

Algebra II

AlpT (@freaknet.org)

December 16, 2013

Abstract

Questo testo e' una rielaborazione personale degli appunti presi durante il corso di Algebra II, tenuto dal Prof. Rosario Strano presso il dipartimento di Matematica, Catania, A.A. 2007/2008.

Non ho mai effettuato una revisione completa. E' molto probabile quindi che ci siano alcuni errori qua e la'. Considera tale possibilita' come una buona motivazione di studio approfondito.

In augurio e letizia,
Andrea

Copyright ©2012 Andrea Lo Pumo aka AlpT <alpt@freaknet.org>. All rights reserved.

This document is free; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This document is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this document; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Contents

1	Teoria dei gruppi	1
1.1	Gruppi e sottogruppi ciclici	6
1.2	Laterali modulo H	17
1.2.1	Teorema di Lagrange	19
1.3	Gruppo simmetrico	21
1.4	Gruppi diedrali	38
1.5	Sottogruppi normali	42
1.6	Gruppo quoziente	46
1.7	Gruppo prodotto	48
1.7.1	Prodotto interno ed esterno	50
1.7.2	Prodotto a piu' fattori	52
1.8	Omomorfismo tra gruppi	56
1.8.1	Teorema di Cayley	67
1.9	Azione di un gruppo	72
1.9.1	Azione di coniugio	77
2	p-gruppo	79
2.1	Teorema di Sylow	84
3	Classificazione degli abeliani	90
4	Proposizioni varie	95
5	Studio dei gruppi	98
6	Esercizi	108

1 Teoria dei gruppi

Definition 1.1. Un **gruppoide** $(M, \cdot)$ e' un insieme non vuoto M dotato di un'operazione binaria interna $\cdot$, ovvero

$$M \neq \emptyset$$

$$\cdot : M \times M \longrightarrow M$$

E' da notare che $\cdot$ deve essere definita per ogni coppia (a, b) con $a, b \in M$ e deve essere ben definita¹.

Definition 1.2. Un **semigrupp** $(S, \cdot)$ e' un gruppoide dotato della proprieta' associativa:

$$\forall a, b, c \in S \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

Proposition 1.3. Per la proprieta' associativa, presi $a_1, \dots, a_n \in S$ e fissati $1 \leq i \leq n$, $1 \leq j \leq n$, si ha

$$(a_1 \cdots a_{i-1}) \cdot (a_i \cdots a_n) = (a_1 \cdots a_{j-1}) \cdot (a_j \cdots a_n)$$

In altre parole, usando le parentesi per specificare un qualsiasi ordine delle moltiplicazioni, non cambia il risultato (f.e., $(ab)cd = a(bc)d$)

Proof: per induzione su n , e per fissare le idee supponiamo $i < j$

$n = 3$: vera per def. di prop. associativa

Hp : $3 < m < n$ vera

$$n : (a_1 \cdots a_{i-1}) \cdot \underbrace{(a_i \cdots a_n)}_{\text{qui vale l'Hp ind.}} = (a_1 \cdots a_{i-1}) \cdot (a_i \cdots a_j) \cdot (a_{j+1} \cdots a_n)$$

$$\underbrace{=}_{\text{prop. ass.}} ((a_1 \cdots a_{i-1}) \cdot (a_i \cdots a_j)) \cdot (a_{j+1} \cdots a_n) = ((a_1 \cdots a_{i-1}) \cdot (a_i \cdots a_{j-1}) \cdot a_j) \cdot (a_{j+1} \cdots a_n) =$$

$$= (((a_1 \cdots a_{i-1}) \cdot (a_i \cdots a_{j-1}) \cdot a_j)) \cdot (a_{j+1} \cdots a_n) =$$

$$= ((a_1 \cdots a_{j-1}) \cdot a_j) \cdot (a_{j+1} \cdots a_n) = (a_1 \cdots a_{j-1}) \cdot (a_j \cdot (a_{j+1} \cdots a_n)) =$$

$$= (a_1 \cdots a_{j-1}) \cdot (a_j \cdots a_n)$$

□

Definition 1.4. In un semigrupp $(S, \cdot)$, definiamo l'operazione di potenza:

$$a^0 = 1$$

$$a^n = a \cdot a^{n-1}, \quad n \in \mathbb{N}$$

¹se gli elementi sono delle classi, l'immagine della coppia non deve dipendere dai rappresentanti degli elementi. Ad esempio, la legge

$$\left(\frac{x}{y} + \frac{t}{z} \right) \longrightarrow \frac{x+t}{y+z}$$

con $x, y, z, t \in \mathbb{Q}_{>0}$, non e' ben posta:

$$\left(\frac{3}{4}, \frac{4}{1} \right) \longrightarrow \frac{7}{5}$$

$$\left(\frac{6}{8}, \frac{12}{3} \right) \longrightarrow \frac{18}{11}$$

Proposition 1.5. Valgono le seguenti proprietà:

$$a^m \cdot a^n = a^{m+n}$$

$$(a^m)^n = a^{mn}$$

Proof:

$$a^m \cdot a^n = \underbrace{a \cdots a}_{m \text{ volte}} \underbrace{a \cdots a}_{n \text{ volte}} = \underbrace{a \cdots a}_{m+n \text{ volte}} = a^{m+n}$$

$$(a^m)^n = \underbrace{a^m \cdots a^m}_{n \text{ volte}} = a^{\overbrace{m + \cdots + m}^{n \text{ volte}}} = a^{mn}$$

Definition 1.6. In un semigruppò può esistere l'elemento **unità** e :

$$ee' \text{ elem. unità di } S \Leftrightarrow \forall a \in S \quad a \cdot e = e \cdot a = a$$

Proposition 1.7. L'elemento unità, se esiste, è unico.

Proof: Supponiamo che ne esistano due diversi e, e' , allora per definizione $ee' = e'$, $e'e = e$, $ee' = e'e$, $e' = e$.

Definition 1.8. In un semigruppò $(S, \cdot)$ con unità e , l'elemento **inverso** a' di $a \in S$ è t.c.

$$a \in S \text{ è invertibile} \Leftrightarrow \exists a' \in S : aa' = a'a = e$$

a' è chiamato inverso di a e si indica con a^{-1} .

Proposition 1.9. L'elemento inverso è unico.

Proof: Supponiamo che ne esistano due distinti a', a'' , ovvero

$$aa' = a'a = aa'' = a''a = e$$

$$aa' = aa'' \Leftrightarrow a'aa' = a'aa'' \Leftrightarrow (a'a)a' = (a'a)a'' \Leftrightarrow a' = a''$$

Definition 1.10. Un gruppo $(G, \cdot)$ è un semigruppò dotato di elemento unitario, in cui tutti gli elementi sono invertibili, esplicitamente:

$$G \neq \emptyset$$

$$\cdot : G \times G \longrightarrow G$$

$$\forall a, b, c \in G \quad (ab)c = a(bc)$$

$$\exists e \in G : \forall a \in G \quad ae = ea = a$$

$$\forall a \in G \quad \exists a^{-1} \in G : aa^{-1} = a^{-1}a = e$$

Se vale la proprietà commutativa, il gruppo viene detto *abeliano*:

$$\forall a, b \in G \quad ab = ba$$

Definition 1.11. In un gruppo $(G, \cdot)$, possiamo estendere la potenza definita nei semigruppò:

$$a^{-n} = (a^n)^{-1} = (a^{-1})^n, \quad n \in \mathbb{N}$$

quindi, in generale, è ben definito l'elemento a^z , $z \in \mathbb{Z}$.

1. Dimostriamo che $(a^n)^{-1} = (a^{-1})^n$

l'inverso di a^n e' proprio $(a^{-1})^n$, infatti,

$$a^n(a^{-1})^n = \underbrace{a \cdots a}_{n \text{ volte}} \underbrace{a^{-1} \cdots a^{-1}}_{n \text{ volte}} = \mathbf{e}$$

Proposition 1.12. *Valgono le seguenti proprieta':*

$$\begin{aligned} a^m \cdot a^n &= a^{m+n}, \quad m, n \in \mathbb{Z} \\ (a^m)^n &= a^{mn} \\ (ab)^{-1} &= b^{-1}a^{-1} \end{aligned}$$

Proof:

$$abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = \mathbf{e} \Leftrightarrow (b^{-1}a^{-1}) \text{ e' l'inverso di } ab$$

Proposition 1.13. *Valgono le leggi di cancellazione (a sinistra e a destra) in un qualsiasi gruppo:*

$$\begin{aligned} ab = ac &\Rightarrow b = c \\ ba = ca &\Rightarrow b = c \end{aligned}$$

Proof:

$$\begin{aligned} ab = ac &\Rightarrow a^{-1}ab = a^{-1}ac \Leftrightarrow eb = ec \Leftrightarrow b = c \\ ba = ca &\Rightarrow baa^{-1} = caa^{-1} \Leftrightarrow be = ce \Leftrightarrow c = b \end{aligned}$$

Theorem 1.14. *Se $(S, \cdot)$ e' un semigrupp finito, in cui valgono le due leggi di cancellazione, allora $(S, \cdot)$ e' anche un gruppo.*

Proof:

1. Prima di tutto troviamo l'elemento unitario $\mathbf{e}$

Poiche' S e' finito, possiamo scrivere

$$S = \{a_1, a_2, \dots, a_n \mid n \in \mathbb{N}\}$$

Fissiamo $a \in S$ e consideriamo l'insieme

$$S_a = \{aa_1, aa_2, \dots, aa_n\}$$

Gli elementi di S_a sono a due a due distinti: se cosi' non fosse esisterebbero $a_i, a_j \in S : a_i \neq a_j$, $aa_i = aa_j$, ma per la legge di cancellazione, $a_i = a_j$, assurdo. Quindi, $|S_a| = |S|$ e in definitiva,

$$\begin{cases} S_a \subseteq S \\ |S_a| = |S| \\ \forall a_i, a_j \in S : a_i \neq a_j \implies aa_i \neq aa_j \end{cases} \Rightarrow S_a = S$$

Analogamente si ha ${}_a S = \{a_1a, a_2a, \dots, a_na\} = S$.

Procediamo:

$$a \in S \Leftrightarrow a \in {}_a S, S_a \Leftrightarrow a = aa_i = a_j a \quad (1)$$

$$\forall b \in S \quad b = a\bar{a}_i = \bar{a}_j a \quad (2)$$

$$(1) \quad \underbrace{\Rightarrow}_{\text{molt. membro a mebro}} \quad a\bar{a}_i = a_j \underbrace{a\bar{a}_i}_b = a_j b \quad (3)$$

$$(2), (3) \Rightarrow b = a\bar{a}_i = a_j b \Leftrightarrow b = a_j b$$

$$(1), (2) \Rightarrow b = \bar{a}_j a = \underbrace{\bar{a}_j a}_b a_i = ba_i$$

$$\Rightarrow b = ba_i$$

$$\forall b \in S \quad b = ba_i = a_j b \quad (4)$$

Ci resta da far vedere che $a_i = a_j$:

$$(4) \Rightarrow a_j a_i = a_i$$

$$(4) \Rightarrow a_j a_i = a_j$$

$$a_i = a_j$$

quindi $a_i = a_j = \mathbf{e}$ e' il nostro elemento neutro.

2. Dimostriamo che G e' un gruppo

Allora, $\mathbf{e} \in S = S_a \Rightarrow \exists a_i \in S : \mathbf{e} = aa_i \quad (1)$. Analogamente, se avessimo moltiplicato a destra gli elementi di S per a , avremmo trovato che $\mathbf{e} = a_k a \quad (2)$. Da questo segue:

$$\mathbf{e} a_i \underbrace{=}_{(2)} a_k a a_i \underbrace{=}_{(1)} a_k \mathbf{e} \Leftrightarrow a_i = a_k =: a^{-1}$$

Percio', ogni elemento e' invertibile.

3. Esempio

In $(\mathbb{N}, +)$ valgono le leggi di cancellazione, ma di certo non e' un gruppo, quindi $\mathbb{N}$ e' infinito.

Example 1.15.

$$(\mathbb{N}, \cdot), (\mathbb{Z}, \cdot), (\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$$

sono tutti gruppi abeliani, pero' e' difficile estrarre da essi gruppi finiti, infatti se prendiamo un elemento $a \in G$ deve poi esistere $a \cdot a$, e poi ancora $a \cdot a \cdot a$. Da $\mathbb{Z}$ possiamo estrarre $\{-1, 0, 1\}$.

Example 1.16. Un gruppo finito estratto da $(\mathbb{C}, \cdot)$ sono le radici n-esime dell'unita': $U_n = \{x \in \mathbb{C} \mid x^n = 1\}$.

1. Dimostriamo che e' un gruppo

Intanto, elenchiamo le radici n -esime:

$$\begin{aligned}x_0 &= 1 \\x_1 &= \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \\x_2 &= \cos \frac{4\pi}{n} + i \sin \frac{4\pi}{n} = x_1^2 \\x_3 &= \cos \frac{6\pi}{n} + i \sin \frac{6\pi}{n} = x_1^3 \\&\dots \\x_k &= x_1^k \\x_n &= \cos \frac{2\pi}{1} + i \sin \frac{2\pi}{1} = 1 = x_0\end{aligned}$$

1. $\cdot$ e' un'operazione:

$$\begin{aligned}x, y \in U_n &\Leftrightarrow x_i = x = x_1^i, y = x_1^j \\x \cdot y &= x_1^i \cdot x_1^j = x_1^{i+j} \in U_n\end{aligned}$$

2. $\cdot$ e' associativa: lo e' in $\mathbb{C}$, e quindi a maggior ragione in U_n

3. L'elemento neutro e' $x_0 = 1$

4. Poiche' il semigruppino fin qui definito e' finito, per il thm [1.14,pg.3], U_n e' un gruppo. Od anche:

$$\begin{aligned}x_i \in U_j &\text{ ha l'inverso in } \mathbb{C}: \frac{1}{x_i}, \text{ che e' l'inverso in } U_n: \\x_i^n &= 1 \Rightarrow \left(\frac{1}{x_i}\right)^n = 1; \quad \frac{x_i}{x_i} = 1 = x_0\end{aligned}$$

Example 1.17. $(\mathbb{Z}_n, +)$ e' un gruppo finito abeliano.

$(\mathbb{Z}_n, \cdot)$ non e' in generale un gruppo finito abeliano (non tutti gli elementi hanno un inverso). Se consideriamo pero' $(U(\mathbb{Z}_n), \cdot)$ ne otteniamo uno, dove

$$U(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\}$$

Si ha $|U(\mathbb{Z}_n)| = \varphi(n)$ dove, φ e' la funzione di Eulero.

Example 1.18. Adesso vediamo dei gruppi non abeliani.

1. gruppo lineare generale: $(GL_n(\mathbb{R}), \cdot)$, dove

$$GL_n(\mathbb{R}) = \{M^{n \times n}(\mathbb{R}) \text{ matrice} \mid \det M \neq 0\}$$

2. gruppo speciale lineare: $(SL_n(\mathbb{R}), \cdot)$, dove

$$GL_n(\mathbb{R}) = \{M^{n \times n}(\mathbb{R}) \text{ matrice} \mid \det M = 1\}$$

Per verificare che e' un gruppo, basta ricordarsi che

$$\det(M^{-1}) = (\det M)^{-1}$$

3. gruppo ortogonale: $(O_n(\mathbb{R}), \cdot)$, dove

$$O_n(\mathbb{R}) = \{M^{n \times n}(\mathbb{R}) \text{ matrice} \mid M^t M = I^{n \times n} \Leftrightarrow {}^t M = M^{-1}\}$$

Qui stiamo trattando le matrici ortogonali (vedi [AL,7.13.1,pg.50]).
Verifichiamo che $\cdot$ e' una operazione:

$$\begin{aligned} M, N \in O_n &\Leftrightarrow {}^tM = M^{-1}, {}^tN = N^{-1} \\ {}^t(MN) &= {}^tN {}^tM = N^{-1} M^{-1} = (MN)^{-1} \Leftrightarrow {}^t(MN) = (MN)^{-1} \Leftrightarrow MN \in O \end{aligned}$$

4. gruppo ortogonale speciale:

$$\begin{aligned} SO_n(\mathbb{R}) &= \{M^{n \times n}(\mathbb{R}) \text{ matrice} \mid {}^tM = M^{-1}, \det M = 1\} \\ O_n(\mathbb{R}) \setminus SO_n(\mathbb{R}) &= \{M^{n \times n}(\mathbb{R}) \text{ matrice} \mid {}^tM = M^{-1}, \det M = -1\} \end{aligned}$$

SO_n e' un sottogruppo di O_n . SO_n sono le rotazioni, mentre $O_n(\mathbb{R}) \setminus SO_n(\mathbb{R})$ i ribaltamenti (nota ²)

Imponendo le condizioni, si vede che l'elemento generale di SO e'

$$M = \begin{pmatrix} \cos \vartheta & \sin \vartheta \\ -\sin \vartheta & \cos \vartheta \end{pmatrix}$$

Proof:

$$\begin{aligned} M &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \\ \begin{cases} \det M = 1 \Leftrightarrow ad - bc = 1 \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \end{cases} &\Leftrightarrow \begin{cases} ad - bc = 1 \\ a^2 + b^2 = 1 \\ ac + bd = 0 \\ c^2 + d^2 = 1 \end{cases} \\ \begin{cases} a = \cos \vartheta, \quad b = \sin \vartheta \\ c = \cos \varphi, \quad d = \sin \varphi \\ -\cos \vartheta \sin \varphi + \sin \vartheta \cos \varphi = -1 \Leftrightarrow \sin(\vartheta - \varphi) = -1 \\ \cos \vartheta \cos \varphi + \sin \vartheta \sin \varphi = 0 \Leftrightarrow \cos(\vartheta - \varphi) = 0 \end{cases} & \\ \Rightarrow \vartheta - \varphi = -\frac{\pi}{2} \Leftrightarrow \varphi = \vartheta + \frac{\pi}{2} & \\ \begin{cases} a = \cos \vartheta, \quad b = \sin \vartheta \\ c = -\sin \vartheta, \quad d = \cos \vartheta \end{cases} & \end{aligned}$$

□

1.1 Gruppi e sottogruppi ciclici

Definition 1.19. Dato il gruppo $(G, \cdot)$, e il sottoinsieme $H \subseteq G$, $H \neq \emptyset$

$$H \leq G \Leftrightarrow H \text{ e' un sottogruppo di } G \Leftrightarrow (H, \cdot) \text{ e' un gruppo}$$

Proposition 1.20. Dato il gruppo $(G, \cdot)$, e $H \subseteq G$, si ha

$$H \leq G \Leftrightarrow \begin{cases} 1. \quad \forall a, b \in H, \quad a \cdot b \in H \\ 2. \quad e \in H \\ 3. \quad \forall a \in H \quad \exists a^{-1} \in H \end{cases}$$

² $O_n(\mathbb{R}) \setminus SO_n(\mathbb{R})$ non e' un gruppo: I non ci sta' perche' $\det I = 1$

Nota: nella seconda condizione, $\mathbf{e}$ indica l'elemento neutro di G . Nella terza condizione, a^{-1} indica l'inverso di a in G , ovvero $a^{-1}a = aa^{-1} = \mathbf{e}$.

Proof:

1. Dim $\Rightarrow$

Intanto, H essendo un gruppo, non è un insieme vuoto.

Per definizione, la 1. è vera.

Poiché H è un gruppo,

$$\exists \mathbf{e}_h \in H : \forall a \in H \quad \mathbf{e}_h a = a \mathbf{e}_h = a \quad (1)$$

sia $\mathbf{e}$ l'elemento unita' di G . Si ha che $\mathbf{e}_h = \mathbf{e}$, infatti,

$$\mathbf{e}_h \mathbf{e}_h = \mathbf{e}_h$$

$$\mathbf{e}_h^{-1} \mathbf{e}_h \mathbf{e}_h = \mathbf{e}_h^{-1} \mathbf{e}_h$$

$$\mathbf{e} \mathbf{e}_h = \mathbf{e}$$

$$H \ni \mathbf{e}_h = \mathbf{e} \Rightarrow \mathbf{e} \in H$$

quindi la 2. è vera.

Dim. la 3.: sia $a \in H$, sia a_1 l'inverso di a in H e a_2 l'inverso di a in G ,

$$aa_1 = \mathbf{e}_h = \mathbf{e} = aa_2 \Leftrightarrow \underbrace{a_1}_{\in H} = a_2 \in H$$

2. Dim $\Leftarrow$

$$H \neq \emptyset$$

$$\mathbf{e} \in H \Rightarrow H \neq \emptyset$$

$$\cdot : H \times H \longrightarrow H$$

per la 1.

$$\forall a, b, c \in H \quad (ab)c = a(bc)$$

poiché $\cdot$ è la stessa operazione di $(G, \cdot)$, che è un gruppo, e quindi rimane associativa in H

$$\exists \mathbf{e} \in H : \forall a \in H \quad a\mathbf{e} = \mathbf{e}a = a$$

per la 2.

$$\forall a \in H \quad \exists a^{-1} \in H : aa^{-1} = a^{-1}a = \mathbf{e}$$

per la 3.

□

Theorem 1.21. Dato il gruppo $(G, \cdot)$, si ha

$$H \leq G \Leftrightarrow \forall a, b \in H \quad ab^{-1} \in H$$

Proof:

1. Dim $\Rightarrow$

$$\begin{cases} H \leq G \Rightarrow \forall b \in H \quad b^{-1} \in H \\ H \leq G \Rightarrow \forall a, c \in H \quad a \cdot c \in H \end{cases} \Rightarrow ab^{-1} \in H$$

2. Dim $\Leftarrow$

$$H_p \Rightarrow bb^{-1} = \mathbf{e} \in H \quad (1)$$

$$H_p, (1) \Rightarrow \mathbf{e}b^{-1} = b^{-1} \in H \quad (2)$$

$$H_p, (2) \Rightarrow \forall a, b^{-1} \in H \quad ab^{-1} = ab \in H$$

Quindi, per [1.20,pg.6], H e' un sottogruppo di G

□

Proposition 1.22. *Caratterizzazione dei sottogruppi finiti.*

Dato il gruppo $(G, \cdot)$, e $S \subseteq G$, $|S| \in \mathbb{N}$, si ha

$$S \leq G \Leftrightarrow \forall a, b \in S \quad ab \in S$$

Proof:

1. $\text{Dim} \Rightarrow$

Per definizione.

2. $\text{Dim} \Leftarrow$

L'Hp equivale a dire che S e' un semigruppato ($\cdot$ e' associativa perche' lo e' in $(G, \cdot)$). Inoltre, per S valgono le due leggi di cancellazione, perche' valgono per G . Allora, per il thm [1.14,pg.3], S e' un gruppo, ed essendo $S \subseteq G$, possiamo affermare che $S \leq G$

□

Proposition 1.23. *Sia dato il gruppo finito G , si ha*

$$\begin{cases} H \leq G \\ |H| = |G| \end{cases} \Rightarrow H = G$$

Proof: $H \leq G \Rightarrow H \subseteq G$, quindi basta dimostrare $G \subseteq H$.

$$|G| = |G \setminus H \cup H| \underset{G \setminus H \cap H = \emptyset}{=} |G \setminus H| + |H| = |G \setminus H| + |G| \Leftrightarrow |G \setminus H| = 0 \Leftrightarrow G \setminus H = \emptyset \Leftrightarrow G \subseteq H$$

□

Definition 1.24. Il seguente sottogruppo si chiama *centro* di G :

$$Z(G) = \{g \in G \mid gx = xg \quad \forall x \in G\}$$

ed e' in sostanza, l'insieme di tutti gli elementi di G che commutano con tutti gli elementi di G .

Il sottogruppo

$$C(G, x) = \{g \in G \mid gx = xg\}$$

si chiama *centralizzante* di x , ed e' in sostanza, l'insieme di tutti gli elementi di G che commutano con x .

E' chiaro che

$$Z(G) \subseteq C(G, x)$$

Proof:

1. Dimostriamo che $Z(G)$ e' un sottogruppo usando la caratterizzazione [1.21,pg.7]

Siano $x, y \in Z(G)$,

$$y^{-1}g = (g^{-1}y)^{-1} \underset{y \in Z}{=} (yg^{-1})^{-1} = gy^{-1} \Rightarrow y^{-1} \in Z$$

$$xy^{-1}g \underset{y^{-1} \in Z}{=} xgy^{-1} \underset{x \in Z}{=} gxy^{-1} \Rightarrow xy^{-1} \in Z$$

Quindi $Z(G)$ e' un sottogruppo di G .

