Complementi agli Appunti di Teoria dei Gruppi.

Roberto Catenacci

Versione del 14 Ottobre 2009

Argomenti selezionati di Teoria dei Gruppi svolti a lezione e nei seminari, non contenuti negli *Appunti per il corso di Teoria dei Gruppi*.

Testi di riferimento consigliati:

I.N. Herstein, *Algebra*, Editori Riuniti, 3a edizione, Roma 1994
M. Artin, *Algebra*, Bollati Boringhieri, Torino 1997
S. Lang: *Algebra* (third ed.) Springer 2002
H. F. Jones: *Groups, representations and physics* Adam Hilger ed. 1990

Indice

1 La Formula delle Classi

Definizione 1.1 *Sia G un gruppo finito. Due elementi del gruppo, a e a', si dicono coniugati se $\exists\ x \in G$ tale che:*

$$a' = x^{-1}ax$$

E' facile verificare che la relazione definita è di equivalenza; ci proponiamo di calcolare la cardinalità dell'insieme $cl(a)$ (detto classe di coniugio) dei coniugati di un dato elemento a :

$$cl(a) = \{x^{-1}ax \text{ con } x \in G\}$$

e dimostrare un'importante formula, detta **formula delle classi.**

Definizione 1.2 *Sia $a \in G$, il centralizzante di a è l'insieme:*

$$C(a) = \{x \in G |\ ax = xa\ \}$$

In altre parole, è l'insieme degli elementi di G che commutano con a. Il centralizzante di ogni elemento contiene il centro del gruppo $Z(G)$, essendo quest'ultimo l'insieme degli elementi di G che commutano con *tutti* gli elementi di G. Quindi $C(a) \supseteq Z(G)$

Lemma 1.1 *$C(a)$ è un sottogruppo di G , inoltre $a \in Z(G)$ se e solo se $C(a) = G$.*

Prova. Se $x, y \in C(a)$ si ottiene: $xya = xay = axy$, inoltre $x^{-1}a = x^{-1}axx^{-1} = x^{-1}xax^{-1} = ax^{-1}$. Inoltre, $C(a) = G$ se e solo se a commuta con ogni elemento di G, e quindi se e solo se $a \in Z(G)$. ■

Lemma 1.2 *Il numero degli elementi coniugati ad a è l'indice di $C(a)$. In altri termini:*

$$\#cl(a) = \frac{\#G}{\#C(a)}$$

Prova. Mostreremo che c'è corrispondenza biunivoca tra coniugati di a e laterali di $C(a)$.Se $x, y \in$ allo stesso laterale, allora $y = cx$ con $c \in C(a)$. Allora $ac = ca$ e quindi

$$y^{-1}ay = x^{-1}c^{-1}acx = x^{-1}c^{-1}cax = x^{-1}ax$$

Allora x e y corrispondono ad uno stesso coniugato di a. Viceversa, laterali distinti corrispondono a coniugati distinti, perchè, se così non fosse:

$$y^{-1}ay = x^{-1}ax \implies xy^{-1}ay = ax \implies xy^{-1}a = axy^{-1} \implies xy^{-1} \in C(a)$$

■

Il lemma 1.2 fornisce la cosiddetta formula delle classi:

Teorema 1.1 *(Formula delle classi) Se S è un insieme di rappresentanti per le classi di coniugio, allora:*

$$\#G = \sum_{a \in S} \frac{\#G}{\#C(a)}$$

Prova. Basta osservare che, per definizione, $\sum_{a \in S} \#cl(a) = \#G$. ■

1.1 Applicazioni

Teorema 1.2 *Un gruppo di ordine p^n con p primo ha centro non banale.*

Prova. L'ordine di qualsiasi centralizzatore (per il teorema di Lagrange) deve essere un divisore di p^n e quindi deve essere p^{n_α} con $n_\alpha \leq n$. Sappiamo dal lemma 1.1 che $a \in Z(G)$ se e solo se $p^n = p^{n_\alpha}$. Se $a \in Z(G)$ si ha chiaramente $\#cl(a) = 1$, quindi spezzando S come una unione *disgiunta*

$$S = Z(G) \cup S' \tag{1}$$

otteniamo un'altra utile espressione per la formula delle classi:

$$\#G = \sum_{a \in Z(G) \cup S'} \frac{\#G}{\#C(a)} = \sum_{a \in Z(G)} \#cl(a) + \sum_{a \in S'} \frac{\#G}{\#C(a)} = \#Z(G) + \sum_{a \in S'} \frac{\#G}{\#C(a)} \tag{2}$$

Abbiamo allora:

$$p^n = \sum_{n_\alpha \leq n} \frac{p^n}{p^{n_\alpha}} = \#Z(G) + \sum_{n_\alpha < n} \frac{p^n}{p^{n_\alpha}}$$

Segue che p deve dividere $\#Z(G)$, che quindi deve essere > 1. ∎

Teorema 1.3 *Un gruppo di ordine p^2 con p primo è abeliano.*

Prova. Basta mostrare che $G = Z(G)$. Sappiamo dal teorema 1.2 e dal teorema di Lagrange che $\#Z(G)$ è p oppure p^2. Supponiamo che sia p, allora $\exists a \notin Z(G)$ e quindi $\#Z(G) < \#C(a)$ perchè $a \in C(a)$. Dal teorema di Lagrange segue ora che $\#C(a)$, dovendo dividere $\#G$ ed essendo $> \#Z(G)$ per l'osservazione precedente, non può che essere p^2. Allora deve essere $C(a) = G$ e, per il lemma 1.1, $a \in Z(G)$, e questa è una contraddizione. Deve quindi aversi $\#Z(G) = p^2 = \#G$ ∎

2 Il teorema di Sylow

Il teorema di Lagrange afferma che l'ordine di un sottogruppo divide l'ordine del gruppo. Nulla però assicura che, se m è un qualsiasi divisore dell'ordine di un gruppo G, ci sia effettivamente un sottogruppo H di ordine m. Il più importante risultato in questa direzione è il cosiddetto Teorema di Sylow.
Prima di darne una semplice dimostrazione, è opportuno richiamare un risultato di carattere combinatorio. Se $\mathcal{S}$ è un insieme di n elementi, il numero dei suoi sottoinsiemi di k elementi è dato dal coefficiente binomiale $\binom{n}{k}$,dove:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)...(n-i)...(n-k+1)}{k(k-1)(k-2)...(k-i)...(k-k+1)}$$

Avremo bisogno anche del seguente risultato:

Lemma 2.1 *Se m è divisibile per p^r ma non per p^{r+1} , allora lo stesso è vero per $\binom{p^\alpha m}{p^\alpha}$.*

Prova. Sia

$$\binom{p^\alpha m}{p^\alpha} = \frac{p^\alpha m(p^\alpha m-1)(p^\alpha m-2)...(p^\alpha m-i)...(p^\alpha m-p^\alpha+1)}{p^\alpha(p^\alpha-1)(p^\alpha-2)...(p^\alpha-i)...(p^\alpha-p^\alpha+1)}$$

Se $(p^\alpha m-i)$ è divisibile per una certa potenza p^β, allora, essendo $i \leq p^\alpha$ è chiaro che $\beta \leq \alpha$. Si ottiene quindi $i = p^\alpha m - qp^\beta = p^\beta(p^{\alpha-\beta}m-q)$. Risulta allora che anche $p^\alpha - i = p^\beta(p^{\alpha-\beta}+q-p^{\alpha-\beta}m)$ è divisibile per p^β. In definitiva tutte le potenze di p si semplificano, eccetto p^r, l'unica che compare anche in m. ∎

Passiamo ora a enunciare e dare una dimostrazione del Teorema di Sylow.

Teorema 2.1 *(Teorema di Sylow) Sia p^α con p primo un divisore dell'ordine $n = p^\alpha m$ di un gruppo G. Allora G ha un sottogruppo H di ordine p^α.*

Prova. Dato il gruppo G, di ordine $p^\alpha m$, sia M l'insieme costituito dai sottoinsiemi di G che contengono p^α elementi. Definiamo in M una relazione binaria: $M_1 \sim M_2$ se $\exists\ g \in G$ tale che $M_2 = M_1 g$. La relazione binaria ora definita è chiaramente di *equivalenza*; infatti $M_i = M_i e$ e quindi la relazione è *riflessiva*; se $M_2 = M_1 g$ allora $M_1 = M_2 g^{-1}$ e quindi la relazione è *simmetrica*; e se $M_2 = M_1 g$ e $M_3 = M_2 g'$ allora $M_3 = M_1 gg'$ e quindi la relazione è anche *transitiva*. Ci occupiamo ora della cardinalità delle classi di equivalenza. Sia p^r la massima potenza di p che divide m. Se la cardinalità di ognuna di queste classi fosse divisibile per p^{r+1}, lo sarebbe anche $\binom{p^\alpha m}{p^\alpha}$, (perchè questo coefficiente binomiale è la cardinalità dell'insieme M che è uguale alla somma delle cardinalità delle singole classi di equivalenza), ma questo è impossibile per il Lemma 2.1. Esiste allora almeno una classe di equivalenza di cardinalità k non divisibile per p^{r+1}. Sia $C = \{M_1, M_2, ...M_k\}$ una tale classe. Costruiamo ora il sottogruppo cercato. Consideriamo il sottoinsieme H di G definito da:

$$H = \{g \in G \mid M_i g = M_i \text{ per } i = 1...k\}$$

E' chiaro che H è un sottogruppo di G; infatti $e \in H$, e se $M_i = M_i g$ e $M_i = M_i g'$ allora $M_i = M_i gg'$; quale è il suo ordine? (Ovviamente vorremmo proprio che $\#H = p^\alpha$). Mostriamo che $\#H \leq p^\alpha$. Sia $m_1 \in M_1$ allora, per la definizione di H, si trova che $m_1 h \in M_1 \forall h$. Siccome M_1 ha p^α elementi, H non può averne di più. Se mostriamo ora che $\#H \geq p^\alpha$, abbiamo finito. Osserviamo che possiamo costruire una funzione

$$\Phi : C = \{M_1, M_2, ...M_k\} \to \{\text{Laterali di } H \text{ in } G\} :$$

$$\Phi(M_i) = Hx$$

(dove x è tale che $M_i x = M_1$; tali x esistono perchè $M_i \sim M_1$). Occorre controllare che la definizione di Φ abbia senso, cioè che se $M_i x = M_1$ e $M_i y = M_1$ allora $Hx = Hy$. Ciò è vero, perchè se $M_i x = M_1$ e $M_i y = M_1$ allora $M_i x = M_i y$ e quindi $xy^{-1} \in H$ e allora x e y danno origine allo stesso laterale di H in G.

