ALMA MATER STUDIORUM
UNIVERSITÀ DEGLI STUDI DI BOLOGNA

Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Matematica

IL GRUPPO SIMMETRICO S_n

Elaborato in Algebra

Tesi di Laurea di:

MARTINA BONANZI

Relatore:

Prof.
LIBERO VERARDI

SESSIONE I
ANNO ACCADEMICO 2012-2013

Indice

Introduzione

Nella prima parte di questo studio (capitoli 1 e 2) sono raccolte in modo sintetico le nozioni di base riguardati il gruppo simmetrico S_n.
Particolare attenzione è rivolta alla rappresentazione di un ciclo come prodotto di trasposizioni, al significato di *cicli disgiunti* e su come ogni elemento di S_n, detto *permutazione*, possa essere scritto in modo univoco come prodotto di tali cicli disgiunti e quindi come prodotto di trasposizioni. Da ciò deriva che l'ordine di una permutazione è il minimo comune multiplo delle lunghezze dei cicli che intervengono in questa rappresentazione.
Tali lunghezze sono valori interi ($\geqslant 2$) e definiscono, permutando adeguatamente i cicli che compaiono nella fattorizzazione, la *sucessione caratteristica* della permutazione, da cui dipende la *classe di coniugio*. Si dimostra, infatti, che due permutazioni sono coniugate se e solo se esse hanno la stessa successione caratteristica.
Sempre nel corso del primo capitolo sono presentati esempi di classi di coniugio ed è indicata una formula tramite la quale si ottiene il numero dei coniugati di una permutazione data.
Nel secondo capitolo viene studiato un particolare sottogruppo normale di S_n, il *gruppo alterno* su n elementi A_n, ovvero il sottogruppo delle permutazioni pari. Viene dimostrato che esso, per $n > 4$ è semplice, ovvero non banale e senza sottogruppi normali propri.
E' inoltre riportato un importante risultato, relativo al fatto che S_n per $n \geqslant 3$ non è risolubile: esso ha come sottogruppi normali, oltre a quelli banali, il rispettivo gruppo alterno A_n, con la sola eccezione del caso $n = 4$ in cui compare anche il sottogruppo di Klein (un gruppo di 4 elementi isomorfo a $\mathbb{Z}_2 \times \mathbb{Z}_2$).
In questa prima parte, infine, vengono studiati i centri di S_n ed A_n dimostrando che, per quest'ultimo, nel caso $n > 3$, il centro è banale.
La seconda parte della tesi (terzo capitolo) è finalizzata alla descrizione dei p-sottogruppi di Sylow di S_n. E' innanzi tutto citato il teorema di Sylow, la cui dimostrazione è stata omessa tanto per la sua complessità quanto perché non particolarmente utile al nostro fine. Di seguito ad esso è presentata la

definizione di *prodotto semidiretto* di due gruppi. Quest'ultima risulta infatti indispensabile per descrivere il *prodotto intrecciato* fra gruppi, applicazione che interviene nella definizione dei p-sottogruppi di Sylow. Entrando sempre più nello specifico di questo argomento, viene effettuato lo studio dell'ordine dei p-sottogruppi di Sylow di S_n sia nel caso particolare in cui $n = p^m$ sia in quello più generale di un n qualsiasi.
Sempre nei seguenti due casi si è cercato gradualmente di determinare la vera e propria struttura di tali sottogruppi di S_n fino ad arrivare all'esposizione di un teorema che, ad esempio, nel primo caso particolare con $n = p^m$, afferma che un p-sottogruppo di Sylow di S_n è isomorfo ad un prodotto intrecciato di m sottogruppi ciclici di ordine p.
Al fine di acquisire una maggiore comprensione degli argomenti studiati sono infine presentati due esempi relativi a questo argomento. Nel primo sono descritti tutti i possibili p-sottogruppi e p-sottogruppi di Sylow di S_4, mentre nel secondo è presente una tabella in cui sono riportati gli ordini dei 2-sottogruppi di Sylow di S_n nel caso in cui n risulti essere potenza di 2.

Capitolo 1

Nozioni base sul gruppo simmetrico di ordine n

Sia X un insieme qualsiasi finito e non vuoto costituito da n elementi. Indicato con $I_n = \{i \in \mathbb{N} \mid 1 \leq i \leq n\}$, per semplicità si facciano coincidere gli n elementi di X esattamente con gli n oggetti di I_n.
Si dice *permutazione su* X una biezione α di X in sé. L'insieme delle permutazioni su X con l'operazione di composizione è un gruppo[1], detto *gruppo simmetrico di ordine* n e viene denotato con S_n.
La scrittura consueta per rappresentare una permutazione $\alpha \in S_n$ è la seguente:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha(1) & \alpha(2) & \alpha(3) & \dots & \alpha(n) \end{pmatrix} \tag{1.1}$$

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

Siano $\alpha, \beta \in S_n$, per eseguire la combinazione di esse, ovvero $(\alpha \circ \beta)(i) = \alpha(\beta(i))$, si procede come nell' esempio seguente.

Esempio 1.1. *In* S_3 *siano* $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ *e* $\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ *; allora si ha:* $(\beta \circ \alpha) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

[1]Un gruppo è una struttura algebrica del tipo $(G,\star)$ con G insieme non vuoto detto *sostegno*, $\star$ operazione associativa, dotato di elemento neutro per $\star$ e con la proprietà che ogni elemento di G possiede il simmetrico.

Dal fatto che $(S_n, \circ)$ è un gruppo scaturisce naturalmente che ogni permutazione $\alpha \in S_n$ ammette inversa, denotata con α^{-1}, e ottenuta come segue.

Esempio 1.2. *In S_3 sia* $\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

Per ottenere α^{-1} basta capovolgerla e riordinare le colonne:

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix} \longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \alpha^{-1}.$$

Teorema 1.3. *Il gruppo simmetrico S_n ha cardinalità n!*

Dimostrazione. Sia $X = \{1, 2, \ldots, n\}$. Si vuole dimostrare che il numero di permutazioni su n oggetti, ovvero il numero di biezioni su X, è pari al fattoriale di n.
Un'idea di dimostrazione consiste nel considerare l'applicazione
$f : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$ biettiva. Si hanno a disposizione n scelte per $f(1)$; restano $n-1$ scelte per $f(2)$; $n-2$ per $f(3)$ ... Procedendo in tale maniera in totale si hanno $(n)(n-1)(n-2)\ldots(1) = n!$ possibili biezioni. □

Teorema 1.4. *Il gruppo S_n per $n \geqslant 3$ non è abeliano*

Dimostrazione. Sia $X = \{1, 2, 3, \ldots, x, \ldots\}$ con x un generico elemento > 3.

Sia $\alpha = \begin{pmatrix} 1 & 2 & 3 & \ldots & x & \ldots \\ 1 & 3 & 2 & \ldots & x & \ldots \end{pmatrix}$, $\beta = \begin{pmatrix} 1 & 2 & 3 & \ldots & x & \ldots \\ 2 & 1 & 3 & \ldots & x & \ldots \end{pmatrix}$.

Si ottiene $(\beta \circ \alpha) = \begin{pmatrix} 1 & 2 & 3 & \ldots & x & \ldots \\ 2 & 3 & 1 & \ldots & x & \ldots \end{pmatrix}$, $(\alpha \circ \beta) = \begin{pmatrix} 1 & 2 & 3 & \ldots & x & \ldots \\ 3 & 1 & 2 & \ldots & x & \ldots \end{pmatrix}$.

Si ha quindi che $\alpha \circ \beta \neq \beta \circ \alpha$. Risulta quindi che S_n non è abeliano per $n \geqslant 3$. □

Definizione 1.5. *Data una permutazione $\alpha \in S_n$, diremo che α opera sugli oggetti $i_1, i_2, \ldots, i_k$ $(k \leq n)$ di X se lascia fermo ogni oggetto di X diverso da $i_1, i_2, \ldots, i_k$.*
Indichiamo con $F(\alpha) = \{i_h \in X | \alpha(i_h) = i_h\}$ l'insieme degli elementi fissi di una permutazione.

Definizione 1.6. *Due permutazioni α e β si definiscono disgiunte se gli oggetti che non sono fissi per una permutazione sono fissi per l'altra, ovvero se:*
$(X \setminus F(\alpha)) \cap (X \setminus F(\beta)) = \oslash$.

Esempio 1.7. *In* S_5, $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 4 & 7 & 5 & 6 & 1 & 8 \end{pmatrix}$ *e* $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 3 & 4 & 5 & 6 & 2 & 8 \end{pmatrix}$
sono disgiunte, infatti $\{1,3,4,7\} \cap \{2,8\} = \oslash$.

Definizione 1.8. *Sia r un intero positivo, $2 \leq r \leq n$ e siano dati r elementi distinti $i_1, i_2, \ldots, i_r \in X = \{1, 2, \ldots, n\}$. Col simbolo $\gamma = \begin{pmatrix} i_1 & i_2 & \ldots & i_r \end{pmatrix}$ si denoti la permutazione $\gamma \in S_n$ tale che:*

1. $\gamma(i_k) = i_k$ *se* $i_k \notin \{i_1, i_2, \ldots, i_r\}$
2. $\gamma(i_k) = i_{k+1}$ *se* $1 \leq k \leq r-1$
3. $\gamma(i_r) = i_1$

Tale permutazione è detta ciclo di lunghezza r.
Se il ciclo ha lunghezza 2 viene detto trasposizione o scambio.

In base a quanto detto, il ciclo γ, di lunghezza r, risulta essere:

$$\gamma = \begin{pmatrix} i_1 & i_2 & \ldots & i_h & \ldots & i_r & \ldots & x & \ldots \\ i_2 & i_3 & \ldots & i_{h+1} & \ldots & i_1 & \ldots & x & \ldots \end{pmatrix} \tag{1.2}$$

ovvero muove gli r elementi dell'insieme $\{i_1, i_2, \ldots, i_r\}$
e fissa quelli di $X \setminus \{i_1, i_2, \ldots, i_r\}$ che sono esattamente $n - r$.

Inoltre si può facilmente dimostrare che $o(\gamma) =\mid \gamma \mid = r$.
Ovvero ordine[2] e lunghezza per un ciclo coincidono.

[2]Dato il gruppo $(G, \star)$, dicesi ordine di un elemento $a \in G$, $o(a) =\mid a \mid$, il minimo intero positivo non nullo n, se esiste, tale che $a^n = 1_G$. Altrimenti, se tale intero non esiste, si dirà che a ha ordine infinito.

Infatti $\forall\ 1 \leq k \leq r-1$ si ha $\gamma^k(i_1) = i_{k+1}$ quindi $\gamma^k \neq id$.
Ma $\gamma^r(i_1) = \gamma(\gamma^{r-1}(i_1)) = \gamma(i_r) = i_1$.
Analogamente $\gamma^r(i_2) = \gamma^r(\gamma(i_1)) = \gamma(\gamma^r(i_1)) = \gamma(i_1) = i_2$.
Procedendo iterativamente anche per $i_3, i_4, \ldots, i_r$ e si ottiene che $\gamma^r = id$, ovvero che $o(\gamma) = r$.

Osservazione: Dalla definizione discende che un r-ciclo $\gamma = \begin{pmatrix} i_1 & i_2 & \ldots & i_r \end{pmatrix}$ può essere ciclicamente permutato senza che subisca cambiamenti, si può cioè scrivere: $\gamma = \begin{pmatrix} i_1 & i_2 & \ldots & i_r \end{pmatrix} = \begin{pmatrix} i_2 & i_3 & \ldots & i_r & i_1 \end{pmatrix} = \cdots = \begin{pmatrix} i_r & i_1 & \ldots & i_{r-1} \end{pmatrix}$.
Ci si può accordare e cominciare a scrivere un ciclo dall'oggetto più piccolo tra quelli spostati ($i_1 \leq i_l$ per $l = 2, 3, \ldots, r$) in modo da avere l'unicità della rappresentazione.

E' quindi immediata la comprensione del teorema.