2. Dimostriamo che $C(G, x) \leq G$

$$\begin{aligned}
a, b \in C(x) &\Rightarrow ax = xa, bx = xb \\
(ab^{-1})x &= x(ab^{-1}) \Leftrightarrow ab^{-1}xba^{-1}x^{-1} = \mathbf{e} \Leftrightarrow \\
&\Leftrightarrow \underbrace{a}_{xb=bx} \underbrace{b^{-1}b}_{=\mathbf{e}} xa^{-1}x^{-1} = \mathbf{e} \Leftrightarrow \\
&\Leftrightarrow axa^{-1}x^{-1} = \mathbf{e} \Leftrightarrow \underbrace{xx^{-1}}_{ax=xa} = \mathbf{e} \Leftrightarrow \mathbf{e} = \mathbf{e}
\end{aligned}$$

Quindi $(ab^{-1})x = x(ab^{-1})$ e' vera.

Allora, $ab^{-1} \in C(G, x)$.

□

Proposition 1.25. Dato il gruppo $(G, \cdot)$

$$H, J \leq G \Rightarrow H \cap J \leq G$$

Proof:

Usiamo la caratterizzazione [1.21,pg.7]: siano $a, b \in H \cap J$

$$a, b \in H \cap J$$

$$\begin{cases} a \in H, a \in J \\ b \in H \Rightarrow b^{-1} \in H \\ b \in J \Rightarrow b^{-1} \in J \end{cases} \Rightarrow \begin{cases} ab^{-1} \in H \\ ab^{-1} \in J \end{cases} \Rightarrow ab^{-1} \in H \cap J$$

□

Proposition 1.26. Dato il gruppo $(G, \cdot)$ e $H, J \leq G$,

$$H \cup J \leq G \Leftrightarrow H \subseteq J \vee J \subseteq H$$

Proof:

1. Dim $\Leftarrow$

$$H \subseteq J \vee J \subseteq H \Rightarrow H \cup J = J \leq G \vee H \cup J = H \leq G$$

2. Dim $\Rightarrow$

Procediamo dimostrando la contronominale, cioe'

$$H \cup J \not\leq G \Leftarrow H \not\subseteq J \wedge J \not\subseteq H$$

Allora,

$$H \not\subseteq J \wedge J \not\subseteq H \Rightarrow \begin{cases} \exists a \in H, a \notin J \\ \exists b \in J, b \notin H \end{cases} \Rightarrow a, b \in H \cup J$$

Se per assurdo $ab \in H \cup J$ si avrebbe:

CASE: $ab = c \in H$

$$b = \underbrace{a^{-1}}_{\in H} \underbrace{c}_{\in H} \Rightarrow b \in H$$

assurdo contro $b \notin H$.

CASE: $ab = c \in J$

$$a = c \underbrace{b^{-1}}_{\in J} \Rightarrow a \in J$$

assurdo contro $a \notin J$.

□

Definition 1.27. Dato un gruppo $(G, \cdot)$ e un suo sottoinsieme X , si definisce $\langle X \rangle$ come il piu' piccolo sottogruppo di G contenente X , ovvero:

$$\exists H \leq G : X \subseteq H \Rightarrow \langle X \rangle \subseteq H$$

Proposition 1.28.

$$\langle X \rangle = \bigcap_{X \subseteq H \leq G} H$$

Proof:

Prima di tutto osserviamo che per la prop [1.25,pg.9] si ha $\langle X \rangle \leq G$. Dimostriamo che e' il piu' piccolo: supponiamo $X \subseteq H'$.

$$X \subseteq H' \Rightarrow H' \in \{H \leq G \mid X \subseteq H\} \Rightarrow \left(\bigcap_{X \subseteq H \leq G} H \right) \subseteq H' \Leftrightarrow \langle X \rangle \subseteq H'$$

□

Theorem 1.29.

$$\langle X \rangle = \{t_1 t_2 \dots t_r \mid t_i \in X \vee t_i^{-1} \in X, r \in \mathbb{N}\} = \{t_1^{z_1} t_2^{z_2} \dots t_r^{z_r} \mid t_i \in X, z_i \in \mathbb{Z}, r \in \mathbb{N}^*\}$$

o in forma equivalente se X e' finito:

$$X = \{x_1, x_2, \dots, x_n\}$$

$$\langle X \rangle = \left\{ (x_1^{m_{11}} x_2^{m_{21}} \dots x_n^{m_{n1}}) (x_1^{m_{12}} x_2^{m_{22}} \dots x_n^{m_{n2}}) \dots (x_1^{m_{1r}} x_2^{m_{2r}} \dots x_n^{m_{nr}}) \mid m_{1i}, m_{2i}, \dots, m_{ni} \in \mathbb{Z}, \right. \\ \left. i = 1, \dots, r, r = 1, 2, \dots \right\}$$

se l'elemento x_1 ha ordine finito, allora il suo esponente m_{1i} variera' variera' da 0 a $o(x_1) - 1$ (definiremo l'ordine piu' avanti (vedi [1.32,pg.11])).

Proof: Poniamo $Y := \{t_1 t_2 \dots t_r \mid t_i \in X \vee t_i^{-1} \in X, r \in \mathbb{N}\}$

1. Dim. $Y \leq G$ usando la caratterizzazione [1.21,pg.7]

Siano $a, b \in Y$

$$a \in Y \Leftrightarrow \exists r \in \mathbb{N} : a = t_1 t_2 \dots t_r$$

$$b \in Y \Leftrightarrow \exists s \in \mathbb{N} : b = u_1 u_2 \dots u_s$$

$$b^{-1} = (u_1 u_2 \dots u_s)^{-1} = u_s^{-1} u_{s-1}^{-1} \dots u_1^{-1}$$

$$ab^{-1} = t_1 t_2 \dots t_r u_s^{-1} u_{s-1}^{-1} \dots u_1^{-1} \Rightarrow ab^{-1} \in Y$$

2. Dim che Y e' il piu' piccolo sottogruppo contenente X

Sia $X \subseteq Z \leq G$. Prendiamo $a \in Y$,

$$a \in Y \Leftrightarrow \exists r \in \mathbb{N} : a = t_1 t_2 \dots t_r$$

$$\begin{cases} X \subseteq Z \\ t_i \in X \vee t_i^{-1} \in X, \forall 1 \leq i \leq r \\ Z \leq G \end{cases} \Rightarrow \text{un qualsiasi prodotto } t_i t_j \in Z \forall 1 \leq i, j \leq r \Rightarrow a \in Z \Rightarrow Y \subseteq Z$$

□

Example 1.30.

1. $\langle \emptyset \rangle = \{\mathbf{e}\}$

Proof: per def: tutti i sottogruppi contengono $\emptyset$, quindi il piu' piccolo e' $\{\mathbf{e}\}$.

2. In $(\mathbb{Z}, +)$, il sottogruppo generato $\langle 2, 3 \rangle$ e'

$$\langle 2, 3 \rangle = \{2s + 3t \mid s, t \in \mathbb{Z}\}$$

infatti, per la proposizione di prima,

$$\langle 2, 3 \rangle = \{2 \cdot 3, 2 \cdot 2 \cdot 3, 2 \cdot 3 \cdot 3, 2 \cdot 3 \cdot 2 \cdot 2, \dots, \}$$

inoltre, $(\mathbb{Z}, +)$ e' abeliano, e quindi i 2 e 3 si possono *raccogliere*.

Definition 1.31. Dato $(G, \cdot)$, $g \in G$,

$$\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$$

inoltre, $\langle g \rangle$ verra' chiamato sottogruppo ciclico generato da g .
 $\langle g \rangle$ potra' essere un sottogruppo ciclico finito o infinito:
 e' infinito nel caso in cui esiste una corrispondenza biunivoca tra $\langle g \rangle$ e $\mathbb{Z}$, ovvero

$$\forall i, j \in \mathbb{Z} : i \neq j \text{ si ha } g^i \neq g^j$$

e' invece finito quando

$$\exists i, j \in \mathbb{Z} : i \neq j \text{ } g^i = g^j$$

Proof: E' facile rendersi conto con la prop. [1.29,pg.10] che

$$\langle g \rangle = \{g^i \mid i \in \mathbb{Z}\}$$

.

Definition 1.32. Dato $(G, \cdot)$, $g \in G$,

$o(g)$, chiamato *ordine o periodo di g*, e' (se esiste) il piu' piccolo intero $p > 0$ t.c. $g^p = \mathbf{e}$

se p non esiste si pone $o(g) = \infty$.

La cardinalita' di un gruppo finito e' chiamata sempre *ordine*: $o(G) = |G|$.

Example 1.33. In $(\mathbb{C}^*, \cdot)$,

$$(i) = \{1, i, -1, -i\}, \quad o(i) = 4$$

Theorem 1.34. Dato $(G, \cdot)$, $g \in G$ si ha

$$o(g) = |\langle g \rangle|$$

Proof: Distinguiamo due casi.

CASE: $o(g) = \infty$

$$o(g) = \infty \Rightarrow \forall p \in \mathbb{Z}_{>0} : g^p \neq \mathbf{e} \quad (*)$$

$$\text{sia } i, j \in \mathbb{Z} : i > j \Leftrightarrow i - j > 0, \quad \underbrace{\Rightarrow}_{(*)} g^{i-j} \neq \mathbf{e} \Leftrightarrow g^i g^{-j} \neq \mathbf{e} \Leftrightarrow g^i \neq g^j$$

$$\forall i, j \in \mathbb{Z} : i \neq j \text{ } g^i \neq g^j$$

ovvero, $\langle g \rangle$ e' infinito (in relazione biunivoca con $\mathbb{Z}$).

CASE: $o(g) = p$

Vogliamo dimostrare che

$$\langle g \rangle = \{g^0, g^1, \dots, g^{p-1}\}$$

poniamo $H := \{g^0, g^1, \dots, g^{p-1}\}$,

0.1. Dim. che $\forall i, j \in \mathbb{Z}_{\geq 0} : 0 \leq j < i < p, i \neq j$ si ha $g^i \neq g^j$, ovvero gli elementi di H sono a due a due distinti. Così facendo, mostreremo che $|H| = p$

Supponiamo per assurdo che $g^i = g^j$

$$g^i = g^j \Leftrightarrow g^{i-j} = \mathbf{e}$$

$$j < i < p \Rightarrow 0 < i - j < p - j < p \Rightarrow i - j < p$$

assurdo, perché $i - j < p$ e p è il periodo, quindi il più piccolo intero positivo t.c. $g^p = \mathbf{e}$.

0.2. Dim. che $\langle g \rangle = H$

Di sicuro $H \subseteq \langle g \rangle$.

Prendiamo $a \in \langle g \rangle \Leftrightarrow a = g^i, i \in \mathbb{Z}$. Utilizziamo l'algoritmo di divisione: $\exists! q, r \in \mathbb{Z} : i = qp + r, 0 \leq r < p$.

$$g^i = g^{qp+r} = g^{qp} g^r = (g^p)^q g^r = \mathbf{e}^q g^r = g^r \quad (**)$$

$$0 \leq r < p, (**) \Rightarrow g^i \in H$$

□

Proposition 1.35. Se $\langle g \rangle$ è un sottogruppo ciclico finito di G , di ordine p , si ha

$$g^i = g^j \Leftrightarrow i = j \quad (\mathbb{Z}_p)$$

Proof:

1. Dim $\Rightarrow$

$$g^i = g^j \Leftrightarrow g^{i-j} = \mathbf{e}$$

$$\exists! q, r : i - j = pq + r, 0 \leq r < p$$

$$\mathbf{e} = g^{i-j} = g^{pq+r} = (g^p)^q g^r = g^r \Rightarrow g^r = \mathbf{e} \Leftrightarrow r = 0$$

$$i - j = pq + r = pq \Rightarrow i = j \quad (\mathbb{Z}_p)$$

2. Dim $\Leftarrow$

$$i = j \quad (\mathbb{Z}_p) \Leftrightarrow i - j = kp \Rightarrow g^{i-j} = g^{kp} \Rightarrow g^{i-j} = \mathbf{e} \Rightarrow g^i = g^j$$

□

Corollary 1.36. Dalla precedente proposizione, con $p = o(g)$, si ha:

$$1. g^i = \mathbf{e} \Leftrightarrow p \mid i$$

$$\textbf{Proof: } g^i = \mathbf{e} = g^p \Leftrightarrow i = p = 0 \quad (\mathbb{Z}_p) \Leftrightarrow i = pq \Leftrightarrow p \mid i$$

$$2. (a^i)^{-1} = a^{p-i}$$

$$\textbf{Proof: } a^{i-1} = a^{-i} \underbrace{=}_{-i=p-i \quad \mathbb{Z}_p} a^{p-i}$$

Proposition 1.37. Dato $(G, \cdot)$ gruppo **abeliano**, si ha

$$G_f = (\{g \in G \mid o(g) \in \mathbb{N}\}, \cdot) \leq G$$

Proof:

Usiamo la caratterizzazione [1.21,pg.7]:

$$a, b \in G_f \Leftrightarrow a, b \in G \wedge p = o(a), q = o(b) \in \mathbb{N} : \\ (ab^{-1})^{qp} \underbrace{=}_{\text{per l'abelianita'}} (a^p)^q b^{-qp} = (b^q)^{-p} = \mathbf{e} \Rightarrow o(ab^{-1}) < qp$$

Nota³

Definition 1.38. Un gruppo $(G, \cdot)$ si dice ciclico $\Leftrightarrow \exists g \in G : G = \langle g \rangle$

Theorem 1.39.

$$(G, \cdot) \text{ gruppo ciclico} \Rightarrow H \leq G \text{ e' pure un gruppo ciclico} \\ \Leftrightarrow$$

Piu' in dettaglio, se $G = \langle g \rangle$, allora $H = \langle g^m \rangle$ con $m = \min \{t \in \mathbb{N}^ \mid g^t \in H\}$*

Proof:

1. Dim $\Rightarrow$

Se $H = \{\mathbf{e}\}$, allora la tesi e' vera. Supponiamo che $\{\mathbf{e}\} \subset H$ e consideriamo i seguenti insiemi:

$$T = \{t \in \mathbb{N} \mid g^t \in H\} \\ T^* = T \setminus \{0\}$$

1.1. Dim $T \neq \emptyset$

$$(G, \cdot) \text{ gruppo ciclico} \Rightarrow \exists g \in G : G = \langle g \rangle \\ h \in H \setminus \{\mathbf{e}\} \subseteq G \Rightarrow h = g^i \in H \Rightarrow g^{-i} \in H \\ \max \{i, -i\} = t \in \mathbb{N} \\ g^t \in H \Rightarrow t \in T$$

Sia $m = \min T^*$, che esiste perche' $\mathbb{N}$ e' ben ordinato.

1.2. Dim $\langle g^m \rangle = H$

$\langle g^m \rangle \subseteq H$ e' vera perche' $g^m \in H$ e quindi $(g^m)^k \in H$.

Sia $g^j \in H$. Per dimostrare che $H = \langle g^m \rangle$ bastera' vedere che $g^j = (g^m)^q = g^{mq}$.

Dividiamo j per m :

$$j = mq + r, 0 \leq r < m \quad (*) \\ g^j = g^{mq} g^r \Leftrightarrow g^r = \underbrace{g^j}_{\in H} \underbrace{(g^m)^{-q}}_{\in H} \in H \Rightarrow g^r \in H \Rightarrow r \in T$$

$$r \in T \Rightarrow r = 0$$

allora, $r = 0$, altrimenti dalla (*) si avrebbe un assurdo contrario al fatto che $m = \min T$.

In definitiva,

$$g^j = g^{mq} = (g^m)^q \Rightarrow g^j \in \langle g^m \rangle$$

□

Proposition 1.40.

$$(G, \cdot) \text{ gruppo ciclico} \Rightarrow G \text{ gruppo abeliano}$$

Non vale il viceversa.

Proof:

³In un gruppo non abeliano $(ab)^2 = abab$, in uno abeliano $(ab)^2 = a^2b^2$

1. Dim $\Rightarrow$

$(G, \cdot)$ gruppo ciclico $\Rightarrow \exists g \in G : G = \langle g \rangle$
siano $a, b \in G$. vogliamo dimostrare che $ab = ba$
 $a, b \in G = \langle g \rangle \Rightarrow a = g^i, b = g^j$
 $ab = g^i g^j = g^{i+j} = g^{j+i} = g^j g^i = ba$

2. Dim $\Leftarrow$

Consideriamo il seguente gruppo abeliano:

$$(G = \{0, 1, 2, 3\}, \cdot)$$

$\cdot$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Quindi $e = 0$, e $a^{-1} = a \quad \forall a \in G$.

L'ordine di ogni elemento e' 2, ma $|G| = 4$, quindi per la prop [1.41,pg.14] G non e' ciclico. $\square$

Proposition 1.41. *Caratterizzazione dei gruppi ciclici finiti.*

Dato il gruppo $(G, \cdot)$, $|G| = n$,

$$g \in G, \quad o(g) = n \Leftrightarrow G = \langle g \rangle$$

Proof:

1. Dim $\Leftarrow$

$$|\langle g \rangle| = |G| = n \quad \underbrace{\Rightarrow}_{[1.34,pg.11]} \quad o(g) = n$$

2. Dim $\Rightarrow$

$$\begin{cases} \langle g \rangle \leq G \Rightarrow \langle g \rangle \subseteq G \\ |\langle g \rangle| = |G| \in \mathbb{N} \end{cases} \Rightarrow \langle g \rangle = G$$

$\square$

Theorem 1.42. *Dato il gruppo ciclico $G = \langle g \rangle$, $|G| = n$,*

$$1. \quad S \leq G \Rightarrow |S| \mid n$$

Ovvero, se S e' un sottogruppo di G allora, il suo ordine divide l'ordine di G

$$2. \quad m \in \mathbb{N}, \quad m \mid n \Rightarrow \exists! S \leq G : |S| = m, \quad \text{inoltre } S = \langle g^{\frac{n}{m}} \rangle$$

Proof:

1. Dim 1.

(Nota ⁴)

$$\begin{aligned}
S \leq G & \underbrace{\Rightarrow}_{\text{thm [1.39,pg.13]}} S = \langle g^i \rangle, \quad i = \min T^* \\
|G| = n \Leftrightarrow |\langle g \rangle| = n & \underbrace{\Rightarrow}_{[1.34,pg.11]} o(g) = n \Rightarrow g^n = \mathbf{e} \\
(g^i)^n = (g^n)^i = \mathbf{e} = \mathbf{e} & \underbrace{\Rightarrow}_{\text{cor [1.36,pg.12]}} o(g^i) \Big/ n \underbrace{\Leftrightarrow}_{[1.34,pg.11]} |S| \Big/ n
\end{aligned}$$

2. Dim 2.

Sia $S = \langle g^{\frac{n}{m}} \rangle$

$|S| = m$, infatti,

$$(g^{\frac{n}{m}})^i = g^{\frac{n}{m}i} = \mathbf{e} \Leftrightarrow \frac{n}{m}i = 0 \mathbb{Z}_n \Leftrightarrow \frac{n}{m}i = \lambda n \Leftrightarrow i = \lambda m$$

quindi, il piu' piccolo $i > 0$: $(g^{\frac{n}{m}})^i = \mathbf{e}$ e' m , ovvero, $o(g^{\frac{n}{m}}) = |S| = m$

Dim che S e' unico. Supponiamo che $\exists H \leq G, |H| = m$.

$$\begin{aligned}
H \leq G & \underbrace{\Rightarrow}_{\text{thm [1.39,pg.13]}} H = \langle g^i \rangle, \quad i = \min T^* \\
|H| = m & \underbrace{\Rightarrow}_{[1.34,pg.11]} o(g^i) = m \Leftrightarrow (g^i)^m = \mathbf{e} \\
g^{im} = \mathbf{e} & \underbrace{\Rightarrow}_{\text{cor [1.36,pg.12]}} o(g) \Big/ mi \Leftrightarrow n \Big/ mi \Leftrightarrow nk = mi \Leftrightarrow i = \frac{n}{m}k \\
& \Rightarrow g^i = g^{\frac{n}{m}k} = (g^{\frac{n}{m}})^k \Rightarrow g^i \in (g^{\frac{n}{m}}) = S \\
& \text{quindi } H \subseteq S. \text{ Poiche' pero' } |H| = |S| = m, \text{ si ha } H = S.
\end{aligned}$$

□

Corollary 1.43. *Dato G ciclico,*

$$\begin{aligned}
\{S \leq G\} & \xleftrightarrow{f} \left\{ m \in \mathbb{Z} \mid m \Big/ n \right\} \\
& \text{con } f \text{ biunivoca}
\end{aligned}$$

Ovvero, i sottogruppi di G e i divisori del suo ordine, sono in relazione biunivoca. f e' proprio $f(S) = |S|$

Proof: Immediata conseguenza del thm [1.42,pg.14].

Theorem 1.44. *Dato un gruppo ciclico $G = \langle g \rangle$ di ordine $|G| = n$, si ha*

$$o(g^m) = \frac{n}{(m, n)}$$

dove $(m, n) = \text{MCD}(m, n)$.