• Φ è iniettiva. Infatti, se $\Phi(M_i) = \Phi(M_j)$ allora $Hx = Hy$ cioè $xy^{-1} \in H$ e quindi $M_i xy^{-1} = M_i$; essendo $M_i x = M_1 = M_j y$ si ha anche che $M_i xy^{-1} = M_j$, e quindi $M_i = M_j$.

• Φ è suriettiva. Infatti, preso un qualsiasi x, $M_1 x^{-1} \sim M_1$ (basta osservare che $(M_1 x^{-1})x = M_1(x^{-1}x) = M_1$) e quindi $M_1 x^{-1} \in C$. Inoltre, per definizione di Φ, si ottiene $\Phi(M_1 x^{-1}) = Hx$. Otteniamo allora una biiezione:

$$\{M_1, M_2, ...M_k\} \overset{\Phi}{\rightleftarrows} \{\text{Laterali di } H \text{ in } G\}$$

Passando alle cardinalità si ottiene :

$$k \times \#H = \#G = p^\alpha m$$

Si ricordi ora che k e m non sono divisibili per p^{r+1} e che m è divisibile per p^r. Sia p^s con $s \leq r$ la massima potenza di p che divide k. Allora abbiamo

$$p^s q' \times \#H = p^\alpha p^r q$$

dove q e q' non contengono il fattore p. Quindi l'unica possibilità è che $p^{\alpha+r-s}$ divida $\#H$, e quindi $\#H \geq p^\alpha$. ■

Esempio 2.1 *Seguiamo passo passo la dimostrazione in un caso semplice, quello del gruppo* $(\mathbb{Z}_5)^* = \{1, 2, 3, 4\}$. *Sappiamo che* $\#(\mathbb{Z}_5)^* = 4$ *e quindi possiamo cercare un sottogruppo* H *di ordine* 2. *E' immediato verificare che ci sono due classi di sottoinsiemi di due elementi :* $C = \{M_1, M_2\}$ *e* $N = \{N_1, N_2, N_3, N_4\}$. *A noi interessa la classe* C *(quella la cui cardinalità è divisibile per* 2 *ma non per* 4*) dove* $M_1 = \{2, 3\}$ *e* $M_2 = \{1, 4\}$.*(Osservare che* $\{1, 4\} \cdot 2 = \{2, 3\}$*). Il sottogruppo* H *risulta essere* $H = \{1, 4\}$, *infatti* $\{2, 3\} \cdot 4 = \{2, 3\}$ *e* $\{1, 4\} \cdot 4 = \{1, 4\}$. *Si vede anche che* $\Phi\{2, 3\} = H = \{1, 4\}$ *e* $\Phi\{1, 4\} = H \cdot 2 = \{2, 3\}$.

Il teorema di Sylow ha molte interessanti conseguenze.

Definizione 2.1 *Dato un primo* p *e un gruppo* G, p *è detto ammissibile se divide l'ordine di* G.

Definizione 2.2 *Un sottogruppo* H *si dice essere un* p*-Sylow (dove* p *è un primo ammissibile) se il suo ordine è* p^m *, dove* p^m *divide l'ordine di* G *ma* p^{m+1} *non divide l'ordine di* G.

Segue dal teorema di Sylow che un gruppo finito ha un *p-Sylow* per ogni p ammissibile. Lo studio dei *p-Sylow* di un gruppo può dare moltissime informazioni sul gruppo.

Definizione 2.3 *Siano* A *e* B *due sottogruppi di* G, *si dice che* A *e* B *sono coniugati se esiste un* $x \in G$ *tale che* $A = xBx^{-1}$.

Definizione 2.4 *Sia* H *un sottogruppo di* G, *il normalizzatore di* H *è il sottogruppo:*

$$N(H) = \{x \in G \mid xHx^{-1} = H\}$$

Seguendo esattamente lo stesso ragionamento che porta alla dimostrazione della formula delle classi, si trova che:

$$\#\{xHx^{-1} \text{ con } x \in G\} = \text{ numero dei coniugati di } H \ = \frac{\#G}{\#N(H)}$$

In particolare, *il numero dei coniugati di H è un divisore dell'ordine di G.*

Si può dimostrare, ma noi non lo faremo, il seguente:

Teorema 2.2 *Tutti i p-Sylow di un gruppo sono coniugati tra loro.*

Segue immediatamente che il numero dei *p-Sylow* divide l'ordine di G (ed è $\frac{\#G}{\#N(H)}$ dove H è un qualsiasi *p-Sylow*). Segue anche che se esiste un *unico p-Sylow,* questo è normale, perchè deve coincidere con ogni suo coniugato (e allora $xHx^{-1} = H$ per tutti gli x).

Si può anche dimostrare, ma noi non lo faremo, il seguente:

Teorema 2.3 *Per ogni dato primo ammissibile p, il numero dei p-Sylow distinti è della forma $1 + np$, dove n è un intero.*

2.1 Applicazioni

Esempio 2.2 *Un gruppo G di ordine $20\,449 = 11^2 \times 13^2$ è abeliano. (questo esempio non è importante per il suo contenuto ma per le idee sviluppate)*

Ragioniamo così: ci sono degli 11-Silow e dei 13-Sylow. Dai teoremi 2.2 e 2.3 segue che devono essere unici e quindi sono normali. Sono inoltre abeliani (hanno ordini che sono il quadrato di un primo, vedi teorema 1.3). G ha quindi un sottogruppo normale abeliano H di ordine 11^2 e un sottogruppo normale abeliano K di ordine 13^2. E' chiaro (per il teorema di Lagrange) che $H \cap K = \{e\}$. Osserviamo ora che si può definire un omomorfismo θ :

$$\theta : G \to \frac{G}{H} \times \frac{G}{K}$$

$$\theta(g) = (gH, gK)$$

Il nucleo di θ è chiaramente $H \cap K = \{e\}$, inoltre θ è suriettivo, e quindi θ è un isomorfismo.

Ma $\frac{G}{H}$ ha ordine 13^2 e $\frac{G}{K}$ ha ordine 11^2 e quindi sono entrambi abeliani. Ne segue che G è abeliano.

In presenza di H e K con le proprietà descritte sopra si può anche ragionare così: consideriamo l'insieme HK; è un sottoinsieme di G, ma essendo l'intersezione ridotta al solo $\{e\}$, deve coincidere con G (le cardinalità sono uguali). Si verifica anche immediatamente che $hk = kh$: infatti $hkh^{-1}k^{-1} \in K$ perchè K è normale, ed inoltre $\in H$ perchè anche H lo è; allora $\in H \cap K = \{e\}$ e quindi $hkh^{-1}k^{-1} = e \Rightarrow hk = kh$. Quindi, utilizzando anche il fatto osservato sopra che H e K sono abeliani, se $g = hk$ e $g' = h'k'$, si ottiene:

$$gg' = hkh'k' = hh'kk' = h'hk'k = h'k'hk = g'g$$

e quindi il gruppo è abeliano. Si può osservare anche che $G = H \times K$. Infatti si può definire un omomorfismo φ :

$$\varphi : G = HK \to H \times K$$

$$\varphi(hk) = (h, k)$$

La scomposizione $g = hk$ è unica:

$$hk = h'k' \Longrightarrow h^{-1}h' = kk'^{-1} \in H \cap K = \{e\} \implies h = h' \text{ e } k = k'$$

Quindi φ è ben definito e il suo nucleo è $\{e\}$; essendo ovviamente suriettivo, è un isomorfismo.

Teorema 2.4 *Sia G un gruppo di ordine $2p$ con $p \geq 3$ primo. Allora $G = \mathbb{Z}_{2p}$ oppure $G = D_p$ (per la definizione di D_p vedere la sezione 4.2)*

Prova. Esistono due tipi di sottogruppi di Sylow, i 2-Sylow e i p-Sylow di ordini, rispettivamente, 2 e p. Il p-Sylow è sempre unico, perchè $1 + kp$ divide $2p$ solo quando vale 1. I 2-Sylow possono essere 1 oppure p, infatti $1 + 2k$ divide $2p$ solo quando vale 1 oppure p.

