Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea Triennale in Matematica

OSSERVAZIONI SUI GRUPPI SIMMETRICI E SUI GRUPPI DI SIMMETRIE

Tesi di Laurea in Algebra 2

Relatore:
Chiar.ma Prof.ssa
Monica Idá

Presentata da:
Marta Fagioli

II Sessione
Anno Accademico 2010-2011

Indice

Introduzione

Lo studio dei gruppi simmetrici costituisce uno strumento molto importante nell'ambito della teoria dei gruppi. Inoltre una delle applicazioni geometriche interessanti della teoria dei gruppi è lo studio delle simmetrie delle figure piane. In entrambi i casi si tratta di gruppi di biezioni su insiemi; nel primo caso biezioni di insiemi finiti, nel secondo caso biezioni su insiemi di punti del piano con l'ulteriore proprietà che vengano mantenute le distanze (si veda Definizione 3.2).
Nella prima parte della mia tesi (primo e secondo capitolo) ho raccolto e riassunto le proprietà di base del gruppo simmetrico S_n; mi sono maggiormente soffermata sulla rappresentazione di un ciclo come prodotto di trasposizioni, sul significato di *"cicli disgiunti"* (ovvero cicli che agiscono su insiemi disgiunti e che tra loro commutano sempre) e su come ogni permutazione si può scrivere in modo unico come prodotto di cicli disgiunti, quindi come prodotto di trasposizioni; pertanto l'ordine di una permutazione è il minimo comune multiplo delle lunghezze dei cicli che intervengono in questa rappresentazione e tali lunghezze sono interi (≥ 2) che definiscono, una volta permutati opportunamente i cicli, la *"successione caratteristica"* della permutazione, successione da cui dipende la sua classe di coniugio. In particolare ho fatto vedere che due permutazioni sono coniugate in S_n se e solo se hanno la stessa successione caratteristica. Ho studiato inoltre alcuni sistemi di generatori di S_n (come per esempio le trasposizioni del tipo $(1\ i)$ per $2 \leq i \leq n$) ed alcuni dei suoi sottogruppi. In particolare ho studiato il sottogruppo dato dalle permutazioni pari, cioè il gruppo alterno su n lettere A_n, mostrando tra l'altro

che A_n è semplice per $n \geq 5$. Ho anche provato che S_4 ha come sottogruppo il gruppo di Klein, cioè il gruppo con 4 elementi isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$. La seconda parte della tesi (terzo e quarto capitolo) rappresenta un'interessante applicazione della teoria dei gruppi. In questa sezione ho esaminato il gruppo M dei movimenti rigidi del piano, che si classificano in *isometrie dirette* (cioè che conservano l'orientazione come traslazioni e rotazioni) ed *isometrie inverse* (cioè quelle che non la conservano come riflessioni e glissoriflessioni), ed alcuni suoi sottogruppi, come per esempio il sottogruppo T delle traslazioni ed il sottogruppo O dei movimenti che tengono fissa l'origine. Quest'ultimo gruppo acquista fondamentale importanza in forza delle caratteristiche dei suoi sottogruppi finiti: per il *teorema del punto fisso* infatti esiste un punto p del piano lasciato fisso da ogni elemento di un sottogruppo G finito di M; facendo in modo che questo punto coincida con l'origine, sarà quest'ultima ad essere fissata da ciascun elemento del gruppo. Quindi per descrivere i sottogruppi finiti di M, basta descrivere quelli di O (dunque quelli di $O(2)$, cioè il gruppo delle matrici ortogonali 2×2, essendo $O \cong O(2)$). Si prova che un sottogruppo G di O può essere il gruppo C_n, ciclico di ordine n, generato dalla rotazione $\rho_{\frac{2\pi}{n}}$, oppure il gruppo D_n, diedrale di ordine $2n$, generato dalla rotazione $\rho_{\frac{2\pi}{n}}$ e dalla riflessione r', rispetto ad una retta per l'origine. La tesi si conclude con delle riflessioni più approfondite sui gruppi diedrali, ovvero i gruppi di simmetrie dei poligoni regolari , con particolare attenzione verso i gruppi D_3 e D_4.

Capitolo 1

Preliminari sul gruppo simmetrico di ordine n

Sia n un intero positivo. L'insieme delle corrispondenze biunivoche sull'insieme $\underline{n} = \{1, 2, \ldots, n\}$ con l'operazione di composizione, è un gruppo detto *gruppo simmetrico su n lettere* e denotato con S_n.
Un elemento $\alpha \in S_n$ si chiama permutazione.
Scriveremo α in questo modo:

$$\alpha = \begin{pmatrix} 1 & 2 & \ldots & n \\ \alpha(1) & \alpha(2) & \ldots & \alpha(n) \end{pmatrix}$$

dove $\alpha(i)$ indica il valore che assume α in i per $i = 1, 2, ..., n$.

Anche se l'operazione è la composizione scriveremo $\alpha\beta$ per indicare $\alpha \circ \beta$ con $\alpha, \beta \in S_n$ ovvero:
$(\alpha\beta)(i) = (\alpha \circ \beta)(i) = \alpha(\beta(i))$.

Esempio 1.1. :

In S_4 siano $\alpha = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 4\ 2\ 1 \end{pmatrix}$ e $\beta = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 4\ 3\ 1 \end{pmatrix}$; allora si ha:
$\alpha\beta = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 1\ 2\ 3 \end{pmatrix}$.

Le notazioni in S_n sono quelle usuali in un gruppo moltiplicativo. In particolare l'inversa di $\alpha \in S_n$ viene denotata con α^{-1} e:

$$\alpha^k = \begin{cases} \alpha\alpha\dots\alpha & \text{k volte se } k > 0 \\ 1 = id & \text{se } k = 0 \\ \alpha^{-1}\alpha^{-1}\dots\alpha^{-1} & \text{- k volte se } k < 0 \end{cases}$$

Teorema 1.0.1. *Il gruppo simmetrico S_n è finito di cardinalità n!*

Dimostrazione. Sia $\underline{n} = \{1, 2, \dots, n\}$. Si vuole dimostrare che l'insieme delle biezioni su $\underline{n}$ ha cardinalità $n!$. L'idea della dimostrazione è la seguente:
si consideri l'applicazione
$f : \{1, 2, \dots, n\} \longrightarrow \{1, 2, \dots, n\}$ biettiva: si hanno a disposizione n scelte per $f(1)$; rimangono $n-1$ scelte per $f(2)$; $n-2$ per $f(3), \dots$. Si procede in questo modo e alla fine si hanno $n(n-1)(n-2)\dots(1) = n!$ scelte possibili. □

Definizione 1.1. Sia $\alpha \in S_n$. Diciamo che α muove gli elementi di $\{j_1, j_2, \dots j_k\} \subseteq \underline{n}$ e fissa gli elementi di $\underline{n} - \{j_1, j_2, \dots j_k\}$ se $\alpha(j_i) \neq j_i$ per $i = 1, 2, \dots, k$ e $\alpha(j) = j$ per ogni altro j.

Definizione 1.2. Si definisce *ciclo di lunghezza k o k-ciclo* e viene denotato con $\gamma = (j_1\ j_2\ \ldots j_k)$ la permutazione $\gamma \in S_n$ tale che:

1 $\gamma(j) = j$ se $j \notin \{j_1, j_2, \ldots, j_k\}$

2 $\gamma(j_l) = j_{l+1}$ per $1 \leq l \leq k-1$

3 $\gamma(j_k) = j_1$

dove $\{j_1, j_2, \ldots, j_k\} \subseteq \underline{n}$ e $2 \leqslant k \leqslant n$.

Per quanto detto il k-ciclo γ muove gli elementi dell'insieme $\{j_1, j_2, \ldots, j_k\}$ e fissa quelli di $\underline{n} - \{j_1, j_2, \ldots j_k\}$, cioè ne fissa esattamente $n-k$.

Se $k = 2$ il ciclo viene detto *trasposizione*.

Un k-ciclo γ di S_n ha ordine k (scriveremo $|\gamma| = k$), cioè k è il più piccolo intero positivo tale che $\gamma^k = id$. Quindi ordine e lunghezza per un ciclo coincidono.

Osservazione 1. Un k-ciclo $\gamma = (j_1\ j_2 \ldots j_k) \in S_n$ può essere ciclicamente permutato senza che subisca cambiamenti, si può cioè scrivere: $\gamma = (j_1\ j_2 \ldots j_k) = (j_2\ j_3 \ldots j_k\ j_1) = \ldots = (j_k\ j_1 \ldots j_{k-1})$.

Lemma 1.0.2. *Ogni ciclo si scrive in modo unico come* $\gamma = (j_1\ j_2\ \ldots j_k)$ *con* $j_1 \leq j_l$ *per* $l = 2, 3, \ldots, k$.

Per la dimostrazione si veda [2] , proposizione 8.2.4.

In particolare, fissato un elemento di un ciclo γ in S_n, gli altri elementi si possono scrivere come potenze del ciclo stesso relative all'elemento fissato, nel modo seguente:

Proposizione 1.0.3. *Sia $\gamma = (j_1\ j_2\ \dots j_k)$ ciclo di S_n. Sappiamo che l'ordine di γ,$|\gamma|$, è k. Si ha:*
$\gamma^0(j_1) = j_1 = id(j_1), \gamma(j_1) = j_2, ..., \gamma^{k-1}(j_1) = j_k,$
$\gamma^k(j_1) = \gamma^0(j_1) = j_1.$

Ogni ciclo può dunque essere scritto nella forma: $\gamma = \big(\gamma^0(j_1)\ \gamma(j_1)\ \dots \gamma^{k-1}(j_1)\big)$.

Per la dimostrazione si veda [1] .

Per quanto detto sopra, fissato per esempio l'elemento j_1, si può scrivere in modo del tutto equivalente:
$\gamma = \big(\gamma^0(j_1)\ \gamma^1(j_1)\ \dots \gamma^{k-1}(j_1)\big) = \big(\gamma(j_1)\ \gamma^2(j_1)\ \dots \gamma^{k-1}(j_1)\gamma^0(j_1)\big)$.