Proof:

⁴Questo punto che stiamo dimostrando e' un fatto particolare di uno piu' generale: $S \leq G \Rightarrow |S| \Big/ |G|$, anche se G non e' un gruppo ciclico. (vedi il thm di Lagrange [1.53,pg.19])

$$\begin{aligned}
k = o(g^m) = |\langle g^m \rangle| &\quad \underbrace{\Rightarrow}_{thm[1.42,pg.14]} \quad k/n \Leftrightarrow kd' = n \Rightarrow d'/n \\
k &= \frac{n}{d'} \\
\mathbf{e} = (g^m)^k = g^{mk} &\Rightarrow o(g)/mk \Leftrightarrow n/m \frac{n}{d'} \Leftrightarrow n\mu = m \frac{n}{d'} \Leftrightarrow d'\mu = m \Leftrightarrow d'/m
\end{aligned}$$

Quindi d'/m , d'/n , ci resta solo da provare che e' il massimo dei divisori. Sia $d = (m, n)$. Dimostriamo che $d = d'$.

$$\begin{aligned}
&\begin{cases} d = (m, n) \\ d'/m \\ d'/n \end{cases} \Rightarrow d \geq d' \Leftrightarrow \frac{n}{d} \leq \frac{n}{d'} = k \quad (1) \\
(g^m)^{\frac{n}{d}} = (g^n)^{\frac{m}{d}} = \mathbf{e} &\quad \underbrace{\Rightarrow}_{[1.36,pg.12]} \Rightarrow o(g^m)/\frac{n}{d} \Rightarrow o(g^m) \leq \frac{n}{d} \Rightarrow k \leq \frac{n}{d} \quad (2) \\
(1), (2) &\Rightarrow \frac{n}{d} = k \\
\text{Per la (1) l'unica possibilita' che rimane e' l'uguaglianza.} \\
\frac{n}{d} = k &\Leftrightarrow \frac{n}{d} = \frac{n}{d'} \Leftrightarrow d = d' \\
k = o(g^m) &= \frac{n}{(m, n)}
\end{aligned}$$

□

Corollary 1.45. Dato $G = \langle g \rangle$, $|G| = n$,

$$G = \langle g^m \rangle \Leftrightarrow (m, n) = 1$$

Proof:

1. $\text{Dim} \Rightarrow$

$$G = \langle g^m \rangle \Rightarrow |G| = |\langle g^m \rangle| \quad \underbrace{\Rightarrow}_{[1.34,pg.11]} \quad o(g^m) = n \quad \underbrace{\Rightarrow}_{[1.44,pg.15]} \quad n = \frac{n}{(m, n)} \Leftrightarrow 1 = \frac{1}{(m, n)} \Rightarrow (m, n) = 1$$

2. $\text{Dim} \Leftarrow$

$$o(g^m) \quad \underbrace{=}_{[1.44,pg.15]} \quad \frac{n}{(m, n)} = n \quad \underbrace{\Rightarrow}_{[1.41,pg.14]} \quad \langle g^m \rangle = G$$

□

Example 1.46. Tutti i sottogruppi di $(\mathbb{Z}, +)$ sono del tipo $x\mathbb{Z}$ con $x \in \mathbb{Z}$.

$$\begin{aligned}
\mathbb{Z} &= \langle 1 \rangle \\
S \leq \mathbb{Z} &\Rightarrow S = \langle x \cdot 1 \rangle = \langle x \rangle = \{zx \mid z \in \mathbb{Z}\} = x\mathbb{Z}
\end{aligned}$$

1.2 Laterali modulo H

Sia $(G, \cdot)$ un gruppo e $H \leq G$. Definiamo i seguenti insiemi:

$$\begin{aligned} aH &= \{ah \mid h \in H\} \\ Ha &= \{ha \mid h \in H\} \end{aligned}$$

chiamati rispettivamente laterale sinistro e destro di a rispetto ad H .
E' ovvio che nel caso generale $aH \neq Ha$.
Osserviamo che $a \in aH$:

$$H \leq G \Rightarrow \mathbf{e} \in H \Rightarrow a\mathbf{e} = a \in aH$$

Si ha anche:

$$\mathbf{e}H = H$$

Proposition 1.47. *L'insieme*

$$\{aH\}_{a \in G}$$

e' una partizione di G , ovvero

1. $\bigcup_{a \in G} aH = G$
2. *Presi $a, b \in G$*
 $aH \neq bH \Rightarrow aH \cap bH = \emptyset$
o equivalentemente
 $aH = bH \Leftrightarrow aH \cap bH \neq \emptyset$

Proof:

1. Dim 1.

$$\begin{aligned} \forall a \in G \quad a \in aH &\Rightarrow G \subseteq \bigcup_{a \in G} aH \\ ah \in aH, \quad h \in H \leq G &\Rightarrow ah \in G \Rightarrow \left(\bigcup_{a \in G} aH \right) \subseteq G \end{aligned}$$

2. Dim 2.

Siano $a, b \in G$: $aH \cap bH \neq \emptyset$.

$$aH \cap bH \neq \emptyset \Rightarrow \exists c \in aH \cap bH \Leftrightarrow c = ah = bh' \quad (1)$$

2.1. Dim $aH \subseteq bH$

$$\begin{aligned} ah_1 &\in aH \\ ah_1 &\underset{(1)}{=} \underbrace{b}_{\in H} \underbrace{h'h^{-1}h_1}_{\in H} \in bH \end{aligned}$$

2.2. Dim $bH \subseteq aH$

$$\begin{aligned} bh_2 &\in bH \\ bh_2 &\underset{(1)}{=} \underbrace{a}_{\in H} \underbrace{hh'^{-1}h_2}_{\in H} \in aH \end{aligned}$$

□

Definition 1.48. Da ogni partizione nasce la relazione d'equivalenza indotta da essa. Definiamo quindi le seguenti relazioni:

$$\begin{aligned}
a \equiv_s b \ (H) &\Leftrightarrow aH = bH \Leftrightarrow aH \cap bH \neq \emptyset \\
&\Leftrightarrow \exists h_1 \in H \exists h_2 \in H : ah_1 = bh_2, \ h = h_2 h_1^{-1} \in H \\
&\Leftrightarrow a = bh \Leftrightarrow b^{-1}a = h \\
a \equiv_a b \ (H) &\Leftrightarrow Ha = Hb \Leftrightarrow Ha \cap Hb \neq \emptyset \\
&\Leftrightarrow \exists h_1 \in H \exists h_2 \in H : h_1 a = h_2 b, \ h = h_1^{-1} h_2 \in H \\
&\Leftrightarrow a = hb \Leftrightarrow ab^{-1} = h
\end{aligned}$$

rispettivamente chiamate “*a congruo b modulo H a destra*” e “*a congruo b modulo H a sinistra*”

Proposition 1.49.

$$|\{aH\}_{a \in G}| = |\{Ha\}_{a \in G}|$$

ovvero

$$\exists \varphi : \{aH\}_{a \in G} \leftrightarrow \{Ha\}_{a \in G}$$

e precisamente

$$\varphi(aH) = Ha^{-1}$$

Proof:

1. φ e' ben posta: $aH = bH \Rightarrow \varphi(aH) = \varphi(bH)$

$$aH = bH \Leftrightarrow b^{-1}a = h \Leftrightarrow a^{-1}b = h^{-1} = h' \Leftrightarrow a^{-1} = h'b^{-1} \Leftrightarrow Ha^{-1} = Hb^{-1}$$

2. Dim l'inniettivita', ovvero $f(aH) = f(bH) \Rightarrow aH = bH$

$$f(aH) = f(bH) \Leftrightarrow Ha^{-1} = Hb^{-1} \underbrace{\Leftrightarrow}_{[1.48, pg. 18]} a^{-1} = hb^{-1} \Leftrightarrow a = bh^{-1}$$

$$ah' \in aH$$

$$ah' = bh^{-1}h' \in bH$$

$$aH \subseteq bH$$

analogamente per l'altra inclusione (basta scambiare a con b).

3. Dim la suriettività, ovvero $\forall b \in G \ \exists a \in G : \varphi(aH) = Hb$

$$\varphi(aH) = Hb \Leftrightarrow Ha^{-1} = Hb \Leftrightarrow a^{-1} = hb \Leftrightarrow a = b^{-1}h^{-1} \Leftrightarrow aH = b^{-1}H$$

quindi l'incognita cercata e' $b^{-1}H$

□

Definition 1.50. Per la precedente proposizione possiamo definire la seguente quantita':

$$i_G(H) = |\{aH\}_{a \in G}| = |\{Ha\}_{a \in G}|$$

che viene chiamata indice di H in G.

$i_G(H)$ sara' $\leq +\infty$.

Proposition 1.51.

$$i_G(H) = 2 \Rightarrow aH = Ha, \forall a \in G$$

Proof: Poiche' H e' di sicuro una classe, l'altra sara' necessariamente $G \setminus H$. Questo vale sia nel caso sinistro che in quello destro. Allora,

$$\begin{aligned} a \notin H &\Leftrightarrow aH \neq H \quad \underbrace{\Leftrightarrow}_{i_G(H)=2} aH = G \setminus H \\ a \notin H &\Leftrightarrow Ha \neq H \quad \underbrace{=}_{i_G(H)=2} G \setminus H = aH \\ a \in H &\Leftrightarrow aH = H = Ha \end{aligned}$$

Quindi,

$$\forall a \in H \quad aH = Ha$$

Lemma 1.52.

$\forall a \in G \quad |aH| = |H|$, infatti, la seguente mappa e' biettiva:

$$\begin{aligned} \varphi : H &\leftrightarrow aH \\ \varphi(h) &= ah \end{aligned}$$

Proof:

1. Dim φ iniettiva: $\forall h_1, h_2 \in H : h_1 \neq h_2 \Rightarrow \varphi(h_1) \neq \varphi(h_2)$

$$\varphi(h_1) = ah_1$$

$$\varphi(h_2) = ah_2$$

se per assurdo $\varphi(h_1) = \varphi(h_2)$ si avrebbe

$$ah_1 = ah_2 \Leftrightarrow h_1 = h_2$$

assurdo

2. E' surriettiva: $\forall ah \in aH : \exists h \in H : \varphi(h) = ah$

ovviamente

□

1.2.1 Teorema di Lagrange

Theorem 1.53. di Lagrange.

$$(G, \cdot) \text{ gruppo finito, } H \leq G \Rightarrow |G| = |H| \cdot i_G(H)$$

In altre parole, se H e' un qualsiasi sottogruppo di G , allora il suo ordine e indice dividono $|G|$. Attenzione, non vale il viceversa, ovvero se $m \mid |G|$, non necessariamente esiste un sottogruppo di ordine m .

Proof:

Dal lemma [1.52,pg.19], segue che tutti i laterali hanno la stessa cardinalita' di H . Poiche' G e' partizionato da $i_G(H)$ classi, avremo che tutti i suoi elementi sono in numero $|H| \cdot i_G(H)$

□

Proposition 1.54. Dato G di ordine finito,

$$a \in G \Rightarrow o(a) \mid |G|$$

Proof:

$$\begin{aligned} o(a) &\stackrel{[1.34, \text{pg.11}]}{=} |\langle a \rangle| \\ \langle a \rangle \leq G &\stackrel{\text{Lagrange}[1.53, \text{pg.19}]}{\Rightarrow} |\langle a \rangle| / |G| \Leftrightarrow o(a) / |G| \end{aligned}$$

□

Corollary 1.55.

$$|G| = p, p \text{ primo} \Leftrightarrow (H \leq G \Rightarrow H = \{e\} \vee H = G)$$

La seconda proposizione equivale a dire che gli unici sottogruppi di $(G, \cdot)$ sono quelli banali: $\{e\}, G$.

Proof:

1. Dim $\Rightarrow$

$$\begin{aligned} H \leq G &\stackrel{\text{Lagrange}[1.53, \text{pg.19}]}{\Rightarrow} |H| / |G| \Leftrightarrow |G| = h|H| \\ \begin{cases} |G| = p \text{ primo} \\ p = h|H| \end{cases} &\Rightarrow |H| = 1 \vee |H| = p \Rightarrow |H| = \{e\} \vee |H| = G \end{aligned}$$

2. Dim $\Leftarrow$

Usando il thm di Cauchy (vedi [1.178, pg.75]), la tesi e' immediata:

$$p \text{ non primo} \Rightarrow \exists q \text{ primo: } q \nmid p \Leftrightarrow q \nmid |G| \stackrel{\text{Cauchy}[1.178, \text{pg.75}]}{\Rightarrow} \exists H \leq G : |H| = q \text{ assurdo contro } H_p$$

Dimostriamo adesso la tesi senza ricorrere a Cauchy.

2.1. G e' finito

Supponiamo per assurdo che G sia infinito, allora $\exists a \in G : a \neq e, \langle a \rangle$ infinito, cioe'

$$a^i \neq a^j \quad \forall i \neq j$$

Da $\langle a \rangle$ possiamo estrarre il seguente sottogruppo:

$$H = \{a^{2^i} \in \langle a \rangle \mid i \in \mathbb{Z}\}$$

Ma per H_p $H = G \vee H = \{e\}$. Ma da tutte e due i casi abbiamo un assurdo.

2.2. G e' ciclico

Se $G = \{e\}$, G e' ciclico. Supponiamo $\{e\} \subset G$.

$$a \in G : a \neq e$$

$$\langle a \rangle \leq G \stackrel{H_p}{\Rightarrow} \langle a \rangle = \{e\} \vee \langle a \rangle = G$$

poiche' e' assurdo che $\langle a \rangle = \{e\}$, si ha $\langle a \rangle = G$. Quindi G e' ciclico. Anzi, e' generato da un qualsiasi elemento $a \neq e$.

2.3. $|G| = p$ e' primo

Se per assurdo non lo fosse, si avrebbe $p = hk, 1 < h, k < p$.

$$\begin{cases} p = hk \Leftrightarrow h \nmid p \\ G \text{ e' ciclico} \end{cases} \stackrel{\text{thm}[1.42, \text{pg.14}]}{\Rightarrow} \exists! S \leq G : |S| = h$$

ma questo e' assurdo, perche' per H_p $|S| = 1 \vee |S| = |G|$.

□

Corollary 1.56. $(G, \cdot)$ finito, dove p e' un primo, si ha

$$|G| = p, p \text{ primo} \Rightarrow \forall a \in G : a \neq e, \quad G = \langle a \rangle$$

In altre parole, se $|G|$ e' primo, allora G e' ciclico, anzi e' generato da qualsiasi suo elemento diverso da e .

Proof:

$$\begin{aligned} a \neq e &\Rightarrow \langle a \rangle \neq [e] \quad (1) \\ \left\{ \begin{array}{l} \langle a \rangle \leq G \\ |G| = p \end{array} \right. &\xRightarrow{\substack{\text{Lagrange} \\ [1.55, \text{pg.20}]}} \langle a \rangle = G \vee \langle a \rangle = \{e\} \xRightarrow{(1)} \langle a \rangle = G \end{aligned}$$

□

Corollary 1.57.

$$|G| = n \Rightarrow \forall a \in G \quad a^n = e$$

Proof:

$$\begin{aligned} \langle a \rangle \leq G &\xRightarrow{\text{Lagrange} [1.53, \text{pg.19}]} |\langle a \rangle| \xRightarrow{[1.34, \text{pg.11}]} o(a) \Big/ |G| = n \Leftrightarrow \\ &\Leftrightarrow o(a)h = n \Leftrightarrow a^{o(a)h} = a^n \Leftrightarrow \left(a^{o(a)} \right)^h = a^n \Leftrightarrow e = a^n \end{aligned}$$

□

Corollary 1.58. Dal teorema di Lagrange discende naturalmente il teorema di Eulero e quello di Fermat:

$$\begin{aligned} (a, n) = 1 &\Rightarrow a^{\varphi(n)} = 1 \quad (\mathbb{Z}_n) \\ p \text{ primo} &\Rightarrow a^{p-1} = 1 \quad (\mathbb{Z}_p) \end{aligned}$$

Proof:

1. Dim Eulero

Consideriamo $(\mathbb{Z}_n, \cdot)$. Sappiamo dall'esempio [1.17,pg.5] che in generale non e' un gruppo.

Pero', $(U(\mathbb{Z}_n), \cdot)$ lo e'. Sia $a \in U(\mathbb{Z}_n)$,

$$(a, n) = 1 \Rightarrow [a] \in U(\mathbb{Z}_n)$$

$$[a]^{|U(\mathbb{Z}_n)|} \xRightarrow{\text{cor}[1.57, \text{pg.21}]} e = [1] \Leftrightarrow [a]^{\varphi(n)} = [1] \Leftrightarrow a^{\varphi(n)} = 1 \quad (\mathbb{Z}_n)$$

2. Dim Fermat

$$\begin{aligned} p \text{ primo} &\Rightarrow \varphi(p) = p - 1 \\ (a, p) = 1 &\Rightarrow a^{p-1} = 1 \quad (\mathbb{Z}_p) \end{aligned}$$

□

1.3 Gruppo simmetrico

Definition 1.59. Sia X un insieme, e sia

$$S(X) = \{f : X \longrightarrow X \mid f \text{ biunivoca}\}$$

$(S(X), \circ)$ e' un gruppo, dove $\circ$ e' la composizione tra funzioni. Ogni sottogruppo di $S(X)$ viene chiamato *gruppo di trasformazioni*. Ad esempio, $\text{Aff}(\mathcal{A})$ e' un gruppo di trasformazione (vedi geometria II).

Proof:

1. Dimostriamo che $(S(X), \circ)$ e' un gruppo
 1. Innanzitutto $S(X) \neq \emptyset$ dato che esiste almeno $\text{id} \in S(X)$, dove id e' l'identita'.
 2. $\circ$ e' un'operazione interna ben definita, poiche' composizione di funzioni biettive e' una funzione biettiva.
 3. $\circ$ e' associativa.
 4. id e' l'elemento neutro:

$$f \circ \text{id} = \text{id} \circ f = f$$

5. f^{-1} e' l'inverso di f , infatti, $f^{-1} \circ f = f \circ f^{-1} = \text{id}$.

□

Definition 1.60. Se X e' finito, $S(X)$ lo indicheremo con S_n , dove $n = |X|$. S_n e' quindi l'insieme delle permutazioni di n elementi, percio'

$$|S_n| = n!$$

S_n non e' abeliano.

Indicheremo gli elementi di S_n con i numeri interi, anche se tutte le proposizioni che enuncieremo valgono nel caso generale.

Per indicare una permutazione $\sigma \in S_n$, useremo la seguente notazione:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix} \Leftrightarrow \begin{cases} \sigma(1) = i_1 \\ \sigma(2) = i_2 \\ \vdots \\ \sigma(n) = i_n \end{cases}$$

dove $i_j \in X, j = 1, 2, \dots, n; i_m \neq i_n \ \forall m \neq n$

Definition 1.61. Dato $x, y \in X$, $\sigma \in S_n$ definiamo la seguente relazione:

$$x \sim y \Leftrightarrow \exists i \in \mathbb{Z} : y = \sigma^i(x)$$

e' una relazione d'equivalenza.

La classe d'equivalenza di x si indica con $\mathcal{O}_\sigma(x)$ e viene chiamata *orbita* di x sotto l'azione di σ .

Proposition 1.62. Dato $x \in X$,

$$\exists m \in \mathbb{Z} : \sigma^m(x) = x$$

Proof:

Poiche' X e' finito,

$$\exists h, k \in \mathbb{N}_{>0} : \sigma^h(x) = \sigma^k(x)$$

$$\text{applicando } \sigma^{-k} \text{ ad ambo i membri: } \sigma^{h-k}(x) = \sigma^0(x) = \text{id}(x) = x$$

□

Proposition 1.63.

$$\mathcal{O}_\sigma(x) = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x)\}$$

dove m e' il minimo intero tale che $\sigma^m(x) = x$.

Proof:

Basta ripetere i passi della dimostrazione del thm [1.34,pg.11] nel caso finito, effettuando le seguenti sostituzioni:

$$\begin{aligned} p &\longrightarrow m \\ \cdot &\longrightarrow \circ \\ \langle g \rangle &\longrightarrow \mathcal{O}_\sigma(x) \end{aligned}$$

e adoperando g come se fosse $\sigma(x)$

□

Definition 1.64. Sia $x \in X$ e m il piu' piccolo intero tale che $\sigma^m(x) = x$. Diremo ciclo γ di σ , generato da x , la seguente permutazione:

$$\begin{aligned} \gamma : X &\longrightarrow X \\ \gamma(y) &= \begin{cases} \sigma(y) & y \in \mathcal{O}_\sigma(x) \\ y & y \notin \mathcal{O}_\sigma(x) \end{cases} \end{aligned}$$

che indicheremo semplicemente con

$$\gamma = (x, \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x))$$

La proposizione [1.63,pg.22] ci garantisce che γ e' biunivoca. Equivalentemente possiamo dire:

$$\gamma = \begin{pmatrix} x & \sigma(x) & \dots & \sigma^{m-1}(x) & x_1 & x_2 & \dots & x_{n-m} \\ \sigma(x) & \sigma^2(x) & \dots & \sigma^m(x) = x & x_1 & x_2 & \dots & x_{n-m} \end{pmatrix}$$

Dove x_1, x_2, x_{n-m} sono gli elementi di $X \setminus \mathcal{O}_\sigma(x)$.
 m si chiama *lunghezza* del ciclo e si puo' indicare con $l(\gamma)$
 Con m -ciclo intendiamo un ciclo di lunghezza m .

Siano γ_1, γ_2 due cicli generati da x_1, x_2 ,

$$\gamma_1, \gamma_2 \text{ sono disgiunti} \stackrel{\text{def}}{\iff} \mathcal{O}_\sigma(x_1) \cap \mathcal{O}_\sigma(x_2) = \emptyset$$

Proof:

1. γ e' biunivoca

E' iniettiva: analizziamo solo il caso $y, y' \in \mathcal{O}_\sigma(x)$

$y \neq y' \Rightarrow (\gamma(y) \neq \gamma(y')) \Leftrightarrow \sigma(y) \neq \sigma(y')$. Quest'ultima e' vera perche' in $\mathcal{O}_\sigma(x)$ gli elementi sono due a due distinti ([1.63,pg.22]).

E' surriettiva: per costruzione di γ e sempre per il fatto che in $\mathcal{O}_\sigma(x)$ gli elementi sono due a due distinti.

Example 1.65.

$$\begin{aligned} \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \\ \mathcal{O}_\sigma(1) &= \{1, 3, 2\} \\ \mathcal{O}_\sigma(4) &= \{4\} \\ \text{cicli: } &(1, 3, 2), (4) \\ (1, 3, 2) &= (3, 2, 1) = \begin{pmatrix} 1 & 3 & 2 \\ 3 & 2 & 1 \end{pmatrix} \\ (3, 1, 2) &\text{ non e' un ciclo di } \sigma \end{aligned}$$

Proposition 1.66. *Il prodotto di cicli disgiunti e' commutativo, cioe' $\gamma_i \gamma_j = \gamma_j \gamma_i$.*

Proof:

Sia $\mathcal{O}_\sigma[\gamma_j]$ l'orbita che da' luogo a γ_j , e $\mathcal{O}_\sigma[\gamma_i]$ quella di γ_i , cioe' $y \in \mathcal{O}_\sigma[\gamma_j] \Rightarrow \sigma(y) = \gamma_j(y)$.

Per definizione di ciclo, abbiamo:

$$\gamma_j(y) = \begin{cases} \sigma(y) & y \in \mathcal{O}_\sigma[\gamma_j] \\ y & y \notin \mathcal{O}_\sigma[\gamma_j] \end{cases}$$

$$\gamma_i(y) = \begin{cases} \sigma(y) & y \in \mathcal{O}_\sigma[\gamma_i] \\ y & y \notin \mathcal{O}_\sigma[\gamma_i] \end{cases}$$

Poiche' $y \in \mathcal{O}_\sigma[\gamma_i] \Rightarrow y \notin \mathcal{O}_\sigma[\gamma_j]$, $\sigma(y) \in \mathcal{O}_\sigma[\gamma_i] \Rightarrow \sigma(y) \notin \mathcal{O}_\sigma[\gamma_j]$

$$\gamma_j(\gamma_i(y)) = \begin{cases} \sigma(y) & y \in \mathcal{O}_\sigma[\gamma_i] \\ \begin{cases} \sigma(y) & y \in \mathcal{O}_\sigma[\gamma_j] \\ y & y \notin \mathcal{O}_\sigma[\gamma_j] \end{cases} & y \notin \mathcal{O}_\sigma[\gamma_i] \end{cases}$$

$$\gamma_i(\gamma_j(y)) = \begin{cases} \sigma(y) & y \in \mathcal{O}_\sigma[\gamma_j] \\ \begin{cases} \sigma(y) & y \in \mathcal{O}_\sigma[\gamma_i] \\ y & y \notin \mathcal{O}_\sigma[\gamma_i] \end{cases} & y \notin \mathcal{O}_\sigma[\gamma_j] \end{cases}$$

si nota subito che le due composizioni sono uguali, ad esempio,

$$y \in \mathcal{O}_\sigma[\gamma_j] \Rightarrow \gamma_i(\gamma_j(y)) = \sigma(y)$$

$$y \in \mathcal{O}_\sigma[\gamma_j] \Rightarrow y \notin \mathcal{O}_\sigma[\gamma_i] \Rightarrow \gamma_j(\gamma_i(y)) = \begin{cases} \sigma(y) & y \in \mathcal{O}_\sigma[\gamma_j] \\ y & y \notin \mathcal{O}_\sigma[\gamma_j] \end{cases}, y \in \mathcal{O}_\sigma[\gamma_j] \Rightarrow \gamma_j(\gamma_i(y)) = \sigma(y)$$

$$\gamma_i(\gamma_j(y)) = \gamma_j(\gamma_i(y))$$

Theorem 1.67. *Sia $\sigma \in S_n$, e siano $\gamma_1, \gamma_2, \dots, \gamma_k$ tutti i suoi cicli disgiunti, allora*

$$\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_k$$

cioe', σ e' prodotto dei suoi cicli.

Proof:

1. Dimostriamo il teorema

Dobbiamo dimostrare che

$$\sigma(x) = \gamma_1 \gamma_2 \dots \gamma_k(x) \quad \forall x \in X$$

Fissiamo $x \in X$. Poiche' $\gamma_1, \dots, \gamma_k$ sono tutti i cicli disgiunti di σ , esistera' un γ_i associato all'orbita $\mathcal{O}_\sigma(x)$, cioe'

$$\gamma_i = (x, \sigma(x), \sigma^2(x), \dots, \sigma^{m-1}(x))$$

dove m e' la lunghezza di γ_i .