Teorema 1.9. *Sia $\gamma = \begin{pmatrix} i_1 & i_2 & \ldots & i_r \end{pmatrix}$ ciclo di S_n. Sapendo che $o(\gamma) = r$, si ha:*
$\gamma^0(i_1) = i_1 = id(i_1)$, $\gamma(i_1) = i_2$, $\ldots$, $\gamma^{r-1}(i_1) = i_r$
$\gamma^r(i_1) = \gamma^0(i_1) = i_1$.
Ogni ciclo può essere scritto dunque nella forma : $\gamma = \begin{pmatrix} \gamma^0(i_1) & \gamma(i_1) & \ldots & \gamma^{r-1}(i_1) \end{pmatrix}$.

I cicli hanno un ruolo fondamentale nel gruppo simmetrico, molto simile a quello che hanno i numeri primi in $\mathbb{N}$. Si vedrà infatti che essi *generano* tale gruppo. Prima di analizzare dettagliatamente tale proprietà, risulta utile citare i seguenti risultati.

Teorema 1.10. *Siano $\alpha,\ \beta \in S_n$ disgiunte, allora $(\alpha \circ \beta)(i) = (\beta \circ \alpha)(i)$.*
(Equivalentemente $(\alpha\beta)(i) = (\beta\alpha)(i)$)[3]

Dimostrazione. Si vuole dimostrare che $\forall\ i \in \{1, 2, \ldots, n\}$ si ha $(\alpha \circ \beta)(i) = (\beta \circ \alpha)(i)$.

Esistono tre casi possibili.

[3] $(\alpha\beta)(i) = \beta(\alpha(i))$.

1. Se $\alpha(i) = i = \beta(i)$ allora

$$\begin{cases} (\alpha \circ \beta)(i) = \alpha(\beta(i)) = \alpha(i) = i \\ (\beta \circ \alpha)(i) = \beta(\alpha(i)) = \beta(i) = i \end{cases}$$

$\Longrightarrow (\alpha \circ \beta)(i) = (\beta \circ \alpha)(i)$.

2. $\alpha(i) = j \neq i$ allora β li fissa entrambi, essendo disgiunta da α, pertanto

$$\begin{cases} (\alpha \circ \beta)(i) = \alpha(\beta(i)) = \alpha(i) = j \\ (\beta \circ \alpha)(i) = \beta(\alpha(i)) = \beta(j) = j \end{cases}$$

$\Longrightarrow (\alpha \circ \beta)(i) = (\beta \circ \alpha)(i)$.

3. Se $\beta(i) = j \neq i$ allora α li fissa entrambi e si procede come sopra.

□

La validità di tale teorema persiste anche nel caso in cui α e β siano cicli disgiunti.

Esempio 1.11. *In* S_5 : $\begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 & 6 \end{pmatrix} = \begin{pmatrix} 3 & 4 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}$.

Analisi del gruppo simmetrico su 3 *elementi:* S_3

Il gruppo simmetrico S_3 ha cardinalità $3! = 6$, i suoi elementi risultano essere:

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$
$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Si devono calcolare $6^2 = 36$ prodotti per riempire quindi una tabella 6X6. Poiché id è l'elemento neutro, 11 di questi prodotti sono immediati.
Infatti per ogni α si ha $id \circ \alpha = \alpha$ oppure $\alpha \circ id = \alpha$. Restano quindi 25 prodotti da stimare. Anche i 5 elementi inversi sono immediati da determinare, di conseguenza rimangono 20 prodotti. Effettuando tutti i calcoli pazientemente si ottiene la seguente tabella:

$\circ$	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
id	id	ρ_1	ρ_2	τ_1	τ_2	τ_3
ρ_1	ρ_1	ρ_2	id	τ_3	τ_1	τ_2
ρ_2	ρ_2	id	ρ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	id	ρ_1	ρ_2
τ_2	τ_2	τ_3	τ_1	ρ_2	id	ρ_1
τ_3	τ_3	τ_1	τ_2	ρ_1	ρ_2	id

Da tale *Tavola di Cayley* si possono vedere direttamente alcune proprietà di S_3. Si può infatti immediatamente vedere che in ogni riga e in ogni colonna ogni elemento compare una sola volta, questo implica che è verificata la *Legge di cancellazione*[4]

[4]Sia $(G,\star)$ un gruppo e siano presi a, b, c, tre elementi qualsiasi di esso.
Se: $a \star b = a \star c \Longrightarrow b = c$ vale in G la Legge di cancellazione a sinistra.
Se $a \star b = c \star b \Longrightarrow a = c$ vale in G la Legge di cancellazione a destra.
Nel caso valgano contemporaneamente si dice che in G vale la Legge di cancellazione.
Ebbene, in ogni gruppo tale legge vale in ogni caso. Infatti:
$a \star b = a \star c \Longrightarrow a^{-1} \star (a \star b) = a^{-1} \star (a \star c) \Longrightarrow (a^{-1} \star a) \star b = (a^{-1} \star a) \star c \Longrightarrow$
$1_G \star b = 1_G \star c \Longrightarrow b = c$.
Analogamente dall'altro lato.

Ovviamente tale gruppo non risulta abeliano in quanto la tavola non è simmetrica rispetto alla diagonale che va da sinistra a destra e per quanto dimostrato in 1.4.

Sottogruppi di S_3 sono:

$A = \{id, \tau_3\}$, $B = \{id, \tau_1\}$, $C = \{id, \tau_2\}$, $D = \{id, \rho_1, \rho_2\}$.

1.1 L'importanza dei cicli in S_n

Teorema 1.12. *Ogni permutazione α, diversa dell'identità, in S_n o è un ciclo oppure può essere decomposta nel prodotto di un numero finito di cicli disgiunti. Tale fattorizzazione è unica a meno dell'ordine dei fattori.*

Dimostrazione. Sia $\alpha \in S_n$.
Se $n = 1, 2$ la tesi è ovvia in quanto α è l'identità oppure una trasposizione.
Sia $n \geq 3$. In tal caso si proceda per induzione su n.
Siano $j \in \{1, 2, \ldots, n\}$ il più piccolo fra gli oggetti spostati da α e m il più piccolo intero positivo tale che $\alpha^m(j) = j$.
Si hanno a questo punto due possibilità:

1. se $n = m$ è banale in quanto risulta che α è un ciclo di lunghezza $n = m$

2. se $m < n$ si consideri una nuova permutazione τ che mantenga fissi $j, \alpha(j), \alpha^2(j), \alpha^3(j), \ldots, \alpha^{m-1}(j)$ e tale che operi come α sui rimanenti $n - m$ elementi.
   Si può osservare che $\alpha = \begin{pmatrix} j & \alpha(j) & a(j) & \alpha^2(j) & \ldots & \alpha^{m-1}(j) \end{pmatrix} \tau$
   Essendo α e τ disgiunti per come sono stati definiti, risulta valida anche $\alpha = \tau \begin{pmatrix} j & \alpha(j) & a(j) & \alpha^2(j) & \ldots & \alpha^{m-1}(j) \end{pmatrix}$.
   Dal momento che τ opera su $n - m$ elementi posso applicare su essa l'ipotesi induttiva e scrivere τ come prodotto di cicli disgiunti. Risulta infine che la stessa α è prodotto di cicli disgiunti in quanto è data dal prodotto di τ con il ciclo $\begin{pmatrix} j & \alpha(j) & a(j) & \alpha^2(j) & \ldots & \alpha^{m-1}(j) \end{pmatrix}$, fra loro disgiunti.

Per provare ora l'unicità della fattorizzazione si consideri che in ogni fattorizzazione di α, poiché il più piccolo oggetto non fisso è j, si ha che il primo ciclo è $\begin{pmatrix} j & \alpha(j) & a(j) & \alpha^2(j) & \ldots & \alpha^{m-1}(j) \end{pmatrix}$.
Allora il prodotto degli altri deve dare τ. A questo punto, quindi, provare l'unicità della fattorizzazione di α equivale a provare l'unicità di τ, per il quale l'unicità della fattorizzazione vale per ipotesi induttiva.
Dal momento che si è di fronte ad un equazione del tipo $\alpha = (\ldots)\tau$ che risulta essere un caso particolare della generale $b = ax$ la quale, nei gruppi, ammette un'unica soluzione x, è banalmente dimostrata l'unicità di τ e quindi della fattorizzazione di α. □

Si riporta in seguito un esempio guidato per comprendere meglio i risultati espressi dal teorema.

Esempio 1.13. *In S_7.*

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

Il primo elemento spostato da α e l' 1. Si ha così:
$1 \longrightarrow 2 \longrightarrow 4 \longrightarrow 3 \longrightarrow 1$ *che fornisce il ciclo* $\gamma_1 = \begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$ *di lunghezza quattro.*

Successivamente, dopo gli elementi del ciclo γ_1, c'è l'elemento 5 che viene spostato:
$5 \longrightarrow 6 \longrightarrow 5$, *determinando il ciclo* $\gamma_2 = \begin{pmatrix} 5 & 6 \end{pmatrix}$ *lungo due.*

Il restante oggetto 7 è fissato da α e anche dai due cicli γ_1 e γ_2.

In conclusione si ottiene $\alpha = \gamma_1\gamma_2 = \gamma_2 \circ \gamma_1 = \gamma_1 \circ \gamma_2 = \gamma_2\gamma_1$.
Per ottenere l' unicità di rappresentazione scegliamo la prima, $\alpha = \gamma_1\gamma_2$, in cui il primo oggetto spostato da γ_1 è minore del primo oggetto spostato da γ_2.

Proviamo ora che

Teorema 1.14. *Se α è una permutazione di S_n tale che $\alpha = \gamma_1\gamma_2\gamma_3 \dots \gamma_r$, prodotto di cicli disgiunti, allora l'ordine di α uguaglia il minimo comune multiplo degli ordini di tutti i cicli che intervengono nella fattorizzazione.*
Ovvero: $| \alpha | = mcm(| \gamma_1 |, | \gamma_2 |, \dots, | \gamma_r |)$.

Dimostrazione. Sia $\alpha = \gamma_1\gamma_2\gamma_3 \dots \gamma_r$, $\alpha \neq id$.
Essendo $\gamma_1, \gamma_2, \gamma_3, \dots, \gamma_r$ tra loro permutabili, in quanto disgiunti, si ha:
$\alpha^m = \gamma_1^m\gamma_2^m \dots \gamma_r^m$, $\forall m \in \mathbb{Z}$
In particolare, se m è il minimo comune multiplo tra le lunghezze (quindi gli ordini) 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 $\gamma_1 = \begin{pmatrix} j_1 & j_2 & \dots & j_l \end{pmatrix}$. Allora α manda $\{j_1, j_2, \dots, j_l\}$ in se stesso e le restrizioni 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 $\gamma_1^k(j) = j \ \forall j \in I_n \setminus \{j_1, j_2, \dots, j_l\}$ si ha che $\gamma_1^k = id$ Quindi k deve essere divisibile per l'ordine di γ_1, $| \gamma_1 |$. Analogamente per gli altri cicli γ_i, con $i = 2, 3, \dots, r$, k è divisibile per $| \gamma_2 |, \dots, | \gamma_r |$. Quindi k deve essere divisibile per m. □

Lemma 1.15. *Ogni ciclo si scrive come prodotto di trasposizioni. Per esempio si ha:*
$\begin{pmatrix} i_1 & i_2 & \dots & i_m \end{pmatrix} = \begin{pmatrix} i_1 & i_m \end{pmatrix} \circ \begin{pmatrix} i_1 & i_{m-1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} i_1 & i_2 \end{pmatrix} = \begin{pmatrix} i_1 & i_2 \end{pmatrix} \dots \begin{pmatrix} i_1 & i_{m-1} \end{pmatrix} \begin{pmatrix} i_1 & i_m \end{pmatrix}$

Osservazione Un esempio banale di decomposizioni di un ciclo $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix} \in S_n$ in trasposizioni può essere: $\gamma = \begin{pmatrix} 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \end{pmatrix}$
Si osservi che è equivalente alla seguente scrittura:
$\gamma = \begin{pmatrix} 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 5 & 4 \end{pmatrix}$, dove la composizione delle ultime due è l'identità.
In conclusione il numero dei fattori non è univocamente determinato in tale fattorizzazione.