Esempio 1.2. In S_4, $\gamma = (2\ 3\ 4\ 5) = (3\ 4\ 5\ 2)$. Inoltre, partendo ad esempio da 2, si ha: $\gamma = (\gamma^0(2)\ \gamma(2)\ \gamma^2(2)\ \gamma^3(2)) = (\gamma(2)\ \gamma^2(2)\ \gamma^3(2)\ \gamma^0(2))$.

Definizione 1.3. Due cicli di S_n si dicono *disgiunti* se gli insiemi che rispettivamente muovono sono disgiunti.

Esempio 1.3. :
In S_7, $\gamma = (3\ 2\ 1)$ e $\delta = (5\ 6\ 7)$ sono disgiunti, infatti
$\{1, 2, 3\} \cap \{5, 6, 7\} = \emptyset$.

Lemma 1.0.4. *Due cicli disgiunti $\gamma, \delta \in S_n$ commutano sempre cioè* $\gamma\delta = \delta\gamma$.

Dimostrazione. Siano $\gamma = (i_1\ i_2 \dots i_k)$ *e* $\delta = (j_1\ j_2 \dots j_s)$ due cicli disgiunti in S_n. Sia i un intero tale che $1 \leq i \leq n$.
Se $i \in \underline{n} - \{i_1, i_2, \dots, i_k\} \cup \{j_1, j_2, \dots, j_s\}$ allora, per definizione di ciclo, si ha $\gamma(i) = i = \delta(i)$ dunque $\gamma\delta(i) = i = \delta\gamma(i)$. Se $i \in \{i_1, i_2, \dots, i_k\}$, per esempio $i = i_1$, allora $\delta\gamma(i) = \delta\gamma(i_1) = \delta(i_2) = i_2$ e $\gamma\delta(i) = \gamma\delta(i_1) = \gamma(i_1) = i_2$. Stessa cosa se $i \in \{j_1, j_2, \dots, j_s\}$. □

Esempio 1.4. :
In S_5: $(1\ 2)\,(3\ 4\ 5) = (3\ 4\ 5)\,(1\ 2)$.

Lemma 1.0.5. *Ogni ciclo si scrive come prodotto di trasposizioni. Per esempio si ha:*
$(i_1 \dots i_m) = (i_1\ i_m)\,(i_1\ i_{m-1}) \dots (i_1\ i_2)$.

Osservazione 2. La scrittura di un ciclo come prodotto di trasposizioni non è unica. Si consideri per esempio $\gamma = (1\ 2\ 3\ 4) \in S_n$.
Allora $\gamma = (1\ 4)\,(1\ 3)\,(1\ 2) = (1\ 4)\,(1\ 3)\,(1\ 2)\,(4\ 5)\,(5\ 4)$, dove il prodotto delle ultime due è l'identità.

Analizziamo più da vicino il gruppo simmetrico su 3 lettere

Il gruppo simmetrico S_3 ha cardinalità $3! = 6$. I cicli di S_3 possono avere lunghezza 2 o 3. I cicli di lunghezza 2 sono $(1\ 2), (1\ 3), (2\ 3)$, quelli di lunghezza 3 invece $(1\ 2\ 3), (1\ 3\ 2)$. Si avrà quindi: $S_3 = \{id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$ e questi sono tutti e soli i suoi elementi. Il gruppo simmetrico S_3 non è abeliano infatti la sua tavola di moltiplicazione non è simmetrica rispetto alla diagonale:

*	1	(1 2 3)	(1 3 2)	(1 2)	(1 3)	(2 3)
1	1	(1 2 3)	(1 3 2)	(1 2)	(1 3)	(2 3)
(1 2 3)	(1 2 3)	(1 3 2)	1	(1 3)	(2 3)	(1 2)
(1 3 2)	(1 3 2)	1	(1 2 3)	(2 3)	(1 2)	(1 3)
(1 2)	(1 2)	(2 3)	(1 3)	1	(1 3 2)	(1 2 3)
(1 3)	(1 3)	(1 2)	(2 3)	(1 2 3)	1	(1 3 2)
(2 3)	(2 3)	(1 3)	(1 2)	(1 3 2)	(1 2 3)	1

La tavola di moltiplicazione di S_3 contiene la tavola di moltiplicazione del sottogruppo ciclico H generato da $(1\ 2\ 3)$ (si noti che $H = \langle(1\ 2\ 3)\rangle = \langle(1\ 3\ 2)\rangle$), e le tavole dei tre sottogruppi ciclici generati dalle trasposizioni di S_3. Poichè $H \cong \mathbb{Z}_3$ e $\langle(1\ 2)\rangle = \langle(1\ 3)\rangle = \langle(2\ 3)\rangle \cong \mathbb{Z}_2$, questi hanno la tavola di moltiplicazione simmetrica rispetto alla diagonale come quelle di $\mathbb{Z}_3$ e di $\mathbb{Z}_2$.

Il gruppo simmetrico S_3 si può pensare per esempio generato da $(1\ 2\ 3), (1\ 2)$, oppure da $(1\ 3\ 2), (1\ 3)$.

Come appena visto per S_3, anche S_n, con $n \geq 4$, non è un gruppo abeliano:

Proposizione 1.0.6. *Per $n \geqslant 3$, S_n non è un gruppo abeliano.*

Dimostrazione. Si consideri infatti in S_n la trasposizione $(1\ 2)$ e il 3-ciclo $(1\ 2\ 3)$; si ha che $(1\ 2)\,(1\ 2\ 3) \neq (1\ 2\ 3)\,(1\ 2)$. □

Capitolo 2

Coniugio in S_n. Sistemi di generatori per S_n

Definizione 2.1. Si consideri $\alpha \in S_n$ e un intero j $\in \underline{n}$. Si chiama *orbita* di j rispetto ad α l'insieme $O(j) := \left\{\alpha^l(j) \mid l \in \mathbb{Z}\right\} \subset \{1, 2, \ldots, n\}$.
In particolare l'orbita di j contiene j ed è uguale a $\{j\}$ se e solo se $\alpha(j) = j$.

Si osservi che le orbite dei vari elementi di $\{1, 2, \ldots, n\}$ formano una partizione di $\{1, 2, \ldots, n\}$, ossia ciascun elemento di $\{1, 2, \ldots, n\}$ sta in una ed una sola orbita. Questo perchè la relazione in S_n: $i \sim_\alpha j \iff \exists\ k \in \mathbb{Z},\ \alpha^k(i) = j$ è una relazione di equivalenza.

Esempio 2.1. Sia $\gamma \in S_7$, $\gamma = (1\ 2\ 3\ 4\ 5)$. Si indica con
$O(1) = O(2) = O(3) = O(4) = O(5) = \{1, 2, 3, 4, 5\}$ l'orbita di 1, 2, 3, 4, 5 e con $O(6) = \{6\}$ e $O(7) = \{7\}$ rispettivamente l'orbita di 6 e di 7 poichè γ non muove gli elementi 6 e 7.

Proposizione-definizione 2.0.7. *Se $\alpha \in S_n$, $i \in \underline{n}$ e $r := min\left\{k \in \mathbb{Z} |\ \alpha^k(i) = i\right\}$, allora $O(i) = \{i, \alpha(i), \ldots, \alpha^{r-1}(i)\}$ è l'orbita di i rispetto ad α.*

Dimostrazione. Sia $i \in \underline{n}$. Sia $G = \left\{k \in \mathbb{Z}, \alpha^k(i) = i\right\}$; $G \neq \emptyset$ perchè $0 \in G$ e se $k, s \ \in G$, allora $\alpha^{k-s}(i) = (\alpha^k(\alpha^s)^{-1})(i) = i \Longrightarrow \ k - s \in G$. Quindi G è un sottogruppo di $\mathbb{Z}$, quindi è ciclico generato da un opportuno r: $G = \langle r \rangle$. Si ha $\alpha^k(i) = \alpha^s(i) \Longleftrightarrow (\alpha^s)^{-1}(\alpha^k(i)) = i \Longleftrightarrow k - s \ \in \langle r \rangle \Longleftrightarrow k \equiv s \, (mod\, r)$. Quindi $O(i) = \{\alpha^0(i), \alpha^1(i), \ldots, \alpha^{r-1}(i)\}$. □

Teorema 2.0.8. *Ogni permutazione $\alpha \in S_n$, $\alpha \neq id$, si può scrivere come $\alpha = \gamma_1\gamma_2 \ldots \gamma_r$, con $\gamma_1, \gamma_2, \ldots, \gamma_r$ cicli tali che γ_i e γ_j sono cicli disgiunti se $i \neq j$. Questa rappresentazione di α come prodotto di cicli disgiunti è unica a meno dell'ordine dei fattori.*

Dimostrazione. Premessa: supponiamo che $\alpha = \gamma_1\gamma_2 \ldots \gamma_r$, dove i γ_k per $k = 1, 2, \ldots, r$ sono cicli a due a due disgiunti. Sia $i \in \underline{n}$. Se i non compare in nessuno dei cicli $\gamma_1, \gamma_2, \ldots, \gamma_r$ allora $\gamma_k(i) = i \ \forall k = 1, 2, \ldots, r$, quindi $\alpha(i) = i$ e l'orbita di i è $\{i\}$. Supponiamo invece che i compaia in uno dei γ_k, per esempio in γ_1. Poichè i γ_k sono cicli a due a due disgiunti, commutano tra loro, dunque possiamo sempre cambiare l'ordine dei γ_k in modo che quello che contiene i, passi al primo posto. Supponiamo dunque $\gamma_1 = (i_1 \ldots i_l)$ e poniamo $i = i_1$ (se $i = i_k$ allora possiamo sempre scrivere $(i_1 \ldots i_l) = (i_k \ldots i_{k-1})$). Allora ciascuno dei γ_k, con $k \geqslant 2$ lascia fisso i e quindi $\alpha(i) = \gamma_1(i) = i_2$. Allo stesso modo $\alpha^2(i) = \alpha(i_2) = \gamma_1(i_2) = i_3$, e così via; si avrà dunque: $\alpha^h(i) = i_{h+1} \neq i_1 = i$ per $1 \leqslant h \leqslant l - 1$, mentre $\alpha^l(i) = \alpha\left(\alpha^{l-1}(i)\right) = \alpha(i_l) = i_1 = i$. L'orbita di i è dunque $\{i_1, \ldots, i_l\}$. Per quanto visto, un elemento i di $\underline{n}$ ha un'orbita con più di un elemento se e solo se compare in uno dei cicli γ_k (che è unico!) e l'orbita di i è l'insieme degli elementi di $\underline{n}$ che compaiono in γ_k. Questo fatto determina una corrispondenza biunivoca tra le orbite di α con più di un elemento, e i cicli γ_k per $k = 1, 2, \ldots, r$.