Nel caso di unicità anche del sottogruppo di ordine due, il gruppo è abeliano ed è il prodotto dei suoi sottogruppi di Sylow ($\mathbb{Z}_2$ e $\mathbb{Z}_p$) per il ragionamento esposto nell'esempio precedente. Si ha quindi: $G = \mathbb{Z}_2 \times \mathbb{Z}_p = \mathbb{Z}_{2p}$.

Nel caso in cui i 2-Sylow sono p, i $2p - 1$ elementi del gruppo diversi dall'identità si ripartiscono in p elementi di ordine 2 denotati con b_i (quelli che stanno nei 2-Sylow) e $p-1$ elementi di ordine p denotati con c_j (quelli che stanno nell'unico p-Sylow che chiameremo C). Un prodotto di tipo $c_1 b_1$ può quindi avere ordine p oppure ordine 2. Il primo caso non può presentarsi perchè sarebbe $c_1 b_1 = c_2$ per qualche elemento di tipo c; ma allora $b_1 = c_1^{-1} c_2$ avrebbe ordine p e questo è assurdo. Quindi il prodotto di un elemento di tipo c e uno di tipo b ha ordine 2 e quindi da $(cb)^2 = e$ segue $cb = b^{-1}c^{-1} = bc^{-1}$ (da questa formula si nota anche che il gruppo non è abeliano); il prodotto di due elementi di tipo c è ancora di tipo c e questi due fatti implicano che il prodotto di due elementi distinti i tipo b sia un elemento di tipo c (infatti da $c_1 b_1 = b_2$ segue che $b_2 b_1 = c_1$). Questa è esattamente la struttura del gruppo diedrale D_p come descritto nella sezione 4.2. ■

Osservazione 2.1 *Questo teorema testimonia sia l'importanza dei gruppi diedrali, caratterizzandoli come gli* ***unici gruppi non abeliani di ordine*** (≥ 6) ***il doppio di un numero primo****, sia quella dei gruppi ciclici, e ne giustifica lo studio affrontato più sotto.*

Osservazione 2.2 *Un risultato simile vale nel caso di gruppi di ordine qp con $q < p$ e q, p primi; se q non divide $p - 1$ allora il gruppo è necessariamente ciclico. Infatti se q non divide $p - 1$ allora esiste un unico q-Sylow ($1 + kq = p$ se e solo se $k = 0$) e anche un unico p-Sylow ($1 + kp = q$ se e solo se $k = 0$). Il gruppo risulta allora ciclico in quanto prodotto di sottogruppi ciclici di ordini primi fra loro. Se invece q divide $p - 1$, appare anche un unico gruppo non abeliano (che non può però, se $q > 2$, essere un gruppo diedrale).*

Esercizi consigliati

- Mostrare che un gruppo di ordine 99 è abeliano, e fornire due esempi non isomorfi. (Usare anche il Teorema Cinese del Resto)
- Un gruppo di ordine $1225 = 5^2 7^2$ è abeliano. (Usare il fatto che un gruppo di ordine primo è ciclico)
- Un gruppo di ordine $5 \times 13 \times 17$ è abeliano. (Usare anche il sottogruppo dei commutatori)
- Un gruppo di ordine 56 ha sottogruppi normali. (Usare il fatto che un gruppo di ordine primo è ciclico e ragionare sugli elementi di ordine 7)

3 Gruppi di mappe

Sia X un insieme qualsiasi non vuoto; denotiamo con $S(X)$ l'insieme di tutte le funzioni di X in sè stesso:

$$S(X) = \{f : X \to X\}$$

Se $f, g \in S(X)$, allora risulta definita la composizione $g \circ f$ mediante:

$$(g \circ f)(x) = g(f(x))$$

che definisce un'operazione naturale sull'insieme $S(X)$. Quello che ci si potrebbe attendere è il fatto che l'insieme $S(X)$ abbia la struttura di gruppo rispetto all'operazione così definita; purtroppo ciò non risulta essere vero, essenzialmente a causa della mancanza di un'inversa per una generica funzione in $S(X)$. L'idea successiva è dunque quella di restringere la nostra attenzione al sottoinsieme delle funzioni invertibili di $S(X)$. Cominciamo tuttavia a dimostrare il seguente:

Teorema 3.1 *La composizione è un'operazione associativa su $S(X)$ con elemento neutro ι_X. In particolare essa risulta essere un'operazione associativa sul sottoinsieme delle funzioni invertibili di $S(X)$.*

Prova. Dobbiamo provare che date $\alpha, \beta, \gamma \in S(X)$, si ha:

$$\gamma \circ (\beta \circ \alpha) = (\gamma \circ \beta) \circ \alpha$$

il che è equivalente a provare che per ogni $x \in X$ si abbia:

$$[\gamma \circ (\beta \circ \alpha)](x) = [(\gamma \circ \beta) \circ \alpha](x).$$

Dunque si ha:

$$\begin{aligned}[\gamma \circ (\beta \circ \alpha)](x) &= \gamma(\beta \circ \alpha(x)) \\ &= \gamma(\beta(\alpha(x))) \\ &= (\gamma \circ \beta)(\alpha(x)) \\ &= [(\gamma \circ \beta) \circ \alpha](x).\end{aligned}$$

Ricordando poi che la mappa ι_X è definita da: $\iota_X(x) = x, \forall x \in X$, è immediato verificare che essa svolge la funzione di elemento neutro rispetto a $\circ$, cioè che $\forall f \in S(X)$, $f \circ \iota_X = \iota_X \circ f = f$. Restringendo il discorso all'insieme $S_{inv}(X)$ delle funzioni invertibili di $S(X)$, è sufficiente notare che la composizione di mappe invertibili risulta essere ancora una mappa invertibile (cioè $\circ$ è un'operazione su $S_{inv}(X)$), e che essendo associativa su $S(X)$ lo è necessariamente anche su un suo sottoinsieme. Infine osserviamo che $\iota_X \in S_{inv}(X)$. ■

Esempio 3.1 *Sia π un piano, e sia $p \in \pi$ un punto fissato. Indichiamo con G l'insieme di tutte le rotazioni del piano intorno ad una retta perpendicolare passante per p. Ogni elemento di G rappresenta un elemento di $S(\pi)$. Se $\alpha, \beta \in G$, allora $\beta \circ \alpha$ è la rotazione ottenuta applicando prima α e poi β. L'elemento neutro è rappresentato dalla rotazione di $0°$ (a meno di multipli di 2π), ed ogni rotazione ha un elemento inverso, cioè la rotazione della stessa ampiezza nella direzione opposta. Si può concludere che G risulta avere la struttura di gruppo commutativo, in quanto la rotazione generata dall'applicazione di rotazioni successive non dipende dall'ordine delle stesse rotazioni.*

Esempio 3.2 *Per ogni coppia (a, b) di numeri reali, dove $a \neq 0$, definiamo:*

$$\alpha_{a,b} : \mathbb{R} \to \mathbb{R} : x \mapsto ax + b$$

cioè $\alpha_{a,b}(x) = ax+b$. Indicato con A l'insieme di tutte le mappe di questo tipo, si vede facilmente che $A \subset S(\mathbb{R})$; infatti la composizioni di tali mappe risulta essere una operazione su A, nel senso che se $(a, b), (c, d)$ sono coppie di numeri reali con $a, c \neq 0$ allora:

$$\begin{aligned}(\alpha_{a,b} \circ \alpha_{c,d})(x) &= \alpha_{a,b}(\alpha_{c,d}(x)) \\ &= \alpha_{a,b}(cx + d) \\ &= acx + ad + b \\ &= \alpha_{ac,ad+b}.\end{aligned}$$

Inoltre tale operazione, per il teorema precedente, risulta essere associativa. L'elemento neutro risulta essere la mappa $\alpha_{1,0}$, mentre l'inverso di $\alpha_{a,b}$ è la mappa $\alpha_{a^{-1},-a^{-1}b}$. Dunque la coppia $(A, \circ)$ risulta essere un gruppo. Tale gruppo è commutativo?

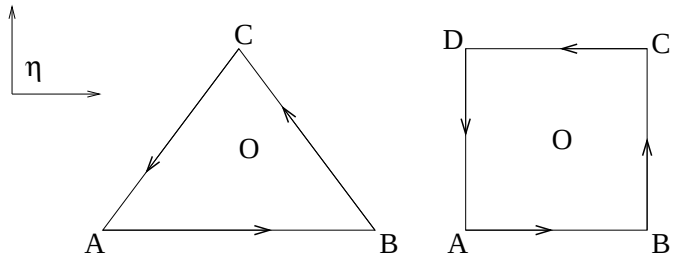

Figura 1: Nel piano cartesiano η sono rappresentati i poligoni orientati soggiacenti ai gruppi ciclici C_3 - il triangolo - e C_4 - il quadrato.

4 Note dai seminari sui gruppi ciclici e diedrali

In queste brevi note ci occuperemo di alcuni fra i principali gruppi finiti ossia i **gruppi puntuali.** Rappresentano uno strumento utile per caratterizzare e classificare le operazioni di simmetrie di un oggetto geometrico che lasciano fisso almeno un punto, e rappresentano uno degli strumenti principali usati per classificare le algebre e i gruppi di matrici (più in generale le algebre e i gruppi di Lie). Nel prosieguo cercheremo di adottare un atteggiamento costruttivo piuttosto che deduttivo per mostrare come le strutture descritte siano concetti naturali, non necessarimente deducibili solo come conseguenza di una serie di opportune definizioni astratte.