Proposizione 1.16. *Se $n > 2$, 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, ciascuno dei quali è a sua volta prodotto di trasposizioni. Quindi ogni permutazione non identica è prodotto di trasposizioni. Inoltre si ha che $id = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 2 & 1 \end{pmatrix}$ □

La rappresentazione di una permutazione come prodotto di cicli disgiunti e le proprietà dei cicli in S_n costituiscono quindi degli strumenti fondamentali per studiare le caratteristiche degli elementi di S_n e capire la natura di tale gruppo. Si è infatti appena visto come l'insieme dei cicli *generi* il gruppo simmetrico S_n nel senso che ogni elemento diverso dall'identità o è un ciclo o prodotto di essi.

Viene naturale quindi domandarsi quanti sono i cicli. La risposta non risulta complessa.
Infatti per $2 \leq k \leq n$ si comincia con lo scegliere $\{i_1, \dots, i_k\} \subseteq I_n$, e tale scelta può essere effettuata in
$C_{n,k} = \binom{a}{b} = \frac{n!}{k!(n-k)!}$ modi diversi.

Con quei k elementi, scelto come elemento iniziale di ogni ciclo il minore fra questi k oggetti, gli altri $k-1$ si possono disporre in $(k-1)!$ modi possibili.

A questo punto col principio di moltiplicazione otteniamo
$(k-1)!\frac{n!}{k!(n-k)!} = \frac{n!}{k(n-k)!} = \frac{D_{n,k}}{k}$ cicli di lunghezza k.

In tutto, sommando su k, ci sono $\sum_{k=2}^{n} \frac{D_{n,k}}{k}$ cicli.

Per 1.16 risulta che S_n è altresì *generato* dall'insieme delle trasposizioni. Queste ultime sono solamente $\binom{n}{2} = \frac{n(n-1)}{2}$.

Teorema 1.17. *Il gruppo simmetrico S_n, per $n \geq 3$, è generato da* $\{\begin{pmatrix}1 & 2 & \dots & n\end{pmatrix}, \begin{pmatrix}1 & 2\end{pmatrix}\}$.

Dimostrazione. E' sufficiente dimostrare che $\begin{pmatrix}1 & 2 & \dots & n\end{pmatrix}$ e $\begin{pmatrix}1 & 2\end{pmatrix}$ generano tutte le possibili trasposizioni. Segue un cenno della dimostrazione.
Siano $\tau = \begin{pmatrix}1 & n\end{pmatrix}, \gamma = \begin{pmatrix}1 & 2 & 3 & \dots & n\end{pmatrix}$.
Ne segue che $\gamma^{-1} = \begin{pmatrix}1 & n & n-1 & \dots & 2\end{pmatrix}$.

Si consideri $\gamma \circ \tau \circ \gamma^{-1} = \begin{pmatrix}1 & 2\end{pmatrix}$.
In seguito $\gamma^2 \circ \tau \circ \gamma^{-2} = \begin{pmatrix}1 & 3\end{pmatrix}$.
...
In fine $\gamma^{n-1} \circ \tau \circ \gamma^{1-n} = \begin{pmatrix}1 & n\end{pmatrix}$.

Con procedimenti simili si ottengono tutte le altre trasposizioni. Si è quindi dimostrato l'asserto. □

1.2 Coniugio in S_n

Definizione 1.18. *Sia $\alpha \in S_n$ e sia $\alpha = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_r$ la sua rappresentazione come prodotto di cicli disgiunti e sia $\mid \gamma_k \mid = m_k$, per $k = 1, 2, 3, \ldots, r$. Permutando adeguatamente i γ_k si può assumere $m_1 \geq m_2 \geq \cdots \geq m_k \geq 2$ e si ha $m_1 + m_2 + \cdots + m_r \leq n$.*
Si chiama successione caratteristica della permutazione la successione di interi $m_1, m_2, \ldots, m_r$. Tale successione è univocamente determinata da α.

Definizione 1.19. *Sia $(G,\star)$ un gruppo e sia a un elemento di G. Sappiamo dal corso di Algebra II che l'applicazione $f_a : G \longrightarrow G$ 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 $y = aza^{-1} = f_a(z)$.*

Si può banalmente verificare che l' *essere coniugati* è una relazione di equivalenza in G e in quanto tale determina delle classi di equivalenze dette *classi di coniugio* di questo tipo:
$[x] = \{y \in G \mid \exists a \in G \text{ tale che } y = axa^{-1}\}$.

Ora in dettaglio si studieranno le classi di coniugio in S_n.

Lemma 1.20. *Sia $\gamma = \begin{pmatrix} i_1 & \ldots & i_l \end{pmatrix}$ un ciclo in S_n di lunghezza l e sia $\rho \in S_n$. Allora $\rho\gamma\rho^{-1} = \begin{pmatrix} \rho(i_1) & \ldots & \rho(i_l) \end{pmatrix}$ ed è a sua volta un ciclo di lunghezza l.*

Dimostrazione. La dimostrazione è banale, basta calcolare e poi confrontare i valori assunti da $\rho\gamma\rho^{-1}$ con quelli del ciclo $\begin{pmatrix} \rho(i_1) & \ldots & \rho(i_l) \end{pmatrix}$, $\forall l \in I_n$. $\square$

Teorema 1.21. *Sia α una permutazione di S_n scritta come prodotto di cicli disgiunti, $\alpha = \gamma_1 \circ \ldots \circ \gamma_r$. Allora*

1. *Ogni permutazione $\beta = \tau\alpha\tau^{-1}$, coniugata di α, ha la stessa struttura ciclica, ovvero la stessa successione caratteristica. Inoltre, per quanto visto nel Lemma precedente, gli interi che compaiono nei cicli di β si ottengono applicando τ agli interi che compaiono nei cicli di α.*

2. *Se α e β hanno la stessa successione caratteristica allora sono coniugate.*

Dimostrazione.

1. Dimostriamo, come prima cosa, che due permutazioni coniugate α e β hanno la stessa successione caratteristica.
   Sia $\alpha \in S_n$, $\alpha \neq id$, $\alpha = \gamma_1 \circ \cdots \circ \gamma_r$ con $\mid \gamma_k \mid = l_k$, $\forall k = 1, 2, \ldots, r$.
   Sia $\tau \in S_n$ e consideriamo α e la sua permutazione coniugata
   $\beta = \tau\alpha\tau^{-1}$.
   Allora si ha che
   $\beta = \tau\alpha\tau^{-1} = \tau(\gamma_1 \ldots \gamma_r) = \tau\gamma_1(\tau^{-1}\tau)\gamma_2 \ldots (\tau^{-1}\tau)\gamma_r\tau^{-1} = (\tau\gamma_1\tau^{-1}) \ldots (\tau\gamma_r\tau^{-1})$.

   Inoltre i cicli $\tau\gamma_1\tau^{-1}$, $\ldots$, $\tau\gamma_r\tau^{-1}$ sono due a due disgiunti.

   Supponiamo infatti che $\tau\gamma_k\tau^{-1}$ e $\tau\gamma_h\tau^{-1}$, per $h \neq k$ non siano disgiunti.

   Poniamo $\gamma_k = \begin{pmatrix} i_1 & \ldots & i_l \end{pmatrix}$ e $\gamma_h = \begin{pmatrix} j_1 & \ldots & j_m \end{pmatrix}$. Per il Lemma precedente $(\tau\gamma_k\tau^{-1}) = \begin{pmatrix} \tau(i_1) & \ldots & \tau(i_l) \end{pmatrix}$ e $(\tau\gamma_h\tau^{-1}) = \begin{pmatrix} \tau(j_1) & \ldots & \tau(j_m) \end{pmatrix}$. Esisteranno un i_t e un j_s tali che $\tau(i_t) = \tau(j_s)$ per cui $i_t = j_s$ in quanto τ è biettiva. Ma allora γ_k e γ_h non sono disgiunti contrariamente all'ipotesi. Sempre il il Lemma precedente i cicli γ_k e $\tau\gamma_k\gamma^{-1}$ sono cicli della stessa lunghezza, dunque α e β hanno la stessa successione caratteristica.

2. Dimostriamo ora il viceversa, ovvero che due permutazioni con la stessa successione caratteristica sono coniugate. Siano α e β tale permutazioni. Possiamo scrivere $\alpha = \gamma_1 \ldots \gamma_r$ e $\beta = \rho_1 \ldots \rho_r$
   con $\gamma_1, \ldots, \gamma_r$ e $\rho_1, \ldots, \rho_r$ cicli disgiunti con $\mid \gamma_k \mid = \mid \rho_k \mid$,
   $\forall k = 1, 2, \ldots, r$.
   Poniamo $\gamma_k = \begin{pmatrix} i_1 & \ldots & i_l \end{pmatrix}$ e $\rho_k = \begin{pmatrix} j_1 & \ldots & j_l \end{pmatrix}$.
   Si consideri la biezione $\tau_k : \{i_1, \ldots, i_l\} \longrightarrow \{j_1, \ldots, j_l\}$ così definita:
   $\tau_k(i_s) = j_s$, $\forall s = 1, 2, \ldots, l$.

   Se A è l'insieme degli interi fra 1 e n che non compaiono nei γ_k e B l'insieme di quelli che non compaiono nei ρ_k, $\forall k$, allora A e B hanno la stessa cardinalità.
   Sia quindi $\sigma : A \longrightarrow B$ una corrispondenza biunivoca . Definiamo una permutazione $\tau : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$ nel seguente modo: $\tau(i) = \tau_k(i)$ se i compare in γ_k e $\tau(i) = \sigma(i)$ se i sta in A.
   Allora si ha che $\tau\gamma_k\tau^{-1} = \rho_k$, $\forall k = 1, 2, \ldots, r$. e quindi $\tau\alpha\tau^{-1} = \beta$.

□

Osservazione Le classi di coniugio sono tante quante sono le possibili strutture cicliche, quindi tante quante sono le possibili partizioni di un numero, naturalmente aggiungendo tanti 1 quanti sono i punti fissi.

Per esempio in S_5:

5=5	classe di $(1\ \ 2\ \ 3\ \ 4\ \ 5)$
5=4+1	classe di $(1\ \ 2\ \ 3\ \ 4)$
5=3+2	classe di $(1\ \ 2\ \ 3)\ (4\ \ 5)$
5=3+1+1	classe di $(1\ \ 2\ \ 3)$
5=2+2+1	classe di $(1\ \ 2)\ (3\ \ 4)$
5=2+1+1+1	classe di $(1\ \ 2)$
5=1+1+1+1+1	classe di id

Osservazione Data una permutazione $\alpha \in S_n$ quanti sono i coniugati di tale permutazione?

Se $\alpha = id$ ovviamente c'è un solo coniugato, α stessa.
Se $\alpha =$ ciclo di lunghezza k, i coniugati sono tutti i cicli di lunghezza k, ovvero sono esattamente $\frac{D_{n,k}}{k}$.

Ma se $\alpha = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_r$, con $\mid \gamma_i \mid = m_i$?
($m_1 \geq m_2 \geq \cdots \geq m_r, \quad m_1 + m_2 + \cdots + m_r + 1 + 1 + \cdots + 1 = n$
con tanti 1 quanti sono i punti fissi)
Esiste una formula.

Nella fattorizzazione di α come prodotto di cicli disgiunti, può capitare, ovviamente, che ci siano due o più cicli con la stessa lunghezza.
Si indichino quindi con $k_1, \ldots, k_s$ le lunghezze distinte dei cicli che compaiono nella fattorizzazione, con $k_1 > k_2 > \cdots > k_s \geq 1$, e siano $f_1, \ldots, f_s$ le loro frequenze, ovvero sia f_i il numero di cicli di lunghezza k_i.