Dimostriamo l'unicità. Supponiamo che esistano due rappresentazioni distinte di α come prodotto di cicli a due a due disgiunti, sia cioè $\alpha = \gamma_1 \dots \gamma_r = \gamma_1^{'} \dots \gamma_t^{'}$. Per quanto visto in precedenza, esiste una corrispondenza biunivoca tra le orbite di α con più di un elemento e i cicli γ_k per $k = 1, 2, \dots, r$ e tra le orbite di α con più di un elemento e i cicli $\gamma_s^{'}$ per $s = 1, 2, \dots, t$. Allora si ha che $r = t$ e permutando i cicli $\gamma_1^{'}, \dots, \gamma_t^{'}$ possiamo assumere che γ_k e $\gamma_k^{'}$ corrispondano alla stessa orbita σ. Se $\gamma_k = (i_1 \dots i_l)$ e $\gamma_k^{'} = (j_1 \dots j_h)$ allora $\{i_1, \dots, i_l\} = \sigma = \{j_1, \dots, j_h\}$ e quindi $\{i_1, \dots, i_l\} = \{j_1, \dots, j_h\}$, allora $l = h$. Inoltre possiamo assumere che $i_1 = j_1$. Allora avremo che $i_2 = \alpha(i_1) = \alpha(j_1) = j_2$, $i_3 = \alpha(i_2) = \alpha(j_2) = j_3$, e così via. Quindi $\gamma_k = \gamma_k^{'}$ per $\forall k = 1, 2, \dots, r$.

Dimostriamo ora l'esistenza di tale scomposizione. Siano $\sigma_1, \dots, \sigma_r$ le orbite di α con più di un elemento. Di queste ne esisterà almeno una (cioè $r \geqslant 1$), altrimenti saremmo nel caso banale di $\alpha = id$. Se σ_k ha l elementi allora $\sigma_k = \left\{i, \alpha(i), \dots, \alpha^{l-1}(i)\right\}$. Poniamo $\gamma_k = \left(i\ \alpha(i) \dots \alpha^{l-1}(i)\right)$. Allora i cicli $\gamma_1, \dots, \gamma_r$ sono a due a due disgiunti, poichè lo sono gli insiemi $\sigma_1, \dots, \sigma_r$. Proviamo che $\alpha = \gamma_1 \dots \gamma_r$. Se j non compare in nessuna delle σ_k, allora l'orbita di j, come visto nella premessa alla dimostrazione, è $\{j\}$ e $\alpha(j) = j$. Inoltre si ha che $\gamma_k(j) = j\ \forall k = 1, 2, \dots, r$ e quindi $\gamma_1 \dots \gamma_r(j) = \alpha(j) = j$. Se invece $j \in \sigma_k$ allora $\alpha(j) = \gamma_k(j)$, mentre γ_h per $h \neq k$ lascia fissi tutti gli elementi di σ_k. Quindi $\alpha(j) = \gamma_k(j) = \gamma_1 \dots \gamma_r(j)$. □

La rappresentazione di una permutazione come prodotto di cicli disgiunti e le proprietà dei cicli in S_n costituiscono uno strumento molto importante per studiare le caratteristiche degli elementi di S_n. Si hanno infatti i seguenti risultati:

Proposizione 2.0.9. *L'ordine di una permutazione $\alpha \in S_n$ è uguale al minimo comune multiplo delle lunghezze di tutti i cicli che intervengono nella scomposizione di α come prodotto di cicli disgiunti.*

Dimostrazione. Sia $\alpha \in S_n$, $\alpha \neq id$. Scriviamo $\alpha = \gamma_1\gamma_2 \dots \gamma_r$, cicli a due a due disgiunti. Poichè $\gamma_1, \gamma_2, \dots \gamma_r$ commutano a due a due avremo $\alpha^m = \gamma_1^m\gamma_2^m \dots \gamma_r^m \ \forall m \in \mathbb{Z}$. In particolare, se m è il minimo comune multiplo tra le lunghezze di $\gamma_1, \gamma_2, \dots \gamma_r$ si ha che $\alpha^m = id$ e quindi l'ordine di α divide m. Sia k l'ordine di α. Poniamo $\gamma_1 = (j_1\ j_2 \dots j_l)$. Allora α manda $\{j_1, j_2, \dots j_l\}$ in se stesso e le restrizione di α e di γ_1 all'insieme $\{j_1, j_2, \dots, j_l\}$ coincidono. Quindi γ_1^k agisce sugli elementi di $\{j_1, j_2, \dots j_l\}$ come α^k ovvero come l'identità. Poichè $\gamma_1^k(j) = j \ \forall j \in \underline{n} - \{j_1, j_2, \dots, j_l\}$ si ha che $\gamma_1^k = id$. Quindi k dev'essere divisibile per l'ordine $|\gamma_1|$ di γ_1. Analogamente per gli altri cicli γ_i, con $i = 2, 3, \dots, r$, k è divisibile per $|\gamma_2|, \dots, |\gamma_r|$ e quindi l dev'essere divisibile per m. □

Proposizione 2.0.10. *Se $n \geq 2$, ogni permutazione $\alpha \in S_n$ è prodotto di trasposizioni.*

Dimostrazione. Sia $\alpha \in S_n, \alpha \neq id$. Allora α è prodotto di cicli disgiunti (per il teorema precedente), ciascuno dei quali è a sua volta prodotto di trasposizioni per il lemma 1.0.5. Quindi ogni permutazione non identica è prodotto di trasposizioni. Inoltre si ha che $id = (1\ 2)\,(1\ 2)$. □

Definizione 2.2. Sia $\alpha \in S_n$, $\alpha = \gamma_1\gamma_2 \dots \gamma_r$ la sua rappresentazione come prodotto di cicli disgiunti e sia l_k la lunghezza del ciclo γ_k per $k = 1, 2, \dots, r$. Permutando opportunamente i γ_k si può assumere $l_1 \geq l_2 \geq \dots \geq l_r \geq 2$; si ha $l_1 + l_2 + \dots + l_r \leq n$. Si chiama *successione caratteristica della permutazione* la successione di interi $l_1, l_2, \dots, l_r$. Tale successione è univocamente determinata da α per il teorema precedente.

Proposizione-definizione 2.0.11. *Sia* $(G, \cdot)$ *un gruppo e sia* a *un elemento di* G. *L'applicazione* $f_a : G \longmapsto G$ *tale che* $f_a(x) = axa^{-1}$ *è un automorfismo di* G. *Diciamo che due elementi* y *e* z *di* G *sono* coniugati *in* G *se esiste un* a $\in$ G *tale che* $y = aza^{-1} = f_a(z)$.

"Essere coniugati" è un relazione di equivalenza in G.
La dimostrazione è immediata.

Lemma 2.0.12. *Sia* $\gamma = (i_1, \ldots, i_l)$ *un ciclo in* S_n *e sia* $\sigma \in S_n$. *Allora* $\sigma\gamma\sigma^{-1} = (\sigma(i_1) \ldots \sigma(i_l))$.

Dimostrazione. Basta confrontare i valori assunti da $\sigma\gamma\sigma^{-1}$ e dal ciclo $(\sigma(i_1) \ldots \sigma(i_l))$ su ogni $j \in \underline{n}$. □

Teorema 2.0.13. *Due permutazioni* $\alpha, \beta \in S_n$ *sono coniugate se e solo se hanno stessa successione caratteristica.*

Dimostrazione. Dimostriamo, come prima cosa, che due permutazioni coniugate hanno stessa successione caratteristica. Sia $\alpha \in S_n$, $\alpha \neq id$, e sia $\alpha = \gamma_1 \ldots \gamma_r$ la sua scomposizione in prodotto di cicli disgiunti, con l_k lunghezza del ciclo γ_k $\forall k = 1, 2, \ldots, r$. Sia $\sigma \in S_n$ e consideriamo le permutazioni coniugate α e $\sigma\alpha\sigma^{-1}$. Allora si ha che $\sigma\alpha\sigma^{-1} = \sigma(\gamma_1 \ldots \gamma_r) = \sigma\gamma_1(\sigma^{-1}\sigma)\gamma_2 \ldots (\sigma^{-1}\sigma)\gamma_r\sigma^{-1} = (\sigma\gamma_1\sigma^{-1}) \ldots (\sigma\gamma_r\sigma^{-1})$.
I cicli $\sigma\gamma_1\sigma^{-1}, \ldots, \sigma\gamma_r\sigma^{-1}$ sono a due a due disgiunti. Supponiamo infatti che $k \neq h$ e che $\sigma\gamma_k\sigma^{-1}$ e $\sigma\gamma_h\sigma^{-1}$ non siano disgiunti. Poniamo $\gamma_k = (i_1 \ldots i_l)$ e $\gamma_h = (j_1 \ldots j_m)$. Per il lemma 2.0.12 $(\sigma\gamma_k\sigma^{-1}) = (\sigma(i_1) \ldots \sigma(i_l))$ e $\sigma\gamma_h\sigma^{-1} = (\sigma(j_1) \ldots \sigma(j_m))$. Esisteranno un i_t e un j_s tali che $\sigma(i_t) = \sigma(j_s)$ e quindi $i_t = j_s$ poichè σ è biettiva. Ma allora γ_k e γ_h non sono disgiunti contrariamente all'ipotesi. Sempre per il lemma 2.0.12 i cicli γ_k e $\sigma\gamma_k\sigma^{-1}$ sono cicli della stessa lunghezza, dunque α e $\sigma\alpha\sigma^{-1}$ hanno stessa successione

caratteristica.