4.1 I gruppi Ciclici C_n

Un gruppo ciclico (*si considerano qui solo gruppi finiti*) è definito come il gruppo di simmetrie rotazionali di un poligono regolare ad n-lati orientati. Come si evince dalla figura 1, il punto fisso che viene lasciato invariato dalla rotazione non è altro che il punto O giacente nel piano η e situato al centro del poligono attraverso il quale passa l'asse di rotazione perpendicolare a η. Gli elementi del gruppo ciclico sono pertanto le rotazioni con orientazione fissata e coerente con quella dei lati del poligono (di solito antioraria) per un angolo pari a $\frac{2\pi k}{n}$ con $k \in [0, ..., n-1] \subset \mathbb{N}$. Possiamo effettuare la seguente identificazione:

$$C_n = \{c_1, ..., c_n\}, \quad c_k = \frac{2\pi k}{n},\ c_n \equiv 0$$

ossia associamo a c_n la rotazione nulla (infatti una rotazione di qualsiasi multiplo di 2π è indistinguibile dalla rotazione nulla). La legge di composizione del gruppo è data dalla somma, *modulo* n, degli indici interi a numeratore:

$$c_k \cdot c_j = \frac{2\pi(k+j)}{n} = c_{k+j},$$

dove $k+j$ appartiene ai numeri naturali *modn* (*i.e.* $k+j$ deve essere un numero intero compreso fra 0 ed $n-1$). L'elemento neutro è la rotazione nulla, e l'inverso è naturalmente dato dalla formula:

$$(c_k)^{-1} = \frac{2\pi(-k)}{n} \equiv \frac{2\pi(n-k)}{n} = c_{-k}$$

Da questa costruzione si evidenziano immediatamente due proprietà essenziali dei gruppi ciclici:

- il gruppo C_n è abeliano per ogni $n \in \mathbb{N}$ poichè, essendo l'operazione interna definita mediante una somma fra numeri naturali, si ha che, per ogni scelta di $k, j \in [0, ..., n-1] \subset \mathbb{N}$
$$c_k \cdot c_j = c_{k+j} = \frac{2\pi(j+k)}{n} = c_j \cdot c_k.$$
- Il gruppo C_n può essere visto come generato da un unico elemento ossia c_1, la più piccola rotazione non nulla. Infatti, dato un qualsiasi $j \in [0, ..., n-1] \subset \mathbb{N}$, l'elemento associato c_j può essere visto come:
$$c_j = \underbrace{c_1 \cdot c_1 \cdot ... \cdot c_1}_{j}.$$
Pertanto, essendo il comportamento identico a quello delle potenze, d'ora in poi intenderemo che $c_j \doteq c_1^j$.

Ciò detto, possiamo finalmente enunciare la definizione formale di gruppo ciclico di ordine n:

Definizione 4.1 *Chiamiamo* ***gruppo ciclico*** $(C_n, \cdot)$ *il gruppo abeliano di ordine n i cui elementi sono generati per moltiplicazione al più $n-1$ volte di un singolo elemento $c \in C_n$ detto generatore. L'elemento $c_n \doteq c^n$ è identificato con l'elemento neutro del gruppo.*

Concludiamo notando che, dalla definizione, si evince l'esistenza di un isomorfismo naturale fra C_n e $\mathbb{Z}_n$.

I gruppi ciclici si prestano come facile esempio per introdurre il concetto di *tavola delle moltiplicazioni*. Questa è un modo alternativo di specificare un gruppo finito benché tale metodo sia sempre meno efficace tanto quanto più è alto l'ordine del gruppo che si vuole assegnare. Per un gruppo ad n elementi essa è una tabella $n \times n$ le cui entrate sono date dalla composizione di due elementi del gruppo stesso. Esemplifichiamo ora nel caso di C_3 che ricordiamo essere un gruppo di 3 elementi ossia, dalla teoria precedente, $c_1 \equiv c = \frac{2\pi}{3}$, $c_2 = c_1^2 = c^2 = \frac{4\pi}{3}$ ed infine $c_3 = c^3 = e$ ossia l'elemento neutro del gruppo inteso come la rotazione di 0 gradi.

g_2/g_1	c	c_2	e
e	c	c^2	e
c	c^2	e	c
c_2	e	c	c^2

Tabella 1: Il prodotto è per convenzione scelto come $g_1 \cdot g_2$. Essendo il gruppo abeliano il risultato finale non dipende dalla convenzione stessa mentre, in generale, la scelta opposta, ossia $g_2 \cdot g_1$, genera la matrice trasposta.

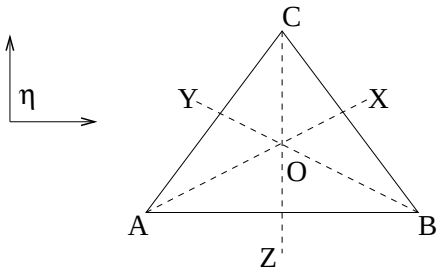

Figura 2: Nel piano cartesiano η è rappresentato il triangolo non orientato e gli assi di simmetria OX, OY ed OZ.

4.2 I gruppi Diedrali D_n

Anche in questa sezione proseguiremo lungo le stesse linee della precedente adottando un atteggiamento costruttivo piuttosto che deduttivo. Pertanto chiamiamo *gruppo diedrale* il gruppo delle simmetrie di un poligono regolare nel piano a n facce **non orientate**. Il punto lasciato fisso da questa classe di operazione è lo stesso del corrispondente gruppo ciclico C_n; è facile convincersi che C_n stesso debba essere un sottogruppo di D_n.

Essendo leggermente più complicato come caso rispetto al precedente, partiamo da $n = 3$. Come si evince dalla figura 2 il gruppo diedrale D_3 contiene sicuramente gli elementi $c_1 \equiv c$, $c_2 \equiv c^2$ ed $e = c_3$ che appartengono anche al gruppo C_3. In più evidenziamo anche le riflessioni rispetto agli assi OX, OY ed OZ a cui ci riferiremo rispettivamente come $b_1 \equiv b$, b_2 e b_3; quindi D_3 ha 6 elementi.

Immediatamente si notano le seguenti proprietà:

- $b_i^2 = e$ per ogni $i = 1, 2, 3$. In altre parole l'applicazione successiva per due volte di una qualsiasi delle riflessioni rispetto agli assi OX, OY od OZ riporta alla posizione iniziale.
- il gruppo D_3 non è abeliano in quanto $b \cdot c \neq c \cdot b$ come si può evincere graficamente.

Quest'ultima considerazione fa sorgere spontanea la seguente domanda: dato che il gruppo ciclico era, indipendentemente dall'ordine, generato da un unico elemento, quanti sono gli elementi che generano D_3 e più in generale D_n? Partiamo dal caso particolare $n = 3$.

Riferendoci alla figura 2, proviamo a vedere cosa succede ai vertici A, B, C (e quindi ai lati corrispondenti), con le seguenti operazioni, ossia:

$$cbc^{-1}(A) = cb(C) = c(B) = C = b_2(A) \quad (3)$$
$$cbc^{-1}(B) = cb(A) = c(A) = (B) = b_2(B) \quad (4)$$
$$cbc^{-1}(C) = cb(B) = c(C) = (A) = b_2(C) \quad (5)$$

Allo stesso modo si riesce a dimostrare che:

$$\begin{aligned} c^{-1} \cdot b \cdot c(A) &= c^{-1} \cdot b(B) = c^{-1}(C) = B = b_3(A) \\ c^{-1} \cdot b \cdot c(B) &= c^{-1} \cdot b(C) = c^{-1}(B) = A = b_3(B) \\ c^{-1} \cdot b \cdot c(C) &= c^{-1} \cdot b(A) = c^{-1}(A) = C = b_3(C). \end{aligned}$$

Pertanto ci accorgiamo che gli elementi b_2, b_3 possono essere costruiti a partire da b e da c che sono quindi i generatori dell'intero gruppo D_3. **Per specificare completamente il gruppo però non bastano le informazioni ottenute in quanto è essenziale anche capire come commutano b e c.** Cosa vuol dire all'atto pratico? Supponiamo di fissare un modo canonico per scrivere tutti gli elementi di D_3 come prodotti di potenze di b e c, ossia tutti del tipo $b^n c^m$ con opportuni interi m, n. Se assegniamo elementi del tipo $c^k b^j$ con k, j interi fissati, come li scrivo nell'altra forma? Basta farlo per cb e tutti gli altri casi seguono per reiterazione. E' immediato verificare che:

$$\begin{aligned} bc(A) &= b(B) = C = b_2(A) \\ bc(B) &= b(C) = B = b_2(B) \\ bc(C) &= b(A) = A = b_2(C) \end{aligned}$$

Inserendo questi risultati nelle (3),(4),(5) otteniamo:

$$bc = cbc^{-1} \Longrightarrow bc^2 = bc^{-1} = cb.$$

Da questo si deriva che possiamo alla fine esprime il gruppo D_3 come

$$(D_3, \cdot) = gp\left\{b, c\right\}, \mid b^2 = c^3 = e,\ cb = bc^2 = bc^{-1}$$

Per concludere notiamo che vale la seguente identità:

$$(bc)^2 = bcbc = b^2c^3 = ee = e \tag{6}$$

Detto ciò possiamo costruire la tabella delle moltiplicazioni per D_3 sfruttando la sua definizione e l'identità (6) per far sì che ogni entrata della matrice associata sia del tipo $b^n c^m$ con n, m interi opportuni. Seguendo sempre la convenzione $g_1 \cdot g_2$ si ottiene la tabella 4.2.

g_2/g_1	e	c	c_2	b	b_2	b_3
e	e	c	c^2	b	b·c	$b{\cdot}c^2$
c	c	c^2	e	b·c	$b{\cdot}c^2$	b
c_2	c^2	e	c	$b{\cdot}c^2$	b	b·c
b	b	$b{\cdot}c^2$	b·c	e	c^2	c
b_2	b·c	b	$b{\cdot}c^2$	c	e	c^2
b_3	$b{\cdot}c^2$	b·c	b	c^2	c	e

Tabella 2: Come nella precedente tabella gli elementi della prima riga sono "i g_1" mentre quelli della prima colonna sono "i g_2" e i **prodotti seguono la convenzione** $g_1 \cdot g_2$.