La formula che indica il numero di coniugati di α risulta essere:

$$\frac{n!}{k_1^{f_1} \ldots k_s^{f_s} f_1! \ldots f_s!}$$

Per esempio in S_5:

5=5	$\frac{5!}{5^1 1!} = 24$
5=4+1	$\frac{5!}{4^1 1^1 1!1!} = 30$
5=3+2	$\frac{5!}{3^1 2^1 1!1!} = 20$
5=3+1+1	$\frac{5!}{3^1 1^2 1!2!} = 20$
5=2+2+1	$\frac{5!}{2^2 1^1 2!1!} = 15$
5=2+1+1+1	$\frac{5!}{2^1 1^3 1!3!} = 10$
5=1+1+1+1+1	$\frac{5!}{1^5 1!} = 1$

Totale: $24 + 30 + 20 + 20 + 15 + 10 + 1 = 120 =\mid S_5 \mid$.

Capitolo 2

Il gruppo alterno A_n

Nel capitolo precedente si è giunti ad affermare che ogni permutazione è prodotto di trasposizioni, ma si è anche sottolineato come tale fattorizzazione non sia unica. Fra tutte le possibili scomposizioni di una stessa permutazione, ad ogni modo, è presente un elemento costante. Qui di seguito si cerca di descriverlo in modo esaustivo.

E' innanzi tutto importante, per dimostrare poi alcuni risultati che seguono, osservare che ad ogni permutazione è possibile associare una matrice, detta appunto, *matrice di permutazione*.
Essa è una matrice che si ottiene scambiando alcune righe o colonne della matrice identità.

Data una permutazione $\alpha \in S_n$, $\alpha : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$, biettiva, la matrice di permutazione P_α con n elementi è definita come:

$$P_\alpha := \begin{bmatrix} e_{\alpha(1)} \\ e_{\alpha(2)} \\ \cdots \\ e_{\alpha(n)} \end{bmatrix}$$

dove e_i denota la i-esima riga della matrice identità $n \times n$.

Le matrici di permutazione sono matrici *binarie*, ovvero esse hanno esattamente un 1 in ogni riga e in ogni colonna e zeri altrove, dando quindi come somma di ogni riga o colonna esattamente 1.
Sono matrici non singolari, di conseguenza invertibili. Il loro determinante vale ± 1 ed esso è, come è spiegato più avanti, precisamente il *segno* della permutazione corrispondente.

Resta da precisare che valgono anche le seguenti due proprietà:

1. $P_\alpha^{-1} = P_{\alpha^{-1}}$ ($= P_\alpha^t$ dato che sono matrici ortogonali)
2. Date α e β due permutazioni su n oggetti vale $P_\alpha P_\beta = P_{\alpha\circ\beta}$

Lemma 2.1. *Ogni permutazione $\alpha \in S_n$ può essere scritta come prodotto di un numero sempre pari o sempre dispari di trasposizioni. In particolare se α è prodotto di un numero pari di trasposizioni, non è prodotto di un numero dispari di trasposizioni.*

Dimostrazione. Sia $\alpha = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_r$, prodotto di r trasposizioni. Ad essa può essere associata da una matrice di permutazione P_α il cui determinante è $(-1)^r$, ottenuta trovando dapprima le matrici di permutazioni associate ai vari τ_i e applicando poi la proprietà 2. vista poco sopra.

Sia ora $\alpha = t_1 \circ t_2 \circ \cdots \circ t_s$ un'altra fattorizzazione di α come prodotto di s trasposizioni.
Procedendo come prima di ottiene la matrice P_α, il cui determinante ora è $(-1)^s$.
Dato che il determinante è unico, deve essere $(-1)^s = (-1)^r \Rightarrow r \equiv s \ (mod 2)$. □

Definizione 2.2. *Si chiamino pari le permutazioni prodotto di un numero pari di trasposizioni, e dispari le altre.*

Proposizione 2.3. *Il prodotto di due permutazioni ambedue pari o ambedue dispari, è pari; il prodotto di una permutazione pari (dispari) per una permutazioni dispari (pari) è una permutazione dispari.*

Dimostrazione. Siamo α e β due permutazioni; sia α esprimibile come prodotto di m trasposizioni e β di n. Allora $\alpha \circ \beta$ è esprimibile come prodotto di $m+n$ trasposizioni, e pertanto, è pari se e solo se $m+n$ è pari, cioè se e solo se m e n sono entrambi pari o entrambi dispari, cioè se α e β sono entrambe pari o dispari. □

Per determinare se $\alpha \in S_n$ è pari o dispari dapprima la si scomponga in cicli disgiunti $\alpha = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_r$, con $r \geq 1$, $\mid \gamma_k \mid = m_k$, $1 \leq k \leq r$.

Si consideri $p(\alpha) = \sum_{k=1}^{r}(m_k - 1) = \sum_{k=1}^{r} m_k - r$.

Ne segue che la permutazione α è pari o dispari a seconda che il numero $p(\alpha)$ sia pari o dispari. Ovviamente $\alpha = id$ segue che $p(\alpha) = 0$ che, per definizione, è una permutazione pari.

Definizione 2.4. *Il segno di una permutazione $\alpha \in S_n$ è 1 se α è pari, e -1 se essa è dispari. Dunque se α è il prodotto di r trasposizioni allora il segno di α, $sgn(\alpha) = (-1)^r$.*

Osservazione Un k-ciclo di S_n è pari se e solo se k è dispari, viceversa è dispari se e solo se k è pari. (si veda il Lemma 1.15).
Banalmente si ha anche che il prodotto di n trasposizioni è una permutazione pari o dispari seconda che n sia un numero pari o dispari.

Proposizione 2.5. *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 e β hanno lo stesso segno $\alpha\beta$ è pari, altrimenti dispari.

Osservazione Presa una permutazione α in S_n ed una trasposizione β, comunque si moltiplichino queste due, il segno di α cambia. Ovvero $\alpha\beta$ è dispari se α è pari e viceversa.

Definizione 2.6. *L'insieme dato dalle permutazioni pari di S_n si denota con A_n ed è detto gruppo Alterno su n oggetti, perché, come mostreremo, è un sottogruppo di S_n.*

Osservazione Per n=3, A_3 contiene tre elementi, ovvero l'identità ed i cicli $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$, $\begin{pmatrix}1 & 3 & 2\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\end{pmatrix}^2$. Si tratta quindi di un gruppo abeliano ciclico[1].
Per $n \geq 4$ invece A_n non è abeliano. Si ha per esempio:
$\begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 4\end{pmatrix} = \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix} \neq \begin{pmatrix}1 & 2 & 3\end{pmatrix}\begin{pmatrix}1 & 2 & 3\end{pmatrix} = \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}$

Teorema 2.7. *Valgono i seguente risultati*

1. *A_n costituisce un sottogruppo di S_n*
2. *Il gruppo simmetrico S_n ha tante permutazioni pari quante dispari. Dunque $\mid A_n \mid = \frac{1}{2} \mid S_n \mid = \frac{n!}{2}$*
3. *Il gruppo alterno A_n è un sottogruppo normale in S_n*

Dimostrazione.

1. L'identità è pari, quindi $id \in A_n$. Date $\alpha, \beta \in A_n$, esistono trasposizioni τ_i e trasposizioni t_j, con $1 \leq i \leq 2h$ e $1 \leq j \leq 2k$, tali che:
   $\alpha = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2h}$
   $\beta = t_1 \circ t_2 \circ \cdots \circ t_{2k}$.
   Allora $\alpha \circ \beta = \tau_1 \circ \tau_2 \circ \cdots \circ \tau_{2h} \circ t_1 \circ t_2 \circ \cdots \circ t_{2k}$, quindi è prodotto di $2h + 2k$ trasposizioni, quindi è pari.
   Infine $\alpha^{-1} = \tau_{2h} \circ \tau_{2h-1} \circ \cdots \circ \tau_1$ è pari.
   Pertanto A_n è sottogruppo di S_n

2. Sia τ una permutazione dispari (per comodità una trasposizione ad esempio $\tau = (12)$.
   Allora, per la proposizione precedente, per ogni $\beta \in A_n$ si ha che $\beta \circ \tau$ è dispari in quanto prodotto di $2h + 1$ trasposizioni.
   Dunque ci sono almeno $\mid A_n \circ \tau \mid = \mid A_n \mid$ permutazioni dispari.
   D'altra parte, se β è una permutazione dispari, precisamente prodotto di $2k + 1$ trasposizioni, si ha che $\beta \circ \tau = \alpha$ è pari, in quanto prodotto di $2k + 2$ trasposizioni.
   Ne segue che $\beta = \alpha \circ \tau \in (A_n \circ \tau)$ quindi le permutazioni dispari appartengono tutte al laterale[2] $A_n \circ \tau = \{\alpha \circ \tau \mid \alpha \in A_n\}$.

[1] Un gruppo $(G, \star)$ si dice ciclico se esiste un elemento g di G, detto *generatore*, tale che G è l'insieme delle potenze di g ad esponente intero.

[2] Sia $(G,\star)$un gruppo e sia H un sottogruppo di G e $a \in G$.
Il *laterale destro di H in G rappresentato da a* è l'insieme $Ha = \{ha \mid h \in H\}$.
Il *laterale sinistro di H in G rappresentato da a* è l'insieme $aH = \{ah \mid h \in H\}$.

Pertanto tutti gli elementi al di fuori di A_n, ossia quelli di $S_n \backslash A_n$, costituiscono il laterale $A_n \circ \tau$
Allora: $n! = \mid S_n \mid = \mid A_n \mid + \mid S_n \backslash A_n \mid = 2 \mid A_n \mid \Rightarrow \mid A_n \mid = \frac{\mid S_n \mid}{2} = \frac{n!}{2}$.

3. Si deve dimostrare che A_n è sottogruppo normale[3] di S_n.
   Esattamente come sopra, anche il laterale sinistro $\tau \circ A_n$ è formato da tutte le permutazioni dispari, quindi $\tau \circ A_n = A_n \circ \tau$.
   Ne segue che dato A_n tutti i suoi (due) laterali destri coincidono con i corrispondenti laterali sinistri, pertanto $A_n \lhd S_n$

□

Osservazione Per quanto visto ora si sottolinea che $S_n \backslash A_n$, ossia l'insieme formato dalle permutazioni dispari non è un sottogruppo di S_n.

Un qualsiasi gruppo $(G, \star)$ contiene come sottogruppi normali quelli banali, ovvero il sottogruppo $\{id_G\}$ e se stesso. Se G è abeliano tutti i suoi sottogruppi sono normali, mentre se non lo è i sottogruppi normali sono molto rari.
Nel caso specifico del gruppo simmetrico S_n, per $n \geq 3$ non abeliano, esso ha come sottogruppi normali oltre a quelli banali il rispettivo gruppo alterno A_n e, con la sola eccezione del caso $n = 4$, questi sono gli unici sottogruppi normali.

Per $n = 4$ c'è anche il *sottogruppo di Klein* studiato qui di seguito.

Si consideri S_n con $n = 4$. $X = \{1, 2, 3, 4\}$. In esso ci sono sei cicli di lunghezza 2, otto di lunghezza 3, sei di lunghezza 4, dunque in tutto venti cicli su ventiquattro permutazioni. Le restanti quattro permutazioni formano il sottogruppo

$K = \{id, \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 4 \end{pmatrix} \begin{pmatrix} 2 & 3 \end{pmatrix}\}$
detto *sottogruppo di Klein di* S_4.

Tale sottogruppo è anche sottogruppo normale in S_4, ossia $\forall \beta \in S_4$ si ha $\beta \circ K = K \circ \beta$ dove $\beta \circ K = \{\beta \circ \alpha \mid \alpha \in K\}$, analogamente per $K \circ \beta$. Inoltre si può vedere anche che esso non è ciclico.

[3] Un sottogruppo H si un dato gruppo $(G, \star)$ è detto *normale* se i suoi laterali destri e sinistri coincidono.

S_4, oltre ad avere questo sottogruppo normale aggiuntivo, ha un ulteriore particolarità.