Dimostriamo ora il viceversa, cioè che due permutazioni con la stessa successione caratteristica sono coniugate. Siano α, β due permutazioni con stessa successione caratteristica. Possiamo quindi scrivere $\alpha = \gamma_1 \dots \gamma_r$ e $\beta = \delta_1 \dots \delta_r$ con $\gamma_1, \dots, \gamma_r$ e $\delta_1, \dots, \delta_r$ cicli disgiunti con la lunghezza di γ_k uguale alla lunghezza di δ_k $\forall k = 1, 2, \dots, r$. Poniamo $\gamma_k = (i_1 \dots i_l)$ e $\delta_k = (j_1 \dots j_l)$.
Si consideri la biezione $\sigma_k : \{i_1, \dots, i_l\} \longmapsto \{j_1, \dots, j_l\}$ così definita:
$\sigma_k(i_s) = j_s$ $\forall s = 1, 2, \dots, l$. Se A è l'insieme degli interi tra 1 e n che non compaiono nei γ_k e B è l'insieme di quelli che non compaiono nei δ_k $\forall k$, allora A e B hanno stessa cardinalità. Sia quindi $\tau : A \longmapsto B$ una corrispondenza biunivoca. Definiamo una permutazione $\sigma : \{1, 2, \dots, n\} \longmapsto \{1, 2, \dots, n\}$ nel seguente modo: $\sigma(i) = \sigma_k(i)$ se i compare in γ_k e $\sigma(i) = \tau(i)$ se i sta in A. Allora si ha che $\sigma\gamma_k\sigma^{-1} = \delta_k$ $\forall k = 1, 2, \dots, r$ e quindi $\sigma\alpha\sigma^{-1} = \beta$. □

Alla luce di quanto detto sul legame tra cicli (in particolare consideriamo ora le trasposizioni) e permutazioni, sono dati dei sistemi di generatori (qui ne diamo due) per il gruppo simmetrico S_n.

Teorema 2.0.14. *Il gruppo simmetrico S_n è generato da* $(1\ 2), (1\ 3), \ldots, (1\ n)$.

Dimostrazione. Bisogna dimostrare che ogni permutazione $\alpha \in S_n$ è prodotto di trasposizioni tra quelle mostrate, cioè che si può esprimere una generica trasposizione $(i\ j)$ nella forma $(1\ i)$. Se $i, j \neq 1$ si ha: $(i\ j) = (1\ i)(1\ j)(1\ i)$ e poichè $(i\ 1) = (1\ i)$ si ottiene il risultato cercato. □

Corollario 2.0.15. *(Esercizio (4) p. 57, [3]) Il gruppo simmetrico S_n è generato da* $(1\ 2), (2\ 3), ..., (n-1\ n)$.

Dimostrazione. Bisogna dimostrare che le trasposizioni che generano S_n, cioè quelle nella forma $(1\ i)$ per $i = 2, \ldots, n$, si possono scrivere come prodotto di trasposizioni del tipo $(i-1\ i)$ per $i = 2, \ldots, n$. Per induzione su n: se $i = 2$ è vero. In generale vale: $(1\ i) = (1\ i-1)(i-1\ i)(1\ i-1)$. Quindi se è vero per $i-1$, scrivendo $(1\ i-1)$ come prodotto di trasposizione del tipo $(j-1\ j)$ si ha la tesi. □

Teorema 2.0.16. *Ogni ciclo $\gamma \in S_n$ può essere scritto come prodotto di un numero sempre pari o sempre dispari di trasposizioni; quindi ogni permutazione $\alpha \in S_n$ può a sua volta essere scritta come prodotto di un numero sempre pari o sempre dispari di trasposizioni.*

Per la dimostrazione si veda per esempio [2] .

Definizione 2.3. Il *segno* di una permutazione $\alpha \in S_n$ è 1 se α è il prodotto di un numero pari di trasposizioni, -1 se è il prodotto di un numero dispari di trasposizioni. Una permutazione è detta *pari* se il suo segno è 1, è *dispari* se il suo segno è -1. Quindi, se α è prodotto di r trasposizioni allora $sgn(\alpha) = (-1)^r$.

Osservazione 3. Un k-ciclo di S_n è pari se e solo se k è dispari, è dispari se e solo se k è pari (si veda il lemma 1.0.5).

Proposizione 2.0.17. *Valgono le seguenti condizioni:*

1 $sgn(id) = 1$.

2 Sia $\alpha \in S_n$, $sgn(\alpha) = sgn(\alpha^{-1})$.

3 $\forall\ \alpha, \beta$ *in* S_n, $sgn(\alpha\beta) = sgn(\alpha)\, sgn(\beta)$.

Quindi se α, β hanno stesso segno $\alpha\beta$ è pari, altrimenti è dispari.

Per la dimostrazione si veda per esempio [2] , proposizione 8.3.5.

Osservazione 4. Comunque si moltiplichi una permutazione $\alpha \in S_n$ per una trasposizione, il segno di α cambia; moltiplicando (in qualunque modo) α per un numero pari di trasposizioni, il segno rimane lo stesso, per un numero dispari di trasposizioni invece cambia.

Definizione 2.4. L'insieme dato dalle permutazioni pari è un sottogruppo di S_n detto *gruppo alterno su n lettere* e denotato con A_n.

Osservazione 5. Per $n = 3$, A_3 contiene tre elementi, ovvero l'identità e i cicli $(1\ 2\ 3)$, $(1\ 3\ 2) = (1\ 2\ 3)^2$. Si tratta dunque di un gruppo abeliano ciclico. Per $n \geq 4$ invece A_n non è abeliano. Si ha per esempio:
$(1\ 2\ 3)\,(1\ 2\ 4) = (1\ 3)\,(2\ 4) \neq (1\ 2\ 4)\,(1\ 2\ 3) = (1\ 4)\,(2\ 3)$.

Proposizione 2.0.18. *Il gruppo simmetrico S_n ha tante permutazioni pari quante dispari. Dunque A_n ha $\frac{n!}{2}$ elementi, come pure $S_n - A_n$.*

Dimostrazione. Sia $\tau \in S_n$ una permutazione dispari (sia per esempio una trasposizione). Allora, per la proposizione precedente, si ha che $\alpha\tau$ è dispari se e solo se α è pari. Si consideri la biezione $f_\tau : S_n \longrightarrow S_n$ (traslazione destra di S_n definita da τ), tale che $f_\tau(\alpha) = \alpha\tau$, la cui inversa manda α in $\alpha\tau^{-1}$. Si ha che $f_\tau(\alpha) \in S_n - A_n$ se e solo se $\alpha \in A_n$. Quindi la restrizione di f_τ ad A_n è iniettiva con immagine $S_n - A_n$, è cioè una biezione tra A_n e $S_n - A_n$, quindi A_n ha esattamente la metà degli elementi di S_n , cioè $\frac{n!}{2}$. □

Osservazione 6. Per quanto detto l'insieme costituito dalle permutazioni dispari, ossia $S_n - A_n$ non è un sottogruppo di S_n essendo l'identità pari.

Corollario 2.0.19. *Il gruppo alterno A_n è un sottogruppo normale in S_n.*

Dimostrazione. Basta osservare che l'indice di A_n in S_n è 2. □

Lemma 2.0.20. *A_n contiene tutti i cicli di lunghezza 3.*

Dimostrazione. Segue direttamente dalla definizione di gruppo alterno: infatti un ciclo di lunghezza tre si scrive come prodotto di due trasposizioni e quindi il suo segno è $(-1)^2 = 1$, cioè è pari. □

Teorema 2.0.21. *A_n è generato da* $(1\ 2\ 3), (1\ 2\ 4), \ldots (1\ 2\ n)$

Dimostrazione. Poichè $(i\ j)(k\ l) = (i\ j\ k)(k\ i\ l)$ e $(i\ j)(i\ k) = (i\ k\ j)$, A_n è generato da tutti i cicli di lunghezza 3 e questi sono tutti esprimibili nella forma $(1\ 2\ i)$ tramite le seguenti formule:

$$(i\ j\ k) = (1\ 2\ i)(2\ j\ k)(1\ 2\ i)^{-1}$$

$$(2\ j\ k) = (1\ 2\ j)(1\ 2\ k)(1\ 2\ j)^{-1}$$

$$(1\ j\ k) = (1\ 2\ k)^{-1}(1\ 2\ j)(1\ 2\ k)$$

□

Proposizione 2.0.22. *Sia G un sottogruppo non banale di S_n, non contenuto in A_n. Allora G ha tante permutazioni pari quante dispari.*

Dimostrazione. Sia G sottogruppo di S_n. Sia $G = P \cup D$, dove $P = \{p_1, p_2, \ldots, p_n\} = G \cap A_n$ è l'insieme delle permutazioni pari di G e $D = \{d_1, d_2, \ldots d_m\} = G \cap (S_n - A_n)$ insieme delle dispari. Si deve dimostrare che $|D| = m = n = |P|$. Sia $D^* = \{d_1d_1, d_2d_1, \ldots, d_md_1\}$ costituito da permutazioni pari (il prodotto di due permutazioni dello stesso segno è pari), tutte distinte tra loro, dato che l'uguaglianza di due elementi di D^* implica quella di due elementi $d_i = d_j$ di D, essendo un gruppo in cui vale certo la legge di cancellazione. Quindi $|D| = |D^*|$. Si ha anche, evidentemente, che $D^* \subseteq P$, quindi passando alle cardinalità $|D| = |D^*| \leq |P|$, quindi $m \leq n$. Si consideri ora l'insieme $P^* = \{p_1d_1, p_2d_1, \ldots, p_md_1\}$ costituito da permutazioni dispari (il prodotto di permutazioni di segno diverso è dispari), tutte distinte tra loro. Con un ragionamento analogo al precedente si vede che $|P| = |P^*| \leq |D|$. Quindi $n \leq m$, quindi si ha l'uguaglianza. □