Poiche' i cicli sono disgiunti,

$$\forall y \in \mathcal{O}_\sigma(x) \quad \forall j \neq i \quad y \notin \mathcal{O}_\sigma[\gamma_j] \quad (1)$$

. Dove con $\mathcal{O}_\sigma[\gamma_j]$ indichiamo l'orbita che da' luogo a γ_j . Quindi

$$(1) \Rightarrow \forall j \neq i \quad \gamma_j(x) = x$$

allora, se $i < k$, vale la seguente:

$$\gamma_1 \gamma_2 \dots \gamma_i \dots \gamma_k(x) = \gamma_1 \gamma_2 \dots \gamma_i(x)$$

$$\gamma_i(x) = \sigma(x) \in \mathcal{O}_\sigma(x) \xRightarrow{(1)} \sigma(x) \notin \mathcal{O}_\sigma[\gamma_j] \quad \forall j \neq i$$

$$\gamma_1 \gamma_2 \dots \gamma_i(x) = \gamma_1 \gamma_2 \dots \gamma_{i-1} \sigma(x) = \sigma(x)$$

□

Proposition 1.68. *L'ordine di un ciclo γ e' pari alla sua lunghezza:*

$$o(\gamma) = l(\gamma)$$

Proof:

Basta osservare che

$$y \in \mathcal{O}_\sigma(x) \Rightarrow \sigma(y) \in \mathcal{O}_\sigma(x) \Rightarrow \gamma^i(y) = \begin{cases} \sigma^i(y) & y \in \mathcal{O}_\sigma(x) \\ y & y \notin \mathcal{O}_\sigma(x) \end{cases}$$

$$(y \in \mathcal{O}_\sigma(x) \Leftrightarrow \exists k : \sigma^k(x) = y) \Rightarrow \gamma^i(y) = \begin{cases} \sigma^{i+k}(x) & \exists k : \sigma^k(x) = y \\ y & \text{altrimenti} \end{cases}$$

Percio' per definizione di lunghezza, otteniamo:

$$\gamma^m(y) = \begin{cases} \sigma^{m+k}(x) = \sigma^k(\sigma^m(x)) = \sigma^k(x) = y & \exists k : \sigma^k(x) = y \\ y & \text{altrimenti} \end{cases} = \begin{cases} y & \\ y & \end{cases} = \text{id}(y)$$

□

Theorem 1.69. *Data la permutazione $\sigma = \gamma_1 \gamma_2 \dots \gamma_k$, prodotto di cicli disgiunti, si ha*

$$o(\sigma) = \text{mcm}(l(\gamma_1), l(\gamma_2), \dots, l(\gamma_k))$$

cioe', l'ordine di una permutazione e' pari al mcm delle lunghezze dei suoi cicli.

Proof:

Siano dati i seguenti oggetti:

$$m_i = l(\gamma_i), \quad i = 1, 2, \dots, k$$

$$M = \text{mcm}(l(\gamma_1), l(\gamma_2), \dots, l(\gamma_k)) = \text{mcm}(m_1, m_2, \dots, m_k)$$

$$q_i = \frac{M}{m_i} \quad i = 1, 2, \dots, k$$

$$N = o(\sigma)$$

Allora

$$(\sigma)^M = (\gamma_1 \gamma_2 \dots \gamma_k)^M \underbrace{=}_{(!)} \gamma_1^M \gamma_2^M \dots \gamma_k^M = \gamma_1^{m_1 q_1} \gamma_2^{m_2 q_2} \dots \gamma_k^{m_k q_k} =$$

$$= (\gamma_1^{m_1})^{q_1} (\gamma_2^{m_2})^{q_2} \dots (\gamma_k^{m_k})^{q_k} \underbrace{=}_{[1.68, \text{pg.25}]} \text{id}$$

$$\underbrace{\Rightarrow}_{[1.36, \text{pg.12}]} N/M$$

Nota: l'uguaglianza (!) e' valida perche' il prodotto di cicli disgiunti e' commutativo.

E' anche vero che:

$$\mathbf{e} = \sigma^N = (\gamma_1 \gamma_2 \dots \gamma_k)^N = \gamma_1^N \gamma_2^N \dots \gamma_k^N$$

$$\gamma_1^N \gamma_2^N \dots \gamma_k^N = \mathbf{e} \underbrace{\Rightarrow}_{(2)} \gamma_i^N = \mathbf{e}, \quad i = 1, 2, \dots, k \quad (3)$$

(2) se per assurdo esistesse un $\gamma_{j_1}^N \neq \text{id}$, allora affinche' $\gamma_1^N \gamma_2^N \dots \gamma_k^N = \mathbf{e}$, dovrebbe almeno esistere il suo inverso nel prodotto, cioe' un $\gamma_{j_2}^N = \gamma_{j_1}^{-N}$. Ma questo e' assurdo perche' $\gamma_{j_1}^{-N}$

non e' disgiunto da $\gamma_{j_1}^N$. Quindi,

$$(3) \quad \underbrace{\Rightarrow}_{[1.36, \text{pg. } 12]} m_i / N, i = 1, 2, \dots, k \Rightarrow M / N$$

$$N / M, M / N \Rightarrow M = N$$

□

Corollary 1.70. *Ogni permutazione e' prodotto di trasposizioni. Una trasposizione e' un ciclo di lunghezza 2.*

Proof:

Un ciclo $\gamma = (x, \sigma(x), \dots, \sigma^{m-1}(x))$ si puo' esprimere come prodotto di trasposizioni:

$$\gamma = (x, \sigma^{m-1}(x))(\sigma(x), \sigma^{m-2}(x)) \dots (x, \sigma(x))$$

graficamente:

$$\begin{aligned} & (x, \sigma^{m-1}(x))(\sigma(x), \sigma^{m-2}(x)) \dots (x, \sigma(x)) = \\ & = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) & \sigma^3(x) & \dots & \sigma^{m-1}(x) \\ \sigma(x) & x & \sigma^2(x) & \sigma^3(x) & \dots & \sigma^{m-1}(x) \\ \sigma(x) & \sigma^2(x) & x & \sigma^3(x) & \dots & \sigma^{m-1}(x) \\ \sigma(x) & \sigma^2(x) & \sigma^3(x) & x & \dots & \sigma^{m-1}(x) \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \sigma(x) & \sigma^2(x) & \sigma^3(x) & \sigma^4(x) & \dots & \sigma^m(x) = x \end{pmatrix} = \\ & = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) & \sigma^3(x) & \dots & \sigma^{m-1}(x) \\ \sigma(x) & \sigma^2(x) & \sigma^3(x) & \sigma^4(x) & \dots & \sigma^m(x) = x \end{pmatrix} = \\ & = \gamma \end{aligned}$$

e quindi per il thm [1.67, pg. 24] si ha la tesi.

□

Example 1.71.

$$(1, 4, 2, 3) = (1, 3)(1, 2)(1, 4) = (3, 1, 4, 2) = (3, 2)(3, 4)(3, 1)$$

come si nota da questo esempio, la scrittura di un ciclo come prodotto di trasposizioni non e' unica.

Definition 1.72. Sia σ una permutazione

$$\sigma \text{ e' pari} \stackrel{\text{def}}{\iff} \exists \tau_1, \dots, \tau_{2h} \text{ trasposizioni t.c. } \sigma = \tau_1 \tau_2 \dots \tau_{2h}$$

Ovvero, σ e' pari se si puo' scrivere come prodotto di un numero pari di trasposizioni.

Theorem 1.73. *Se una permutazione $\sigma \in S_n$ e' esprimibile come prodotto di un numero pari di trasposizioni, allora ogni sua altra scrittura come prodotto di trasposizioni sara' pari.*

Proof: Costruiamo un polinomio P a cui possiamo applicare trasposizioni τ e il cui segno viene influenzato proprio da τ .

Faremo poi vedere che applicando un numero pari di trasposizioni, avra' segno positivo.

Definiamo il polinomio:

$$P(x_1, x_2, \dots, x_n) = \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

e l'azione di σ su di esso:

$$\sigma(P(x_1, x_2, \dots, x_n)) := P(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)})$$

Ad esempio,

$$P(x_1, x_2, x_3, x_4) = ((x_1 - x_2)(x_1 - x_3)(x_1 - x_4))((x_2 - x_3)(x_2 - x_4))(x_3 - x_4)$$

$$(1, 3, 2, 4)(P) = ((x_3 - x_4)(x_3 - x_2)(x_3 - x_1))((x_4 - x_2)(x_4 - x_1))(x_2 - x_1)$$

dove $(1, 3, 2, 4)$ e' un ciclo.

Sia $\tau = (i, j)$ una qualsiasi trasposizione, con $1 \leq i < j \leq n$. Siano $a, b \in \mathbb{N} : 1 \leq a, b \leq n$, $a, b \neq i, j$. Esaminiamo cosa accade ai monomi di P quando gli applichiamo τ :

$$a < j \quad \tau(x_a - x_j) = x_a - x_i = \begin{cases} x_a - x_i & a < i \\ -(x_i - x_a) & a > i \end{cases}$$

$$a > j > i \quad \tau(x_j - x_a) = x_i - x_a$$

$$a < i < j \quad \tau(x_a - x_i) = x_a - x_j$$

$$a > i \quad \tau(x_i - x_a) = x_j - x_a = \begin{cases} x_j - x_a & a > j \\ -(x_a - x_j) & a < j \end{cases}$$

$$\tau(x_i - x_j) = x_j - x_i = -(x_i - x_j)$$

$$a < b \quad \tau(x_a - x_b) = x_a - x_b$$

$$a > b \quad \tau(x_b - x_a) = x_b - x_a$$

Quindi, il segno influenza solo i fattori dove c'è almeno un x_i, x_j . Più precisamente $\tau(x_a - x_j)$ cambia segno quando $i < a < j$, $\tau(x_i - x_a)$ quando $i < a < j$, e $\tau(x_i - x_j)$ in ogni caso.

Allora ci saranno un totale di

$$(j - i - 1) + (j - i - 1) + 1 = 2(j - i - 1) + 1$$

cambiamenti di segno. Indipendentemente da i, j e quindi da τ , il numero di cambiamenti è sempre dispari. Da questo deduciamo che se applichiamo k trasposizioni, il segno sarà positivo se $k \in 2\mathbb{N}$, negativo altrimenti.

1. Q.E.D.

Poiché σ è prodotto di trasformazioni ([1.70,pg.26]), avremo:

$$\sigma(P) = \pm P$$

Se per assurdo σ è esprimibile una volta come permutazione pari e un'altra come permutazione dispari, avremo:

$$\sigma(P) = +P$$

$$\sigma(P) = -P$$

Il che è assurdo, perché σ è una funzione e quindi associa ad ogni elemento del suo dominio uno ed un solo elemento del codominio.

□

Proposition 1.74. Data la permutazione $\sigma = \gamma_1 \gamma_2 \dots \gamma_c$, con γ_i ciclo $\forall i = 1, \dots, c$, si ha

$$\sigma \text{ e' pari} \Leftrightarrow L - c \text{ e' pari}$$

$$L = \sum_{i=1}^c l(\gamma_i)$$

Proof: Scriviamo ogni ciclo γ_i come prodotto di trasposizioni utilizzando il metodo visto nella dimostrazione del cor [1.70,pg.26]. Quindi, ogni ciclo di lunghezza $l_i = l(\gamma_i)$ lo esprimiamo come prodotto di $l_i - 1$ trasposizioni. Quindi, in totale avremo

$$\sum_{i=1}^c (l_i - 1) = \underbrace{\left(\sum_{i=1}^c l_i \right)}_L - c = L - c$$

trasposizioni.

1. Dim. $\Rightarrow$

Se σ e' pari, per il thm [1.73,pg.26] $L - c$ deve essere pari.

1. Dim. $\Leftarrow$

Per Hp $L - c$ e' pari, quindi siamo riusciti a esprimere σ come prodotto di un numero pari di trasposizioni. □

Proposition 1.75.

$$A_n = \{\sigma \in S_n \mid \sigma \text{ e' pari}\}$$

$$A_n \leq S_n$$

Proof:

Siano $\sigma_1, \sigma_2 \in A_n$, che esprimiamo come prodotto di trasposizioni:

$$\sigma_1 = \tau_1 \tau_2 \dots \tau_{2k}$$

$$\sigma_2 = \vartheta_1 \vartheta_2 \dots \vartheta_{2h}$$

$$\sigma_1 \sigma_2 = \tau_1 \tau_2 \dots \tau_{2k} \vartheta_1 \vartheta_2 \dots \vartheta_{2h} = \tau'_1 \tau'_2 \dots \tau'_{2(h+k)} \in A_n$$

A_n e' finito, quindi per la caratterizzazione [1.22,pg.8] $A_n \leq S_n$. □

Proposition 1.76.

$$|A_n| = |S_n \setminus A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

Proof:

Per il thm di Lagrange ([1.53,pg.19]), abbiamo:

$$|S_n| = |A_n| i_G(A_n)$$

d'altra parte, prendendo $\rho \in A_n$, $\sigma \in S_n$, $\sigma\rho$ o sta' in A_n o in $S_n \setminus A_n$, cioe' $\rho\sigma$ e' una permutazione pari o dispari. Quindi le uniche classi modulo A_n sono A_n e $S_n \setminus A_n$, ovvero $i_G(A_n) = 2$, percio'

$$|A_n| = \frac{|S_n|}{2}$$

$$\text{Infine, } |S_n \setminus A_n| = |S_n| - |A_n| = \frac{|S_n|}{2}$$
□

Definition 1.77. Sia $\sigma \in S_n$ espressa come prodotto dei suoi cicli disgiunti:

$$\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_k$$

diremo che la struttura ciclica di σ e' la seguente tupla **non ordinata**:

$$\text{sc}(\sigma) = (l(\gamma_1), l(\gamma_2), \dots, l(\gamma_k))$$

Definition 1.78. Diremo che $\sigma \in S_n$ e' una coniugata di $\sigma' \in S_n$ sse esiste una permutazione $\tau \in S_n$ t.c.

$$\sigma' = \tau \sigma \tau^{-1}$$

Theorem 1.79. In S_n ,

$$\sigma \text{ coniugata } \sigma' \Leftrightarrow \text{sc}(\sigma) = \text{sc}(\sigma')$$

Proof:

1. Dim $\Rightarrow$

$$\sigma' = \tau\sigma\tau^{-1}$$

$$\sigma'(\tau(x)) = \tau\sigma\tau^{-1}\tau(x) = \tau(\sigma(x))$$

$$\sigma'(\tau(x)) = \tau(\sigma(x))$$

Ovvero, il corrispondente in σ' del successivo di x in σ , cioè $\tau(\sigma(x))$, è il successivo in σ' del corrispondente di x in σ' .

Quindi ogni ciclo di σ ha la stessa lunghezza del ciclo corrispondente in σ' . Questo dimostra che σ, σ' hanno la stessa struttura ciclica.

Ad esempio, se $\sigma = (1, 3, 2)(5, 4)$, allora la sua coniugata σ' sarà $\sigma' = (\tau(1), \tau(3), \tau(2))(\tau(5), \tau(4))$.

2. Dim $\Leftarrow$

Sia $\mathcal{O}$ la famiglia di tutte le orbite di σ , e $\mathcal{O}'$ quella di σ' .

Come abbiamo visto prima, condizione caratteristica di τ , è che

$$\forall O \in \mathcal{O} \forall x \in O \quad \sigma'(\tau(x)) = \tau(\sigma(x))$$

allora poniamo $y = \tau(x)$, e abbiamo

$$\tau(\sigma(x)) = \sigma'(y)$$

a questo punto, poiché τ deve essere biunivoca, imponiamo che $y \in O' \in \mathcal{O}'$, dove $|O'| = |O|$.

Per ipotesi O' esiste sicuramente.

Abbiamo così definito τ : τ è una qualsiasi permutazione di S_n tale che:

$$x \in O \in \mathcal{O} \mapsto y \in O' \in \mathcal{O}'$$

$$\sigma(x) \in O \mapsto \sigma'(y) \in O'$$

$$\text{con } |O| = |O'|$$

Ricapitolando:

1. prendiamo una qualsiasi orbita $O \in \mathcal{O}$
2. prendiamo un qualsiasi elemento $x \in O$
3. prendiamo una qualsiasi orbita $O' \in \mathcal{O}' : |O| = |O'|$
4. prendiamo un qualsiasi elemento $y \in O'$
5. poniamo $\tau(x) = y, \tau(\sigma(x)) = \sigma'(y)$

□

Example 1.80. Se $\sigma = (1, 3, 2)(5, 4)$, allora la sua coniugata σ' sarà $\sigma' = (\tau(1), \tau(3), \tau(2))(\tau(5), \tau(4))$. Viceversa, consideriamo $\sigma' = (5, 4, 1)(2, 3)$, che è una permutazione con la stessa struttura ciclica di σ , allora una τ t.c. $\sigma' = \tau\sigma\tau^{-1}$ sarà:

$$\tau(1) = 5$$

$$\tau(3) = 4$$

$$\tau(2) = 1$$

$$\tau(5) = 2$$

$$\tau(4) = 3$$

ovvero

$$\tau = (1, 5, 2)(3, 4)$$

Proposition 1.81. *L'essere coniugato è una relazione di equivalenza.*

Proof:

1. Riflessività: $\sigma \sim \sigma$
 $\sigma = \text{id}\sigma\text{id}^{-1}$

2. Simmetria: $\sigma \sim \sigma' \Rightarrow \sigma' \sim \sigma$

$$\sigma' = \tau \sigma \tau^{-1} \Rightarrow \tau^{-1} \sigma' \tau = \sigma$$

3. Transitività: $\sigma \sim \sigma', \sigma' \sim \sigma'' \Rightarrow \sigma \sim \sigma''$

$$\begin{aligned} \sigma' &= \tau \sigma \tau^{-1}, \sigma'' = \rho \sigma' \rho^{-1} \\ \Rightarrow \sigma'' &= \rho(\tau \sigma \tau^{-1}) \rho^{-1} = (\rho \tau) \sigma (\tau^{-1} \rho^{-1}) \end{aligned}$$

□

Proposition 1.82. Data P partizione di S_n secondo la relazione d'equivalenza data prima, ovvero P e' l'insieme di tutte le classi coniugate, si ha

$$|P| = |\{\text{strutture cicliche di } S_n\}|$$

Proof:

Diretta conseguenza del thm [1.79,pg.28]: se σ, σ' sono coniugate, allora hanno la stessa struttura ciclica e viceversa, per ogni classe di P esiste una ed una sola struttura ciclica di S_n .

□

Proposition 1.83.

$$|\{\text{strutture cicliche di } S_n\}| = p(n) = \bar{p}(1, n)$$

$$\bar{p}(k, n) = \begin{cases} 0 & n < k \\ 1 & n = k \\ \bar{p}(k, n-k) + \bar{p}(k+1, n) & n > k \end{cases}$$

dove $p(n)$ e' il numero di partizioni dell'intero n .

Una partizione di un intero n e' una tupla **non ordinata** di numeri positivi $n_1 \geq n_2 \geq \dots \geq n_k$ t.c. $n = n_1 + n_2 + \dots + n_k$. Ad esempio, tutte le partizioni di 4 sono: $\{(4), (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1)\}$, inoltre $p(4) = |\{(4), (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1)\}| = 5$.

Proof:

1. Dimostriamo la prima uguaglianza

Consideriamo $\sigma \in S_n$ come prodotto di cicli disgiunti. Poiche' la lunghezza di ogni ciclo e' $\leq n$ e poiche' i cicli sono disgiunti, al massimo la somma delle loro lunghezze e' n :

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_k$$

$$h = \sum_{i=1}^k l(\gamma_i) \leq n$$

La differenza $n - h$ puo' essere pero' "recuperata" adoperando il ciclo identita' (x) , con x un qualsiasi elemento di S_n , senza cosi' cambiare σ :

$$\sigma = \gamma_1 \gamma_2 \dots \gamma_k \underbrace{(x)(x) \dots (x)}_{n-h \text{ volte}} \longrightarrow l(\gamma_1) + l(\gamma_2) + \dots + l(\gamma_k) + \underbrace{1 + 1 + \dots + 1}_{n-h \text{ volte}} = h + n - h = n$$

Quindi la tupla non ordinata $(l(\gamma_1), l(\gamma_2), \dots, l(\gamma_k), \underbrace{1 + 1 + \dots + 1}_{n-h \text{ volte}})$ e' una partizione di n . Ma

per definizione, e' anche una struttura ciclica. Abbiamo cosi' mostrato che a ogni struttura ciclica corrisponde una partizione di n . Analogamente, si vede che vale il viceversa.

2. Dimostriamo $p(n) = \bar{p}(1, n)$

$\bar{p}(k, n)$ e' il numero di partizioni di n formate da elementi tutti $\geq k$. Quindi $\bar{p}(1, n)$ e' proprio $p(n)$.

Dimostriamo allora che $\bar{p}(k, n)$ e' quanto detto.

Fissiamo k positivo. Possono verificarsi tre casi:

CASE: $n < k$

In questo caso non esistono partizioni di n che hanno un elemento $\geq k$. Quindi $p(k, n) = 0$

CASE: $n = k$

In questo caso esiste una sola partizione di n che ha un elemento $\geq k = n$, ovvero un elemento $= n$. Essa e' proprio la partizione (n) . Quindi $p(k, n) = 1$.

2.1. $n > k$

Poiche' $n > k$ possiamo scrivere: $n = (n - k) + k$.

A questo punto possiamo esaminare quante partizioni del numero $(n - k)$ esistano che abbiano elementi tutti $\geq k$, cosi' ad esempio, se $(k_1, k_2, \dots, k_t)$ e' una tale partizione, potremo scrivere:

$$n = \underbrace{(k_1 + k_2 + \dots + k_t)}_{=n-k} + k \quad (1)$$

Tali partizioni saranno in numero $\bar{p}(k, n - k)$.

Le partizioni di n di tipo (1), hanno tutte almeno un elemento $= k$. Allora, poiche' la definizione di $\bar{p}(k, n)$ richiede anche partizioni di n con elementi tutti $> k$, contiamo tutte le partizioni di n che hanno elementi tutti $\geq k + 1$, ossia $\bar{p}(k + 1, n)$.

Concludendo: $\bar{p}(k, n) = \bar{p}(k, n - k) + \bar{p}(k + 1, n)$

□

Proposition 1.84. *Il numero di permutazioni di S_n che hanno tutte una prefissata struttura ciclica $(m_1, m_2, \dots, m_k)$ e':*

$$Pc(m_1, m_2, \dots, m_k) = \frac{1}{k!} \prod_{i=1}^k C(m_i, n - \sum_{j=0}^{i-1} m_j)$$

$$C(k, n) := \frac{n!}{k(n - k)!}$$

$$m_0 := 0$$

Proof:

1. Contiamo intanto quante permutazioni si possono esprimere con un ciclo di lunghezza m .

Consideriamo $X = \{x_1, x_2, \dots, x_n\}$. Possiamo esprimere ogni k -ciclo con una k -upla di elementi di X (cosi' come abbiamo fatto in precedenza). Vediamo quante sono tutte le possibili k -uple distinte di elementi di X :

Tutte le disposizioni semplici di k elementi di X

in tuple ordinate di k elementi, sono $\frac{n!}{(n - k)!}$

Pero', un k -ciclo, a differenza di una tupla ordinata, resta uguale a se stesso anche se lo trasliamo a sinistra, ad esempio $(a, b, c) = (b, c, a)$. Tutte le traslazioni a sinistra distinte sono k .

Quindi, poiche' le disposizioni semplici considerano anche l'ordine di disposizione degli elementi, cioe' $(a, b, c) \neq (a, c, b)$, $(a, b, c) \neq (b, c, a)$, nel nostro conteggio dobbiamo considerare una sola volta tutti le k traslazioni di ogni tupla. Quindi, basta dividere per k il numero di

disposizioni semplici, e otteniamo:

$$C(k, n) := \frac{n!}{k(n-k)!}$$

2. Consideriamo anche il prodotto di cicli disgiunti

Siano $T_1, T_2, \dots, T_h$ rispettivamente gli insiemi di tutti i cicli di lunghezza $m_1, m_2, \dots, m_h$.

Supponiamo che i cicli di un T_i siano tutti disgiunti dai cicli di un T_j , con $i \neq j$.

Quello che dobbiamo fare e' contare tutti i possibili prodotti del tipo:

$$t_1 t_2 \dots t_h$$

$$t_i \in T_i, i = 1, 2, \dots, h$$

Scegliamo un m_1 -ciclo come primo fattore. Tutte le possibili scelte sono: $C(m_1, n)$.

Adesso scegliamo un m_2 -ciclo come secondo fattore. Poiche' i cicli m_1 sono disgiunti da quelli m_2 , adesso ogni m_2 -ciclo che sara' possibile formare avra' a disposizione $n - m_1$ elementi di X . Quindi tutte le possibili scelte rimaste di m_2 cicli sono in numero: $C(m_2, n - m_1)$.

Cosi' procedendo arriviamo fino all'ultimo fattore m_h -ciclo. Le possibili scelte per l'ultimo fattore saranno: $C(m_h, n - (m_1 + \dots + m_{h-1}))$.

