Istituzioni di A & G — ALGEBRA, lezione 10

17/10/22

Il gruppo simmetrico S_n

Riprendiamo in considerazione uno dei primi esempi visti, e approfondiamone lo studio.

Definizione 1. *Una biezione di $I_n = \{1, 2, \ldots, n\}$ in se stesso è detta* ***permutazione****. L'insieme di tutte le permutazioni di I_n è un gruppo rispetto alla composizione di funzioni, detto* ***gruppo simmetrico di ordine*** n *e indicato con S_n (a volte anche $\mathfrak{S}_n$ o Σ_n).*

Ricordiamo che S_n ha $n!$ elementi. (Perché?)

Notazione:

$$S_n \ni \sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Def: $\sigma \in S_n$: $sgn(\sigma) :=$ parità del numero di trasposizioni in cui si decompone $\sigma = \begin{cases} +1 \\ -1 \end{cases}$

8

La decomposizione in trasposizioni non è unica, ma vale il seguente risultato.

Teorema 6. *Il numero di trasposizioni in cui si può decomporre una permutazione o è sempre pari o è sempre dispari.*

Questo ci permette di dare la seguente definizione.

Definizione 7. *Una permutazione è detta* **pari** *(o* **dispari***) se tale è il numero di trasposizioni in cui si decompone.*

Definizione 8. *Le permutazioni pari di S_n formano un gruppo, detto* **gruppo alterno** *e denotato con A_n.*

dim (teorema 6)

· Sia $\sigma \in S_n$. Sia $P \in \mathbb{N}$ definito come

$$P = \prod_{\substack{i,j \in I_n \\ i<j}} (i-j) = (1-2)(1-3) \cdots (1-n) \cdots ((n-1)-n)$$

· Operiamo su P con la permutazione σ:

$$\sigma(P) = \prod_{\substack{i,j \in I_n \\ i<j}} (\sigma(i) - \sigma(j)) = \pm P$$

Vediamo come agisce una trasposizione $\tau = (h\,k)$, $h < k$ su P:

caso 1: il fattore $(i-j)$ con $\{i,j\} \neq \{h,k\}$ non cambia

9

caso 2: il fattore $(h-k)$ diventa $(k-h) = -(h-k)$

caso 3: se $j > k \Rightarrow$ il fattore $(h-j) \to (k-j)$

$(k-j) \to (h-j)$

stesso segno

caso 4: se $i < h \Rightarrow$

$(i\,h) \to (i\,k)$

$(i,k) \to (i\,h)$

caso 5: se $h < j < k$, allora:

$(h-j) \to (k-j) = -(j-k)$

$(j-k) \to (j-h) = -(h-j)$

si cancellano mutualmente

Allore $\tau_{hk}(P) = -P$

siano $\sigma = \tau_1 \cdots \tau_n = \mu_1 \cdots \mu_m$ due scomposizione di σ come prodotto di trasposizioni. Allore

$$\left.\begin{array}{l} \sigma(P) = \tau_1 \cdots \tau_n(P) = (-1)^n P \\ \quad \shortparallel \\ \mu_1 \cdots \mu_m(P) = (-1)^m P \end{array}\right\} \Rightarrow n \text{ è } m \text{ hanno le stesse parità}$$

$\square$

Oggi possiamo definire

$$\begin{aligned} sgn : S_n &\to \{\pm 1\} \\ \sigma &\to sgn(\sigma) \end{aligned}$$

sgn è omomorfismo di gruppo:

$$sgn(\sigma_1 \cdot \sigma_2) = sgn(\sigma_1) \cdot sgn(\sigma_2)$$

$Ker(sgn) = A_n$ gruppo alterno

Scanned with CamScanner

6

L'importanza del gruppo simmetrico segue dal seguente risultato.