Proposizione 2.0.23. *Sia $n \geq 3$. Sia N un sottogruppo normale di A_n. Se N contiene un 3-ciclo allora $N = A_n$.*

Dimostrazione. Sia N un sottogruppo normale di A_n. Si consideri $n = 3$. $A_3 = \{id, \alpha = (1\ 2\ 3), \alpha^{-1} = (1\ 3\ 2)\}$. N è normale in A_3, se $\alpha \in N$ allora $\alpha^{-1} \in N$ (stessa cosa se $\alpha^{-1} \in N$), quindi $N = A_3$. Sia $n \geq 4$ e sia $(1\ 2\ 3) \in N$. In A_n si consideri l'elemento $(3\ k)\,(1\ 2)$ con $k \neq 1, 2, 3$, (esiste di certo poichè è una permutazione pari e $n \geq 4$).
Essendo $[(3\ k)\,(1\ 2)]^{-1} = (1\ 2)\,(3\ k)$, N normale in A_n e $(1\ 2\ 3) \in N$, si ha: $(3\ k)\,(1\ 2)\,(1\ 2\ 3)\,(1\ 2)\,(3\ k) \in N$ cioè $(2\ 1\ k) \in N$, $\forall\ k \neq 1, 2, 3$. Inoltre $(1\ 2\ 3)^{-1} = (2\ 1\ 3)$, quindi i cicli $(1\ 2\ j) \in N$, $\forall\ j \neq 1, 2$ e questi $n-2$ 3-cicli, per quanto visto nel teorema 2.0.21, generano A_n e quindi $N = A_n$. □

Definizione 2.5. Un gruppo G è *semplice* se non è banale e non ha sottogruppi normali propri.

Teorema 2.0.24. *Per $n \geq 5$, A_n è semplice.*

Dimostrazione. Sia N un sottogruppo non banale di A_n con $n \geq 5$. Sia $\alpha \in N$, $\alpha \neq$id, una permutazione di N tra quelle che lasciano fissi il massimo numeri di elementi. Si consideri la rappresentazione di α come prodotto di cicli disgiunti, $\alpha = \gamma_1 \dots \gamma_r$ $(*)$.

(a) Suppongo che in $(*)$ compaia un ciclo di lunghezza almeno 4: sia $\alpha = (1\ 2\ 3\ 4 \dots)\,(i\ j \dots) \dots$ e sia $\beta = (1\ 2\ 3)\,\alpha\,(1\ 2\ 3)^{-1} = (2\ 3\ 1\ 4 \dots)\,(i\ j \dots) \dots$. Essendo N normale in A_n si ha $\beta \in N$ e $\beta^{-1}\alpha \in N$. Risulta: $\beta^{-1}\alpha = (2)\,(3\ 1 \dots) \dots$; inoltre se $\alpha(k) = k$ con $k \geq 5$, allora anche $\beta(k) = k$ e $\beta^{-1}\alpha(k) = k$, quindi $\beta^{-1}\alpha \in N$, $\beta^{-1}\alpha \neq id$ e poichè $\beta^{-1}\alpha(2) = 2$ la permutazione $\beta^{-1}\alpha$ fissa almeno un elemento in più rispetto ad α, e ciò è assurdo. Quindi ogni ciclo in $(*)$ è di lunghezza ≤ 3.

(b) Suppongo che in $(*)$ compaia un ciclo di lunghezza 3: sia $\alpha = (1\ 2\ 3)\,(4\ 5\ldots)\ldots$ e sia $\gamma = (4\ 1\ 2)\,\alpha\,(4\ 1\ 2)^{-1}$. N è normale in A_n, $\gamma \in N$; inoltre $\gamma\alpha \in N$ e $\gamma\alpha \neq id$. Infatti $\gamma = (1\ 5\ldots)\,(2\ 4\ 3)\ldots$ e $\gamma\alpha = (2)\,(1\ 4\ldots)\ldots$. Se $j \neq 1, 2, 3$, $\alpha(j) = j$ allora $\gamma(j) = j$ e $\gamma\alpha(j) = j$; poichè $\gamma\alpha(2) = 2$ si ha che $\gamma\alpha$ fissa più elementi di α che è assurdo. Quindi se in $(*)$ compare un ciclo di lunghezza 3 questo è l'unico ciclo di α.

(c) Suppongo che in $(*)$ compaiono due trasposizioni: sia $\alpha = (1\ 2)\,(3\ 4)\ldots$ e $\delta = (1\ 2\ 5)\,\alpha\,(1\ 2\ 5)^{-1}$. Si ha che $\delta = (2\ 5)\,(3\ 4)\ldots$, $\delta\alpha = (3)\,(4)\,(2\ 1\ 5\ldots)$, $\delta \in N$, $\delta\alpha \neq id, \delta\alpha\ \in N$. Solo l'elemento 5 può essere fisso per α e non per δ, ogni altro elemento fissato da α è anche fissato da δ. Dunque $\delta\alpha$ fissa tutti gli elementi fissati da α tranne al più 5, ma $\delta\alpha$ fissa sia il 3 che il 4 quindi fissa un numero maggiore di elementi rispetto ad α e questo è assurdo. Quindi in $(*)$ non possono esserci due trasposizioni.

Da (a),(b),(c) si ha che α è un 3-ciclo o una trasposizione, ma $\alpha \in N \subseteq A_n$ è pari, quindi è un 3-ciclo allora, per la proposizione precedente, $N = A_n$. □

Definizione 2.6. Sia X un insieme qualunque non vuoto. Chiamiamo *gruppo simmetrico su X* e lo denotiamo con $S(X)$, il gruppo il cui insieme sottogiacente è $\{f | f : X \longmapsto X, f \textit{ biettiva}\}$ e l'operazione è la composizione . In particolare se $X = \{1, 2, \ldots, n\}$ è finito allora $S(X) = S_n$. Si chiama *gruppo di trasformazioni* un sottogruppo di $S(X)$.

La teoria sui gruppi di permutazioni fornisce un metodo di rappresentazione degli elementi di un gruppo G; il prossimo teorema ci mostra infatti come ogni gruppo è isomorfo ad un sottogruppo di un gruppo simmetrico.

Teorema 2.0.25. *(Teorema di Cayley)*
Ogni gruppo G è isomorfo a un gruppo di trasformazioni. Precisamente G è isomorfo a un sottogruppo di $S(G)$.

Per la dimostrazione si veda [2] .

Osservazione 7. Ogni gruppo finito G è isomorfo a un sottogruppo di S_n, dato che $S(G) = S|G|$. Conoscere i sottogruppi di S_n ci aiuta a conoscere i gruppi finiti.

Osservazione 8. Siano X e Y due insiemi, sia $\varphi : X \longrightarrow Y$ una funzione biettiva. Definiamo una funzione $\Phi : S(X) \longrightarrow S(Y)$ nel modo seguente:
$\forall\ \alpha\ \in S(X), \Phi(\alpha) = \varphi \circ \alpha \circ \varphi^{-1} : X \longrightarrow Y$. Allora se α e $\alpha^{'} \in S(X)$ abbiamo che $\Phi(\alpha)\Phi(\alpha^{'}) = (\varphi \circ \alpha \circ \varphi^{-1}) \circ (\varphi \circ \alpha^{'} \circ \varphi^{-1}) = \varphi \circ \alpha \circ \alpha^{'} \circ \varphi^{-1} = \varphi \circ (\alpha\alpha^{'}) \circ \varphi^{-1} = \Phi(\alpha\alpha^{'})$, e quindi Φ è un morfismo. Inoltre Φ è biettiva con inversa $\Psi : S(Y) \longrightarrow S(X)$ data da $\Psi(\beta) = \varphi^{-1} \circ \beta \circ \varphi$. In particolare, come già detto, se X è un insieme finito con n elementi allora S(X) è isomorfo a S_n.

Consideriamo ora due interi m, n con $n \geq m$. Allora
$\underline{m} = \{1, \ldots, m\} \subset \underline{n} = \{1, \ldots, n\}$. Consideriamo la funzione
$f : S(\underline{m}) = S_m \longrightarrow S_n = S(\underline{n})$, che manda α nella permutazione $f(\alpha)$ definita così: $f(\alpha)(i) = \alpha(i)$, se $i \leq m$, $f(\alpha)(i) = i$ se $i \geq m + 1$. Si vede facilmente che f è un morfismo iniettivo e dunque induce un *isomorfismo* tra S_m e un sottogruppo di S_n, precisamente il sottogruppo delle permutazioni $\beta \in S_n$ tali che $\beta(i) = i$ se $i \geq m + 1$.

Ricordiamo il teorema fondamentale di omomorfismo per gruppi:

Teorema 2.0.26. *Sia $f : G \longrightarrow H$ un morfismo di gruppi. Allora esiste un morfismo $F : G/Ker(f) \longrightarrow f(G)$ con $F([x]) = f(x) \in f(G)$.*

Per la dimostrazione si veda [2] , teorema 8.7.9 .

Corollario 2.0.27. *Se $f : G \longrightarrow H$ è un morfismo di gruppi e G è finito allora:*
$|G| = |Ker(f)||f(G)|$.

Per la dimostrazione si veda [2] , corollario 8.7.10 .

Osservazione 9. Si consideri il gruppo simmetrico S_4, gli elementi di S_4 con successione caratteristica 2,2 (ovvero i prodotti di due trasposizioni disgiunte): $(12)(34), (13)(24), (14)(23)$, e sia $V = \{id, (12)(34), (13)(24), (14)(23)\}$. V è chiamato *Gruppo di Klein* ed ha le seguenti proprietà:

(a) V è un sottogruppo di S_4.

(b) V è normale in S_4, quindi V è sottogruppo normale in A_4.