Ecco la tabella **trasposta** che contiene invece i prodotti del tipo $g_2 \cdot g_1$.

Mediante un processo induttivo, considerando poligono regolari di n lati possiamo ora generalizzare i risultati ottenuti per dare una definizione generale ad ogni ordine per i gruppi diedrali:

g_2/g_1	e	c	c_2	b	b_2	b_3
e	e	c	c^2	b	b·c	$b\cdot c^2$
c	c	c^2	e	$b\cdot c^2$	b	b·c
c_2	c^2	e	c	b·c	$b\cdot c^2$	b
b	b	b·c	$b\cdot c^2$	e	c	c^2
b_2	b·c	$b\cdot c^2$	b	c^2	e	c
b_3	$b\cdot c^2$	b	b·c	c	c^2	e

Tabella 3: Come nella precedente tabella gli elementi della prima riga sono "i g_1" mentre quelli della prima colonna sono "i g_2" e i **prodotti seguono invece la convenzione** $g_2 \cdot g_1$.

Definizione 4.2 *Si chiama* ***gruppo diedrale*** D_n *il gruppo di ordine* $2n$ *generato da* 2 *elementi* b, c *con una relazione i.e.:*

$$(D_n, \cdot) = Gp\{c, b\} \quad | \quad b^2 = c^n = e, \ \wedge\, c \cdot b = b \cdot c^{n-1} = b \cdot c^{-1}.$$

Osservazione 4.1 *L'importanza dei gruppi diedrali risiede anche nel fatto che costituiscono un modo per costruire gruppi* ***non abeliani di qualsiasi ordine pari*** ≥ 6 *(è infatti immediato verificare che per* $n = 1$, D_1 *è isomorfo a* $\mathbb{Z}_2$, *mentre per* $n = 2$, D_2 *è isomorfo a* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *e quindi sono gruppi abeliani).*

Osservazione 4.2 *Non esiste una costruzione generale di questo tipo per gli ordini dispari !*

Osservazione 4.3 *Abbiamo anche dimostrato, vedi teorema 2.4 e osservazione 2.1, che, per* n ***primo***, D_n *è* ***l'unico*** *gruppo non abeliano di ordine* $2n$.

4.3 I gruppi C_∞ e D_∞.

Il caso di un poligono di n lati può essere generalizzato al caso di un poligono di infiniti lati di lunghezza finita . Consideriamo infinite copie dell'intervallo $[0, 1]$ unite per gli estremi e disposte in modo da ricoprire l'intera retta reale (possiamo quindi vedere la nostra costruzione come un poligono rettilineo con infiniti lati di lunghezza unitaria e infiniti vertici in corrispondenza dei numeri interi; la stessa costruzione si può immaginare anche per i poligoni di n lati, a patto di identificare l'ultimo vertice con il primo). La rotazione più piccola (che nel caso finito può anche essere immaginata come traslazione di un lato sul lato adiacente , in virtù dell'isomorfismo naturale tra C_n e $\mathbb{Z}_n$) è ora rappresentata dalla funzione (reale di variabile reale):

$$c(x) = x + 1$$

mentre la riflessione rispetto ad un vertice è data dalla funzione:

$$b(x) = -x$$

Si verifica subito che sono soddisfatte relazioni del tipo di quelle che definiscono il gruppo diedrale: $b^2(x) = b(-x) = x,\ \ c(b(x)) = c(-x) = 1 - x,\ \ b(c^{-1}(x) = b(x-1) = 1 - x$, cioè:

$$b^2 = e,\ \wedge\ c \cdot b = b \cdot c^{-1}.$$

Il gruppo **ciclico** generato dalle potenze di c è ovviamente isomorfo al gruppo degli interi $\mathbb{Z}$: $c^n(x) = x + n$ e quindi potremmo scrivere la formula suggestiva:

$$C_\infty = \lim_{n\to\infty} C_n = \lim_{n\to\infty} \mathbb{Z}_n = \mathbb{Z}$$

Sulla stessa linea, definiamo gruppo diedrale infinito D_∞ il gruppo generato dalle funzioni c e b.

Osservazione 4.4 *Il limite indicato sopra non va ovviamente inteso nel senso usuale del concetto di limite e, inoltre, non è l'unico possibile. Ad esempio si potrebbe pensare a un poligono di infiniti lati di lunghezza infinitesima, cioè a una circonferenza. In questo caso, il gruppo C_n può essere visto come il gruppo delle radici complesse n – esime dell'unità che, nel piano complesso, rappresentano i vertici di un poligono regolare di n lati inscritto in una circonferenza di raggio* 1. *In questo ambito risulterebbe molto naturale definire come limite di un poligono la circonferenza, e quindi si potrebbe scrivere anche:*

$$C_\infty = \lim_{n\to\infty} C_n = S^1$$

dove $S^1 = \{$gruppo moltiplicativo dei numeri complessi di modulo $1\} = \{e^{ix}$ *con x reale*$\}$ *. Tale limite però* ***non produce un gruppo ciclico****, cioè generato da un solo elemento, e non si presta quindi a costruire un limite sensato per i gruppi diedrali.*

4.4 I gruppi di Permutazioni S_n

In questa sezione ci occuperemo del più importante fra i gruppi finiti ossia quello delle permutazioni.

Sia pertanto X un qualsiasi insieme non vuoto con numero finito di elementi $n < \infty$; questi ultimi possono essere per semplicità messi in corrispondenza biunivoca con il set dei primi n-numeri naturali. In altre parole supporremo d'ora in poi $X = \{1, 2, ..., n\}$. Una *permutazione* di questi n elementi è una mappa invertibile $f : X \to X$ ossia $f(i) \neq f(j)$ per ogni $i \neq j \in X$. Graficamente una permutazione P è rappresentabile nel seguente modo:

$$P = \begin{pmatrix} 1 & 2 & ... & n \\ p_1 & p_2 & ... & p_n \end{pmatrix}, \tag{7}$$

dove $p_i = f(i) \in \mathbb{N}$ per ogni $i = 1, 2, ..., n$ e $p_k \neq p_j$ per ogni $k \neq j$ (implicitamente la funzione biettiva f è assegnata). Per ottenere una struttura di gruppo dobbiamo prima specificare al lettore una operazione interna fra due diversi tipi di elementi (7) e la più naturale è la composizione

reitarata delle permutazioni da destra a sinistra (puramente convenzionale!). Esemplifichiamo con 4 elementi cosa intendiamo:

$$PQ = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix},$$

ossia, se guardiamo cosa succede all'elemento 1, la prima permutazione Q manda 1 in 3 mentre P manda 3 in 4 ossia, complessivamente, $1 \to 4$ etc. etc....

L'insieme S_n di tutte i possibili riordinamenti dei primi n numeri naturali è un gruppo rispetto all'operazione di composizione.

L'operazione su S_n data dalle applicazioni successive è ben definita in quanto chiusa nell'insieme S_n. Data la corrispondenza fra permutazioni e funzioni invertibili su X ne discende l'associatività che è mutuata dalla medesima proprietà per il gruppo delle funzioni invertibili su X rispetto alla operazione di composizione. Bisogna ora stabilire se esiste un elemento neutro ma questo è dato in maniera naturale da

$$I = \begin{pmatrix} 1 & 2 & ... & n \\ 1 & 2 & ... & n \end{pmatrix}.$$

Sfruttando la regola di composizione delle permutazioni è immediato determinare che $PI = IP = P$ per ogni $P \in S_n$. Rimane solo da dimostrare l'esistenza di un elemento inverso. A tal fine fissiamo $P \in S_n$ come in (7) e la seconda permutazione Q data da

$$Q = \begin{pmatrix} p_1 & p_2 & ... & p_n \\ 1 & 2 & ... & n \end{pmatrix}.$$

Una applicazione diretta della composizione interna fra elementi di S_n ci mostra che $PQ = QP = I$ indipendentemente dalla scelta originaria di P.

N.B. Il gruppo $(S_n, \cdot)$ non è abeliano.