Allora, il numero totale delle scelte possibili e':

$$C(m_1, n)C(m_2, n - m_1)C(m_3, n - (m_1 + m_2)) \dots C(m_h, n - (m_1 + \dots + m_{h-1}))$$

Considerando pero' che il prodotto tra cicli disgiunti e' commutativo, non dobbiamo contare i prodotti che sono permutazione di altri prodotti, quindi bastera' dividere per $h!$:

$$Pc(m_1, m_2, \dots, m_h) =$$

$$= \frac{1}{h!} (C(m_1, n)C(m_2, n - m_1)C(m_3, n - (m_1 + m_2)) \dots C(m_h, n - (m_1 + \dots + m_{h-1})))$$

che e' la tesi. □

Proposition 1.85.

$$S_n = \langle (1, 2), (2, 3), (3, 4), \dots, (n-1, n) \rangle = \langle (1, 2), (1, 2, 3, \dots, n) \rangle$$

Proof: Sia $G = \langle (1, 2), (2, 3), (3, 4), \dots, (n-1, n) \rangle$. E' chiaro che $G \subseteq S_n$

$$(1, s), (s, s+1) \in G \Rightarrow (1, s)(s, s+1)(1, s) = (1, s+1) \in G$$

$$\text{quindi, } \forall s \in 2, \dots, n \quad (1, s) \in G$$

$$(1, r)(1, s)(1, r) = (r, s) \in G$$

$$\text{quindi, } \forall s \in 2, \dots, n, \quad \forall r \in 1, \dots, n \quad (r, s) \in G$$

Quindi G contiene tutte le possibili trasposizioni di n elementi. Essendo un gruppo contiene tutti i loro prodotti, e poiche' ogni $\sigma \in S_n$ e' prodotto di trasposizioni, si ha $G \supseteq S_n$.

Infine, sia $\tau = (1, 2, 3, \dots, n)$. Considerando che $\tau^i(x) = x+i$, per il thm [1.79,pg.28] (vedi anche [1.80,pg.29]), si ha

$$\tau^i(1, 2)\tau^{-i} = (1+i, 2+i) \quad \forall i = 0, 1, \dots, n-2$$

$$\Rightarrow (1, 2), (2, 3), (3, 4), \dots, (n-1, n) \in \langle (1, 2), (1, 2, 3, \dots, n) \rangle$$

$$\Rightarrow S_n = \langle (1, 2), (2, 3), (3, 4), \dots, (n-1, n) \rangle \subseteq \langle (1, 2), (1, 2, 3, \dots, n) \rangle \subseteq S_n$$

□

Proposition 1.86. Sia $n > 2$, allora

$$Z(S_n) = \{\text{id}\}$$

Ovvero, il centro di S_n e' banale.

Da qui si capisce perche' S_n non e' abeliano.

Proof:

$$\sigma \in Z(S_n) \Leftrightarrow \forall \tau \in S_n \quad \tau\sigma = \sigma\tau \Leftrightarrow \forall \tau \in S_n \quad \tau\sigma\tau^{-1} = \sigma \quad (1)$$

Se per assurdo, $\sigma \neq \text{id}$, ovvero $\exists i \in \{1, \dots, n\} : \sigma(i) = j, j \neq i$. Scegliendo $\tau = (x, i)$, dove $x \notin \{i, j\}$ [scelta lecita perche' $n > 2$]

abbiamo

$$\text{Sia } \sigma' = \tau\sigma\tau^{-1}$$

$$\sigma' = \tau\sigma\tau^{-1} \Leftrightarrow \sigma'\tau = \tau\sigma$$

$$\sigma'(\tau(x)) = \tau(\sigma(x)) \Leftrightarrow \sigma'(i) = \tau(\sigma(x))$$

CASE: $\sigma(x) = x$

$$\sigma'(i) = \tau(x) = i \neq j \Rightarrow \sigma' \neq \sigma$$

assurdo contro la (1)

CASE: $\sigma(x) \neq x$

CASE: $\sigma(x) = i$

$$\sigma'(i) = \tau(\sigma(x)) = \tau(i) = x \neq j \Rightarrow \sigma' \neq \sigma$$

assurdo contro la (1)

CASE: $\sigma(x) \notin \{x, i\}$

$$\begin{aligned} & \begin{cases} x \neq i \\ \sigma(i) = j \end{cases} \xRightarrow[\sigma \text{ biettiva}]{} \sigma(x) \neq j \\ & \begin{cases} \sigma(x) \notin \{x, i\} \\ \tau = (x, i) \end{cases} \Rightarrow \tau(\sigma(x)) = \sigma(x) \\ & \sigma'(i) = \tau(\sigma(x)) = \sigma(x) \neq j \Rightarrow \sigma' \neq \sigma \end{aligned}$$

assurdo contro la (1)

Tutti questi assurdi derivano dall'aver supposto $\sigma \neq \text{id}$. Quindi, $\sigma = \text{id}$. □

Example 1.87. Studiamo S_3 .

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

$$|S_3| = 3! = 6$$

$$A_3 = \{(1), (1, 2, 3), (1, 3, 2)\}$$

$$|A_3| \underset{[1.76, \text{pg. 28}]}{=} \frac{3!}{2} = 3$$

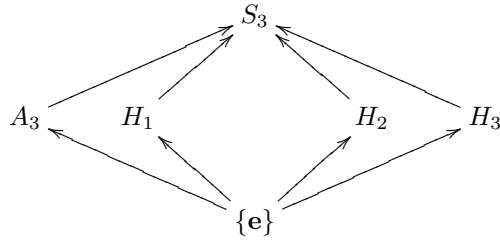
$$H_1 = \{(1), (1, 2)\}$$

$$H_2 = \{(1), (2, 3)\}$$

$$H_3 = \{(1), (1, 3)\}$$

$$\{H \leq S_3\} = \{\{\mathbf{e} = (1)\}, A_3, H_1, H_2, H_3\}$$

Il diagramma delle inclusioni dei sottogruppi:



I laterali sinistri di H_1 :

$$|S_3| = 6 \quad \underbrace{=}_{\text{Lagrange}[1.53, \text{pg.19}]} \quad |H_1| i_G(H_1) \Rightarrow i_G(H_1) = 3$$

$$\begin{aligned} \{aH_1\}_{a \in S_3} &= \{H_1, (1, 2)H_1, (2, 3)H_1, (1, 3)H_1, (1, 2, 3)H_1, (1, 3, 2)H_1\} = \\ &= \{H_1, \{(2, 3), (2, 3)(1, 2) = (1, 3, 2)\}, \{(1, 3), (1, 3)(1, 2) = (1, 2, 3)\}\} = \\ &= \{H_1, \{(2, 3), (1, 3, 2)\}, \{(1, 3), (1, 2, 3)\}\} \\ \{H_1 a\}_{a \in S_3} &= \{H_1, H_1(1, 2), H_1(2, 3), H_1(1, 3), H_1(1, 2, 3), H_1(1, 3, 2)\} = \\ &= \{H_1, \{(2, 3), (1, 2)(2, 3) = (1, 2, 3)\}, \{(1, 3), (1, 2)(1, 3) = (1, 3, 2)\}\} = \\ &= \{H_1, \{(2, 3), (1, 2, 3)\}, \{(1, 3), (1, 3, 2)\}\} \\ \{aH_1\}_{a \in S_3} &\neq \{H_1 a\}_{a \in S_3} \end{aligned}$$

Quindi, questo e' anche un esempio di laterali destri non coincidenti con laterali sinistri.

1. $A_3 \leq S_3$ e' normale ed e' l'unico sottogruppo di ordine 3

$$|A_3| = \frac{|S_3|}{2} \quad \underbrace{\Rightarrow}_{[1.103, \text{pg.42}]} \quad A_3 \leq S_3 \text{ normale}$$

$$\begin{cases} |S_3| = 3 \cdot 2, & |A_3| = 3 \\ A_3 \text{ e' un 3-sottogruppo di Sylow} \\ A_3 \text{ e' normale} \end{cases} \quad \underbrace{\Rightarrow}_{[2.9, \text{pg.88}]} \quad A_3 \text{ e' l'unico sott.gruppo di ordine 3}$$

Example 1.88. In S_4 consideriamo

$$V = \{\text{id}, (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3)\}$$

V , chiamato gruppo Vier, e' il gruppo formato dalle permutazioni di S_4 che hanno la struttura ciclica $(--)(--)$ (con l'aggiunta di id).

$V \leq A_4$ e' normale.

V e' abeliano.

Proof:

1. Dim. che $V \leq A_4$

Sia $a \in V \setminus \{\text{id}\}$

a pari (per la prop [1.74,pg.27]) $\Rightarrow a \in A_4 \Rightarrow V \setminus \{\text{id}\} \subseteq A_4 \Rightarrow V \subseteq A_4$

Sia $a = (1, 2)(3, 4)$, $b = (1, 3)(2, 4)$, $c = (1, 4)(2, 3)$

$ab = c$ [si verifica]

$$o(a) = o(b) = o(c) \underbrace{=} \text{mcm}(2, 2) = 2$$

[1.69,pg.25]

$$\Rightarrow a^2 = \mathbf{e}, a = a^{-1}, b^2 = \mathbf{e}, b = b^{-1}$$

$$(ab)^2 = c^2 = \mathbf{e} \Leftrightarrow abab = \mathbf{e} \Leftrightarrow ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

$$\begin{cases} ab = ba \\ o(a) = o(b) = 2 \end{cases} \Rightarrow \langle a, b \rangle = \{a^i b^j \mid i, j = 0, 1\} =$$

$$= \{a^0 b^0 = \text{id}, a^1 b^0 = a, a^0 b^1 = b, a^1 b^1 = ab = c\} = \{\text{id}, a, b, c\} = V$$

Quindi V e' un gruppo contenuto in A_4

2. Dim che V e' normale in A_4

Usiamo la caratterizzazione [1.104,pg.42]

Sia $a \in V$, $g \in A_4$

$$\text{sc}(gag^{-1}) \underbrace{=} \text{sc}(a) = (-)(-)(-) \Rightarrow gag^{-1} \in V$$

[1.79,pg.28]

3. V e' abeliano

$$|V| = 2^2 \underbrace{\Rightarrow} V \text{ abeliano}$$

[2.6,pg.81]

□

Lemma 1.89.

1. $\sigma \in A_n \setminus \{\text{id}\}$, $n \geq 3 \Rightarrow \sigma$ e' prodotto di 3-cicli

2. $n \geq 5$, σ_1, σ_2 3-cicli di $S_n \Rightarrow \sigma_1, \sigma_2$ sono coniugati in A_n , ovvero $\exists \sigma \in A_n : \sigma_1 = \sigma \sigma_2 \sigma^{-1}$

Proof:

1. Dim 1.

$$\sigma \in A_n \setminus \text{id} \Rightarrow \sigma = \tau_1 \cdots \tau_{2h}, \tau_i \text{ trasposizione } (*)$$

Se $n = 3$, consideriamo $a, b, c \in [1, 2, n = 3]$ distinti tra loro. Se $n > 3$, consideriamo $a, b, c, d \in \{1, \dots, n\}$ distinti tra loro. Abbiamo i seguenti casi:

$$\tau_i \tau_{i+1} = (a, b)(a, c) = (a, c, b)$$

$$\tau_i \tau_{i+1} = (a, b)(a, b) = \text{id}$$

$$\tau_i \tau_{i+1} = (a, b)(c, d) = (a, c, b)(c, d, a) \text{ [questo nel caso } n > 3]$$

Quindi sostituendo a due a due le trasposizioni in $(*)$ otteniamo solo il prodotto di tre cicli.

Nota: se $n = 2$, allora $|A_2| = \frac{|S_2|}{2} = 1 \Rightarrow A_2 = \{\text{id}\}$ e quindi non possiamo considerare $\sigma \in A_n \setminus \text{id}$.

2. Dim 2.

Siano

$$\sigma_1 = (a, b, c), \sigma_2 = (d, e, f)$$

$$\tau \in S_n : \tau(a) = d, \tau(b) = e, \tau(c) = f$$

Per il thm [1.79,pg.28] (vedi anche [1.80,pg.29]), abbiamo

$$\sigma_2 = \tau \sigma_1 \tau^{-1}$$

se τ e' pari, allora la tesi e' vera. Supponiamo τ dispari. Poiche' $n \geq 5$, possiamo trovare $g, h \in \{1, \dots, n\}$ distinti tra loro e da a, b, c , allora prendendo la permutazione $\tau' = (g, h)\tau$, abbiamo (sempre per il thm [1.79,pg.28])

$$\sigma_2 = \tau' \sigma_2 \tau'^{-1}$$

$$\tau' \text{ pari} \Rightarrow \tau' \in A_n$$

□

Definition 1.90. Sia G un gruppo.

$$G \text{ e' semplice} \stackrel{\text{def}}{\iff} \text{gli unici sottogruppi normali sono } \{e\}, G$$

Proposition 1.91. A_n e' semplice $\forall n \geq 5$

Proof: Supponiamo per assurdo che

$$\exists H \leq A_n \text{ normale, } \{e\} \subsetneq H \subsetneq A_n$$

PROOF SKETCH: Troveremo un 3-ciclo $\sigma \in H$. Poiche' tutti i 3-cicli sono coniugati in A_n (lemma [1.89,pg.35]) avremo che $H = A_n$.

Sia $\sigma \in H \setminus \{e\}$ l'elemento che fissa il maggior numero di elementi, ovvero,

$$\text{Fix} : S_n \longrightarrow \mathcal{P}(S_n)$$

$$\text{Fix}(s) = \{i \in \{1, \dots, n\} \mid s(i) = i\}$$

$$|\text{Fix}(\sigma)| = \max \{|\text{Fix}(h)| \mid h \in H \setminus \{e\}\}$$

1. σ e' un 3-ciclo

Scriviamo σ come prodotto di cicli disgiunti:

$$\sigma = \sigma_1 \dots \sigma_t$$

Supponiamo per assurdo che σ non sia un 3-ciclo, allora abbiamo i seguenti casi:

1. $\exists \sigma_i : l(\sigma_i) \geq 3$.

Abbiamo i seguenti sottocasi:

a. $\sigma = \gamma$, $l(\gamma) > 3$, anzi sappiamo che

$$\sigma \in A_n \Rightarrow \sigma \text{ pari} \Rightarrow l(\gamma) \neq 4 \Rightarrow l(\gamma) \geq 5$$

Quindi, σ e' un ciclo del tipo

$$\sigma = (a_1, \dots, a_5, \dots)$$

dove gli a_i sono distinti fra loro.

b. $\sigma = \sigma_1 \dots \sigma_t$ con almeno un σ_i di lunghezza ≥ 3 e un altro $\sigma_j \neq \text{id}$. Quindi, σ e' del tipo

$$\sigma = \sigma_i \sigma_j \dots = (a_1, a_2, a_3, \dots)(a_4, a_5, \dots) \dots$$

2. $l(s_i) < 2 \ \forall i = 1, \dots, t$. Quindi, escludendo gli s_i di lunghezza 1 (le identita'), σ e' del tipo

$$\sigma = \tau_1 \tau_2 \dots \tau_r, \ \tau_i \text{ permutazione}$$

$$\sigma \neq e \Rightarrow r \geq 1$$

inoltre,

$$\sigma \in A_n \Rightarrow r = 2k, \ k \geq 1$$

ovvero

$$\sigma = (a_1, a_2)(a_3, a_4) \dots$$

Poiche' $n \geq 5$, possiamo considerare un a_5 distinto da $a_1, \dots, a_4$.

In ogni caso, possiamo considerare il ciclo pari

$$\beta = (a_3, a_4, a_5) \in A_n$$

abbiamo

$$H \text{ normale in } A_n \Rightarrow \beta \sigma \beta^{-1} \in H \quad \underbrace{\Rightarrow}_{H \text{ gruppo}} \underbrace{\beta \sigma \beta^{-1} \sigma^{-1}}_{\gamma} \in H$$

1.1. $\gamma \neq \text{id}$

Distinguiamo i due casi:

1.

$$\sigma = (a_1, \dots, a_5, \dots) \vee \sigma = (a_1, a_2, a_3, \dots)(a_4, a_5, \dots) \dots \quad (*)$$

$$\gamma(a_3) = \beta\sigma\beta^{-1}\sigma^{-1}(a_3) \underbrace{=}_{(*)} \beta\sigma\beta^{-1}(a_2) = \beta\sigma(a_2) = \beta(a_3) = a_4$$

$$\gamma(a_3) = a_4, \quad a_3 \neq a_4 \Rightarrow \gamma \neq \text{id}$$

2.

$$\sigma = (a_1, a_2)(a_3, a_4) \dots$$

$$\gamma(a_3) = \beta\sigma\beta^{-1}\sigma^{-1}(a_3) = \beta\sigma\beta^{-1}(a_4) = \beta\sigma(a_3) = \beta(a_4) = a_5$$

$$\gamma(a_3) = a_5, \quad a_3 \neq a_5 \Rightarrow \gamma \neq \text{id}$$

1.2. $|\text{Fix}(\gamma)| > |\text{Fix}(\sigma)|$

Distinguiamo i due casi:

1. Per costruzione di β abbiamo

$$\text{Fix}(\sigma) \subseteq \text{Fix}(\beta)$$

infatti,

$$\sigma = (a_1, \dots, a_5, \dots) \vee \sigma = (a_1, a_2, a_3, \dots)(a_4, a_5, \dots) \dots \quad (*)$$

$$\sigma(a_i) = a_i \Rightarrow a_i \notin \{a_3, a_4, a_5\} \Rightarrow \beta(a_i) = a_i$$

inoltre, per qualsiasi permutazione τ , si ha

$$\text{Fix}(\tau^{-1}) = \text{Fix}(\tau), \text{ infatti}$$

$$\tau(a_i) = a_i \Leftrightarrow a_i = \tau^{-1}(a_i)$$

quindi,

$$\text{Fix}(\sigma) \subseteq \text{Fix}(\beta) \Rightarrow \text{Fix}(\sigma) = \text{Fix}(\sigma) \cap \text{Fix}(\beta) \subseteq \text{Fix}(\beta\sigma\beta^{-1}\sigma^{-1}) = \text{Fix}(\gamma)$$

$$\text{Fix}(\sigma) \subseteq \text{Fix}(\gamma)$$

Dimostriamo che l'inclusione e' stretta:

$$\gamma(a_2) = \beta\sigma\beta^{-1}\sigma^{-1}(a_2) = \beta\sigma\beta^{-1}(a_1) = \beta\sigma(a_1) = \beta(a_2) = a_2 \Rightarrow a_2 \in \text{Fix}(\gamma)$$

$$\sigma(a_2) = a_3 \Rightarrow a_2 \notin \text{Fix}(\sigma)$$

2.

$$\sigma = (a_1, a_2)(a_3, a_4) \dots$$

$$\sigma(a_i) = a_i \Rightarrow a_i \notin \{a_3, a_4\}$$

$$\underbrace{\Rightarrow}_{\beta=(a_3, a_4, a_5)} \text{Fix}(\sigma) \setminus \{a_5\} \subseteq \text{Fix}(\beta)$$

$$\text{Fix}(\sigma) \setminus \{a_5\} = \text{Fix}(\sigma) \setminus \{a_5\} \cap \text{Fix}(\beta) \subseteq \text{Fix}(\gamma)$$

Quindi, se $a_5 \in \text{Fix}(\sigma)$ oppure no, si ha

$$|\text{Fix}(\sigma)| - 1 \leq |\text{Fix}(\gamma)| \vee |\text{Fix}(\sigma)| \leq |\text{Fix}(\gamma)|$$

In ogni caso, γ fissa due elementi in piu' di σ :

$$\gamma(a_1) = a_1, \quad \gamma(a_2) = a_2$$

$$\sigma(a_1) = a_2, \quad \sigma(a_2) = a_1$$

quindi

$$\text{Fix}(\sigma) \setminus \{a_5\} \subseteq \text{Fix}(\beta) \setminus \{a_1, a_2\} \Rightarrow |\text{Fix}(\sigma)| - 1 \leq |\text{Fix}(\gamma)| - 2 \vee |\text{Fix}(\sigma)| \leq |\text{Fix}(\gamma)| - 2 \Rightarrow$$

$$\Rightarrow |\text{Fix}(\sigma)| < |\text{Fix}(\gamma)|$$

Il 1.1 e 1.2 sono in contrasto con la massimalita' di $|\text{Fix}(\sigma)|$. Abbiamo cosi' trovato l'assurdo.

Quindi σ e' un 3-ciclo.

2. Q.E.D.

Sia σ' un 3-ciclo di S_n ,

$$\sigma, \sigma' \text{ 3-cicli, } n \geq 5 \quad \underbrace{\Rightarrow}_{[1.89, \text{pg.35}]} \quad \exists a \in A_n : \sigma' = a\sigma a^{-1} \quad \underbrace{\in}_{H \leq A_n \text{ normale}} \quad H$$

$$\Rightarrow \text{Tutti i tre cicli sono in } H \text{ [e quindi anche i loro prodotti]} \quad \underbrace{\Rightarrow}_{[1.89, \text{pg.35}]} \quad A_n \subseteq H$$

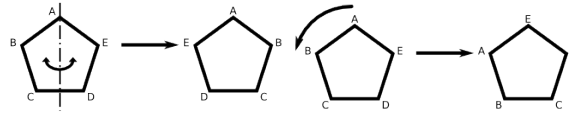
$$\begin{cases} A_n \subseteq H \\ H \leq A_n \end{cases} \Rightarrow A_n = H$$

E questo e' assurdo.

□

1.4 Gruppi diedrali

Definition 1.92. Il gruppo diedrale D_n e' un gruppo di trasformazioni, ovvero un sottogruppo di $(S(X), \circ)$, dove X e' un poligono regolare di n lati.



Proposition 1.93.

$$|D_n| = 2n$$

Proof:

I possibili elementi di D_n sono le rotazioni del poligono per angoli di

$$r_k = \frac{2\pi}{n} k$$

$$R = \{r_k \mid k = 0, 2, \dots, n-1\}$$

e i ribaltamenti lungo gli assi e le bisettrici del poligono:

n pari, $n = 2k$

$S = \{k \text{ ribaltamenti lungo gli assi e altri } k \text{ ribaltamenti lungo le bisettrici}\}$

n dispari : le bisettrici coincidono con gli assi

$S = \{\text{ribaltamenti lungo le } n \text{ bisettrici}\}$

$$|S| = n$$

Quindi, in totale $|D_n| = 2n$.

Nota: $r_n = r_0 = \mathbf{e}$

□

Proposition 1.94.

$$D_n \leq S_n$$

$$n = 3 \Leftrightarrow D_n = S_n$$

Proof:

Possiamo associare a ogni elemento di D_n la relativa permutazione di vertici. In questo modo, ogni $d \in D_n$ puo' essere pensato come un $\sigma \in S_n$. Quindi $D_n \subseteq S_n$. Non vale sempre il viceversa perche':

$$|D_n| = 2n, \quad |S_n| = n!$$

$$2n = n! \Leftrightarrow n = 3$$

Poiche' D_n e' un gruppo con la medesima operazione di S_n ed e' un sottoinsieme di S_n , per definizione $D_n \leq S_n$.

Nel caso di $n = 3$ (il triangolo), scrivendo i vertici in senso antiorario abbiamo:

$$\begin{aligned} r_1 &\longleftrightarrow (1, 2, 3) \\ r_2 &\longleftrightarrow (1, 3, 2) \\ r_3 = \mathbf{e} &\longleftrightarrow (1) \\ s_1 &\longleftrightarrow (2, 3) \\ s_2 &\longleftrightarrow (1, 3) \\ s_3 &\longleftrightarrow (1, 2) \end{aligned}$$

dove s_i e' il ribaltamento secondo la bisettrice dell'angolo al vertice i .

□

Proposition 1.95. *Sia $r = r_1$, e s un qualsiasi ribaltamento, allora*

$$\begin{aligned} R &\leq D_n, \quad R = \langle r \rangle \\ o(r^k) &= \frac{n}{(k, n)} \\ o(s) &= 2 \end{aligned}$$

Proof:

Chiaramente si ha che

$$r \circ r \circ \dots \circ r = r^k = r_k$$

E quindi

$$R = \{r_k \mid k = 0, 1, \dots, n-1\} = \{r^k \mid k = 0, 1, \dots, n-1\} = \langle r \rangle$$

$$R \leq D_n$$

Allora, per il thm [1.44,pg.15], si ha

$$o(r^k) = \frac{n}{(k, n)}$$

□

Lemma 1.96. *In D_n ,*

$$\begin{aligned} sr &= r^{n-1}s = r^{-1}s \\ s_i &= rs_{i-1}r \\ s_i &= r^j s_{i-j} r^j \quad \forall j \in \mathbb{N} \end{aligned}$$

Dove $r = r_1$ e s e' un qualsiasi ribaltamento.