Lemma 2.8. *Per ogni divisore k di* $\mid S_4 \mid = 24$*, esiste un sottogruppo d'ordine k di* S_4*.*

Infatti:

k	sottogruppo
1	id
2	$\langle (1 \quad 2) \rangle$
3	$\langle (1 \quad 2 \quad 3) \rangle$
4	$\langle (1 \quad 2 \quad 3 \quad 4) \rangle$
6	$\{\alpha \in S_4 \mid \alpha(4) = 4\}$
8	D_4
12	A_4
24	S_4

Con D_4 il gruppo delle simmetrie del quadrato.[4]

Lemma 2.9. *Il risultato precedente non vale per* A_n*: esso infatti non possiede sottogruppi di ordine 6.*

Dimostrazione. Il gruppo alterno A_4 è formato dalle permutazioni pari di S_4, esso ha $\binom{n!}{2} = 12$ elementi.
Otto elementi di periodo 3:
$\{(1 \quad 2 \quad 3), (1 \quad 2 \quad 3), (1 \quad 3 \quad 3), (1 \quad 3 \quad 4), (1 \quad 4 \quad 3), (1 \quad 2 \quad 4), (1 \quad 4 \quad 3),$
$(2 \quad 3 \quad 4), (2 \quad 4 \quad 3)\}$.

Tre di periodo due $\{(1 \quad 2)(3 \quad 4), (1 \quad 3)(2 \quad 4), (1 \quad 4)(2 \quad 3)\}$.
Inoltre, ovviamente, A_4 contiene l'identità.
Vediamo come dovrebbe essere fatto un ipotetico sottogruppo H, $\mid H \mid = 6$.
Innanzi tutto osserviamo che il sottogruppo di Klein $K = \{id, (1 \quad 2)(3 \quad 4), (1 \quad 3)(2 \quad 4), (1 \quad 4)(2$
è l'unico sottogruppo di A_4 che ha ordine 4.

[4] Tale gruppo agisce sui 4 vertici permutandoli. Ha proprio 8 elementi perché è formato da 4 rotazioni sui vertici e da 4 riflessioni rispetto ai quattro assi dei quattro lati del quadrato.

Allora H sicuramente non conterrà K perché 4 non divide 6 per il teorema di Lagrange[5].
Perciò H avrà al più due elementi di ordine 2. In tal caso, perché H abbia 6 elementi, è necessario aggiungere altri 3 elementi e prenderli quindi fra quelli di ordine 3. Per ognuno di questi, però, portiamo nel gruppo anche il suo inverso, quindi non riusciamo a prenderne 3, che è numero dispari.

Notiamo che:
$\begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \begin{pmatrix}1 & 3 & 2\end{pmatrix}$ e
$\begin{pmatrix}1 & 3 & 4\end{pmatrix}^{-1} = \begin{pmatrix}1 & 4 & 3\end{pmatrix}$ e
$\begin{pmatrix}1 & 2 & 4\end{pmatrix}^{-1} = \begin{pmatrix}1 & 4 & 2\end{pmatrix}$ e
$\begin{pmatrix}2 & 3 & 4\end{pmatrix}^{-1} = \begin{pmatrix}2 & 4 & 3\end{pmatrix}$.

Cioè possiamo scrivere $A_4 = \{id, \begin{pmatrix}1 & 2\end{pmatrix}\begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}\begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}\begin{pmatrix}2 & 3\end{pmatrix}, \langle\begin{pmatrix}1 & 2 & 3\end{pmatrix}\rangle, \langle\begin{pmatrix}1 & 3 & 4\end{pmatrix}\rangle, \langle\begin{pmatrix}1 & 2 & 4\end{pmatrix}\rangle, \langle\begin{pmatrix}2 & 3 & 4\end{pmatrix}\rangle\}$.

(Ad ogni modo, se H avesse due elementi di ordine 2, avrebbe anche il terzo, in quanto esso è il loro prodotto, ed avremmo quindi K contenuto in H che è assurdo per quanto detto.)

A questo punto è evidente che l'unico modo per costruire H è prendere un solo elemento di ordine 2 e due elementi di ordine 3, ognuno con i suo inverso. Cioè si prenda $h \in A_4$ con $\mid h \mid = 2$ nel gruppo K e si prendano $\langle\alpha\rangle$, $\langle\beta\rangle$ fra $\langle\begin{pmatrix}1 & 2 & 3\end{pmatrix}\rangle, \langle\begin{pmatrix}1 & 3 & 4\end{pmatrix}\rangle, \langle\begin{pmatrix}1 & 2 & 4\end{pmatrix}\rangle, \langle\begin{pmatrix}2 & 3 & 4\end{pmatrix}\rangle$.

Basta fare pochi calcoli per vedere che $\langle\{\alpha, \beta\}\rangle = A_4$ e che $h \neq \alpha h \alpha^{-1}$.
Ma $h \in H$ e $\alpha h \alpha^{-1} \in H$ ed hanno entrambi periodo 2.
Questo è assurdo perché abbiamo detto che deve esserci al massimo un elemento di periodo 2.
Si è così provato che non esistono sottogruppi H si A_4 di ordine 6. □

Osservazione Dimostrando che A_4, gruppo di ordine 12, non ha sottogruppi di ordine 6, si è provato che, in generale, non è vero che ogni divisore dell'ordine di un gruppo è ordine di un sottogruppo.
Il teorema di Lagrange, quindi, non è totalmente invertibile in ogni gruppo finito.

[5] *Teorema di Lagrange* Se G è un gruppo e H un sottogruppo di G, allora l'ordine di H divide l'ordine di G. In particolare $\mid G \mid = \mid H \mid \mid\mid G : H \mid$.

2.1 Semplicità del gruppo alterno A_n

Definizione 2.10. *Un gruppo è semplice se non è banale e non ha sottogruppi normali propri.*

Si è finora illustrato come il gruppo alterno A_n sugli $n \geq 2$ oggetti $\{1, 2, \ldots, n\}$ abbia come insieme sostegno l'insieme delle $\frac{n!}{2}$ permutazioni pari e come esso sia un sottogruppo normale del gruppo simmetrico.
Per $n = 2$, A_n è ovviamente il gruppo banale.
Per $n = 3$ si ha che $\mid A_3 \mid = 3$, quindi A_3 è semplice abeliano.
A_4, dal momento che contiene il sottogruppo di Klein che è normale in S_4, non è semplice.
Nel seguito sarà provato che per $n > 4$ il gruppo A_n è semplice.

Si può invece, da quanto già studiato, affermare che, per $n \leq 2$, S_n ha al massimo due elementi quindi non ha sottogruppi propri. Il gruppo alterno su n oggetti, per $n \geqslant 2$, è sempre un sottogruppo normale di S_n e, in particolare, non banale per $n \geqslant 3$. Esso è infatti il solo sottogruppo normale non banale di S_n con l'unica eccezione per $n = 4$ dove c'è un ulteriore sottogruppo normale per S_4, ovvero il *sottogruppo di Klein*.
Riassumendo, per $n \neq 4$, i soli sottogruppi normali di S_n sono id, A_n ed S_n.

Lemma 2.11. *Per $n > 2$, A_n è generato da cicli di lunghezza 3.*

Dimostrazione. Ogni $\alpha \in A_n$ è ovviamente, per definizione, prodotto di un numero pari di trasposizioni, per cui, per provare la veridicità del lemma, basterà provare che ogni prodotto di due trasposizioni $\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} c & d \end{pmatrix}$ è prodotto di cicli di lunghezza tre (che a loro volta sono permutazioni pari).

Se $\begin{pmatrix} a & b \end{pmatrix} = \begin{pmatrix} c & d \end{pmatrix}$ allora $\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} c & d \end{pmatrix} = id$, e non c'è nulla da provare.

Se $a = c$, ma $b \neq d$, allora $\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} c & d \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} a & d \end{pmatrix} = \begin{pmatrix} a & d & b \end{pmatrix}$.

Infine, se i quattro oggetti sono tutti diversi, si ha:
$\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} c & d \end{pmatrix} = \begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} a & c \end{pmatrix}\begin{pmatrix} c & a \end{pmatrix}\begin{pmatrix} c & d \end{pmatrix} = \begin{pmatrix} a & c & b \end{pmatrix}\begin{pmatrix} c & d & a \end{pmatrix}$. □

Teorema 2.12. *Per ogni $n > 4$ il gruppo alterno A_n è semplice.*

Dimostrazione. Sia $N \lhd A_n$, $N \neq id$.
Poiché si vuole dimostrare che A_n è semplice, occorre fare vedere che N coincide con A_n, ovvero dimostrare che N contiene tutti i cicli di lunghezza 3, cioè contiene un insieme di generatori di A_n.
Innanzi tutto proviamo che N contiene almeno un ciclo di lunghezza 3.
Preso $\alpha \in N$, con $id \neq \alpha = \alpha_1 \circ \alpha_2 \circ \alpha_3 \circ \cdots \circ \alpha_m$ scomposto in cicli disgiunti per comodità con lunghezze non crescenti.

Supponiamo $\mid \alpha_1 \mid > 3$, $\alpha_1 = \begin{pmatrix} a & b & c & d & \dots & x \end{pmatrix}$.
Allora N, poiché contiene α, contiene anche la coniugata:

$$\alpha^* = \begin{pmatrix} a & b & c \end{pmatrix} \circ \alpha \circ \begin{pmatrix} c & b & a \end{pmatrix} = \begin{pmatrix} b & c & a & d & \dots & x \end{pmatrix} \circ \alpha_2 \circ \cdots \circ \alpha_m$$

per cui contiene anche $\begin{pmatrix} a & b & d \end{pmatrix} = \alpha^* \circ \alpha^{-1} \in N$.

Supponiamo ora $\mid \alpha_1 \mid = 3$, $\alpha_1 = \begin{pmatrix} a & b & c \end{pmatrix}$.
Se è l'unico ciclo di lunghezza 3, gli altri α_i sono trasposizioni, per cui $\alpha^2 = \alpha_1^2 = \begin{pmatrix} c & a & b \end{pmatrix} \in N$.
Se invece $\alpha_2 = \begin{pmatrix} d & e & f \end{pmatrix}$, si ha anche:

$$\alpha^* = \begin{pmatrix} c & d & e \end{pmatrix} \circ \alpha \circ \begin{pmatrix} e & d & c \end{pmatrix} = \begin{pmatrix} a & b & d \end{pmatrix} \circ \begin{pmatrix} e & c & f \end{pmatrix} \circ \alpha_3 \circ \cdots \circ \alpha_m \in N$$

per cui anche $\alpha^* \circ \alpha = \begin{pmatrix} a & b & c & d & e & f \end{pmatrix} \circ \alpha_3^2 \circ \alpha_4^2 \circ \cdots \circ \alpha_m^2 \in N$.
Siamo così nel caso precedente.

Supponiamo ora che ogni α_i sia una trasposizione.
Allora m è pari dal momento che, ricordiamo, $\alpha \in N \lhd A_n$.
Sia $m = 2$ e siano $\alpha_1 = \begin{pmatrix} a & b \end{pmatrix}$, $\alpha_2 = \begin{pmatrix} c & d \end{pmatrix}$.
Sia f un oggetto diverso da a, b, c, d, che esiste perché $n > 4$.
Allora N contiene anche $\alpha^* = \begin{pmatrix} a & b & f \end{pmatrix} \circ \alpha \circ \begin{pmatrix} f & b & a \end{pmatrix} = \begin{pmatrix} b & f \end{pmatrix} \circ \begin{pmatrix} c & d \end{pmatrix}$, quindi si ha anche $\begin{pmatrix} a & f & b \end{pmatrix} = \alpha^* \circ \alpha \in N$.

Sia infine $m \geq 4$ e siano $\alpha_3 = \begin{pmatrix} e & f \end{pmatrix}$, $\alpha_4 = \begin{pmatrix} g & h \end{pmatrix}$.
Allora N contiene anche

$$\begin{gathered} \alpha^* = \begin{pmatrix} d & e \end{pmatrix} \circ \begin{pmatrix} b & c \end{pmatrix} \circ \alpha \circ \begin{pmatrix} b & c \end{pmatrix} \circ \begin{pmatrix} d & e \end{pmatrix} = \\ \begin{pmatrix} a & c \end{pmatrix} \circ \begin{pmatrix} b & e \end{pmatrix} \circ \begin{pmatrix} d & f \end{pmatrix} \circ \begin{pmatrix} g & h \end{pmatrix} \circ \alpha_5 \circ \cdots \circ \alpha_m, \end{gathered}$$

e quindi anche $\alpha^* \circ \alpha = \begin{pmatrix} a & e & d \end{pmatrix} \circ \begin{pmatrix} c & f & b \end{pmatrix} \in N$, che ci riconduce ai casi precedenti.