Rimane da chiarire l'ordine di questo gruppo finito:

Teorema 4.1 *Il numero di elementi di S_n è $n!$.*

Prova. Sia $X = \{1, 2, ..., n\}$ e sia $\alpha : X \to X$ l'applicazione biettiva corrispondente ad una qualsiasi fissata permutazione. Esplicitamente possiamo sapere quante "diverse α" ci sono notando che, detto $k = \alpha(1)$, allora k può assumere a priori n valori diversi ossia tanti quanti sono gli elementi di X. Fissiamone uno e sia ora $k' = \alpha(2)$ allora k' può solo assumere $n - 1$ valori e così via fino a $\alpha(n)$ che è fissato dalle $n - 1$ precedenti scelte. Quindi posso costruire $n \cdot n - 1 \cdot ... \cdot 1$ funzioni α diverse ossia $n!$ da cui discende il teorema. ■

Ora vogliamo introdurre una notazione alternativa, ma spesso utile per il gruppo delle permutazioni S_n ossia *i cicli*. Sia X un insieme di n elementi, allora un k-ciclo è dato da $(a_1, a_2, ..., a_k)$ dove $a_i \in X$ per ogni $i = 1, 2, ..., k$. Questa scrittura individua univocamente una permutazione giacente in S_n nel seguente modo: l'elemento a_1 è mappato in a_2 mentre a_2 in a_3 e così via fino ad a_k che è mappato in a_1. Per completare la permutazione i rimanenti $n - k$ elementi

si intendono implicitamente mappati in se stessi. A volte questo fatto viene esplicitamente indicato mediante gli 1-cicli del tipo (a_{k+1}), una riscrittura dell'asserzione "l'elemento a_{k+1} è mappato in se stesso". In questa notazione quindi

$$P \in S_n \longrightarrow (a_1, a_2, ..., a_k)\,(a_{k+1})...(a_n)$$

Facciamo ora 2 esempi concreti per il gruppo S_4:

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \longleftrightarrow (1,3,4,2),$$

oppure

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \longleftrightarrow (1,3,2)(4) \equiv (1,3,2).$$

I diversi cicli che compongono un singolo elemento di S_n sono detti *disgiunti* ed S_n contiene tutti i possibili k-cicli con $k \leq n$. Il concetto di cicli disgiunti può essere generalizzato dicendo che $(a_1, a_2, ..., a_l)$ e $(b_1, b_2, ..., b_k)$ sono disgiunti se e solo se $a_i \neq b_j$ per ogni $i = 1, 2, ..., l$ e per ogni $j = 1, 2, ..., k$.

Definizione 4.3 *Chiamiamo* ***trasposizione*** *(di due elementi) una qualsiasi permutazione $P \in S_n$ identificata da un 2-ciclo*[1] *(a_i, a_{i+1}).*

Vediamo ora in un caso concreto come si usa la suddivisione in cicli e quale sia la sua utilità pratica.

Esempio 4.1 *Per definizione S_3 è il gruppo delle permutazioni di un insieme di 3 elementi, per semplicità $X = \{1, 2, 3\}$. Allora in notazione a cicli il gruppo è:*

$$S_3 = \{(1,2,3), (1,3,2), (1,3)(2), (1,2)(3), (1)(2,3), (1)(2)(3)\}.$$

Chiamiamo ora $c = (1,2,3)$ e calcoliamo

$$c \cdot c = (1,2,3)(1,2,3) = (1,3,2),$$

mentre

$$c \cdot c \cdot c = (1,2,3)(1,2,3)(1,2,3) = (1,2,3)(1,3,2) = (1)(2)(3) = e,$$

dove e è l'elemento neutro di S_3. Quindi notiamo che l'insieme generato da $\{(1)(2)(3), (1,2,3), (1,3,2)\}$ è un sottogruppo di S_3 isomorfo a C_3 da cui la scelta del simbolo c. Chiamiamo ora $b = (2,3)(1)$; si verifica facilmente che

$$b \cdot b = (2,3)(1) \cdot (2,3)(1) = (1)(2)(3) = e,$$

[1] Il lettore noti che a_i ed a_{i+1} sono intesi come elementi arbitrari di un generico insieme finito non vuoto. Non utilizziamo pertanto aprioristicamente la convenzione di identificarli con degli opportuni numeri naturali.

mentre

$$c \cdot b \cdot c^{-1} = (1,2,3) \cdot (2,3)(1) \cdot (2,1,3) = (1,2,3) \cdot (2,1)(3) = (1,3)(2),$$
$$c^{-1} \cdot b \cdot c = (2,1,3) \cdot (2,3)(1) \cdot (1,2,3) = (2,1,3) \cdot (1,3)(2) = (1,2)(3).$$

Infine notiamo anche che

$$b \cdot c \cdot c = (2,3)(1) \cdot (1,2,3) \cdot (1,2,3) = (2,3)(1) \cdot (1,3,2) = \\ = (1,2)(3) = (1,2,3) \cdot (2,3)(1) = c \cdot b.$$

Da questa analisi possiamo dedurre che S_3 è generato da 2 elementi ossia $c = (1,2,3)$ e $b = (2,3)(1)$ che soddisfano le relazioni

$$b^2 = c^3 = e \ , \ cb = bc^2.$$

Abbiamo dimostrato che esiste un isomorfismo *fra D_3 ed S_3. Pertanto si invita riscrivere la precedente tavola delle moltiplicazioni per D_3 in termini di quella di S_3 con i cicli.*

Sorge ora quasi spontanea la domanda se il legame fra permutazioni e gli altri gruppi puntuali non sia più forte dell'esistenza di un isomorfismo in casi particolari. Ebbene la risposta si traduce nel seguente teorema:

Teorema 4.2 (di Cayley) *Ogni gruppo finito G di ordine n è isomorfo ad un opportuno sottogruppo di S_n.*

Prova. Sia $S_{inv}(G)$ l'insieme delle applicazioni invertibili da G in se stesso (quindi, essendo G finito per ipotesi, sono anche biettive) e sia $I : G \to S_{inv(G)}$ l'applicazione che associa a g l'elemento $I(g)$ definito come la moltiplicazione a sinistra *i.e.* $I(g)h = gh$ per qualunque $h \in G$. Ovviamente, a fissato $g \in G$, la moltiplicazione a sinistra è una applicazione iniettiva ossia $I(g)h = I(g)h'$ se e solo se $gh = gh'$ da cui, moltiplicando a sinistra per g^{-1}, si ha $h = h'$. Essendo G finito, l'iniettività implica la biettività e, quindi, la mappa I che associa a $g \in G$ l'elemento $I(g)$ è ben definita. Guardiamo ora l'applicazione I cioè facciamo variare l'elemento g tenendo fisso h. È immediato notare che I è iniettiva poichè, se $[I(g)]\, h = [I(g')]\, h$, allora, per la definizione precedente, vale che $gh = g'h$ ossia, moltiplicando a destra per h^{-1}, si ha $g = g'$. Per concludere, basta ricordare che le permutazioni di un insieme finito sono, per costruzione, isomorfe al gruppo delle applicazioni biettive dall'insieme in se stesso, *i. e.* $S_{inv}(G) = S_n$ con $n = \#G$. Quindi possiamo rileggere I come una mappa da G in S_n ma, essendo I iniettiva e preservando l'operazione di gruppo (ossia è un omomorfismo), si ha che $I(G)$ è isomorfo a G e $I(G) \hookrightarrow S_n$ per cui G è un sottogruppo delle permutazioni. ■

Per concludere la sezione vogliamo definire in maniera rigorosa un concetto intuitivo e spesso utilizzato ossia *il segno di una permutazione.* A questo fine, introduciamo l'insieme $\Omega = \{h : \mathbb{Z}^n \to \mathbb{Z}\}$ il cui generico elemento verrà indicato $h(X_1, X_2, ..., X_n)$ con $X_k \in \mathbb{Z}$ per

ogni $k = 1, ..., n$. Su Ω possiamo definire un'azione[2] naturale del gruppo delle permutazioni S_n ossia, dato un qualsiasi $h \in \Omega$ e $\sigma \in S_n$ chiamiamo

$$(\sigma(h))(X_1, X_2, ..., X_n) = h\left(X_{\sigma(1)}, X_{\sigma(2)}, ..., X_{\sigma(n)}\right).$$

In particolare ora scegliamo una specifica funzione in Ω ossia

$$D(X_1, X_2, ..., X_n) = \prod_{1 \le i < j \le n} (X_i - X_j),$$

su cui le permutazioni agiscono al più cambiando il segno ossia

$$\sigma\left(D(X_1, X_2, ..., X_n)\right) = \pm D(X_1, X_2, ..., X_n).$$

Tralasciando per un secondo la costruzione generale, cerchiamo di convincere il lettore della bontà dell'ultima identità mediante un esempio esplicito. Nella fattispecie consideriamo $X \equiv \{X_1, X_2, X_3\}$, da cui

$$D(X_1, X_2, X_3) = (X_1 - X_2)(X_1 - X_3)(X_2 - X_3).$$

Sia $\sigma \in S_3$ la permutazione individuata dal ciclo (132). Ne segue che

$$\begin{aligned}\sigma\left(D(X_1, X_2, X_3)\right) &= (X_3 - X_1)(X_3 - X_2)(X_1 - X_2) = \\ &= (X_1 - X_2)(X_1 - X_3)(X_2 - X_3) = D(X_1, X_2, X_3).\end{aligned}$$

Riassumendo, ne discende pertanto la seguente definizione naturale:

Definizione 4.4 *Chiamiamo* segno *della permutazione $\sigma \in S_n$ l'elemento $\epsilon(\sigma) \in \mathbb{Z}_2$ tale che*

$$\sigma\left(D(X_1, X_2, ..., X_n)\right) = \epsilon(\sigma) D(X_1, X_2, ..., X_n). \tag{8}$$

*Se $\epsilon(\sigma) = 1$ le permutazioni sono dette **pari**, se no **dispari**.*

Sfruttiamo ora la definizione per provare le seguenti proprietà delle permutazioni:

[2]Il concetto di *azione di un gruppo* G su un insieme (non necessariamente finito) X è formulabile in due modi equivalenti. Nel primo chiamiamo azione una mappa $\pi : G \times X \to X$ tale che $(g, x) \mapsto x' \doteq \pi(g)x$ e tale che

- $\pi(gg')x = \pi(g)\left[\pi(g')x\right] \quad \forall g, g' \in G, \wedge \forall x \in X,$
- se e è l'elemento neutro di G, allora $\pi(e)x \equiv x$ per ogni $x \in X$.