Proof:

Alla rotazione r associamo la permutazione $(1, 2, \dots, n)$

Al ribaltamento s_i possiamo associare:

$$\begin{cases} n = 2k + 2 & n \text{ pari} \\ n = 2k + 1 & n \text{ dispari} \end{cases}$$

$$s_i \rightarrow (i, i)(i+1, i-1)(i+2, i-2) \dots (i+(k-1), i-(k-1))(i+k, i-k)$$

dove le addizioni si intendo in $\mathbb{Z}_n$

quindi se come s scegliamo s_1 , abbiamo:

$$s \rightarrow (2, n)(3, n-1) \dots (k, n-k+2)(k+1, n-k+1)$$

Calcoliamo la coniugata r' di r secondo s usando il thm [1.79,pg.28] (vedi es. [1.80,pg.29]):

$$r' = sr s^{-1} = (1, n, n-1, \dots, 2)$$

ovvero

$$r' = r^{-1}$$

quindi

$$r^{-1} = sr s^{-1} \Leftrightarrow sr = r^{-1}s = r^{n-1}s$$

Nota: $r^{-1} = r^{n-1}$ perche' $r \in R = \langle r \rangle$ e per il cor [1.36,pg.12].

In generale abbiamo:

$$s_i \rightarrow (i+1, i-1)(i+2, i-2) \dots (i+k-1, i-(k-1))(i+k, i-k)$$

$$s(i+1) = i-1, \dots, s(i+k) = i-k, s(i+(k+1)) = i-(k+1), \dots$$

$$s_i r s_i^{-1} = (i-1, i-2, \dots, i-k, i-(k+1), \dots, i) = r^{-1}$$

$$s_i r = r^{n-1} s_i$$

Nota, poiche' $i - (k+1) = i+k$, $i - (k+2) = i+(k-1)$ Calcoliamo la coniugata di s_i secondo r :

$$r s_i r = (i+2, i)(i+3, i-1) \dots (i+k, i-(k-2))(i+k+1, i-(k-1)) = s_{i+1}$$

$$s_{i+1} = r s_i r$$

dove $i+1$ e' in $\mathbb{Z}_n$

allora, adoperando l'ultima relazione trovata:

$$s_i = r s_{i-1} r$$

$$s_{i-1} = r s_{i-2} r$$

$$s_i = r^2 s_{i-2} r^2$$

e per induzione

$$s_i = r^j s_{i-j} r^j \quad \forall j \in \mathbb{N}$$

□

Theorem 1.97.

$$D_n = \langle r, s \rangle = \{r^i s^j \mid i = 0, 1, \dots, n-1, j = 0, 1\}$$

dove s e' un qualsiasi ribaltamento.

Proof:

1. Dimostriamo $D_n = \langle r, s \rangle$

Per definizione $\langle r, s \rangle \subseteq D_n$. Dimostriamo quindi che $D_n \subseteq \langle r, s \rangle$.

Ovviamente, $r, s \in D_n \Rightarrow r, s \in \langle r, s \rangle$.

Supponiamo $s = s_i$.

Prendiamo allora $s_j \in D_n$,

$$s_j \underbrace{=}_{\text{lemma [1.96,pg.39]}} r^{j-i} s_i r^{j-i} \Rightarrow s_j \in \langle r, s \rangle$$

ora rimangono solo i prodotti tra elementi di D_n :

$$r^a s_j = r^a r^{j-i} s_i r^{j-i} \in \langle r, s \rangle$$

$$s_j r^a = r^{j-i} s_i r^{j-i} r^a \in \langle r, s \rangle$$

2. Dimostriamo $\langle r, s \rangle = \{r^i s^j \mid i = 0, 1, \dots, n, j = 0, 1\}$

Di certo il secondo insieme sta' nel primo. Dimostriamo il viceversa.

Per il thm [1.29,pg.10] conosciamo esattamente $\langle r, s \rangle$:

$$\langle r, s \rangle = \{r^{a_1} s^{b_1} r^{a_2} s^{b_2} \dots r^{a_r} s^{b_r}, a_i, b_i \in \mathbb{Z}, r = 1, 2, \dots, \}$$

ma poiche' conosciamo gli ordini di r e s possiamo dire che $a_i = 0, 1, 2, \dots, n-1$, $b_i = 0, 1$.
 Notiamo che i casi in cui $b_i = 0$, si riducono a prodotti del tipo $r^{a_i} r^{a_{i+1}} \dots = r^{a_i + a_{i+1}} \dots$,
 quindi possiamo direttamente supporre $b_i = 1$.

Abbiamo:

$$\begin{aligned} sr & \underbrace{=} r^{-1}s \quad (1) \\ & \text{lemma}[1.96, \text{pg.39}] \\ r^\alpha sr^\beta &= r^\alpha sr^{\beta-1} \underbrace{=} r^\alpha r^{-1} sr^{\beta-1} = r^\alpha r^{-2} sr^{\beta-2} = \dots = r^\alpha r^{-\beta} s = r^{\alpha-\beta} s \\ & (1) \\ \Rightarrow r^{a_1} sr^{a_2} sr^{a_3} s \dots r^{a_r} s &= r^{a_1-a_2} \underbrace{ss}_{=e} r^{a_3} \dots r^{a_r} s = r^{a_1-a_2+a_3} \dots r^{a_r} s = r^{a_1-a_2+a_3-a_4+\dots+a_r} s \end{aligned}$$

dove abbiamo supposto r dispari, con r pari si avrebbe:

$$r^{a_1-a_2+a_3-a_4+\dots+a_{r-1}-a_r} s$$

chiaramente tutte le somme le stiamo facendo in $\mathbb{Z}_n$, perche' n e' anche l'ordine di r .
 La tesi e' acquisita. □

Proposition 1.98. D_n , con $n > 2$ non e' abeliano.

Proof: si ha

$$sr \underbrace{=} r^{-1}s \quad \text{lemma}[1.96, \text{pg.39}]$$

ma $r \neq r^{-1}$ se $n > 2$ □

Proposition 1.99.

$$Z(D_n) = \begin{cases} \{e\} & n \text{ dispari} \\ \{e, r^{\frac{n}{2}}\} & n \text{ pari} \end{cases}$$

Proof:

1. Scelto $0 < i < n$, dimostriamo che

$$sr^i = r^i s \Leftrightarrow r^i = r^{\frac{n}{2}}$$

$$\begin{aligned} \text{Sia } i \in \{1, \dots, n-1\}, \\ sr^i &= sr r^{i-1} \underbrace{=} r^{-1} sr^{i-1} = r^{-2} sr^{i-2} = \dots = r^{-i} s \\ & [1.96, \text{pg.39}] \end{aligned}$$

$$sr^i = r^i s \Leftrightarrow r^{-i} s = r^i s \Leftrightarrow r^{-i} = r^i \Leftrightarrow -i = i \pmod{n} \Leftrightarrow 2i = 0 \pmod{n} \Leftrightarrow 2i = \lambda n$$

$$0 < i < n \Leftrightarrow 0 < 2i < 2n \Leftrightarrow 0 < \lambda n < 2n \Leftrightarrow 0 < \lambda < 2 \Leftrightarrow \lambda = 1$$

$$2i = \lambda n = n \Leftrightarrow i = \frac{n}{2}$$

$$sr^i = r^i s \Leftrightarrow r^i = r^{\frac{n}{2}} \quad (1)$$

2. Q.E.D.

Per il thm vedi [1.97, pg.40], tutti gli elementi di D_n sono del tipo $s^j r^i$, con $j = 0, 1$ e $i = 0, 1, \dots, n-1$.

Vediamo quali possono stare in $Z(D_n)$:

1. s non puo' starci: come visto nel passo precedente

$$i \neq \frac{n}{2} \Rightarrow sr^i \neq r^i s \Rightarrow s \notin Z$$

2. sr^i non puo' starci:

$$sr^i \in Z \Leftrightarrow (sr^i)(s^{j'} r^{i'}) = (s^{j'} r^{i'})(sr^i) \quad \forall s^{j'} r^{i'} \in D_n$$

Scegliamo $j' = 0$,

$$(sr^i)(s^{j'}r^{i'}) = (s^{j'}r^{i'})(sr^i) \underbrace{\Leftrightarrow sr^{i+i'}}_{j'=0} = r^{i'}sr^i \Leftrightarrow sr^{i'} = r^{i'}s$$

e come abbiamo già visto

$$i' \neq \frac{n}{2} \Rightarrow sr^{i'} \neq r^{i'}s$$

3. Gli ultimi elementi da considerare sono quelli del tipo r^h .

$$r^h \in Z \Leftrightarrow r^h(s^j r^i) = (s^j r^i)r^h \quad \forall s^j r^i \in D_n \quad (2)$$

E' chiaro che se scegliamo $j = 0$, allora la (2) e' verificata. Sia allora $j = 1$,

$$r^h(sr^i) = (sr^i)r^h \Leftrightarrow r^h s = sr^h \Leftrightarrow h = \frac{n}{2}$$

Quindi $r^{\frac{n}{2}}$ e' l'unico elemento di tipo r^h che commuta con tutti gli altri.

In definitiva, l'unico elemento che commuta con tutti gli altri e'

$$r^{\frac{n}{2}}$$

se n e' dispari, tale elemento non esiste.

Appena commutano s, r^i , commutano tutti gli altri elementi, dato che sono del tipo $r^i s^h$, con $i = 0, 1, \dots, n-1$, $h = 0, 1$. (vedi [1.97,pg.40]). $\square$

1.5 Sottogruppi normali

Definition 1.100. Dato $(G, \cdot)$

$$H \leq G \text{ e' normale} \Leftrightarrow aH = Ha \quad \forall a \in G$$

Example 1.101. $Z(G)$ e' un sottogruppo normale di G (vedi [1.24,pg.8])

Proposition 1.102. Se G e' abeliano, ogni suo sottogruppo e' normale.

Proposition 1.103.

$$H \leq G, |H| = \frac{|G|}{2} \Rightarrow H \text{ normale}$$

Proof:

$$|H| = \frac{|G|}{2} \underbrace{\Rightarrow}_{\text{Lagrange}[1.53,pg.19]} i_G(H) = 2 \underbrace{\Rightarrow}_{\text{prop}[1.51,pg.19]} H \text{ normale}$$

$\square$

Proposition 1.104. caratterizzazione dei sottogruppi normali: dato $H \leq G$, le seguenti condizioni sono equivalenti:

1. H e' normale
2. $aha^{-1} \in H \quad \forall a \in G \quad \forall h \in H$
3. $aHa^{-1} = H \quad \forall a \in G$

dove aHa^{-1} e' il gruppo coniugato di H , ovvero e' il seguente gruppo: $aHa^{-1} = \{aha^{-1} \mid h \in H\}$

4. H e' unione di classi di coniugazione

Proof:

1. Dim 2.

1.1. Dim $\Rightarrow$

Sia $a \in G$, $h \in H$. Per Hp $aH = Ha$.

$$ah \in aH = Ha \Rightarrow ah = \bar{h}a \Leftrightarrow aha^{-1} = \bar{h} \in H$$

1.2. Dim $\Leftarrow$

1.2.1. Dim $aH \subseteq Ha$

$$\begin{aligned} ah &\in aH \\ aha^{-1} &\underbrace{\in}_{[\text{per Hp}]} H \Leftrightarrow aha^{-1} = \bar{h} \Leftrightarrow ah = \bar{h}a \in Ha \Rightarrow ah \in Ha \end{aligned}$$

$$aH \subseteq Ha$$

1.2.2. Dim $aH \supseteq Ha$

$$\begin{aligned} ha &\in Ha \\ a^{-1}ha &\underbrace{\in}_{[\text{per Hp}]} H \Leftrightarrow a^{-1}ha = \bar{h} \Leftrightarrow ha = a\bar{h} \in aH \\ Ha &\subseteq aH \end{aligned}$$

2. Dim 3.

2.1. Dim $\Rightarrow$

$$H \text{ normale} \Rightarrow aha^{-1} \in H \forall a \in G \forall h \in H \Rightarrow aHa^{-1} \subseteq H$$

$$b = a^{-1}$$

$$\begin{aligned} h \in H \text{ normale} &\Rightarrow bhb^{-1} \in H \Leftrightarrow bhb^{-1} = h' \Leftrightarrow h = b^{-1}h'b = ah'a^{-1} \in aHa^{-1} \\ &\Rightarrow H \subseteq aHa^{-1} \end{aligned}$$

2.2. Dim $\Leftarrow$

Preso un qualsiasi $a \in G$

$$aHa^{-1} = H \Rightarrow \forall h \in H \quad aha^{-1} \in H$$

e quindi H e' normale.

3. Dim 4.

Basta usare la prop. [1.182,pg.78]

□

Proposition 1.105. Sia $J, K \leq G$,

$$H \leq K \text{ normale} \Rightarrow H \cap J \leq K \cap J \text{ normale}$$

Proof:

$$\text{Sia } a \in H \cap J, b \in K \cap J$$

$$\begin{aligned} a \in H, b \in K &\quad \Rightarrow \quad bab^{-1} \in H \\ &\quad \quad \quad \underbrace{\quad}_{H \leq K \text{ normale, [1.104,pg.42]}} \end{aligned}$$

$$\begin{aligned} a, b \in J &\quad \Rightarrow \quad bab^{-1} \in J \\ &\quad \quad \quad \underbrace{\quad}_{J \text{ gruppo}} \end{aligned}$$

$$\Rightarrow bab^{-1} \in H \cap J$$

Quindi per la prop [1.104,pg.42] si ha la tesi.

□

Proposition 1.106.

$H \leq G$ e' normale $\Rightarrow$ la relazione d'equiv $\equiv(H)$, e' compatibile col prodotto, ovvero

$$\begin{cases} a \equiv b & (H) \\ c \equiv d & (H) \end{cases} \Rightarrow ac \equiv bd & (H)$$

dove $\equiv(H)$ e' la relazione modulo H definita in [1.48,pg.18], che in questo caso coincide sia con $\equiv_s$ che con $\equiv_d$.

Proof:

$$\begin{aligned} \begin{cases} a \equiv b & (H) \\ c \equiv d & (H) \end{cases} &\Leftrightarrow \begin{cases} aH = bH \\ cH = dH \end{cases} \Leftrightarrow \begin{cases} a = bh \\ c = d\bar{h} \end{cases} \Rightarrow ac = bhd\bar{h} & (1) \\ hd \in Hd = dH &\Leftrightarrow hd = dh_2 \\ (1) \Leftrightarrow ac = bdh_2\bar{h} \in bdH &\Leftrightarrow acH = bdH \Leftrightarrow ac \equiv bd & (H) \end{aligned}$$

□

Proposition 1.107. Dato $(G, \cdot)$

$\sim$ e' una rel. d'equiv. su G compatibile col prodotto $\Rightarrow \exists! H \leq G$ normale t.c. $\sim$ coincide con $\equiv(H)$

Proof:

Per Hp presi $a, b, c, d \in G$

$$\begin{cases} a \sim b \\ c \sim d \end{cases} \Rightarrow ac \sim bd$$

Consideriamo la classe d'equiv. di $\mathbf{e}$ secondo $\sim$:

$$H = [\mathbf{e}] = \{a \in G \mid a \sim \mathbf{e}\}$$

0.1. H e' un sottogruppo di G

$$1. \mathbf{e} \sim \mathbf{e} \Rightarrow \mathbf{e} \in H$$

$$2. a, b \in H \Leftrightarrow \begin{cases} a \sim \mathbf{e} \\ b \sim \mathbf{e} \end{cases} \underbrace{\Rightarrow}_{Hp} ab \sim \mathbf{e} \Leftrightarrow ab \in H$$

$$3. \begin{cases} a \sim \mathbf{e} \\ a^{-1} \sim a^{-1} \end{cases} \Rightarrow aa^{-1} \sim a^{-1} \Leftrightarrow \mathbf{e} \sim a^{-1} \Leftrightarrow a^{-1} \sim \mathbf{e} \Leftrightarrow a^{-1} \in H$$

0.2. Dim H e' normale

Utilizziamo la caratterizzazione [1.104,pg.42]. Sia $a \in G$, $h \in H$.

$$h \in H \Leftrightarrow h \sim \mathbf{e} \underbrace{\Rightarrow}_{Hp} ah \sim a \Rightarrow aha^{-1} \sim \mathbf{e} \Leftrightarrow aha^{-1} \in H$$

(Nota ⁵)

0.3. Dim $\equiv = \sim$

⁵Abbiamo scritto direttamente $h \sim \mathbf{e} \Rightarrow ah \sim a$ perche'

$$\begin{cases} h \sim \mathbf{e} \\ a \sim a \end{cases} \Rightarrow ah \sim a$$

Quello che dobbiamo dimostrare e':

$$a \sim b \Leftrightarrow a \equiv b \ (H) \Leftrightarrow aH = bH$$

allora,

$$a \sim b \Leftrightarrow ab^{-1} \sim \mathbf{e} \Leftrightarrow ab^{-1} \in H \Leftrightarrow ab^{-1} = h \Leftrightarrow a \equiv b \ (H)$$

0.4. Dim che H e' unico

Prendiamo un altro $J \leq G$ normale t.c. $\sim$ coincide con $\equiv(J)$.

$$\begin{aligned} a \in J &\Leftrightarrow a \equiv \mathbf{e} \ (J) \Leftrightarrow a \sim \mathbf{e} \Leftrightarrow a \in H \\ J &= H \end{aligned}$$

□

Proposition 1.108. $|G| = n$

$$\begin{cases} m/n \\ \exists! H \leq G : |H| = m \end{cases} \Rightarrow H \text{ e' normale}$$

Nota: il viceversa vale solo se H e' un sottogruppo di Sylow normale (vedi [2.9,pg.88])

Proof: Sia $a \in G$. Consideriamo il coniugato aHa^{-1} , e' facile vedere⁶ che $|H| = |aHa^{-1}|$, e quindi

$$|H|/n \Rightarrow |aHa^{-1}|/n$$

ma per Hp esiste un solo sottogruppo di ordine $|H|$ che divide n , quindi si deve necessariamente avere:

$$H = aHa^{-1}$$

Per l'arbitrarieta' di a e per la prop [1.104,pg.42] si ha la tesi.

Proposition 1.109.

$$\begin{cases} H, K \leq G \text{ normali} \\ H \cap K = \{\mathbf{e}\} \\ a \in H, b \in K \end{cases} \Rightarrow ab = ba$$

Proof:

Consideriamo $aba^{-1}b^{-1} \in G$. Questo elemento si chiama *commutatore*.

$$\begin{aligned} &\begin{cases} b \in K \\ K \text{ normale} \end{cases} \xRightarrow{[1.104,pg.42]} aba^{-1} \in K \\ &b^{-1} \in K \Rightarrow aba^{-1}b^{-1} \in K \\ &\begin{cases} a \in H \Leftrightarrow a^{-1} \in H \\ H \text{ normale} \end{cases} \Rightarrow ba^{-1}b^{-1} \in H \\ &a \in H \Rightarrow aba^{-1}b^{-1} \in H \\ &aba^{-1}b^{-1} \in H \cap K = \{\mathbf{e}\} \Rightarrow aba^{-1}b^{-1} = \mathbf{e} \Leftrightarrow ab = ba \end{aligned}$$

□

⁶basta usare la seguente applicazione biettiva:

$$\begin{aligned} f : H &\longrightarrow aHa^{-1} \\ f(h) &= aha^{-1} \end{aligned}$$

Example 1.110. $A_n \leq S_n$ e' un sottogruppo normale. (Per la def di A_n vedi [1.75,pg.28])

Proof:

$$|A_n| \underbrace{=}_{\text{prop [1.76,pg.28]}} \frac{|S_n|}{2} \underbrace{\Rightarrow}_{\text{prop [1.103,pg.42]}} A_n \text{ normale}$$

□

1.6 Gruppo quoziente

Definition 1.111. Dato il gruppo $(G, \cdot)$ sia $H \leq G$ normale.

$$G/H = \{aH\}_{a \in G}$$

si chiama *gruppo quoziente* di G rispetto al sottogruppo normale H .
Si tratta dell'insieme quoziente di G rispetto alla relazione d'equivalenza modulo H .

Proposition 1.112.

$$(G/H, \cdot)$$

e' un gruppo, dove $\cdot$ e' l'operazione definita nel seguente modo:

$$aH \cdot bH = abH$$

Proof:

1. Prima di tutto dimostriamo che $\cdot$ e' ben posta

Prendiamo $aH = a'H$, $bH = b'H$. Proviamo che $a'Hb'H = aHbH$.

$$\begin{cases} aH = a'H \Leftrightarrow a \equiv a' \pmod{H} \\ bH = b'H \Leftrightarrow b \equiv b' \pmod{H} \end{cases} \underbrace{\Rightarrow}_{\text{prop[1.106,pg.43]}} ab \equiv a'b' \pmod{H} \Leftrightarrow abH = a'b'H$$

2. Dimostriamo che G/H e' un gruppo

2.1. $\cdot$ e' associativa

Lo e' perche' $\cdot$ del gruppo G e' associativa.

2.2. $e = eH = H$

Infatti,

$$aHeH = eHaH = aeH = eaH = aH$$

2.3. $(aH)^{-1} = a^{-1}H$

Infatti,

$$aHa^{-1}H = eH = a^{-1}HaH$$

□

Example 1.113. Consideriamo $(\mathbb{Z}, +)$. Esso e' un gruppo ciclico generato da -1 o da 1 . Poiche' e' ciclico, e' anche abeliano (prop [1.40,pg.13]). Poiche' e' ciclico, ogni suo sottogruppo e' ciclico.

Consideriamo allora $H = \langle n \rangle = n\mathbb{Z}$

Esso e' ciclico e quindi abeliano e quindi normale.

Possiamo allora costruire il gruppo quoziente:

$$\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\} = \mathbb{Z}_n$$

Quindi $(\mathbb{Z}_n, +)$, con l'operazione definita in [1.112,pg.46], e' un gruppo! Il suo ordine e' n . $\mathbb{Z}_n$ e' ciclico: $\mathbb{Z}_n = \langle 1 + n\mathbb{Z} \rangle = \langle \bar{1} \rangle$, dove con $\bar{1}$ indichiamo la classe di resto di 1. Allora, per il cor [1.45,pg.16], i suoi generatori sono del tipo $m + n\mathbb{Z} = \bar{m}$ con $(m, n) = 1$. Consideriamo $8\mathbb{Z}$.

I suoi generatori sono:

$$1, 3, 5, 7$$

I suoi sottogruppi avranno ordine:

$$1, 2, 4, 8$$

essi sono

$$\begin{aligned} \{0 + 8\mathbb{Z}\} &= \{[0]_8\} \\ \{[0]_8, [4]_8\} \\ \{[0]_8, [2]_8, [4]_8, [6]_8\} \\ \mathbb{Z}_8 \end{aligned}$$

Proposition 1.114. Dato G finito e $H \leq G$ normale, allora

$$\left| \frac{G}{H} \right| = \frac{|G|}{|H|}$$

Proof: Per il thm di Lagrange (vedi [1.53,pg.19]),

$$|G| = |H| i_G(H)$$

Poiche' H e' normale, per definizione di $i_G()$, abbiamo

$$i_G(H) = \left| \frac{G}{H} \right|$$

quindi

$$|G| = |H| \left| \frac{G}{H} \right|$$

□

Proposition 1.115. Dato G qualsiasi, $H, K \leq G$: $H \subseteq K$, H normale in G , si ha

$$K \text{ normale in } G \Leftrightarrow \frac{K}{H} \text{ normale in } \frac{G}{H}$$

Proof:

1. Dim. $\Rightarrow$

$$H \text{ normale in } G \Rightarrow \frac{G}{H} \text{ gruppo } (*)$$

$$(gH)(kH)(gH)^{-1} \underbrace{=}_{(*)} \underbrace{gkg^{-1}H}_{K \text{ normale in } G} \underbrace{\in}_{\frac{K}{H}} \frac{K}{H}$$

1. Dim. $\Leftarrow$

Consideriamo la seguente composizione di surriezioni naturali:

$$G \xrightarrow{\pi_1} \frac{G}{H} \xrightarrow{\pi_2} \frac{G/H}{K/H}$$

Si ha:

$$\ker \pi_2 \circ \pi_1 = \left\{ g \in G \mid (\pi_2 \circ \pi_1)(g) = K/H \Leftrightarrow (gH) \frac{K}{H} = \frac{K}{H} \Leftrightarrow gH \in \frac{K}{H} = \{kH \mid k \in K\} \Leftrightarrow g \in K \right\} =$$

$$= G \cap K = K$$

Quindi, $K = \ker \pi_2 \circ \pi_1$ e' normale in G .