E' stato così provato che in ogni caso N contiene almeno un ciclo di lunghezza 3 del tipo $\begin{pmatrix} a & b & c \end{pmatrix}$.

Ciò posto, si proverà ora che N contiene tutti i cicli di lunghezza 3.
Infatti, per ogni altri ciclo $\begin{pmatrix} a' & b' & c' \end{pmatrix}$, siano u, v oggetti diversi da a, b, c e siamo u', v' diversi da a', b', c'.
Delle due permutazioni

$$\begin{pmatrix} a & b & c & u & v & \dots & x & \dots \\ a' & b' & c' & u' & v' & \dots & y & \dots \end{pmatrix} \text{ e } \begin{pmatrix} a & b & c & u & v & \dots & x & \dots \\ a' & b' & c' & v' & u' & \dots & y & \dots \end{pmatrix},$$

una è pari e, detta τ tale permutazione, si ha

$$\begin{pmatrix} a' & b' & c' \end{pmatrix} = \tau \circ \begin{pmatrix} a & b & c \end{pmatrix} \circ \tau^{-1} \in N.$$

Il teorema è così provato.

□

Osservazione Il gruppo A_5 ha ordine $\dfrac{120}{2} = 60$, e, a parte i gruppi ciclici di ordine primo, è il più piccolo gruppo semplice.
Infatti si dimostra abbastanza facilmente che i gruppi di ordine non primo minore di 60 non sono semplici: i gruppi semplici, infatti, hanno ordine prodotto di almeno tre primi distinti (*Teorema di Burside*), e multiplo di 8 o di 12 (*Teorema di Burside e di Feit-Thompson*).
Inoltre, se G è semplice di ordine 60 è necessariamente isomorfo ad A_5, ma la dimostrazione non è elementare.

2.2 Il centro di A_n e di S_n

Definizione 2.13. *Dato un gruppo $(G, \star)$ il centro di G è il sottoinsieme di G così definito:*
$Z(G) = \{c \in G \mid g \star c = c \star g,\ \forall g \in G\}$.

Si tratta perciò degli elementi di G che commutano con tutti gli elementi di G. Se G è abeliano chiaramente $Z(G) = G$. Il centro è banalmente un sottogruppo abeliano di G ed inoltre è anche un sottogruppo normale di G.

Teorema 2.14. *Sia $n > 2$. Il centro di S_n, $Z(S_n)$, è banale.*

Dimostrazione. Sia $\sigma \in Z(S_n)$, $\sigma \neq id$.
Allora esistono, distinti, $a, b \in \{1, 2, \ldots, n\}$ tale che $\sigma(a) = b$.
Sia $c \in \{1, 2, \ldots, n\}$, con $c \neq a$, e $c \neq b$.
Posto $g = \begin{pmatrix} b & c \end{pmatrix}$ si ha che $g\sigma(a) = g(b) = c$ mentre $\sigma g(a) = \sigma(a) = b$.
Questo mostra che in $Z(S_n)$ non possono esserci elementi di S_n diversi da id, quindi $Z(S_n)$ è banale e coincide con $\{id\}$. □

Teorema 2.15. *Sia $n > 3$. Il centro di A_n, $Z(A_n)$, è banale.*

Dimostrazione. Sia $\sigma \in Z(A_n)$, $\sigma \neq id$.
Si prendano due distinti, $a, b \in \{1, 2, \ldots, n\}$ tale che $\sigma(a) = b$.
Si scelgano poi $c, d \in \{1, 2, \ldots, n\}$, con entrambi diversi fra loro e divers sia da a che da b.
Posto $g = \begin{pmatrix} b & c & d \end{pmatrix}$ si ha analogamente alla dimostrazione precedente che $g\sigma \neq \sigma g$ poiché le due permutazioni mandano a in due elementi differenti.
Ne segue che il centro di A_n è banale. □

La dimostrazione del Teorema 2.15, per il solo caso $n > 4$, è banale in quanto diretta conseguenza del teorema 2.12.

Teorema 2.16. *Sia $n > 4$. Allora i soli sottogruppi normali di S_n sono $\{id\}$, A_n, S_n.*

Dimostrazione. Sia $K \lhd S_n$. Dato che A_n è semplice e vale $K \cap A_n \lhd A_n$, allora $K \cap A_n = A_n$ oppure $K \cap A_n = \{id\}$.
Nel primo caso, $A_n \leqslant K \leqslant S_n \Longrightarrow K = S_n$ oppure $K = A_n$,
poichè $\mid S_n \diagup A_n \mid = 2$.
Nel secondo caso K è isomorfo a un sottogruppo di $S_n \diagup A_n$, quindi $\mid K \mid = 1$ oppure $\mid K \mid = 2$.
Se $\mid K \mid = 2$ allora $K = \{id, \alpha\}$. Essendo $K \lhd S_n$, $\forall \beta \in S_n$ si avrebbe $\beta \circ \alpha \circ \beta^{-1} \in K$ e d'ordine 2, quindi $\beta \circ \alpha \circ \beta^{-1} = \alpha \Rightarrow \alpha \in Z(S_n) = \{id\}$.
Ne segue che $\mid K \mid = 1$ e quindi i soli sottogruppi normali di S_n sono $\{id\}$ A_n e S_n. □

Definizione 2.17. *Un gruppo G si dice risolubile se possiede una serie normale abeliana, ovvero se esiste una catena di sottogruppi*

$$\{id\} \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n \subseteq G$$

in cui ogni H_i è normale in H_{i+1} e il quoziente $H_{i+1} \diagup H_i$ è abeliano.

Segue dalla definizione che S_n, per $n > 4$, non è risolubile, perché i soli sottogruppi di S_n sono $\{id\}$ A_n e S_n e questa non è una serie abeliana perché A_n non lo è.

Nota Questo risultato, dalla *teoria di Galois*, implica che le equazioni algebriche di grado ≥ 5 non hanno una formula risolutiva per radicali (*Teorema di Ruffini-Abel*).

Capitolo 3

p-sottogruppi di Sylow di S_n

3.1 π-gruppi, p-gruppi e p-sottogruppi di Sylow

Se π è un insieme non vuoto di numeri primi, un elemento di un gruppo G dicesi *π-elemento* se il suo periodo è finito ed i divisori primi di tale periodo appartengono tutti a π. Se π consta di un solo elemento, un solo numero primo p, un π-elemento è detto anche *p-elemento*.
In altri termini un p-elemento di un gruppo è un elemento il cui periodo è finito ed è potenza di p.

Definizione 3.1. *Un gruppo G dicesi π-gruppo (p-gruppo) quando ogni suo elemento è un π-elemento (p-elemento).*

Definizione 3.2. *Dato π un insieme di numeri primi e G un gruppo, diremo π-sottogruppo di G ogni sottogruppo di G che sia un π gruppo.*
Un π-sottogruppo H di G dicesi π-sottogruppo di Sylow di G se non esiste nessun π-sottogruppo di G che contenga H senza coincidere con esso.

In particolare, se π consta si un solo elemento primo p, un π-sottogruppo di G si dice anche *p-sottogruppo* e un π-sottogruppo di Sylow di G dicesi *p-sottogruppo di Sylow*.
Questi ultimi sono anche semplicemente chiamati *sottogruppi di Sylow*, mentre i π-sottogruppo di Sylow diconsi *sottogruppi di Sylow generalizzati* o *π-sottogruppi di Hall*.

Teorema 3.3. *(Teorema di Sylow) Sia G un gruppo finito di ordine $p^a m$, con p primo, $(p, m) = 1$, $a \geq 1$. Allora:*

1. *G possiede p-sottogruppi di ordine p^a*
2. *Ogni p-sottogruppo è incluso in un p-sottogruppo di ordine p^a; per tanto questi ultimi sono i soli p-sottogruppi di Sylow*
3. *Tutti i p-sottogruppi di Sylow sono coniugati*
4. *Detto n_p il loro numero, si ha che $n_p \equiv 1 (mod\ p)$ ed n_p è divisore di m.*

Corollario 3.4. *Se G è un gruppo finito, p un numero primo, e p^α la massima potenza di p che divide l'ordine di G, ogni sottogruppo di G d'ordine p^α è un p-sottogruppo di Sylow di G.*

Vogliamo ora descrivere i p-sottogruppi di Sylow di S_n per ogni p divisore di $n!$
Osserviamo che p primo divide $n! \iff p \leq n$.
Per questo scopo introduciamo le nozioni di prodotto semidiretto e prodotto intrecciato di gruppi.

3.2 Prodotto intrecciato di due gruppi

Definizione 3.5. *Dati due gruppi H e K e*
$\tau : K \longrightarrow Aut(H)$ un omomorfismo.
Si dice prodotto semidiretto (esterno) dei gruppi H e K rispetto a τ, il gruppo:

$$H \rtimes_\tau K = \{(h, k) \mid h \in H, k \in K\}$$

rispetto al prodotto definito da:

$$(h_1, k_1)(h_2, k_2) = (h_1\tau(k_1)(h_2), k_1k_2) = (h_1\tau_{k_1}(h_2), k_1k_2).$$

Osserviamo che $\tau(k_1)(h_2)$ è un elemento di H, infatti $\tau(k_1)$ è un automorfismo di H e viene proprio applicato ad $h_2 \in H$.

Si può banalmente osservare che se τ è l'omomorfismo banale, ossia se $\tau(k) = id \ \forall k \in K$, allora l'operazione di prodotto semidiretto coincide col prodotto diretto componente per componente. Ovvero si ha $H \rtimes_\tau K = H \times K$. Altre proprietà immediate del prodotto semidiretto sono:

1. l'elemento neutro è $(1_H, 1_K)$
2. l'inverso di (h, k) è $(\tau(k^{-1})h^{-1}, k^{-1})$

Teorema 3.6. *Sia G un gruppo, e siano $H \lhd G$ e $K < G$ due suoi sottogruppi tali che $H \cap K = \{id\}$ e $G = HK$. Allora*

$$G \cong H \rtimes_{cG} K$$

dove $cG : K \longrightarrow Aut(H)$ è l' omomorfismo che associa ad ogni $k \in K$ l'automorfismo dato dal coniugio (in G) per k, ossia l'automorfismo $H \longrightarrow H$ definito da $h \longrightarrow khk^{-1}$.

Dimostrazione. La mappa

$$\begin{aligned} \phi : H \rtimes_{cG} K &\longrightarrow G \\ (h, k) &\longrightarrow hk \end{aligned}$$

definisce un isomorfismo. Infatti è naturalmente un omomorfismo.
Inoltre la condizione $H \cap K = \{id\}$ garantisce l'iniettività, e la surgettività è banale. □

Esempio 3.7. *Consideriamo S_n ed i sottogruppi $A_n \lhd S_n$, $\langle (1 \quad 2) \rangle < S_n$.*
I due sottogruppi si intersecano solo nell'identità, in quanto il secondo è generato da una permutazione dispari; inoltre, per questioni di cardinalità, deve essere $S_n = A_n \langle (1 \quad 2) \rangle$.
Allora per il teorema precedente $S_n \cong A_n \rtimes_{cS_n} \langle (1 \quad 2) \rangle$.

Si andrà ora a definire il *prodotto intrecciato* di due gruppi.
Esso è un particolare prodotto fra gruppi che si basa sul prodotto semidiretto. E' uno strumento molto importante usato per la classificazione dei sottogruppi di Sylow di S_n.

Definizione 3.8. *Siano A e H due gruppi. $\forall h \in H$ sia A_h una "copia" di A e sia B il prodotto diretto $B = \prod_{h \in H} A_h$.*
Definiamo ora una applicazione

$$\varphi : H \longrightarrow Aut(B)$$

definita ponendo $\forall x \in H$ e $\forall b = \{a_h\}_{h \in H} \in B$

$$\varphi_x(b) = \varphi(x)(b) = \{a'_h\}_{h \in H},\ a'_h = a_{\varphi^{-1}(h)}$$

Si definisce prodotto intrecciato dei gruppi A e H, e si indica con Aw_rH, il prodotto semidiretto $B \rtimes_\varphi H$.