Pertanto l'applicazione $g \to \pi(g)$ è un omomorfismo.

Alternativamente chiamiamo azione di G su X (non necessariamente finito) un omomorfismo $\pi : G \to S_{inv}(X)$ essendo $S_{inv}(X)$ il gruppo delle funzioni invertibili da X in se stesso rispetto all'operazione di composizione fra mappe. È lasciata al lettore la semplice dimostrazione dell'equivalenza fra le due definizioni.

Lemma 4.1 *Siano $\sigma, \tau \in S_n$ qualsiasi. Allora*

$$\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau).$$

Prova. Dalla definizione 4.4 e da quella di gruppo delle permutazioni, si ha che

$$\begin{gathered}\epsilon(\sigma\tau)D(X_1, X_2, ..., X_n) = (\sigma\tau)\, D(X_1, X_2, ..., X_n) = \sigma\left[\tau\left(D(X_1, X_2, ..., X_n)\right)\right] = \\ = \sigma\left(\epsilon(\tau)D(X_1, X_2, ..., X_n)\right) = \epsilon(\tau)\sigma\left(D(X_1, X_2, ..., X_n)\right) = \\ = \epsilon(\tau)\epsilon(\sigma)D(X_1, X_2, ..., X_n),\end{gathered}$$

da cui, confrontando il primo e l'ultimo termine nella catena di uguaglianze, discende la tesi. ■

Il messaggio di questo lemma è semplicemente che l'applicazione "segno" $\epsilon : S_n \to \mathbb{Z}_2$ è un omomorfismo.

Lemma 4.2 *Sia $(a_1, a_2, ..., a_k)$ un k-ciclo di S_n. Allora:*

1. *Ogni k-ciclo è prodotto di trasposizioni del tipo (a_i, a_{i+1}) ossia*

$$(a_1, a_2, ..., a_k) = (a_1, a_2) \cdot (a_2, a_3) \cdot ... \cdot (a_{k-1}, a_k).$$

   Il prodotto va inteso come l'operazione di composizione interna in S_n una volta che il k-ciclo $(a_1, a_2, ..., a_k)$ è univocamente identificato con l'elemento di S_n $(a_1, a_2, ..., a_k)(a_{k+1})...(a_n)$ mentre

$$(a_i, a_{i+1}) \equiv (a_1)...(a_{i-1})\,(a_i, a_{i+1})\,(a_{i+2})...(a_n) \in S_n \quad \forall i = 1, ..., n.$$

2. *Per ogni trasposizione il segno è -1 ed, in generale, per ogni k-ciclo $\tau \in S_n$, $\epsilon(\tau) = (-)^{k-1}$.*

3. *ogni permutazione è prodotto di trasposizioni e, se σ è il prodotto di j trasposizioni, allore $\epsilon(\sigma) = (-1)^j$.*

Prova. *1)* Consideriamo un generico $\sigma = (a_1, a_2)(a_2, a_3)...(a_{k-1}, a_k) \in S_n$ ed in particolare, ricordando che la moltiplicazione fra cicli segue la regola "da destra a sinistra" come la composizione di funzione, estraiamo gli ultimi due cicli i.e.

$$\begin{gathered}(a_{k-1}, a_k) \equiv (a_1)...(a_{k-2})(a_{k-1}, a_k)(a_{k+1})...(a_n) \\ (a_{k-2}, a_{k-1}) \equiv (a_1)...(a_{k-3})(a_{k-2}, a_{k-1})(a_k)(a_{k+1})...(a_n).\end{gathered}$$

La loro moltiplicazione (come elementi di S_n) genera la seguente permutazione:

$$(a_{k-2}, a_{k-1})(a_{k-1}, a_k) \equiv (a_1)...(a_{k-3})(a_{k-2}, a_{k-1}, a_k)(a_{k+1})...(a_n).$$

Reiterando il processo per un numero finito di volte, ossia k, si ottiene

$$(a_1, a_2)(a_2, a_3)...(a_{k-1}, a_k) \equiv (a_1, a_2, ..., a_k)(a_{k+1})...(a_n) \equiv (a_1, a_2, ..., a_k),$$

ossia la tesi al punto 1).

2) Sia ora data una trasposizione qualsiasi $\tau = (a_i, a_{i+1})$. È immediato notare che, usando le definizione e nomenclatura delle precedenti proposizioni e chiamando ancora con τ la permutazione univocamente identificata dalla trasposizione (a_i, a_{i+1}),

$$\tau\left(D(X_1, X_2, ..., X_k)\right) = -D(X_1, X_2, ..., X_k),$$

poichè l'effetto è solo quello di cambiare il segno a $X_i - X_{i+1}$. Pertanto il segno di una trasposizione è -1. Se ora utilizziamo quanto già dimostrato al punto 1) possiamo decomporre ogni k-ciclo $\sigma = (a_1, ...a_k)$ nel prodotto di $k-1$ trasposizioni del tipo (a_j, a_{j+1}) ognuna delle quali identifica univocamente una permutazione τ_j, essendo $j = 1, ..., k-1$. Dal lemma 4.1 ne discende che $\epsilon(\sigma) = \epsilon(\tau_1 \cdot \tau_2 .. \cdot ... \cdot \tau_{k-1}) = \prod_{j=1}^{k-1} \epsilon(\tau_j) = (-)^{k-1}$ da cui segue la tesi.

3) La tesi di questo punto discende immediatamente ricordando che ogni permutazione può espressa come prodotto di opportuni cicli. Dato che ogni ciclo è a sua volta decomponibile nel prodotto di trasposizioni, otteniamo il risultato desiderato. ■

N.B. In realtà il punto 3) del precedente lemma può apparire triviale. Questo discende dal fatto che abbiamo adottato una nozione generalizzata di trasposizione che permette lo scambio di due elementi (a_k, a_{k+1}) generici in un generico insieme finito e non vuoto X. In letteratura spesso è consuetudine invece attivare la corrispondenza fra elementi di X e numeri naturali imponendo pertanto che $a_{k+1} = a_k + 1$ - per esemplificare, nella notazione alternativa, $(2, 3)$ è una trasposizione mentre $(2, 4)$ no. In questo caso per dimostrare la tesi al punto 2) e soprattutto al punto 3) bisognerebbe provare che il segno di un 2-ciclo qualsiasi (a, b) sia ancora -1. Questo comunque discende dalla seguente identità fra 2-cicli:

$$(a, b) = (b, a+1) \cdot (a, a+1) \cdot (b, a+1),$$

da cui per il lemma 4.1

$$\epsilon(a, b) = \epsilon(b, a+1)\epsilon(a, a+1)\epsilon(b, a+1) = \epsilon^2(b, a+1)\epsilon(a, a+1) = \epsilon(a, a+1) = -1.$$

Ciò detto le dimostrazioni proseguono come quelle proposte in queste note.

4.5 I gruppi Alternanti A_n

Nello studio del gruppo delle permutazioni, la nozione di segno gioca un ruolo fondamentale nel dividere gli elementi di S_n in due sottoclassi fondamentali (ossia "permutazioni con il segno +" e quelle "con il segno -") ed, in particolare, proponiamo la seguente definizione.