□

1.7 Gruppo prodotto

Definition 1.116. $HK = \{hk \mid h \in H, k \in K\}$

Proposition 1.117. *Siano $H, K \leq G$*

$$HK \leq G \Leftrightarrow HK = \langle H \cup K \rangle$$

Proof:

1. Dim $\Rightarrow$

$$H, K \leq G \Rightarrow e \in H, e \in K$$

Poiche' $ek, he \in HK$, $H \subseteq HK$, $K \subseteq HK$, ovvero $H \cup K \subseteq HK$.

Inoltre, HK e' il piu' piccolo sottogruppo contenente $H \cup K$, infatti, supponiamo che $\exists J \leq G : H \cup K \subseteq J$.

Prendiamo $hk \in HK$.

$$\begin{cases} h \in H \subseteq J \\ k \in K \subseteq J \\ J \text{ sottogruppo} \end{cases} \Rightarrow hk \in J$$

quindi $HK \subseteq J$

2. Dim $\Leftarrow$

Per definizione

$$\langle H \cup K \rangle \leq G$$

quindi $HK \leq G$.

□

Proposition 1.118. *Dati $H, K \leq G$*

$$HK \leq G \Leftrightarrow HK = KH$$

Proof:

1. Dim $\Rightarrow$

1.1. Dim $HK \subseteq KH$

$$hk \in HK \leq G \Rightarrow \exists (hk)^{-1} = h_1 k_1 \in HK$$

$$hk = (h_1 k_1)^{-1} = k_1^{-1} h_1^{-1} \in KH$$

1.2. Dim $HK \supseteq KH$

$$kh \in KH$$

$$kh = \underbrace{(h^{-1}k^{-1})^{-1}}_{\in HK} \underbrace{\in}_{HK \leq G} HK$$

2. Dim $\Leftarrow$

Presi $hk, h_1 k_1 \in HK$ dimostriamo che $hk(h_1 k_1)^{-1} \in HK$,

$$hk(h_1 k_1)^{-1} = h k k_1^{-1} h_1^{-1} =$$

$$h k k_1^{-1} \in HK = KH \Rightarrow h k k_1^{-1} = k_2 h_2$$

$$= k_2 h_2 h_1^{-1} \in KH = HK \Rightarrow k_2 h_2 h_1^{-1} = h_3 k_3 \in HK$$

$$hk(h_1 k_1)^{-1} = h_3 k_3 \in HK$$

□

Proposition 1.119. *Siano $H, K \leq G$*

$$\begin{aligned} H \text{ normale} \vee K \text{ normale} &\Rightarrow HK \leq G \\ H, K \text{ normali} &\Rightarrow HK \leq G \text{ normale} \end{aligned}$$

Proof:

1. Supponiamo che solo H sia normale

$$H \text{ normale} \Rightarrow HK = KH \quad \underbrace{\Rightarrow}_{\text{prop. [1.118, pg. 48]}} \quad HK \leq G$$

2. Supponiamo che H, K siano normali

Usiamo la caratterizzazione dei gruppi normali [1.104, pg. 42],

$$hk \in HK, \quad a \in G$$

$$ahka^{-1} = \underbrace{aha^{-1}}_{\in H} \underbrace{aka^{-1}}_{\in K} \in HK$$

Nota: $aha^{-1} \in H$ perche' H e' normale.

□

Proposition 1.120. *Dati G gruppo finito, $H, K \leq G$ sottogruppi, con K normale, si ha*

$$\begin{cases} H \cap K = \{e\} \\ |G| = |H||K| \end{cases} \Rightarrow G = HK$$

Proof:

$$\begin{aligned} K \text{ normale} &\quad \underbrace{\Rightarrow}_{[1.119, \text{pg. 49}]} \quad HK \leq G \\ H \cap K = \{e\} &\Rightarrow |H \cap K| = 1 \quad (*) \\ \begin{cases} H, K \leq G \text{ finiti} \\ K \text{ normale} \end{cases} &\quad \underbrace{\Rightarrow}_{[1.153, \text{pg. 63}]} \quad |HK| = \frac{|H||K|}{|H \cap K|} \quad \underbrace{=}_{(*)} \quad |H||K| = |G| \\ \begin{cases} HK \leq G \\ |HK| = |G| \\ G \text{ finito} \end{cases} &\quad \underbrace{\Rightarrow}_{[1.23, \text{pg. 8}]} \quad HK = G \end{aligned}$$

□

Proposition 1.121. *Dato G e $H, K \leq G$,*

$$\begin{cases} G = HK \\ H \cap K = \{e\} \end{cases} \Leftrightarrow \forall g \in G \exists!(h, k) \in H \times K : g = hk$$

Proof:

1. Dim $\Rightarrow$

Per ipotesi

$$G = HK, \quad H \cap K = \{e\}$$

Sia $g \in G$,

$$g \in G = HK \Rightarrow g = hk$$

supponiamo che $g = h'k'$, allora

$$hk = h'k' \Leftrightarrow k = h^{-1}h'k' \Leftrightarrow \underbrace{kk'^{-1}}_{\in K} = \underbrace{h^{-1}h'}_{\in H} =: a$$

$$a \in K, a \in H \Rightarrow a \in H \cap K = \{e\} \Rightarrow a = e \Leftrightarrow \begin{cases} kk'^{-1} = e \\ h^{-1}h' = e \end{cases} \Leftrightarrow \begin{cases} k = k' \\ h = h' \end{cases}$$

2. Dim $\Leftarrow$

Dall'ipotesi segue subito che $G = HK$.

2.1. $H \cap K = \{e\}$

Supponiamo che $g \in H \cap K$, allora

$$g \in H \cap K \Rightarrow \begin{cases} (g, e) \in H \times K \\ (e, g) \in H \times K \end{cases} \quad (1)$$

$$g \in G \Rightarrow \exists! (h, k) \in H \times K : g = hk \quad (2)$$

$$\begin{cases} g = ge = eg \\ (1), (2) \end{cases} \Rightarrow (h, k) = (g, e) = (e, g) \Rightarrow g = e$$

□

1.7.1 Prodotto interno ed esterno

Definition 1.122. Sia dati due gruppi $(G, \cdot), (G', *)$, allora, definendo l'operazione

$$\begin{aligned} \times : G \times G' \times G \times G' &\longrightarrow G \times G' \\ (g_1, g'_1) \times (g_2, g'_2) &= (g_1 g_2, g'_1 g'_2) \end{aligned}$$

$(G \times G', \times)$ e' un gruppo e si chiama *prodotto esterno* dei gruppi G, G'

Proof:

1. Dim. che $(G \times G', \times)$ e' un gruppo

1. Prop. associativa:

$$((a, b) \times (c, d)) \times (c', d') = (ac, bd) \times (c', d') = (acc', bdd') = (a, b) \times (cc', dd') = (a, b) \times ((c, d) \times (c', d'))$$

2. Elem. neutro: (e, e')

3. Inverso:

$$(a, b) \times (a^{-1}, b^{-1}) = (aa^{-1}, bb^{-1}) = (e, e') = (a^{-1}, b^{-1}) \times (a, b)$$

quindi,

$$(a, b)^{-1} = (a^{-1}, b^{-1})$$

□

Definition 1.123. Sia dato G gruppo, se

$$H, K \leq G \text{ normali tali che } \begin{cases} H \cap K = \{e\} \\ G = HK \end{cases}$$

allora diremo che G e' prodotto interno di H, K .

Proposition 1.124.

$(G \times G', \cdot)$, il gruppo prodotto esterno di G, G' , e' prodotto interno di $i_1(G), i_2(G')$, dove i_1, i_2

sono i seguenti omomorfismi iniettivi (vedi [1.8,pg.56])

$$\begin{aligned} i_1 : G &\longrightarrow G \times G' \\ i_1(g) &= (g, \mathbf{e}') \\ i_2 : G' &\longrightarrow G \times G' \\ i_2(g') &= (\mathbf{e}, g') \end{aligned}$$

Inoltre, poiche' i_1, i_2 sono iniettivi, abbiamo

$$\begin{aligned} G &\simeq i_1(G) \\ G' &\simeq i_2(G') \end{aligned}$$

Proof:

1. i_1 e' un omomorfismo iniettivo

$$i_1(a)i_1(b) = (a, \mathbf{e}')(b, \mathbf{e}') = (ab, \mathbf{e}') = i_1(ab)$$

$$\ker i_1 = \{g \in G \mid i_1(g) = (\mathbf{e}, \mathbf{e}') \Leftrightarrow (g, \mathbf{e}') = (\mathbf{e}, \mathbf{e}') \Leftrightarrow g = \mathbf{e}\} = \{\mathbf{e}\} \Rightarrow i_1 \text{ e' iniettivo}$$

2. Analogamente per i_2

3. $i_1(G), i_2(G')$ sono normali in $G \times G'$

Poniamo $\overline{G} = i_1(G)$, $\overline{G}' = i_2(G')$. Utilizziamo la caratterizzazione [1.104,pg.42]: preso $(g, g') \in G \times G'$ e $(\bar{g}, \mathbf{e}') \in \overline{G}$,

$$(g, g')(\bar{g}, \mathbf{e}')(g, g')^{-1} = (g\bar{g}g^{-1}, g'g'^{-1}) = (g\bar{g}g^{-1}, \mathbf{e}') \in \overline{G}$$

Analogamente per $\overline{G}'$

4. $G \times G' = \overline{G}\overline{G}'$

$$G \times G' \ni (g, g') = (g, \mathbf{e}')(\mathbf{e}, g') \in \overline{G}\overline{G}'$$

□

Proposition 1.125. Sia G prodotto interno di H, K , allora gli elementi di H, K commutano tra loro, ovvero

$$hk = kh \quad \forall h \in H \forall k \in K$$

Proof: Diretta conseguenza della definizione e della prop. [1.109,pg.45]

□

Theorem 1.126. Dato il gruppo G prodotto interno di H, K , si ha

$$G \simeq H \times K$$

dove $H \times K$ e' il prodotto esterno di H, K .

In particolare, un isomorfismo e':

$$\begin{aligned} f : H \times K &\longrightarrow G \\ f(h, k) &= hk \end{aligned}$$

Proof: Dimostriamo che f e' un isomorfismo.

1. f e' un omomorfismo

Ricordiamo che grazie alla prop. [1.109,pg.45], gli elementi di H e K commutano fra loro.

$$f((h, k)(h', k')) = f(hh', kk') = hh'kk'$$

$$f(h, k)f(h', k') = hkh'k' = hh'kk'$$

2. f e' biettiva

E' iniettiva:

$$\begin{cases} hk \in G \\ G = HK \\ H \cap K = \{e\} \end{cases} \xRightarrow[\text{prop. [1.121,pg.49]}]{\quad} \exists!(h, k) \in H \times K : hk = f(h, k) \quad (1)$$

$$f(h, k) = f(h', k') \Leftrightarrow hk = h'k' \xRightarrow[(1)]{\quad} \begin{cases} h = h' \\ k = k' \end{cases}$$

E' surriettiva:

$$g \in G = HK \Rightarrow \exists(h, k) \in H \times K : g = hk = f(h, k)$$

□

Example 1.127. Consideriamo il gruppo ciclico $G = (\mathbb{Z}_6, +)$.

$$G = \langle 1 \rangle \Rightarrow G \text{ ciclico} \Rightarrow G \text{ abeliano} \Rightarrow \forall H \leq G \quad H \text{ normale}$$

$$t \mid |G| = 6 \xRightarrow[\text{[1.42,pg.14]}]{\quad} \exists! H \leq G : |H| = t$$

quindi gli unici sottogruppi non banali di G sono:

$$H, K \leq G, \quad |H| = 3, \quad |K| = 2$$

$$H = \{0, 2, 4\}, \quad K = \{0, 3\}$$

abbiamo:

$$H \cap K = \{0\}$$

$$|HK| \xRightarrow[\text{[1.153,pg.63]}]{=} \frac{|H||K|}{|H \cap K|} = \frac{3 \cdot 2}{1} = 6 \Rightarrow HK = G$$

Quindi G e' un prodotto interno di H, K , e per il thm [1.126,pg.51], si ha

$$\mathbb{Z}_6 \simeq H \times K$$

e inoltre per la prop [1.121,pg.49], ogni $g \in \mathbb{Z}_6$ si puo' scrivere in modo unico come somma di un elemento di H e di K : ad esempio, 5 si puo' scrivere unicamente come $5 = 3 + 2$.

1.7.2 Prodotto a piu' fattori

Definition 1.128. Possiamo estendere per induzione il prodotto esterno tra due gruppi al prodotto esterno tra t gruppi. Poniamo:

$$(G_1 \times G_2 \times \dots \times G_t, \times) \stackrel{\text{def}}{=} (G_1 \times G_2 \times \dots \times G_{t-1}, \times) \times (G_t, \cdot)$$

Si dimostrano tutte le proprietà che abbiamo già visto per il prodotto tra due gruppi. Analogamente si estende la definizione di prodotto interno: dato A ed $H_1, \dots, H_p \leq A$ normali,

$$\begin{aligned} A \text{ e' loro prodotto interno} &\stackrel{\text{def}}{\Leftrightarrow} A \text{ e' prodotto interno di } H_i \text{ e } H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_t \quad \forall i = 1, 2, \dots, t \Leftrightarrow \\ &\Leftrightarrow \begin{cases} H_i \cap (H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_t) = \{e\} & \forall i = 1, 2, \dots, t \\ A = H_1 H_2 \dots H_t \end{cases} \Leftrightarrow \\ &\Leftrightarrow \forall a \in A \quad \exists (h_1, h_2, \dots, h_t) \in H_1 \times H_2 \times \dots \times H_t : \quad a = \prod_{i=1}^t h_i \end{aligned}$$

Poiché per il thm [1.126,pg.51] sussiste un isomorfismo tra il prodotto interno ed esterno, e poiché per il thm [1.126,pg.51] un prodotto esterno è anche un prodotto interno, in seguito, a volte, non specificheremo se G è un prodotto interno o esterno.

Proposition 1.129. *Sia $G = G_1 \times G_2 \times \dots \times G_t$, allora*

$$|G| < +\infty \Leftrightarrow |G_i| < +\infty \quad \forall i = 1, 2, \dots, t$$

E in particolare, se $|G| < +\infty$, si ha

$$|G| = \prod_{i=1}^t |G_i|$$

Proposition 1.130. *Sia $G = G_1 \times G_2 \times \dots \times G_t$, allora*

$$G \text{ e' abeliano} \Leftrightarrow G_i \text{ e' abeliano} \quad \forall i = 1, 2, \dots, t$$

Proof:

1. Dim. $\Rightarrow$

Consideriamo gli omomorfismi

$$G \text{ abeliano} \Rightarrow \text{ogni sottogruppo abeliano}$$

$$G_j \xrightarrow[\text{[1.124,pg.50]}]{\simeq} i_j(G_j) \leq G \Rightarrow G_j \text{ abeliano}$$

1. Dim. $\Leftarrow$

$$g, g' \in G$$

$$gg = (g_1, g_2, \dots, g_t)(g'_1, g'_2, \dots, g'_t) = (g_1 g'_1, \dots, g_t g'_t) \xrightarrow[\text{G}_i \text{ abeliano}]{=} (g'_1 g_1, \dots, g'_t g_t) = g'g$$

□

Proposition 1.131. *Sia $G = G_1 \times G_2 \times \dots \times G_t$, allora è facile verificare che:*

$$Z(G) = Z(G_1) \times Z(G_2) \times \dots \times Z(G_t)$$

Proposition 1.132. *Sia $G = G_1 \times G_2 \times \dots \times G_t$, allora preso $g = (g_1, \dots, g_t) \in G$*

$$o(g) < +\infty \Leftrightarrow o(g_i) < +\infty \quad \forall i = 1, 2, \dots, t$$

E in particolare, se $o(g) < +\infty$, si ha

$$o(g) = \text{mcm}(o(g_1), o(g_2), \dots, o(g_t))$$

Proof:

1. Dim. $\Rightarrow$

Supponiamo $o(g) = n$, e sia

$$m = \text{mcm}(o(g_1), o(g_2), \dots, o(g_t))$$

allora

$$\begin{aligned} g^n = \mathbf{e} &\Leftrightarrow (g_1^n, g_2^n, \dots, g_t^n) = (\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n) \Rightarrow o(g_i) < +\infty \quad \forall i = 1, 2, \dots, t \\ &\Rightarrow o(g_i) \mid n \quad \forall i = 1, 2, \dots, t \Rightarrow m \mid n \end{aligned}$$

1. Dim. $\Leftarrow$

Per Hp $o(g_i) < +\infty$, allora

$$g^m = (g_1^m, g_2^m, \dots, g_t^m) = \mathbf{e} \Rightarrow \begin{cases} o(g) < +\infty \\ o(g) \mid m \Leftrightarrow n \mid m \end{cases}$$

questo perche' tra i fattori di m ci sono i multipli di ogni esponente e_i tale che $g_i^{e_i} = \mathbf{e}_i$

1. Q.E.D.

Allora, appena vale una sola delle condizioni si ha che vale anche l'altra e quindi

$$\begin{cases} n \mid m \\ m \mid n \end{cases} \Rightarrow n = m$$

□

Proposition 1.133. *Sia $G = G_1 \times G_2 \times \dots \times G_t$, finito, allora*

$$\begin{cases} G \text{ e' ciclico} \\ G = \langle g \rangle \end{cases} \Leftrightarrow \begin{cases} G_i \text{ e' ciclico} & \forall i = 1, 2, \dots, t \\ G_i = \langle g_i \rangle \\ (|G_i|, |G_j|) = (o(g_i), o(g_j)) = 1 & \forall i \neq j \end{cases}$$

Proof:

1. Dim. $\Rightarrow$

G ciclico $\Rightarrow$ ogni sottogruppo e' ciclico

$G_j \simeq i_j(G_j) \leq G \Rightarrow G_j$ e' ciclico

$g_i \in G_i \Rightarrow o(g_i) \mid |G_i| \Rightarrow o(g_i) \leq |G_i|$ (*)

$$G = \langle g \rangle \Rightarrow |G| = o(g) \underbrace{=}_{[1.132, \text{pg.53}]} mcm(o(g_1), o(g_2), \dots, o(g_t)) \leq \prod_{i=1}^t o(g_i) \underbrace{\leq}_{(*)} \prod_{i=1}^t |G_i| \underbrace{=}_{[1.129, \text{pg.53}]} |G|$$

$$\Leftrightarrow mcm(o(g_1), o(g_2), \dots, o(g_t)) = \prod_{i=1}^t o(g_i) = \prod_{i=1}^t |G_i| \quad (**)$$

$$mcm(o(g_1), o(g_2), \dots, o(g_t)) = \prod_{i=1}^t o(g_i) \Rightarrow (o(g_i), o(g_j)) = 1 \quad \forall i \neq j$$

$$\prod_{i=1}^t o(g_i) = \prod_{i=1}^t |G_i| \Rightarrow o(g_i) = |G_i|, \text{ infatti,}$$

$$\begin{cases} o(g_1) \leq |G_1| \\ o(g_2) \leq |G_2| \\ \dots \\ o(g_t) \leq |G_t| \end{cases} \quad \text{quindi, se per ass. } \exists h : o(g_h) < |G_h|, \text{ moltiplicando membro a membro si ha}$$

$$\prod_{i=1}^t o(g_i) < \prod_{i=1}^t |G_i| \text{ assurdo contro } (**)$$

$$o(g_i) = |G_i| \Rightarrow G_i = \langle g_i \rangle$$

1. Dim. $\Leftarrow$

Consideriamo $g = (g_1, g_2, \dots, g_t)$,

$$o(g) \underbrace{=}_{[1.132, \text{pg.53}]} mcm(o(g_1), o(g_2), \dots, o(g_t)) \underbrace{=}_{(o(g_i), o(g_j))=1 \quad i \neq j} \prod_{i=1}^t o(g_i) \underbrace{=}_{G_i = \langle g_i \rangle} \prod_{i=1}^t |G_i| = |G|$$

$$o(g) = |G| \Rightarrow G = \langle g \rangle$$

□

Proposition 1.134. Considerando $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_m, +)$, si ha

$$(n, m) = 1 \Leftrightarrow \mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$$

e in particolare, l'isomorfismo e'

$$\phi([i]_{nm}) = ([i]_n, [i]_m)$$

Proof:

$$\begin{cases} \mathbb{Z}_n, \mathbb{Z}_m \text{ sono ciclici} \\ \mathbb{Z}_n = \langle 1 \rangle \\ \mathbb{Z}_m = \langle 1 \rangle \\ (|\mathbb{Z}_m| = m, |\mathbb{Z}_n| = n) = 1 \end{cases} \quad \underbrace{\Leftrightarrow}_{[1.133, \text{pg.54}]} \mathbb{Z}_n \times \mathbb{Z}_m \text{ e' ciclico, } \mathbb{Z}_n \times \mathbb{Z}_m = \langle (1, 1) \rangle \quad \underbrace{\Leftrightarrow}_{[1.150, \text{pg.61}]} \mathbb{Z}_n \times \mathbb{Z}_m \simeq \mathbb{Z}_{nm}$$

Per trovare l'isomorfismo ϕ , basta vedere l'isom. usato dalla prop. [1.150, pg.61]: prima si definiva

l'omomorfismo

$$f : \mathbb{Z} \longrightarrow G = \langle (1, 1) \rangle$$

$$f(i) = ([1]_n, [1]_m)^i = ([i]_n, [i]_m)$$

e poi si usava l'isomorfismo ϕ dato dal thm dell'omomorfismo:

$$\phi : \mathbb{Z}/\ker f = \mathbb{Z}/nm\mathbb{Z} = \mathbb{Z}_{nm} \longrightarrow \mathbb{Z}_n \times \mathbb{Z}_m$$

$$\phi([i]_{nm}) = f(i) = ([i]_n, [i]_m)$$

Ed ecco che otteniamo il nostro isomorfismo:

$$\phi([i]_{nm}) = f(i) = ([i]_n, [i]_m)$$

□

Proposition 1.135. *Dati G_1, G_2 gruppi ciclici di ordine n, m ,*

$$(n, m) = 1 \Leftrightarrow G_1 \times G_2 \text{ e' ciclico}$$

Proof:

1. Dim. $\Rightarrow$

Considerando che ogni gruppo ciclico di ordine n e' isomorfo a $\mathbb{Z}_n$ (vedi [1.150,pg.61]),

$$G_1 \simeq \mathbb{Z}_n, \quad G_2 \simeq \mathbb{Z}_m \Rightarrow G_1 \times G_2 \simeq \mathbb{Z}_n \times \mathbb{Z}_m$$

$$(n, m) = 1 \Rightarrow G_1 \times G_2 \simeq \mathbb{Z}_n \times \mathbb{Z}_m \underbrace{\simeq}_{[1.134,pg.55]} \mathbb{Z}_{nm} \Rightarrow G_1 \times G_2 \text{ e' ciclico}$$

1. Dim. $\Leftarrow$

$$G_1 \times G_2 \text{ ciclico} \underbrace{\Rightarrow}_{[1.133,pg.54]} (|G_1|, |G_2|) = 1$$

□

1.8 Omomorfismo tra gruppi

Definition 1.136. Dati due gruppi $(G, \cdot), (G', *)$,

$$f : G \longrightarrow G' \text{ e' un omomorfismo} \Leftrightarrow f(a \cdot b) = f(a) * f(b)$$

Nota: da ora in poi indicheremo con il solo simbolo $\cdot$ le due operazioni.

Se f e' iniettiva, si dira' *immersione*.

Se f e' suriettiva, si dira' *epimorfismo*.

Se f e' biettiva, si dira' *isomorfismo*.

Definiamo l'insieme di tutti gli omomorfismi da G a G' :

$$\text{Hom}(G, G') \stackrel{\text{def}}{=} \{f : G \longrightarrow G' \text{ omomorfismo}\}$$

Proposition 1.137.