Osservazione Se G è un qualsiasi gruppo finito ed H è un gruppo di permutazioni su n elementi ($H \leqslant S_n$), consideriamo

$$B = G \times G \times \cdots \times G = G^n$$

l'insieme delle n-uple ordinate di elementi di G.
Allora Il prodotto intrecciato di G con H, indicato con Gw_rH, è $B \rtimes H = G^n \rtimes H$, è l'insieme $B \times H$ con la moltiplicazione definita da:

$$(g, \sigma)(h, \pi) = ((g_1 h_{\sigma^{-1}(1)}, \ldots, g_n h_{\sigma^{-1}(n)}), \sigma\pi)$$

ove $g = \{g_1, g_2, \ldots, g_n\}$, $h = \{h_1, h_2, \ldots, h_n\} \in B$; $\sigma, \pi \in H$.

Generalizzando ulteriormente, se $H = S_n$ avremo $Gw_rS_n = G^n \rtimes S_n$.

3.3 Sottogruppi di Sylow del gruppo delle permutazioni su n oggetti

Per mezzo della costruzione di opportuni prodotti intrecciati si può giungere alla determinazione dei p-sottogruppi di Sylow del gruppo delle permutazioni S_n, su n oggetti, con p primo, n intero, $n \geq p$.

Si studia, per prima cosa, l'ordine dei p-sottogruppi di Sylow di S_n.

Teorema 3.9. *Se p^m è la massima potenza di p che risulti $\leq n$, l'ordine di un p-sottogruppo di Sylow di S_n vale:*

$$p^{a_1+a_2+\cdots+a_m}$$

ove a_i, $\forall i = 1, 2, \ldots, m$, è il massimo intero che riusulti $\leq \dfrac{n}{p^i}$.

Dimostrazione. Indichiamo con p^{b_n} l'ordine di un p-sottogruppo di Sylow di S_n, cioè la massima potenza di p che divide $n!$, per 3.4.
I soli interi positivi $\leq n$ che siano divisibili per p sono $p, 2p, \ldots, a_1 p$, onde p^{b_n} eguagli la massima potenza di p che divide il prodotto:
$p(2p)\ldots(a_1 p) = p^{a_1} a_1!$
Se $m = 1$, $p^1 = p$ è la massima potenza di p che risulti $\leq n$, pertanto $p^2 > n$, allora nessuno dei numeri $1, 2, \ldots, n$ è divisibile per p^2 e pertanto nessuno dei numeri $1, 2, \ldots, a_1$ è divisibile per p. Allora $a_1!$ è primo con p, e pertanto $p^{b_n} = p^{a_1}$ il teorema così nel caso $m = 1$ è dimostrato.

Si può ora procedere per induzione rispetto ad m.
Si avrà: $p^{b_n} = p^{a_1+b_{a_1}}$, dove $p^{b_{a_1}}$ è la massima potenza di p che divide $a_1!$.
Si osservi ora che la massima potenza di p che risulti $\leq a_1$ è p^{m-1}; infatti è $p^m \leq n < p^{m+1}$, e poiché $a_1 p$ è il massimo multiplo di p che sia $\leq n$, è $p^m \leq p a_1 < p^{m+1}$, onde $p^{m-1} \leq a_1 < p^m$.

Inoltre il massimo intero a_i che risulti $\leq \dfrac{n}{p^i}$ eguaglia il massimo intero che risulti $\leq \dfrac{a_1 p}{p^i}$, perchè gli interi $a_1 p + 1$, $a_1 p + 2$, $\ldots$, $a_1 + n$ non sono divisibili per p.

Ma $\dfrac{a_1 p}{p^1} = \dfrac{a_1}{p^{i-1}}$, onde a_i fornisce il massimo intero che risulti $\leq \dfrac{a_1}{p^{i-1}}$.

In base all'ipotesi induttiva si ha pertanto che la massima potenza di p che divide $a_1!$ vale $p^{a_2+\cdots+a_m}$, cioè $p^{b_{a_1}} = p^{a_2+\cdots+a_m}$.
Segue che $p^{b_n} = p^{a_1+a_2+\cdots+a_m}$ come si voleva. □

Osservazione In particolare, se $n = p^m$ (p primo, m intero ≥ 1) l'ordine di un p-sottogruppo di Sylow di S_n vale

$$p^{\vartheta(p^m)},$$
$$\text{ove } \vartheta(p^m) = p^{m-1} + p^{m-2} + \cdots + p + 1.$$

Infatti il massimo intero che sia $\leq \frac{n}{p^i} = \frac{p^m}{p^i}$ è p^{m-i}.

Una cosa molto semplice è vedere quanti sono i p-sottogruppi di Sylow del gruppo S_p, con p primo.

Teorema 3.10. *Per un numero p primo, il numero dei p-sottogruppi di Sylow del gruppo simmetrico S_p, su p elementi, è $(p-2)!$*

Dimostrazione. Dato che $\mid S_p \mid = p!$ con p primo, si ha che p è la massima potenza di p che divide $\mid S_p \mid$. Quindi i p-sottogruppi di Sylow hanno ordine p e quindi sono ciclici.
Ciascuno è generato da un elemento di S_p di ordine p, ossia dai p-cicli, che sono in numero $(p-1)!$. Dato che in ogni gruppo di ordine p ci sono $p-1$ elementi di ordine p e dato che due gruppi diversi di ordine p hanno intersezione ridotta al solo elemento neutro, ne segue che il numero dei p-sottogruppi di Sylow è

$$\frac{(p-1)!}{(p-1)} = (p-2)!$$

□

Determiniamo ora, in primo luogo, la struttura dei p-sottogruppi di Sylow di S_n nel caso in cui $n = p^m$.

L'insieme costituito dagli $n = p^m$ oggetti su cui operano le permutazioni appartenenti a S_n può suddividersi in p sottoinsiemi, ciascuno di p^{m-1} oggetti, a due a due privi di oggetti in comune.

Tali sottoinsiemi siano:

H_1, costituito da $1, \ldots, p^{m-1}$
H_2, costituito da $p^{m-1}+1, p^{m-1}+2, \ldots, 2p^{m-1}$
H_3, costituito da $2p^{m-1}+1, 2p^{m-1}+2, \ldots, 3p^{m-1}$
...
H_p, costituito da $(p-1)p^{m-1}+1, (p-1)p^{m-1}+2, \ldots, pp^{m-1} = p^m$.

Le permutazione appartenenti a S_n e che lasciano fermo ciascuno degli oggetti contenuti in $H_2, H_2, \ldots, H_p$, costituiscono un sottogruppo di S_n che sostanzialmente si riduce al gruppo di tutte le permutazioni su H_1, ed ha quindi ordine $p^{m-1}!$
Si consideri Q_1 un suo p-sottogruppo di Sylow. Esso avrà ordine $p^{\vartheta(p^{m-1})}$.
Si ponga:

$$\sigma = \begin{pmatrix} 1 & p^{m-1}+1 & 2p^{m-1}+1 & \ldots & (p-1)p^{m-1}+1 \end{pmatrix}$$
$$\begin{pmatrix} 2 & p^{m-1}+2 & 2p^{m-1}+2 & \ldots & (p-1)p^{m-1}+2 \end{pmatrix} \ldots$$
$$\ldots$$
$$\ldots \begin{pmatrix} p^{m-1} & 2p^{m-1} & 3p^{m-1} & \ldots & p^m \end{pmatrix}$$

Ovviamente σ ha periodo p per il teorema 1.14. Inoltre σ^{i-1} porta ciascun oggetto di H_1 in un oggetto di H_i $(i = 1, 2, \ldots, p)$.
Allora posto $Q_i = \sigma^{-i+1} Q_1 \sigma^{i-1}$, si ha che le permutazioni appartenenti a Q_i lasciano fermo ogni oggetto appartenente ad $H_1, \ldots, H_{i-1}, H_{i+1}, \ldots, H_p$, onde Q_i è un p-sottogruppo di Sylow del gruppo delle permutazioni S_n e che lasciano fermo ogni oggetti di H_i.
Gli oggetti non lasciati fermi da ogni permutazione appartenente a Q_1 sono quelli di H_1, i quali però sono invece lasciati fermi da ogni permutazione appartenente a Q_2.
Ne segue che Q_1, Q_2 sono disgiunti e quindi permutabili elemento per elemento, onde $Q_1 \cup Q_2 = Q_1 \times Q_2$.
Così seguitando si prova che $Q_1 \cup Q_2 \cup Q_3 \cup \cdots \cup Q_p = Q_1 \times Q_2 \times Q_3 \times \cdots \times Q_p$.

Il sottogruppo P di S_n generato da Q_1 e da σ contiene $Q_2, \ldots, Q_p$ perché

questi sono i trasformati di Q_1 mediante le potenze di σ; pertanto esso contiene $Q_1 \times Q_2 \times \cdots \times Q_p$. Inoltre, detto T il sottogruppo di S_n d'ordine p generato da σ, si ha che $Q_1 \times Q_2 \times Q_3 \times \cdots \times Q_p$ è normale in P.
Si ha in conclusione che P è il prodotto intrecciato $Q_1 \rtimes T$.

Poiché Q_1 e T hanno rispettivamente ordine $p^{\vartheta(p^{m-1})}$ e p, si ha che P ha ordine $p^{\vartheta(p^{m-1})p}p = p^{\vartheta(p^{m-1})p+1}$.

Ma si ha

$$\vartheta(p^{m-1})p + 1 = (p^{m-2} + p^{m-3} + \cdots + p + 1)p + 1 = \\ (p^{m-1} + p^{m-2} + \cdots + p + 1 = \vartheta(p^m)$$

onde P è un p-gruppo d'ordine $p^{\vartheta(p^m)}$ di S_n. Inoltre $p^{\vartheta(p^m)}$ è l'ordine dei p-sottogruppi di Sylow di S_n pertanto P è un p-sottogruppo di Sylow di S_n.
Concludendo:

Teorema 3.11. *Sia P un p-sottogruppo di Sylow di S_n con $n = p^m$, $m > 0$ intero, e sia Q un p-sottogruppo di Sylow di S_l con $l = p^{m-1}$. Allora, detto T un gruppo d'ordine p, si ha che P è isomorfo al prodotto intrecciato $Q \rtimes T$.*

Ripetute applicazioni di questo teorema, assieme al fatto che per $m = 1$, P ha ordine p, ci danno che:

Corollario 3.12. *Se P è un p-sottogruppo di Sylow di S_n con $n = p^m$ si ha che P è isomorfo a*

$$((T_1 \; w_r \; T_2) \; w_r \; T_3) \; w_r \; \ldots \; w_r \; T_m$$

ove $T_1, \ldots, T_m$ sono gruppi ciclici d'ordine p.

Esaminiamo ora il caso n qualsiasi.

Se p^m è la massima potenza di p che sia $\leq n$, si avrà $n = cp^m + r$, con $0 \leq r < p^m$.
Dovrà essere inoltre $c < p$, altrimenti si avrebbe $n \geq cp^m \geq p^{m+1}$, contro l'ipotesi su p^m.

Essendo inoltre $\frac{n}{p^m} = c + \frac{r}{p^m}$, con $\frac{r}{p^m} < 1$, si ha che c è il massimo intero che sia $\leq \frac{n}{p^m}$, cioè l'intero già indicato in precedenza con a_m, onde $n = a_m p^m + r$.
Sia ora p^t la massimo potenza di p che sia $\leq r$, e sia d_i, $(i = 1, \ldots, t)$ il massimo intero che sia $\leq \frac{r}{p^i}$.
Si avrà, per $i = 1, 2, \ldots, m$,

$$\frac{n}{p^i} = a_m p^{m-1} + \frac{r}{p^i}$$

onde, se $t < i \leq m$, si ha che il massimo intero a_i il quale risulti $\leq \frac{n}{p^i}$ è dato che $a_m p^{m-i}$ (visto che vale $\frac{r}{p^i} < \frac{p^{t+1}}{p^i} \leq 1$).
Mentre, se $1 \leq i \leq t$, si ha $a_i = a_m p^{m-i} + d_i$.
Ne segue che:

$$a_1 + a_2 + \cdots + a_m = a_m(p^{m-1} + p^{m-2} + \cdots + 1) + d_1 + d_2 + \cdots + d_t$$

e pertanto,

$$p^{a_1+a_2+\cdots+a_m} = p^{a_m \vartheta(p^m)} p^{d_1+d_2+\cdots+d_t}$$

Essendo dunque $n = a_m p^m + r$ possiamo ora ripartire gli n oggetti nei seguenti sottoinsiemi disgiunti:

K_1, costituito da $1, 2, \ldots, p^m$
K_2, costituito da $p^m + 1, p^m + 2, \ldots, 2p^m$
$\ldots$
K_{a_m}, costituito da $(a_m - 1)p^m + 1, (a_m - 1)p^m + 2, \ldots, a_m p^m$
K_{a_m+1}, costituito da $a_m p^m + 1, a_m p^m + 2, \ldots, a_m p^m + r = n$.

