G'-insieme con $\varphi \circ f\colon G' \to S(X)$.
- Se X è munito di qualche struttura (spazio topologico, spazio metrico, ...) di solito è interessante vedere X come G-insieme per qualche omomorfismo $G \to \mathrm{Aut}(X) < S(X)$, dove $f \in S(X)$ è un "automorfismo" se preserva la struttura (omeomorfismo, isometria, ...).

Rappresentazioni di gruppi

Sia K un campo e V un K-spazio vettoriale. Un'azione di G su V è una rappresentazione K-lineare di G se è definita da un omomorfismo di gruppi $G \to \mathrm{Aut}_K(V) < S(V)$, dove

$$\mathrm{Aut}_K(V) := \{f \in S(V) \,:\, f \text{ è } K\text{-lineare}\}.$$

Indicando con KG un K-spazio vettoriale con base G (i suoi elementi sono dunque della forma $\sum_{g \in G} a_g g$ con $a_g \in K$ quasi tutti nulli), KG è un anello (anche una K-algebra) con prodotto che estende quello di G per K-bilinearità.

Non è difficile dimostrare che le rappresentazioni K-lineari di G si identificano con i KG-moduli: a un KG-modulo definito da un omomorfismo di anelli $\alpha \colon KG \to \mathrm{End}_K(V) \subseteq \mathrm{End}(V)$ si associa l'omomorfismo di gruppi $\alpha|_G \colon G \to \mathrm{Aut}_K(V) = \mathrm{End}_K(V)^*$ (ben definito perché $G < KG^*$).

L'azione per coniugio di G su G è definita da

$$G \times G \to G \qquad (g, a) \mapsto gag^{-1}$$

(vale (A1) perché $(gh)a(gh)^{-1} = g(hah^{-1})g^{-1}\ \forall\, g, h, a \in G$ e (A2) perché $1a1^{-1} = a$).
Il corrispondente omomorfismo di gruppi $\Gamma \colon G \to S(G)$ è tale che

$$\mathrm{Int}(G) := \mathrm{im}(\Gamma) < \mathrm{Aut}(G) < S(G)$$

(dove $\mathrm{Aut}(G) := \{f \in S(G) \ : \ f \text{ omomorfismo}\}$ è il gruppo degli automorfismi di G) perché $\forall\, g, a, b, \in G$

$$\Gamma(g)(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \Gamma(g)(a)\Gamma(g)(b).$$

Gli elementi di $\mathrm{Int}(G)$ si dicono automorfismi interni di G.
Ricordiamo anche che

$$\ker(\Gamma) = \{g \in G \ : \ \Gamma(g)(a) = gag^{-1} = a\ \forall\, a \in G\} = Z(G).$$

Azione per traslazione

L'azione per traslazione (o per moltiplicazione) a sinistra di G su G è definita da

$$G \times G \to G \qquad (g, a) \mapsto ga$$

(vale (A1) perché il prodotto di G è associativo e (A2) perché 1 è elemento neutro). Il corrispondente omomorfismo di gruppi $L\colon G \to S(G)$ è iniettivo (teorema di Cayley).

Azione per traslazione

L'azione per traslazione (o per moltiplicazione) a sinistra di G su G è definita da

$$G \times G \to G \qquad (g, a) \mapsto ga$$

(vale (A1) perché il prodotto di G è associativo e (A2) perché 1 è elemento neutro). Il corrispondente omomorfismo di gruppi $L \colon G \to S(G)$ è iniettivo (teorema di Cayley).

Analogamente, dato $H < G$, la funzione

$$G \times G/H \to G/H \qquad (g, C) \mapsto gC := \{gc \, : \, c \in C\}$$

(ben definita perché se $C = aH$, $gC = g(aH) = (ga)H$) è un'azione (esercizio). Indicheremo ancora con $L \colon G \to S(G/H)$ il corrispondente omomorfismo di gruppi (in generale non iniettivo).

Azioni sinistre e azioni destre

Le azioni definite prima andrebbero più correttamente chiamate azioni sinistre.

Analogamente un'azione destra di un gruppo G su un insieme X è una funzione

$$X \times G \to X \qquad (x, g) \mapsto xg$$

tale che $\forall\, g, h \in G$ e $\forall\, x \in X$ si ha:

- $x(gh) = (xg)h$;
- $x1 = x$.

È facile vedere che dare un'azione destra di G su X equivale a dare un omomorfismo di gruppi $G^{op} \to S(X)$ (il gruppo opposto G^{op} di G coincide con G come insieme, ma il prodotto gh in G^{op} è definito come il prodotto hg in G).

Osservazione

La funzione $G \to G^{op}$, $g \mapsto g^{-1}$ è un isomorfismo di gruppi (esercizio).