(c) V è isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$, quindi V è il più piccolo gruppo non ciclico ed è abeliano.

(d) Il gruppo quoziente S_4/V è isomorfo a S_3.

Dimostrazione. (a) L'identità sta in V e si vede facilmente che il prodotto di due elementi qualsiasi di V e l'inverso di un elemento di V sono ancora elementi di V.

(b) Per il teorema 2.0.13 tutte e sole le permutazioni coniugate in S_4 di una permutazione di successione caratteristica 2,2 hanno successione caratteristica 2,2 e dunque stanno ancora in V. Quindi, $\forall\ \sigma \in S_4\ \sigma V \sigma^{-1} = V$, cioè V è normale in S_4. Poichè $V \subset A_4$, perchè i suoi elementi sono tutti pari, V è normale anche nel sottogruppo A_4 di S_4.

(c) V è un gruppo di ordine 4, ma non è isomorfo a $\mathbb{Z}_4$ perchè non è ciclico, in quanto gli elementi di V diversi dall'identità hanno tutti ordine 2. È facile stabilire un isomorfismo di gruppi $V \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$. Infatti la tavola di moltiplicazione di V è la seguente:

$\cdot$	1	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
1	1	(1 2)(3 4)	(1 3)(2 4)	(1 4)(2 3)
(1 2)(3 4)	(1 2)(3 4)	1	(1 4)(2 3)	(1 3)(2 4)
(1 3)(2 4)	(1 3)(2 4)	(1 4)(2 3)	1	(1 2)(3 4)
(1 4)(2 3)	(1 4)(2 3)	(1 3)(2 4)	(1 2)(3 4)	1

mentre quella di $\mathbb{Z}_2 \times \mathbb{Z}_2$:

+	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

(d) Poniamo $\alpha_1 = (12)\,(34)$, $\alpha_2 = (13)\,(24)$ e $\alpha_3 = (14)\,(23)$. Si consideri $X = V - id = \{\alpha_1, \alpha_2, \alpha_3\}$. Per dimostrare che S_4/V è isomorfo a S_3,basta dimostrare che esiste un morfismo suriettivo $\pi : S_4 \longrightarrow S(X)$ con nucleo V, perchè in questo caso per il teorema 2.0.26, S_4/V sarebbe isomorfo a $S(X) \cong S_3$. Si consideri $\sigma \in S_4$ e sia
$\pi(\sigma) : X \longrightarrow X$ tale che $\pi(\sigma)(x) = \sigma x \sigma^{-1}$, allora $\pi(\sigma)$ è una permutazione di X. Inoltre $\forall\, x \in X$, $\pi(\sigma\tau)(x) = (\sigma\tau)x(\sigma\tau)^{-1} = \sigma\tau x(\tau)^{-1}(\sigma)^{-1} = \pi(\sigma)(\tau x \tau^{-1}) = \pi(\sigma)(\pi(\tau)(x)) = (\pi(\sigma)\pi(\tau))(x)$, e quindi
$\pi(\sigma\tau) = \pi(\sigma)\pi(\tau)$, cioè π è un morfismo. Come abbiamo visto V è un gruppo abeliano, quindi se $\sigma \in V$, allora $\sigma x \sigma^{-1} = x$
per ogni $x \in X \subset V$. Di conseguenza $V \subset Ker(\pi)$. Se dimostriamo che π è suriettivo,per il corollario 2.0.27 si avrà $Ker(\pi) = V$.
Dimostriamo la suriettività: $\pi((12))\alpha_1 = (12)\alpha_1(12)^{-1} = \alpha_1$,
$(12)\alpha_2(12)^{-1} = \alpha_3$ e $(12)\alpha_3(12)^{-1} = \alpha_2$. Quindi $\pi((12)) \neq 1$
e $\pi((12))^2 = 1$. Allora $\pi((12))$ ha ordine 2 e quindi $\pi(S_4)$ ha ordine divisibile per 2. D'altra parte $(123)\alpha_1(123)^{-1} = \alpha_3$, $(123)\alpha_3(123)^{-1} = \alpha_2$ e $(123)\alpha_2(123)^{-1} = \alpha_1$, per cui $\pi((123))$ ha ordine 3. L'ordine di $\pi(S_4)$

dev'essere divisibile per 3, oltre che per 2, e quindi sarà divisibile per 6, dato che $\pi(S_4) \subset S(X)$ che ha ordine 6, ne segue che $\pi(S_4) = S(X)$.

□

Capitolo 3

Il gruppo delle isometrie del piano

Lo studio delle simmetrie rappresenta una delle più interessanti applicazioni della teoria dei gruppi. In questo capitolo riassumiamo brevemente i risultati di base sulle simmetrie del piano, rimandando il lettore a [4] per i dettagli ed alcune dimostrazioni. Tali risultati verranno utilizzati nel quarto capitolo.

Definizione 3.1. Sia P un piano. Si chiama *movimento rigido o isometria* un'applicazione del piano P in sè che conserva le distanze, cioè un'applicazione $m : P \longrightarrow P$ tale che dati due punti qualsiasi $p, q \in P$, la distanza tra p e q è uguale a quella tra $m(p), m(q)$.

L'insieme dei movimenti rigidi del piano, con l'operazione di composizione, forma un gruppo denotato con $(M, \circ)$.

Fissiamo un sistema di coordinate euclidee sul piano P, quindi un'origine O e una base ortonormale dello spazio vettoriale $\mathbb{R}^2$. Un punto x verrà identificato dalle sue coordinate (x_1, x_2). Si dimostra, (si veda per esempio [5]),

che un movimento rigido $m : P \longrightarrow P$ ha un'equazione del tipo:

$$m(x) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$$

dove $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ è una matrice ortogonale. Se $det(A) = 1$ si dice che m è un'isometria diretta, se $det(A) = -1$ si dice che m è un'isometria inversa.

Definizione 3.2. Sia F un sottoinsieme del piano P; diremo anche che F è una figura del piano. Si chiama *simmetria di F* un movimento rigido che porta F in sè. L'insieme delle simmetrie di F, con l'operazione di composizione, costituisce un gruppo che è un sottogruppo di M.

Teorema 3.0.28. *Ogni movimento rigido del piano $m : P \longrightarrow P$ è una delle seguenti applicazioni:*

- *una traslazione mediante un vettore a se m muove il piano parallelamente a sè stesso di un vettore a, cioè porta p in $p + a$, $\forall\ p \in P$.*
- *una Rotazione di un angolo θ intorno ad un punto.*
- *una Riflessione rispetto ad una retta l.*
- *una Glissoriflessione se m è dato dalla composizione di una riflessione rispetto ad una retta l e di una traslazione di un vettore a non nullo parallelo alla retta l.*

Per la dimostrazione si veda per esempio [4] , Teorema 2.2. del quinto capitolo.

Osservazione 10. La classificazione dei movimenti rigidi del piano usa la distinzione tra quelli che conservano l'orientazione, e quelli che non la conservano:

movimenti che conservono l'orientazione, cioè isometrie dirette:

Traslazioni

Rotazioni

movimenti che invertono l'orientazione, cioè isometrie inverse:

Riflessioni

Glissoriflessioni

Si osservi che la composizione di due rotazioni di angoli rispettivamente θ ed η intorno ad uno stesso punto è una rotazione di angolo $\theta + \eta$ intorno a quel punto, e che la composizione di due traslazioni mediante due vettori a, b è una traslazione mediante il vettore somma $a + b$. Si noti inoltre che una traslazione non lascia fisso alcun punto, tranne nel caso in cui sia una traslazione mediante il vettore nullo, ovvero l'identità, e così pure una glissoriflessione. Inoltre le rotazioni di un angolo $\neq 0$ lasciano fisso un solo punto, cioè il centro di rotazione, e le riflessioni rispetto ad una retta l lasciano fissi tutti i punti della retta l. Di conseguenza la composizione di due riflessioni intorno a due rette non parallele è una rotazione intorno al punto di intersezione p delle due rette e la composizione di due riflessioni rispetto a due rette parallele distinte è una traslazione mediante un vettore ortogonale alla rette. Infatti componendo due isometrie inverse si ha un'isometria diretta, e guardando gli eventuali punti fissi della composizione si riesce a concludere.

Osservazione 11. Per rendere più agevoli calcoli come questi, si possono scegliere alcuni movimenti come generatori del gruppo M. Si considerino i seguenti movimenti come generatori di M:

- Traslazione mediante un vettore a:

$$t_a(x) = x + a = \begin{bmatrix} x_1 + a_1 \\ x_2 + a_2 \end{bmatrix}$$

- Rotazione di angolo θ intorno all'origine:

$$\rho_\theta(x) = \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

- Riflessione intorno all'asse x_1:

$$r(x) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} x_1 \\ -x_2 \end{bmatrix}$$

Le rotazioni ρ_θ e le riflessioni r lasciano fissa l'origine, dunque sono operatori ortogonali su $\mathbb{R}^2$. Osserviamo intanto che gli operatori ortogonali con determinante 1, cioè le isometrie dirette che fissano l'origine, sono le rotazioni ρ_θ. Se μ è un'isometria inversa che fissa l'origine, cioè un operatore ortogonale con determinante -1, allora μr è diretta, quindi $\rho_\theta = \mu r$, da cui $\mu r^2 = \rho_\theta r$, cioè $\mu = \rho_\theta r$ dato che $r^2 = 1$ (con 1 denotiamo qui l'identità). Una traslazione non è un operatore lineare infatti non manda il vettore nullo in sè, a meno che non sia l'identità.
È facilmente verificabile che i movimenti sopra elencati generano tutti i movimenti rigidi del piano. Precisamente se m è un elemento di M allora:

$m = t_a\rho_\theta$ oppure $m = t_a\rho_\theta r$. $(*)$

per un qualche vettore a e per un qualche angolo θ (eventualmente anche nulli), a seconda che m sia diretta o inversa.