Sia R_j, $j = 1, 2, \ldots, a_m - 1$, il gruppo delle permutazioni appartenenti a S_n che lasciano fermo ogni oggetto non appartenente a K_j. Allora R_j coincide sostanzialmente con il gruppo delle permutazioni su K_j. Pertanto in base all' Osservazione del teorema 3.9 detto Q_j un suo p-sottogruppo di Sylow, l'ordine di di Q_j vale $p^{\vartheta(p^m)}$ per $j = 1, 2, \ldots, a_m$, mentre è $p^{d_1+d_2+\cdots+d_t}$ per $j = a_m + 1$.
Inoltre, se j_1, j_2 sono due distinti tra gli interi $1, 2, \ldots, a_m + 1$, si ha che R_{j_1} e R_{j_2}, e quindi Q_{j_1} e Q_{j_2} sono permutabili elemento per elemento.

Ciascuno dei sottogruppo $R_1, \ldots, R_{a_m+1}$ incontra l'unione dei rimanenti secondo la sola unità, allora è:

$$R_1 \cup R_2 \cup \cdots \cup R_{a_m+1} = R_1 \times R_2 \times \cdots \times R^{a_m+1}.$$

Ma $R_1 \times R_2 \times \cdots \times R^{a_m+1}$ contiene $Q_1 \times Q_2 \times \cdots \times Q^{a_m+1}$ il quale ha ordine $a_m p^{\vartheta(p^m)} p^{d_1+d_2+\cdots+d_t}$, cioè, in base a quanto visto precedentemente, $p^{a_1+a_2+\cdots+a_m}$, che eguaglia l'ordine di un p-sottogruppo di Sylow R di S_n.
Essendo un p-sottogruppo di S_n risulta esso stesso un p-sottogruppo di Sylow di S_n.
Concludendo:

Teorema 3.13. *Se p^m è la massima potenza di p che risulti $\leq n$, detti a_m ed r rispettivamente il quoziente e il resti della divisione di n per p_m, si ha che un p-sottogruppo di Sylow di S_n è dato che un prodotto diretto*

$$Q_1 \times Q_2 \times \cdots \times Q_{a_m} \times Q_{a_m+1}$$

ove Q_j $(j = 1, 2, \ldots, a_m)$ è isomorfo ad un p-sottogruppo di Sylow di S_{p^m}, mentre Q_{a_m+1} è isomorfo ad un p-sottogruppo di Sylow di S_r.

Poiché la struttura di $Q_1, Q_2, \ldots, Q_{a_m}$ è data dal corollario 3.12 si ha che il problema è ricondotto alla determinazione di Q_{a_m+1}. Sarà $r = qp^t + s$,con $1 \leq q < p$, $0 \leq s < p^t$, allora, in base al teorema immediatamente precedente applicato a S_r, si ha che Q_{a_m+1} è isomorfo al prodotto diretto di q p-sottogruppi di Sylow di S_{p^t} per un p-sottogruppo di S_s.
Così seguitando si ottiene alla fine:

Teorema 3.14. *Sia p^m l massima potenza di p che divida n. Allora sono univocamente determinati $d_0, d_1, d_2, \ldots, d_m$ tali che*

$$n = d_0 p^m + d_1 p^{m-1} + \cdots + d_m$$

e $0 \leq d_i < p$, per $i = 0, \ldots, m$.
Un p-sottogruppo di Sylow di S_n è dato dal prodotto diretto di d_0 gruppi isomorfi ad un p-sottogruppo di Sylow di S_{p^m}, per d_1 gruppi isomorfi ad un p-sottogruppo di Sylow di $S_{p^{m-1}}$, ..., per d_{m-1} gruppi isomorfi ad un p-sottogruppo di Sylow di S_p (cioè ad un gruppo ciclico di ordine p).

Esempio 3.15. *Determiniamo i p-sottogruppi ed i p-sottogruppi di Sylow di* S_4.
I valori da considerare sono $p = 2$ *e* $p = 3$.
I 2*-Sylow hanno ordine 8, mentre i* 3*-Sylow hanno ordine 3.*

I sottogruppi di ordine 2 sono:
$\langle(1\ \ 2)\rangle$, $\langle(1\ \ 3)\rangle$, $\langle(1\ \ 4)\rangle$, $\langle(2\ \ 3)\rangle$, $\langle(2\ \ 4)\rangle$, $\langle(3\ \ 4)\rangle$.

I sottogruppi di ordine 4 sono:
$\langle(1\ \ 2\ \ 3\ \ 4)\rangle = \{id, (1\ \ 2\ \ 3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4\ \ 3\ \ 2)\}$
$\langle(1\ \ 2\ \ 4\ \ 3)\rangle = \{id, (1\ \ 2\ \ 4\ \ 3), (1\ \ 4)(2\ \ 3), (1\ \ 3\ \ 4\ \ 2)\}$
$\langle(1\ \ 3\ \ 2\ \ 4)\rangle = \{id, (1\ \ 3\ \ 2\ \ 4), (1\ \ 2)(3\ \ 4), (1\ \ 4\ \ 2\ \ 3)\}$
$\{id, (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3)\}$

(I primi tre sottogruppi di ordine 4 sono isomorfi)

I sottogruppi di ordine 3, ovvero i 3*-Sylow, sono:*
$\langle(1\ \ 2\ \ 3)\rangle$, $\langle(1\ \ 2\ \ 4)\rangle$, $\langle(1\ \ 3\ \ 4)\rangle$, $\langle(2\ \ 3\ \ 4)\rangle$

Si nota che un sottogruppo 3*-Sylow* $\approx C_3$.
Essi sono 4 che risulta essere infatti congruo a 1 modulo 3.

I sottogruppi di ordine 8, ovvero i 2*-Sylow, sono:*
$C((1\ \ 2)(3\ \ 4)) = \{id, (1\ \ 2)(3\ \ 4), (1\ \ 3)(2\ \ 4), (1\ \ 4)(2\ \ 3), (1\ \ 2), (3\ \ 4), (1\ \ 3\ \ 2\ \ 4), (1\ \ 4\ \ 2\ \ 3)\}$
$C((1\ \ 3)(2\ \ 4)) = \{id, (1\ \ 3)(2\ \ 4), (1\ \ 2)(3\ \ 4), (1\ \ 4)(2\ \ 3), (1\ \ 3), (2\ \ 4), (1\ \ 2\ \ 3\ \ 4), (1\ \ 4\ \ 3\ \ 2)\}$
$C((1\ \ 4)(2\ \ 3)) = \{id, (1\ \ 4)(2\ \ 3), (1\ \ 3)(2\ \ 4), (1\ \ 2)(3\ \ 4), (1\ \ 4), (2\ \ 3), (1\ \ 3\ \ 4\ \ 2), (1\ \ 2\ \ 4\ \ 3)\}$

Si nota che un sottogruppo 2*-Sylow* $\approx D_4$.
Volendo si può dimostrare che i 2*-Sylow sono a due a due coniugati, quindi isomorfi, e che ogni gruppo di ordine 2 o 4 è contenuto in un sottogruppo di ordine 8.*
Inoltre, il numero dei 2*-Sylow è congruo a 1 modulo 2: è infatti uguale a 3.*

Osservazione Si osservi che effettivamente D_4 è il prodotto intrecciato di C_2 con se stesso.

Nel teorema 3.9 e, in particolare, nell'osservazione ed esso riferita, abbiamo visto quale è l'ordine di un p-sottogruppo di Sylow di S_n.
Nell' esempio che segue è presentata una tabella in cui vengono riportati gli ordini dei 2-sotttogruppi di Sylow di S_n con n potenza di 2, ovvvero $n = 2^k$. Tali ordini dei 2-sottogruppi di Sylow di S_n coincidono con la massima potenza di 2 che compare nella scomposizione dell'ordine di S_n, ovvero nella scomposizione di $n! = 2^k!$, in potenze di primi. I risultati così ottenuti e riportati nell'esempio coincidono perfettamente con quelli che si otterrebbero applicando il metodo esposto nel teorema 3.9.

Esempio 3.16. *Consideriamo $S_n = S_{2^k}$. Come spiegato precedentemente occorre scomporre in fattori primi $n! = 2^k!$ e prendere poi la massima potenza di 2 che compare nella fattorizzazione. Dal momento che per il nostro fine interessa solo quest'ultima tralasceremo nella scomposizione i fattori primi diversi da 2 e ci preoccuperemo di riportare solamente le potenze di 2.*

Ad esempio di $8! = 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 2^3 \cdot 7 \cdot (3 \cdot 2) \cdot 5 \cdot 2^2 \cdot 3 \cdot 2 \cdot 1$
sarà presa in considerazione solamente la parte $2^3 \cdot 2 \cdot 2^2 \cdot 2 = 2^{3+1+2+1} = 2^7$,
quindi i 2-sottogruppi di Sylow di S_8 avranno ordine 2^7.

k	S_n	*ordine dei 2-Sylow di S_n (massima potenza di 2 nella decomposizione)*
2	$S_4 = S_{2^2}$	$4! = 2^{2+1} = 2^3$
3	$S_8 = S_{2^3}$	$8! = 2^{3+1+2+1} = 2^7$
4	$S_{16} = S_{2^4}$	$16! = 2^{4+1+2+1+7} = 2^{15}$
5	$S_{32} = S_{2^5}$	$32! = 2^{5+1+2+1+3+1+2+15} = 2^{31}$
6	$S_{64} = S_{2^6}$	$64! = 2^{6+1+2+1+3+1+2+1+4+1+2+1+3+1+2+1+31} = 2^{63}$

Già da questi primi cinque esempi è possibile ricavare una regola generale che permette di determinare immediatamente l'ordine dei 2-Sylow di S_n con n potenza di 2.

Dato $S_n = S_{2^k}$ *di ordine* $n! = 2^k!$ *si ha che un* 2*-Sylow di esso risulta avere ordine*

$$2^{2^k-1}$$

Come ultima cosa, preso come esempio il solo caso di S_8*, si fa vedere che il risultato ottenuto applicando il teorema* 3.9 *equivale perfettamente a quello in tabella.*

In S_8 *si ha* $n = 8 = 2^3$*, quindi, seguendo il ragionamento proposto dal teorema, si ha* $m = 3$*,* $p = 2$*.*
L'ordine di un 2*-sottogruppo di Sylow di* S_8 *vale* $2^{\vartheta(2^3)}$*, ove* $\vartheta(2^3) = 2^{3-1} + 2^{3-2} + 2^{3-3} = 2^2 + 2^1 + 1 = 7$*, da cui l'ordine risulta essere quindi* 2^7*, analogo al valore in tabella.*

Bibliografia

[1] L. Verardi, *Appunti di Algebra 1*, A. A. 2012-2013, Bologna.

[2] L. Verardi, *Appunti di Algebra Superiore*, A. A. 2012-2013, Bologna.

[3] G. Zappa, *Fondamenti di teoria dei gruppi, Volume I*, Cremonese, 1965, Roma.

[4] G. Zappa, *Fondamenti di teoria dei gruppi, Volume II*, Cremonese, 1970, Roma.

[5] W. R. Scott, *Group Theory*, Prentice-Hall, 1964, New Jersey.