Definizione 4.5 *Chiamiamo A_n il sottoinsieme di S_n costituito da tutte le permutazioni $\sigma \in S_n$ tale che $\epsilon(\sigma) = 1$.*

Teorema 4.3 *L'insieme $(A_n, \cdot)$ - essendo "$\cdot$" la stessa operazione del gruppo S_n - è un sottogruppo proprio di S_n detto* ***gruppo alternante****.*

Prova. Si considerino due elementi qualsiasi $\sigma, \tau \in A_n$. Verifichiamo se $\sigma \cdot \tau \in S_n$ giace anche in A_n; per fare ciò invochiamo il lemma 4.1 per cui $\epsilon(\sigma \cdot \tau) = \epsilon(\sigma)\epsilon(\tau)$, da cui, essendo per costruzione $\epsilon(\sigma) = \epsilon(\tau) = 1$, ne discende $\epsilon(\sigma \cdot \tau) = 1$. Pertanto A_n è chiuso rispetto l'operazione naturale indotta dal gruppo delle permutazioni. L'associatività è direttamente mutuata da quella del gruppo S_n che a sua volta era indotta da quella del gruppo $S_{inv}(X)$ con X insieme finito e non vuoto. L'elemento neutro è lo stesso del gruppo S_n ossia la permutazione $\rho = (a_1)(a_2)...(a_n)$. Il segno di ρ si deduce direttamente dalla definizione 4.4 *i.e.*, dati $X_j \in \mathbb{Z}$ con $j = 1, 2, ..., n$,

$$\rho\left(D(X_1, X_2, ..., X_n)\right) = \prod_{1 \le i < j \le n} \left(X_{\rho(i)} - X_{\rho(j)}\right) = \prod_{1 \le i < j \le n} \left(X_i - X_j\right),$$

dove abbiamo semplicementre sfruttato $\rho(i) = i$ per ogni $i = 1, 2, ..., n$. Quindi $\epsilon(\rho) = 1$. L'esistenza di un elemento inverso può essere dimostrata prendendo un generico $\sigma \in A_n$. Essendo $A_n \subset S_n$ possiamo costruire l'inverso $\sigma^{-1} \in S_n$. Dato che l'operazione interna ad A_n è la medesima di S_n ci basta dimostrare che il segno di σ^{-1} è 1. Sfruttando ancora il lemma 4.1, la seguente catena di identità vale:

$$1 = \epsilon\left(\rho\right) = \epsilon\left(\sigma\sigma^{-1}\right) = \epsilon\left(\sigma\right)\epsilon\left(\sigma^{-1}\right) = \epsilon\left(\sigma^{-1}\right),$$

dove ρ è la permutazione "identità". ■

Da quest'ultimo teorema possiamo subito evidenziare alcune peculiarità del gruppo alternante:

- il gruppo alternante è per costruzione un sottogruppo proprio di S_n. È immediato notare che non bisogna specificare alcuna mappa di immersione[3] di A_n in S_n poichè esiste un unica copia di $A_n \subset S_n$ ossia quella che identifica ogni elemento di A_n con il corrispondente in S_n. In altre parole, per A_n, la nozione di sottogruppo astratto è ridondante.
- il gruppo A_n non è abeliano come può essere provato moltiplicando fra loro due opportuni elementi di A_n.
- non esiste una controparte del gruppo alternante per l' insieme delle permutazioni a segno dispari. Infatti, supponendo di indurre su questo insieme l'operazione di composizione di S_n, il lemma 4.1 ci garantisce che il segno del prodotto di due qualsiasi permutazioni dispari è pari *i.e.* l'insieme non sarebbe chiuso rispetto all'operazione interna.

Concludiamo questa dissertazione sul gruppo alternante provando una proposizione sui generatori di A_n.

[3]Per convincersi della rilevanza di questo fatto, il lettore è invitato a riflettere sul caso semplice dei numeri reali $\mathbb{R}$ intesi come gruppo abeliano rispetto alla somma. È immediato notare che $\mathbb{R}$ è un sottogruppo di $\mathbb{R}^2$ inteso anche esso come gruppo abeliano rispetto all'addizione. Al contrario del caso sotto analisi, in questo ultimo esempio però esistono infiniti sottogruppi isomorfi ad $\mathbb{R}$ in $\mathbb{R}^2$ ossia tanti quante sono le rette nel piano. In questo caso è essenziale pertanto assegnare la mappa di immersione di $\mathbb{R}$ in $\mathbb{R}^2$ per identificare un unico concreto sottogruppo.

Teorema 4.4 *Il gruppo A_n è generato dai 3-cicli di S_n.*

Prova. Consideriamo ora A_n come sottogruppo di S_n. Allora per ogni $\sigma \in A_n$, il lemma 4.2 ci permette di decomporre σ nel prodotto di un opportuno numero di trasposizioni. Dato che il segno di σ è 1 e dato che ogni trasposizione identifica univocamente una permutazione dispari, possiamo sfruttare ancora il lemma 4.1 per concludere che il numero di trasposizione necessarie per scrivere σ è pari (altrimenti il segno sarebbe -1.). Ora basta notare che possiamo considerare σ come la composizione del prodotto di *coppie* di trasposizioni e, pertanto, per concludere la dimostrazione bisogna provare che ogni prodotto di 2 trasposizione è identificabile con un 3-ciclo o, al limite, con un prodotto di 3-cicli. Si consideri ora $\sigma = (a_1, a_2) \cdot (a_3, a_4) \cdot ... \cdot (a_{k-1}, a_k)$ e si estraggano le prime due coppie $(a_1, a_2) \cdot (a_3, a_4)$. Possiamo incorrere in due situazioni: nella prima[4] $a_2 = a_3$, ma, per definizione di operazione interna fra permutazioni, avremmo $(a_1, a_2) \cdot (a_2, a_4) \equiv (a_1, a_2, a_4)$. Nel secondo caso i due 2-cicli sono disgiunti però sfruttiamo la seguente identità $I = (a_1)(a_2)(a_3)...(a_n) = (a_1)(a_2)(a_2, a_3)(a_3, a_2)...(a_n)$; inserendola nella composizione dei 2-cicli si ha

$$(a_1, a_2) \cdot (a_3, a_4) = (a_1, a_2) \cdot I \cdot (a_3, a_4) =$$
$$= (a_1, a_2) \cdot (a_2, a_3) \cdot (a_3, a_2) \cdot (a_3, a_4) = (a_1, a_2, a_3) \cdot (a_2, a_3, a_4).$$

Da quest'ultima identità discende la tesi del teorema. ■

Esempio 4.2 *Mostriamo come si calcola esplicitamente il segno della seguente permutazione $\sigma \in S_8$:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 1 & 4 & 8 & 5 & 7 & 2 & 3 \end{pmatrix}.$$

Come primo passo riscriviamo la permutazione in notazione a cicli: partendo da 1 *e proseguendo si costruisce direttamente*

$$\sigma \longleftrightarrow (1, 6, 7, 2)(3, 4, 8)(5).$$

Per calcolare il segno basta ricordarsi che ogni k-ciclo identifica univocamente una permutazione ossia, nel dettaglio,

$$(1, 6, 7, 2) \longleftrightarrow \rho_1 = (1, 6, 7, 2)(3)(4)(5)(8),$$
$$(3, 4, 8) \longleftrightarrow \rho_2 = (3, 4, 8)(1)(2)(5)(6)(7),$$
$$(5) \longleftrightarrow \rho_3 = (1)(2)(3)(4)(5)(6)(7)(8) \equiv I.$$

Pertanto abbiamo decomposto $\sigma = \rho_1 \cdot \rho_2 \cdot \rho_3$. Ora sfruttiamo il lemma 4.1 per dire che $\epsilon(\sigma) = \prod_{i=1}^{3} \epsilon(\rho_i)$. Per quanto detto nella proposizione 4.3, $\epsilon(\rho_3) = \epsilon(I) = 1$ ossia l'identità ha segno

[4] Si noti che l'ordinamento in una trasposizione è puramente convenzionale poichè $(a_i, a_j) = (a_j, a_i)$ indipendentemente dalla scelta degli elementi a_i, a_j in un qualsiasi insieme finito non vuoto X. Pertanto se incorressimo in una situazione diversa da quella proposta - tipo $a_1 = a_4$, basta riordinare opportunamente gli elementi per ricondurci al caso trattato.

1. Dalla proposizione 4.4 sappiamo invece che ogni 3-ciclo genera un elemento del gruppo alternante che è pari. Quindi $\epsilon(\rho_2) = 1$. *Rimane solo il* 4*-ciclo (1,6,7,2) il cui segno può essere ricavato dal punto 2) del lemma 4.2 il quale ci garantisce che il segno* $\epsilon(\rho_1) = -1$*; per cui ne discende*

$$\epsilon(\sigma) = \prod_{i=1}^{3} \epsilon(\rho_i) = -1.$$

Esempio 4.3 *Mostriamo come si calcola esplicitamente il segno della seguente permutazione* $\sigma \in S_9$*:*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 4 & 1 & 8 & 9 & 6 & 7 & 2 \end{pmatrix}.$$

Come primo passo riscriviamo la permutazione in notazione a cicli: partendo da 1 *e proseguendo si costruisce direttamente*

$$\sigma \longleftrightarrow (1,3,4)(2,5,8,7,6,9).$$

Per calcolare il segno basta ricordarsi che ogni k*-ciclo identifica univocamente una permutazione ossia, nel dettaglio,*

$$(1,3,4) \longleftrightarrow \rho_1 = (1,3,4)(2)(5)(6)(7)(8)(9),$$
$$(2,5,8,7,6,9) \longleftrightarrow \rho_2 = (2,5,8,7,6,9)(1)(3)(4).$$

Pertanto abbiamo decomposto $\sigma = \rho_1 \cdot \rho_2$*. Ora sfruttiamo il lemma 4.1 per dire che* $\epsilon(\sigma) = \epsilon(\rho_1)\epsilon(\rho_2)$ *e successivamente il punto 2) del lemma 4.2 per concludere che il segno del* 3*-ciclo* ρ_1 *è* 1 *mentre quello del* 6*-ciclo* ρ_2 *è* -1*. In conclusione*

$$\epsilon(\sigma) = \epsilon(\rho_1)\epsilon(\rho_2) = -1.$$