Un movimento rigido del piano è dato infatti dalla composizione di un operatore ortogonale e di una traslazione, cioè possiamo scrivere $m \in M$ in questo modo: $m = t_a m'$, con m' operatore ortogonale come già ricordato precedentemente. Quindi $m = t_a \rho_\theta$ oppure $m = t_a \rho_\theta r$ a seconda che sia diretta o inversa. Questa rappresentazione inoltre è unica: sia infatti per assurdo $m = t_a \rho_\theta r^i = t_b \rho_\eta r^j$, dove i e j sono 0 oppure 1. Poichè m conserva l'orientazione se $i = 0$ e l'inverte se $i = 1$, risulta necessariamente che $i = j$, e quindi, se necessario, per la legge di cancellazione posso eliminare r in entrambi i membri per ottenere $t_a \rho_\theta = t_b \rho_\eta$. Moltiplicando ora ambo i membri a sinistra per t_{-b} e a destra per $\rho_{-\theta}$, si ottiene $t_{a-b} = \rho_{\eta-\theta}$. Poichè una traslazione coincide con una rotazione solo nel caso in cui siano entrambe l' identità, si ha che $a = b$ e $\theta = \eta$.

Per fare i calcoli nel gruppo M si possono usare le forme $(*)$ insieme alle relazioni fondamentali che sussistono tra i generatori scelti. Tali relazioni sono:

$$t_a t_b = t_{a+b}, \quad \rho_\theta \rho_\eta = \rho_{\theta+\eta}, \quad rr = 1$$

$$\rho_\theta t_a = t_{a'} \rho_\theta, \text{ con } a' = \rho_\theta(a)$$

$$r t_a = t_{a'} r, \text{ con } a' = r(a)$$

$$r \rho_\theta = \rho_{-\theta} r$$

Osservazione 12. Esistono molti sottogruppi notevoli di M, ad esempio:

T, il gruppo delle traslazioni

O, il gruppo degli operatori ortogonali

Il gruppo O è costituito dai movimenti che lasciano fissa l'origine: le rotazioni intorno all'origine e le riflessioni rispetto a rette passanti per l'origine. Il gruppo delle traslazioni è isomorfo al gruppo additivo $(\mathbb{R}^2, +)$; infatti basta considerare la biezione $\mathbb{R}^2 \longrightarrow T$ che manda un vettore a nella traslazione t_a; questo è un isomorfismo perchè $t_a t_b = t_{a+b}$. Gli elementi di O sono operatori lineari, dunque se $O(2)$ è il gruppo della matrici ortogonali 2×2, associando a ciascun elemento la sua matrice corrispondente si ottiene un isomorfismo tra $O(2)$ e O.

Proposizione 3.0.29. *(1) Sia p un punto del piano. Denotiamo con $\rho_{\theta'}$ la rotazione intorno a p di un angolo θ e con r' la riflessione intorno alla retta passante per p e parallela all'asse x. Allora vale che:*
$\rho'_\theta = t_p \rho_\theta t_p^{-1}, \quad r' = t_p r t_p^{-1}$

(2) Il sottogruppo di M costituito dai movimenti che lasciano fisso il punto p è il sottogruppo coniugato di O:
$O' = t_p O t_p^{-1}$

Dimostrazione. Dimostriamo il punto (1). Per ottenere la rotazione ρ'_θ trasportiamo il punto p nell'origine, poi facciamo ruotare il piano intorno all'origine di un angolo θ e infine riportiamo l'origine in p:
$\rho'_\theta = t_p \rho_\theta t_{-p} = t_p \rho_\theta t_p^{-1}$. A partire dalla riflessione r, si ottiene in modo analogo r':
$r' = t_p r t_{-p} = t_p r t_p^{-1}$.

Dimostriamo (2). Ogni movimento che lascia fisso p ha la forma di $\rho_\theta^{'}$ oppure di $\rho_\theta^{'} r^{'}$ per la rappresentazione dei movimenti rigidi data nell'osservazione 11, dunque (2) segue da (1). □

Esiste un morfismo notevole $\varphi : M \longrightarrow O$, di nucleo T che si ottiene eliminando la traslazione dai prodotti nella forma $(*)$, cioè $\varphi(t_a \rho_\theta) = \rho_\theta$, $\varphi(t_a \rho_\theta r) = \rho_\theta r$.
Poichè T è il nucleo di un morfismo da M in O, T è un sottogruppo normale in M.

Proposizione 3.0.30. *Sia p un punto qualunque del piano e sia $\rho_\theta^{'}$ la rotazione intorno a p di un angolo θ. Allora $\varphi(\rho_\theta^{'}) = \rho_\theta$. Analogamente, se $r^{'}$ è la riflessione intorno alla retta per p e parallela all'asse x, allora $\varphi(r^{'}) = r$.*

Dimostrazione. Segue direttamente dal punto (1) della proposizione precedente perchè t_p appartiene al nucleo di φ. □

La proposizione può essere anche enunciata nel modo seguente:

Proposizione 3.0.31. *Il morfismo φ non dipende dalla scelta dell'origine.*

Capitolo 4

Sottogruppi finiti del gruppo delle isometrie del piano. Gruppi diedrali

In questo capitolo vogliamo studiare i sottogruppi finiti del gruppo M dei movimenti rigidi del piano. Utilizzeremo il seguente teorema:

Teorema 4.0.32. *(Teorema del punto fisso) Sia G un sottogruppo finito del gruppo M dei movimenti rigidi del piano. Allora esiste un punto p nel piano che è lasciato fisso da ogni elemento di G, cioè esiste un punto p tale che $g(p) = p$ per ogni $g \in G$.*

Dimostrazione. Sia s un punto del piano e sia $O(s) = \{s' \in P | \exists\, g \in G, s' = g(s)\}$ l'insieme dei punti che sono immagine di s rispetto ai vari movimenti del gruppo G. Tale insieme è l'orbita di s rispetto all'azione di G. L'elemento s sta nell'orbita, poichè 1 sta in G e $s = 1(s)$. Ogni elemento di G permuta l'orbita $O(s)$, cioè se $s' \in O(s)$ e $x \in G$, allora $x(s') \in O(s)$. Sia infatti $s' = g(s)$, con $g \in G$: essendo G un gruppo $xg \in G$, dunque, per definizione, $xg(s) = x(s') \in O(s)$. Sia $O(s) = \{s_1, s_2, \ldots, s_n\}$. Il punto fisso che cerchiamo è chiamato *centro di gravità dell'orbita* ed è definito da $p = \frac{s_1+s_2+\ldots+s_n}{n}$,

dove l'espressione al secondo membro è la somma tra vettori in un arbitrario sistema di coordinate nel piano.

Lemma 4.0.33. *Sia $S = \{s_1, s_2, \ldots, s_n\}$ un insieme finito di punti del piano, e sia $p = \frac{s_1+\ldots+s_n}{n}$ il suo centro di gravità. Sia m un movimento rigido, e sia $m(s_i) = s_i^{'}$ e $m(p) = p^{'}$. Allora $p^{'} = \frac{s_1^{'}+\ldots+s_n^{'}}{n}$, cioè i movimenti rigidi portano centri di gravità in centri di gravità.*

Per la dimostrazione si veda per esempio [4] , lemma 3.3 pagina 195.

Il centro di gravità dell'insieme S è un punto fisso rispetto all'azione di G: infatti un elemento arbitrario g_i di G permuta l'orbita $\{s_1, \ldots, s_n\}$ e per il lemma 4.0.33 manda il centro di gravità in sè. □

Osservazione 13. Questo teorema ci assicura che esiste un punto lasciato fisso da ogni elemento di G, e possiamo scegliere le coordinate in modo che questo vada a coincidere con l'origine. Dunque G sarà un sottogruppo di O. Per descrivere i sottogruppi finiti G di M, basta quindi descrivere i sottogruppi finiti di O, o equivalentemente quelli del gruppo $O(2)$ delle matrici ortogonali 2×2.

Il seguente teorema descrive appunto i sottogruppi finiti di O.

Teorema 4.0.34. *Sia G un sottogruppo finito del gruppo O dei movimenti rigidi che lasciano fissa l'origine. Allora G è uno dei seguenti gruppi:*

(1) $G = C_n$, il gruppo ciclico di ordine n, generato dalla rotazione $\rho_{\frac{2\pi}{n}}$.

(2) $G = D_n$, il gruppo diedrale di ordine $2n$, generato dalla rotazione $\rho_{\frac{2\pi}{n}}$ e da una riflessione $r^{'}$ intorno a una retta per l'origine.

Dimostrazione. Sia G sia un sottogruppo finito di O. Poniamo $\theta = \frac{2\pi}{n}$. Poichè gli elementi di O sono le rotazioni ρ_θ e le riflessioni $\rho_\theta r$, possono verificarsi due casi:

1 Caso in cui tutti gli elementi di G siano rotazioni. Bisogna provare che G è ciclico. Se $G = \{1\}$, allora $G = C_1$; altrimenti G contiene una rotazione non banale ρ_θ. Sia θ il più piccolo angolo di rotazione positivo tra gli elementi di G, allora G è generato da ρ_θ. Sia infatti ρ_α un elemento arbitrario di G, dove l'angolo di rotazione α è rappresentato da un numero reale, come di solito. Sia $n\theta$ il più grande multiplo intero di θ, minore di α, cioè $\alpha = n\theta + \beta$, con $\beta \in [0, \theta)$. Poichè G è un gruppo e ρ_θ e $\rho_\alpha \in G$, anche $\rho_\beta = \rho_\alpha \rho_{-n\theta} \in G$; ma per ipotesi θ è il più piccolo angolo di rotazione positivo in G, quindi $\beta = 0$ e $\alpha = n\theta$. Questo dimostra che G è ciclico. Sia ora $n\theta$ il più piccolo multiplo di θ maggiore o uguale a 2π, $n\theta \in [2\pi, 2\pi + \theta)$. Poichè θ è il più piccolo angolo di rotazione positivo in G, allora si ha che $n\theta = 2\pi$. Dunque per qualche intero n, $\theta = \frac{2\pi}{n}$.