Teorema 9 (Teorema di Cayley). *Ogni gruppo è isomorfo a un gruppo di permutazioni sull'insieme dei suoi elementi.*

Corollario 10. *Sia G un gruppo finito di ordine n, allora G è isomorfo ad un sottogruppo del gruppo simmetrico S_n.*

dim (Teorema Cayley): sia $Simm(G) := \{$ permutazione di $G \}$

sia $a \in G$. Definiamo:

$$\lambda_a : G \to G$$
$$g \to \lambda_a(g) := a \cdot g$$

λ_a è biettiva:

iniettiva: i) se $\lambda_a(g) = \lambda_a(g') \Rightarrow a \cdot g = ag' \underset{\uparrow}{\Rightarrow} g = g'$

legge cancellazione

suriettiva ii) sia $g \in G$, allora $\lambda_a(a^{-1}g) = a(a^{-1}g) = g$

Altrimenti: $\lambda_{a^{-1}}$ è inversa di λ_a

Abbiamo definito:

$$\lambda : G \longrightarrow Sym(G)$$
$$a \longmapsto \lambda_a$$

- λ è omomorfismo:
  - $\lambda_{a \cdot a'}(g) = (a \cdot a')g = a \cdot (a'g) = a \cdot (\lambda_{a'} g) = \lambda_a \cdot \lambda_{a'}(g)$
- λ è iniettiva: Sia e il neutro di G. Allora

$$\lambda_e(g) = e \cdot g = g \quad \forall g \Rightarrow \lambda_e = Id \in Sym(G)$$

$\square$

Gruppi ciclici

Un gruppo $(G, \cdot)$ è ciclico se esiste un elemento $x \in G$ tale che $G =< x >= \{x^n \mid n \in \mathbb{Z}\}$.

Proposizione 11. *Ogni gruppo ciclico è abeliano.*

dim: $x^n, x^m \in G$: $x^n \cdot x^m = x^{n+m} = x^{m+n} = x^m \cdot x^n$ $\square$

Attenzione che non vale il viceversa!

Proposizione 12. *Siano $(G, \cdot)$ un gruppo e $x \in G$ un suo elemento. Se esistono $s, t \in \mathbb{Z}$ tali che $s \neq t$ e $x^s = x^t$, allora:*

1. *esiste un minimo intero positivo n tale che $x^n = 1_G$;*
2. *se m è un intero, $x^m = 1_G$ se e solo se $n|m$;*
3. *gli elementi $x^0 = 1_G$, $x^1 = x, \ldots, x^{n-1}$ sono tutti distinti e $< x >= \{1, x, x^2, \ldots, x^{n-1}\}$.*

Corollario 13. *L'ordine di un elemento coincide con la cardinalità del sottogruppo ciclico da lui generato.*

dim (prop 12).

1) $x^s = x^t$ con $s > t$. Allora $x^{s-t} = 1 \Rightarrow$

$\exists$ n tale che $x^n = 1$. Sia

$S = \{n \in \mathbb{N} \mid x^n = 1\}$

Per il principio del buon ordinamento, $\exists \min(S) = ord(x)$

2) visto prima

3) se $x^i = x^j$ con $0 \le i < j < n = \text{ord}(x) \Rightarrow$

$x^{j-i} = 1 \Rightarrow j - i = 0$

n è il minimo

con questa proprietà

14

Vediamo che $\langle x \rangle = \{1, -, x^{n-1}\}$

$\langle x \rangle \subseteq \{1 - x^{n-1}\}$: sia $m \in \mathbb{Z}$ m si scrive

$m = a \cdot n + b$ $0 \le b < n$

$x^m = x^{a \cdot n} \cdot x^b = 1 \cdot x^b \in \{1 - x^{n-1}\}$

$\{1 - x^{n-1}\} \subseteq \langle x \rangle$: ovvio.

Proposizione 14. *Ogni sottogruppo di un gruppo ciclico è ciclico.*

dim: (oss: stessa dimostrazione che nel caso di $(\mathbb{Z}, +)$)

sia $G = \langle x \rangle$, sia $H < G$ sottogruppo:

i) se $H = \{1_G\} \Rightarrow H = \langle x^0 \rangle$ è ciclico

ii) se $H \neq \{1_G\}$ contiene potenze positive di x

sia $S = \{ n \in \mathbb{N} \mid x^n \in H \} \neq \emptyset$

Prendiamo $n_0 = \min(S) \in \mathbb{N}$

Allora $H = \langle x^{n_0} \rangle$

$\square$