2 Caso in cui G contenga una riflessione. Supponiamo che la riflessione standard r appartenga a G (altrimenti possiamo sempre attuare un cambiamento di coordinate opportuno). Indicando con R il sottogruppo delle rotazioni in G, possiamo applicare al gruppo R quanto dimostrato nel primo caso, per concludere che R è ciclico: $R = C_n$. I $2n$ prodotti ρ_θ^i, $\rho_\theta^i r$, con $0 \leq i \leq n-1$, appartengono a G, dunque G contiene il gruppo diedrale D_n. Devo mostrare che $G = D_n$. Se un elemento g di G è una rotazione, allora $g \in R$ per definizione di R; dunque g è un elemento di D_n. Se invece g è una riflessione, allora g può essere scritto nella forma $\rho_\alpha r$ per qualche rotazione ρ_α. Poichè r è

un elemento di G, lo sarà anche il prodotto $\rho_\alpha rr = \rho_\alpha$. Dunque ρ_α è una potenza di ρ_θ, e anche g appartiene a D_n, quindi $G = D_n$.

□

Osservazione 14. Come abbiamo visto nella dimostrazione precedente il gruppo diedrale D_n dipende dalla retta di riflessione, ma possiamo sempre scegliere le coordinate in modo che essa coincida con l'asse delle ascisse, in modo da far diventare r' la riflessione standard r.

Corollario 4.0.35. *Sia G un sottogruppo finito del gruppo dei movimenti rigidi del piano M. In un opportuno sistema di coordinate, G è uno dei gruppi C_n o D_n, rispettivamente generati da $\rho_{\frac{2\pi}{n}}$ e da $\rho_{\frac{2\pi}{n}}$ ed r.*

Dimostrazione. La dimostrazione segue dal teorema precedente e da quello del punto fisso. □

Osservazione 15. Dal teorema precedente, per $n \geq 3$ segue che il gruppo diedrale D_n è il gruppo delle simmetrie di un poligono regolare di n lati. Questo infatti ha un gruppo di simmetria che contiene la rotazione di $\frac{2\pi}{n}$ intorno al suo centro e alcune riflessioni. Il teorema precedente ci assicura che questo gruppo è proprio D_n.

Esempio 4.1. Si consideri per esempio D_6, che è il gruppo delle simmetrie di un esagono regolare: oltre alle 6 riflessioni rispetto agli assi di simmetria della figura, il gruppo ha come elementi anche 6 rotazioni; l'ordine di D_6 è infatti 12.

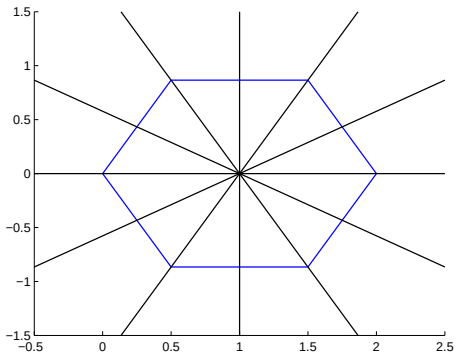

Figura 4.1: esagono

I gruppi diedrali D_1 e D_2 sono troppo piccoli per essere considerati,nel senso usuale, gruppi di simmetria di un poligono regolare di n lati: D_1 ha due elementi, è il gruppo $\{1,\ r\}$, quindi è ciclico come C_2, anche se l'elemento non banale del primo è una riflessione, del secondo invece una rotazione di π; D_1 è inoltre isomorfo a $\mathbb{Z}_2$. Il gruppo D_2 invece contiene quattro elementi, è il gruppo $\{1,\ \rho_\pi,\ r,\ \rho_\pi\, r\}$ ed è isomorfo al gruppo di Klein descritto nel secondo capitolo.

Proposizione 4.0.36. *Il gruppo diedrale D_n può essere descritto come il gruppo generato da due elementi x e y che soddisfano le relazioni:*

$$x^n = 1, \quad y^2 = 1, \quad yx = x^{-1}y.$$

Gli elementi di D_n sono:

$$\{1, x, x^2, \ldots, x^{n-1}, y, xy, x^2y, \ldots, x^{n-1}y\} = \{x^i y^j | 0 \leq i \leq n-1, 0 \leq j \leq 1\}.$$

Dimostrazione. Poniamo $\alpha = \frac{2\pi}{n}$. Gli elementi $x = \rho_\alpha$ e $y = r$ generano il gruppo D_n, per definizione. Le relazioni $y^2 = 1$ e $yx = x^{-1}y$ sono tra

le relazioni riportate nell'osservazione 11 del terzo capitolo riguardanti il gruppo M, esse sono: $rr = 1$ e $r\rho_\theta = \rho_{-\theta}r$. La relazione $x^n = 1$ segue dal fatto che $\alpha = \frac{2\pi}{n}$, che prova che anche gli elementi $1, x, \ldots, x^{n-1}$ sono distinti. Dunque anche $y, xy, x^2y, \ldots, x^{n-1}y$ sono distinti, e quindi poichè quest'ultimi sono riflessioni, mentre le potenze di x rotazioni, non ci sono ripetizioni nella lista $1, x, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y$. Infine le relazioni possono venire usate per ridurre un prodotto arbitrario di x, y, x^{-1}, y^{-1}, nella forma x^iy^j, con $0 \leq i \leq n-1$ e $0 \leq j \leq 1$. Dunque la lista contiene tutti gli elementi del gruppo generato da x e da y, e poichè questi generano D_n, la lista è completa. □

Osservazione 16. Considerando le prime due relazioni della proposizione precedente, la terza può essere scritta in funzione di queste due:
$yx = x^{n-1}y$ oppure $xyxy = 1$.

Proposizione 4.0.37. *Il gruppo diedrale D_3 è isomorfo al gruppo simmetrico S_3.*

Dimostrazione. Il gruppo $D_3 = \{1, x, x^2, y, xy, x^2y\}$ e la tavola di moltiplicazione è la seguente:

$\cdot$	1	x	x^2	y	xy	x^2y
1	1	x	x^2	y	xy	x^2y
x	x	x^2	1	xy	x^2y	y
x^2	x^2	1	x	x^2y	y	xy
y	y	x^2y	xy	1	x^2	x
xy	xy	y	x^2y	x	1	x^2
x^2y	x^2y	xy	y	x^2	x	1

Confrontandola con la tavola di moltiplicazione di S_3 (vedi primo capitolo), si conclude che i gruppi sono isomorfi, con un isomorfismo $\varphi : S_3 \longrightarrow D_3$ tale che $\varphi((1\ 2\ 3)) = x$ e $\varphi((1\ 2)) = y$.

□

Osservazione 17. Per $n \geq 4$ il gruppo diedrale e il gruppo simmetrico non sono certo isomorfi in quanto D_n ha ordine $2n$, mentre S_n ha ordine $n!$.

Osservazione 18. Per $n \geq 3$ inoltre il gruppo diedrale D_n non è abeliano. Infatti in questo caso $x \neq x^{-1}$ perchè x ha ordine maggiore di 2, mentre $x = x^{-1}$ implica $x^2 = 1$, quindi la relazione $yx = x^{-1}y \neq xy$ ci dice che x e y non commutano.

Esempio 4.2. Analizziamo più da vicino il gruppo diedrale D_4. Ricordiamo che $D_4 = \langle x, y \rangle$ con le relazioni $x^4 = y^4 = 1$, $yx = x^3y$. La tavola di moltiplicazione di D_4 è la seguente:

$\cdot$	1	x	x^2	x^3	y	xy	x^2y	x^3y
1	1	x	x^2	x^3	y	xy	x^2y	x^3y
x	x	x^2	x^3	1	xy	x^2y	x^3y	y
x^2	x^2	x^3	1	x	x^2y	x^3y	y	xy
x^3	x^3	1	x	x^2	x^3y	y	xy	x^2y
y	y	x^3y	x^2y	xy	1	x^3	x^2	x
xy	xy	y	x^3y	x^2y	x	1	x^3	x^2
x^2y	x^2y	xy	y	x^3y	x^2	x	1	x^3
x^3y	x^3y	x^2y	xy	y	x^3	x^2	x	1

Descriviamo tutti gli elementi di D_4: come sappiamo x è la rotazione di angolo $\frac{\pi}{2}$ in senso antiorario, quindi x^2 è una rotazione di angolo π, che manda un punto (a, b) in $(-a, -b)$, mentre x^3 è una rotazione di angolo $\frac{3\pi}{2}$ in senso antiorario, o di un angolo $\frac{\pi}{2}$ in senso orario. Per come è stata definita y è una riflessione rispetto all'asse delle ascisse; inoltre xy è una riflessione lungo la bisettrice del primo quadrante, x^2y lungo l'asse delle ordinate e infine x^3y è una riflessione lungo la bisettrice del secondo quadrante.

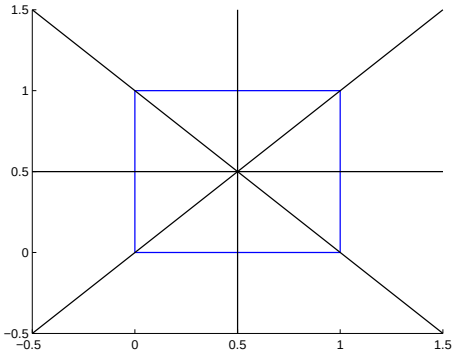

Figura 4.2: quadrato

Quindi D_4, come ci aspettavamo, è il gruppo delle simmetrie del quadrato.

Bibliografia

[1] M.Idà, *Appunti di Algebra 1 e di Algebra 2*, Bologna, 2008/2009 e 2009/2010.

[2] A.Vistoli, *Note di Algebra*, Bologna, 1993/1994.

[3] P.M.Cohn *Algebra*, John Wiley and sons, London, 1974.

[4] M.Artin, *Algebra*, Bollati Boringhieri, Torino, 1997.

[5] E.Sernesi, *Geometria 1*, Bollati Boringhieri, Torino, 1989.