1. $f(e) = e'$
2. $(f(a))^{-1} = f(a^{-1})$
3. f, g omomorfismi $\Rightarrow f \circ g$ omomorfismo

dove e e' l'elemento unita' di G' .

Proof:

1. Dim 1.

$$\begin{aligned} f(\mathbf{e}) &= f(\mathbf{e}\mathbf{e}) = f(\mathbf{e})f(\mathbf{e}) \\ (f(\mathbf{e}))^{-1}f(\mathbf{e}) &= (f(\mathbf{e}))^{-1}f(\mathbf{e})f(\mathbf{e}) \\ \mathbf{e}' &= f(\mathbf{e}) \end{aligned}$$

2. Dim 2.

$$\begin{aligned} f(a^{-1})f(a) &= f(a^{-1}a) = f(\mathbf{e}) = \mathbf{e}' \\ f(a)f(a^{-1}) &= f(aa^{-1}) = f(\mathbf{e}) = \mathbf{e}' \end{aligned}$$

quindi $f(a^{-1})$ e' l'inverso di $f(a)$.

3. Dim 3.

$$fg(a \cdot b) = f(g(a \cdot b)) = f(g(a) \cdot g(b)) = f(g(a)) \cdot f(g(b))$$

□

Example 1.138.

$$\begin{aligned} f : (\mathbb{Z}, +) &\longrightarrow (\mathbb{Q}, +) \\ f(z) &= z + 1 \end{aligned}$$

non e' un omomorfismo perche' $f(0) = 0 + 1 \neq 0$.

Definition 1.139.

$$\ker f = \{a \in G \mid f(a) = \mathbf{e}'\}$$

di sicuro $\mathbf{e} \in \ker f$.

Proposition 1.140. $\ker f = \{\mathbf{e}\} \Leftrightarrow f$ e' *iniettiva*

1. Dim $\Leftarrow$

Supponiamo per assurdo che $a \neq \mathbf{e}, a \in \ker f$, allora

$$\begin{aligned} f(a) &= \mathbf{e}' \\ f(\mathbf{e}) &= \mathbf{e}' \end{aligned}$$

assurdo contro l'iniettivita'.

2. Dim $\Rightarrow$

Sia $f(a) = f(b)$ dimostriamo che $a = b$

$$f(a) = f(b) \Leftrightarrow f(a)(f(b))^{-1} = \mathbf{e}' \Leftrightarrow f(ab^{-1}) = \mathbf{e}' \Leftrightarrow ab^{-1} \in \ker f = \{\mathbf{e}\} \Rightarrow ab^{-1} = \mathbf{e} \Leftrightarrow a = b$$

□

Proposition 1.141.

$$\begin{aligned} \text{Im } f &\leq G' \\ \ker f &\leq G \\ H \leq G &\Rightarrow f(H) \leq G' \\ H' \leq G' &\Rightarrow f^{-1}(H') \leq G \end{aligned}$$

dove $f^{-1}(H')$ e' la controimmagine di H'

1. $\dim \operatorname{Im} f \leq G$ usando la prop [1.21,pg.7]

$$f(a), f(b) \in \operatorname{Im} f$$

$$f(a)(f(b))^{-1} = f(ab^{-1}) \in \operatorname{Im} f$$

2. $\dim \ker f \leq G$ usando la prop [1.21,pg.7]

$$a, b \in \ker f \Leftrightarrow f(a) = f(b) = \mathbf{e}'$$

$$f(ab^{-1}) = f(a)f(b^{-1}) = \underbrace{f(a)}_{=\mathbf{e}'} \underbrace{(f(b))^{-1}}_{=\mathbf{e}'} = \mathbf{e}'$$

3. $\dim H \leq G \Rightarrow f(H) \leq G'$

$$f(h_1), f(h_2) \in f(H)$$

$$f(h_1)f(h_2)^{-1} = f(\underbrace{h_1h_2^{-1}}_{\in H}) \in f(H)$$

4. $\dim H' \leq G' \Rightarrow f^{-1}(H') \leq G$

$$h_1, h_2 \in f^{-1}(H') \Leftrightarrow f(h_1), f(h_2) \in H'$$

$$H' \leq G' \Rightarrow f(h_1)f(h_2)^{-1} \in H' \Leftrightarrow f(h_1h_2^{-1}) \in H' \Leftrightarrow h_1h_2^{-1} \in f^{-1}(H')$$

□

Proposition 1.142. Sia $f : G \longrightarrow G'$ un omomorfismo,

$$f \text{ suriettivo, } H \leq G \text{ normale} \Rightarrow f(H) \text{ e' normale}$$

Proof:

Intanto per la prop [1.141,pg.57], $f(H) \leq G'$ Usiamo la caratterizzazione dei gruppi normali [1.104,pg.42]

$$h' \in f(H) \Leftrightarrow \exists h \in H : f(h) = h'$$

$$a' \in G' \quad \underbrace{\Rightarrow}_{f \text{ suriettivo}} \quad \exists a \in G : f(a) = a'$$

$$a'h'(a')^{-1} = f(a)f(h)f(a)^{-1} = f(aha^{-1}) \in f(H)$$

□

Proposition 1.143. Sia $f : G \longrightarrow G'$ un omomorfismo,

$$H' \leq G' \text{ normale} \Rightarrow f^{-1}(H') \leq G \text{ normale}$$

Proof:

Usiamo la caratterizzazione dei gruppi normali [1.104,pg.42]

$$a \in G$$

$$h \in f^{-1}(H') \Leftrightarrow f(h) \in H'$$

$$f(a)f(h)f(a)^{-1} \underbrace{\in}_{H' \text{ e' normale}} H' \Leftrightarrow f(aha^{-1}) \in H' \Leftrightarrow aha^{-1} \in f^{-1}(H')$$

Corollary 1.144. Sia $f : G \longrightarrow G'$ omomorfismo.

$$\ker f \leq G \text{ e' normale}$$

Proof: Basta considerare $H' = \{e'\} \leq G'$. H' e' ovviamente normale. $f^{-1}(H') = \ker f$. Per la prop di prima [1.143,pg.58], $\ker f$ e' normale. $\square$

Proposition 1.145. Sia $f : G \longrightarrow G'$ un omomorfismo e sia $g \in G$, si ha

1. G ciclico $\Rightarrow \text{Im } f$ ciclico
2. $o(g) < +\infty \Rightarrow o(f(g)) \mid o(g)$

Se f e' un isomorfismo, f preserva ogni proprieta' di G e quindi $o(f(g)) = o(g)$.

Proof:

1. Dim 1.

$$G = \langle a \rangle$$

$$\text{Im } f = f(G) = f(\langle a \rangle) = \{f(a^i) \mid i = 0, 1, \dots, \} = \{f(a)^i \mid i = 0, 1, \dots, \} = \langle f(a) \rangle$$

2. Dim 2.

Sia $p = o(g)$

$$g^p = e$$

$$f(g^p) = f(e) = e \Leftrightarrow f(g)^p = e \Leftrightarrow o(f(g)) \mid p$$

$\square$

Proposition 1.146. Sia $G = \langle g \rangle$, allora

CASE: $|G| = n$

$$\text{Hom}(G, G') = \left\{ f_h : G \longrightarrow G' \mid (f_h(g^i) = h^i \forall i \in \mathbb{Z}), h \in G', o(h) \mid n \right\}$$

CASE: $|G| = +\infty$

$$\text{Hom}(G, G') = \left\{ f_h : G \longrightarrow G' \mid (f_h(g^i) = h^i \forall i \in \mathbb{Z}), h \in G' \right\}$$

Dove $\text{Hom}(G, G')$ e' l'insieme definito in [1.136,pg.56].

In altre parole, quando G e' ciclico, conosciamo esplicitamente tutti gli omomorfi da G a G' .

Proof:

CASE: $|G| = n$

Chiamiamo H il secondo insieme.

0.1. $\text{Dim Hom}(G, G') \subseteq H$

Sia $f \in \text{Hom}(G, G')$, allora, $f(g^i) = f(g)^i$, e per la prop [1.145,pg.59] si ha

$$o(f(g)) \mid o(g) = |G| = n$$

Quindi, ponendo $h = f(g)$, si ha $f \in H$

0.2. $\text{Dim Hom}(G, G') \supseteq H$

Sia $f \in H$.

0.2.1. Dimostriamo che f e' una applicazione ben posta, ovvero, poiche' G e' ciclico, sappiamo che $g^i = g^{i+\lambda n}$, dobbiamo quindi verificare che $f(g^i) = f(g^{i+\lambda n})$

$$o(h) \mid n \Leftrightarrow n = \mu o(h)$$

$$f(g^{i+\lambda n}) = h^{i+\lambda n} = h^i h^{\lambda n} = h^i (h^{o(h)})^{\lambda \mu} = h^i = f(g^i)$$

0.2.2. Dimostriamo che f e' un omomorfismo

$$f(g^i g^j) = f(g^{i+j}) = h^{i+j} = h^i h^j = f(g^i) f(g^j)$$

Quindi, $f \in \text{Hom}(G, G')$

CASE: $|G| = +\infty$

Si procede in modo analogo a prima.

□

Theorem 1.147. Dato un omomorfismo $f : G \longrightarrow G'$, si ha

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \downarrow \pi & \nearrow \varphi & \\ G/\ker f & & \end{array}$$

con $f = \varphi \circ \pi$ e $\pi(a) = a \ker f$.

Inoltre, φ e' un omomorfismo, ed e' iniettiva.

Se consideriamo la restrizione del codominio di φ alla sua immagine:

$$\varphi : G/\ker f \longrightarrow \text{Im } \varphi$$

abbiamo che φ e' un isomorfismo e quindi

$$G/\ker f \simeq \text{Im } \varphi = \text{Im } f$$

In particolare,

$$f \text{ surriettiva} \Rightarrow \text{Im } f = G' \Rightarrow G/\ker f \simeq G'$$

Proof:

1. Definiamo φ

$$\varphi(a \ker f) = f(a)$$

dove $a \ker f$ e' un laterale di $G/\ker f$. (nota ⁷)

Questa definizione e' ben posta, infatti, prendiamo un elemento $b \in a \ker f$

$$b \in a \ker f \Leftrightarrow b = ah, \quad h \in \ker f \Leftrightarrow f(h) = \mathbf{e}'$$

$$f(b) = f(ah) = f(a) \underbrace{f(h)}_{=\mathbf{e}'} = f(a)$$

$$\varphi(b \ker f) = \varphi(a \ker f)$$

2. φ e' un omomorfismo

Poniamo $H = \ker f$

$$\varphi(aHbH) = \varphi(abH) = f(ab) = f(a)f(b) = \varphi(aH)\varphi(bH)$$

3. φ e' iniettiva

$$\varphi(aH) = \varphi(bH) \Leftrightarrow f(a) = f(b) \Leftrightarrow f(a)f(b)^{-1} = \mathbf{e}' \Leftrightarrow f(ab^{-1}) = \mathbf{e}' \Leftrightarrow ab^{-1} \in \ker f = H$$

$$ab^{-1} \in H \Leftrightarrow ab^{-1} = h \in H \Leftrightarrow a = hb \Leftrightarrow Ha = Hb \quad \underbrace{\Rightarrow}_{\ker f \text{ e' normale}} \quad aH = Ha = Hb = bH \Leftrightarrow aH = bH$$

4. $\text{Dim } f = \varphi \circ \pi$

⁷Poiche' come abbiamo visto in [1.144,pg.58], $\ker f$ e' normale, $G/\ker f$ e' un gruppo (vedi [1.112,pg.46])

$$\varphi \circ \pi(a) = \varphi(a \ker \varphi) = f(a) \quad \forall a \in G$$

quindi $f = \varphi \circ \pi$

5. $\dim \operatorname{Im} f = \dim \varphi$

$$f = \varphi \circ \pi \Rightarrow \operatorname{Im} f = \operatorname{Im}(\varphi \circ \pi)$$

Sia $a \ker f \in G / \ker f$. Poiché π è surriettiva, $\exists a \in G : \pi(a) = a \ker f$. Allora,

$$(\varphi \circ \pi)(a) = \varphi(a \ker f) \quad (1)$$

E questo vale $\forall a \ker f \in G / \ker f$, quindi $\operatorname{Im} \varphi \subseteq \operatorname{Im}(\varphi \circ \pi)$.

La (1) vale certamente $\forall a \in G$, quindi $\operatorname{Im}(\varphi \circ \pi) \subseteq \operatorname{Im} \varphi$.

□

Corollary 1.148. *Se G è finito, dato $f : G \rightarrow G'$ omomorfismo si ha*

$$\left| \frac{G}{\ker f} \right| = \frac{|G|}{|\ker f|} = |\operatorname{Im} f|$$

o equivalentemente

$$|G| = |\ker f| |\operatorname{Im} f| \Leftrightarrow i_G(\ker f) = |\operatorname{Im} f|$$

Corollary 1.149. *Dal cor [1.148,pg.61] segue immediatamente che*

$$|\operatorname{Im} f| \mid |G|$$

Inoltre, se G' è finito, per Lagrange, si ha

$$|\operatorname{Im} f| \mid |G'|$$

Proof: Poiché $\ker f$ è normale, per definizione di $i_G()$, abbiamo

$$i_G(\ker f) = \left| \frac{G}{\ker f} \right|$$

Per la prop. [1.114,pg.47] abbiamo

$$\left| \frac{G}{\ker f} \right| = \frac{|G|}{|\ker f|}$$

e per il thm [1.147,pg.60]:

$$\frac{G}{\ker f} \simeq \operatorname{Im} f \Rightarrow \left| \frac{G}{\ker f} \right| = |\operatorname{Im} f|$$

quindi la tesi:

$$i_G(\ker f) = |\operatorname{Im} f|$$

$$|G| = |\ker f| |\operatorname{Im} f|$$

□

Theorem 1.150. *Ogni gruppo ciclico è isomorfo a $\mathbb{Z}_n$ o a $\mathbb{Z}$.*

Sia $G = \langle a \rangle$ un gruppo ciclico finito, con $|G| = n$, allora

$$(G, \cdot) \simeq (\mathbb{Z}_n, +)$$

Se invece, $G = \langle a \rangle$ è un gruppo ciclico infinito, allora

$$(G, \cdot) \simeq (\mathbb{Z}, +)$$

Proof:

1. Caso 1

Consideriamo il seguente omomorfismo:

$$f : \mathbb{Z} \longrightarrow G$$

$$f(i) = a^i$$

e' un omomorfismo:

$$f(i + i') = a^{i+i'} = a^i a^{i'} = f(i)f(i')$$

Vediamo $\ker f$:

$$\ker f = \{i \in \mathbb{Z} \mid a^i = \mathbf{e}\} = n\mathbb{Z}$$

Poiche' $G = \langle a \rangle = \{a^0, a^1, \dots, a^{n-1}\}$, f e' certamente surriettivo. Allora per il cor [1.147,pg.60], anche φ e' surriettiva, e quindi

$$\mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n \simeq G$$

2. Caso 2

Poiche' G e' ciclico infinito, f e' anche iniettiva:

$$\ker f = \{i \in \mathbb{Z} \mid a^i = \mathbf{e}\} = \{0\}$$

e quindi f e' un isomorfismo.

□

Example 1.151.

$$(\mathbb{R}/\langle 2\pi \rangle, +) \simeq (S^1, \cdot)$$

dove S^1 e' la sfera unitaria a una dimensione, ovvero la circonferenza unitaria.

Proof:

Consideriamo il seguente omomorfismo:

$$f : (\mathbb{R}, +) \longrightarrow (\mathbb{C}, \cdot)$$

$$f(\theta) = \cos \theta + i \sin \theta$$

0.1. f e' un omomorfismo

$$f(\theta + \theta') = \cos(\theta + \theta') + i \sin(\theta + \theta') = \cos \theta \cos \theta' - \sin \theta \sin \theta' + i(\cos \theta \sin \theta' + \sin \theta \cos \theta')$$

$$f(\theta)f(\theta') = (\cos \theta + i \sin \theta)(\cos \theta' + i \sin \theta') = \cos \theta \cos \theta' - \sin \theta \sin \theta' + i(\cos \theta \sin \theta' + \sin \theta \cos \theta')$$

$$f(\theta + \theta') = f(\theta)f(\theta')$$

0.2. f non e' surriettiva, ne' iniettiva

$$1 + 2i \in \mathbb{C}, \quad 1 + 2i \notin \text{Im } f$$

$$f(\theta) = f(\theta + 2\pi)$$

0.3. Troviamo il $\ker f$

$$\ker f = \{\theta \in \mathbb{R} \mid f(\theta) = 1 = 1 + i0 \Leftrightarrow \cos \theta = 1, \sin \theta = 0\} = \{2h\pi \mid h \in \mathbb{Z}\} = \langle 2\pi \rangle$$

0.4. Usiamo il thm dell'omomorfismo ([1.147,pg.60])

Sappiamo che

$$G/\ker f \simeq \text{Im } f$$

e quindi nel nostro caso

$$\mathbb{R}/\langle 2\pi \rangle \simeq \text{Im } f$$

$\text{Im } f$ e' proprio S^1

□

Theorem 1.152. *teorema dell'isomorfismo I.*

Dati $H, K \leq G$,

$$K \text{ normale in } G \Rightarrow \frac{H}{H \cap K} \simeq \frac{HK}{K}$$

Proof:

$$\begin{cases} H, K \leq G \\ K \text{ normale in } G \end{cases} \xRightarrow[\text{prop}[1.119, \text{pg.49}]]{} HK \leq G$$

$$\begin{cases} K \subseteq HK \leq G \\ K \text{ normale in } G \end{cases} \Rightarrow K \leq HK, \text{ normale} \quad (1)$$

per la (1) possiamo considerare il gruppo quoziente

$$\frac{HK}{K}$$

Consideriamo la seguente composizione di funzioni:

$$H \xrightarrow{i} HK \xrightarrow{\pi} \frac{HK}{K}$$

dove

$$i(h) = h\mathbf{e}$$

e π e' la suriezione naturale. Chiaramente sono tutti e due omomorfismi.

Sia $\varphi = \pi i$,

$$\varphi(h) = \pi i(h) = \pi(h\mathbf{e}) = h\mathbf{e}K = hK$$

1. φ e' un omomorfismo perche' composizione di omomorfismi

2. φ e' surriettiva

Se prendiamo un $hkK \in \frac{HK}{K}$,

$$hkK = hK$$

quindi bastera' prendere h :

$$\varphi(h) = hK = hkK$$

3. $\ker \varphi = H \cap K$

$$\ker \varphi = \{h \in H \mid \varphi(h) = K \Leftrightarrow hK = K \Leftrightarrow h \in K\} = H \cap K$$

Allora, per il cor [1.147,pg.60]

$$H/\ker \varphi \simeq \frac{HK}{K} \Leftrightarrow \frac{H}{H \cap K} = \frac{HK}{K}$$

□

Corollary 1.153. *Dati $H, K \leq G$ finiti⁸, con K normale, si ha*

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Proof: Per il thm [1.152,pg.63], si ha

$$\frac{HK}{K} \simeq \frac{H}{H \cap K} \Rightarrow \left| \frac{HK}{K} \right| = \left| \frac{H}{H \cap K} \right| \xLeftrightarrow[1.114, \text{pg.47}]{} \frac{|HK|}{|K|} = \frac{|H|}{|H \cap K|} \Leftrightarrow |HK| = \frac{|H||K|}{|H \cap K|}$$

□

Corollary 1.154. *Dati $H, K \leq G$, con K normale in G , si ha:*

$$\psi \text{ e' surriettiva} \Leftrightarrow G = HK$$

⁸ G non e' necessariamente finito

dove

$$\begin{aligned}\psi : H &\longrightarrow \frac{G}{K} \\ \psi(h) &= hK\end{aligned}$$

Proof: Dimostreremo solo il caso in cui $|G|$ e' finito.

E' facile verificare che ψ e' un omomorfismo.

1. Dim. $\Rightarrow$

$$\ker \psi = H \cap K$$

$$\psi \text{ surr} \underbrace{\Rightarrow}_{[1.147, \text{pg.} 60]} \frac{H}{\ker \psi} \simeq \frac{G}{K} \Leftrightarrow \frac{H}{H \cap K} \simeq \frac{G}{K} \underbrace{\Rightarrow}_{\text{Lagrange } [1.53, \text{pg.} 19]} \frac{|H||K|}{|H \cap K|} = |G| \underbrace{\Leftrightarrow}_{[1.153, \text{pg.} 63]} |HK| = |G|$$

$$\begin{cases} HK \subseteq G \\ |HK| = |G| \end{cases} \Rightarrow HK = G$$

1. Dim. $\Leftarrow$

$$G = HK \Rightarrow \frac{G}{K} = \frac{HK}{K} \underbrace{\simeq}_{[1.152, \text{pg.} 63]} \frac{H}{H \cap K} = \frac{H}{\ker \psi} \simeq \text{Im } \psi$$

□

Theorem 1.155. dell'isomorfismo II.

Dati $H, K \leq G$, entrambi normali,

$$H \subseteq K \Rightarrow \frac{G/H}{K/H} \simeq \frac{G}{K}$$

Proof:

$$\begin{cases} H \subseteq K \\ H \leq G \text{ normale} \\ K \leq G \end{cases} \Rightarrow H \leq K \text{ normale rispetto a } K$$

Poiche' H e' normale in G , e quindi anche in K , ha senso considerare

$$\frac{K}{H}, \frac{G}{H}$$

Poiche' $K \leq G$ e' normale, ha senso considerare

$$\frac{G}{K}$$

Inoltre, per la prop [1.115, pg. 47], ha senso considerare

$$\frac{G/H}{K/H}$$

Sia

$$\varphi : \frac{G}{H} \longrightarrow \frac{G}{K}$$

$$\varphi(aH) = aK$$

0.1. φ e' ben posta e surriettiva ed e' un omomorfismo

$$\begin{aligned}
b \in aH &\Leftrightarrow b = ah \\
\varphi(bH) &= bK = ahK \underbrace{=}_{H \subseteq K} aK = \varphi(aH) \\
\varphi(bH) &= \varphi(aH)
\end{aligned}$$

E' immediato verificare che φ e' surriettiva ed e' un omomorfismo.

0.2. $\ker \varphi = K/H$

$$\ker \varphi = \{gH \mid gK = K \Leftrightarrow g \in K\} = \frac{K}{H}$$

0.3. Usiamo il cor [1.147,pg.60] su φ

$$\frac{G/H}{\ker \varphi} \simeq \frac{G}{K} \Leftrightarrow \frac{G/H}{K/H} \simeq \frac{G}{K}$$

□

Proposition 1.156. *Nelle ipotesi del teorema precedente ([1.155,pg.64]), considerando*

$$\begin{array}{ccccc}
\frac{K}{H} & \xrightarrow{i} & \frac{G}{H} & \xrightarrow{\varphi} & \frac{G}{K} \\
& \searrow \alpha & & \swarrow \beta & \\
& & \{e\} & &
\end{array}$$

con

$$\begin{aligned}
\alpha(e) &= H \\
\beta(aK) &= e \quad \forall aK \in \frac{G}{K}
\end{aligned}$$

si ha che in ogni posto della sequenza, l'immagine dell'omomorfismo precedente e' uguale al nucleo dell'omomorfismo successivo.

Si suole dire che questa e' una sequenza esatta corta di 4 omomorfismi.

Questo tipo di sequenze viene studiato in algebra omologica.

Theorem 1.157. *teorema di corrispondenza.*

Dato l'omomorfismo $\varphi : G \longrightarrow G'$, surriettivo, si ha

$$|\{H \leq G \mid H \supseteq \ker \varphi\}| = |\{H' \leq G'\}|$$

La biezione f tra i due insiemi e' indotta da φ stessa:

$$\begin{aligned}
f : M &\longrightarrow N \\
f(H) &= \varphi(H)
\end{aligned}$$

dove M, N sono i due insiemi.

Proof: Poniamo

$$\begin{aligned}
M &= \{H \leq G \mid H \supseteq \ker \varphi\} \\
N &= \{H' \leq G'\}
\end{aligned}$$

1. Dobbiamo far vedere che esiste una funzione biettiva tra M, N

Consideriamo

$$\begin{aligned} f &: M \longrightarrow N \\ f(H) &= \varphi(H) \\ g &: N \longrightarrow M \\ g(H') &= \varphi^{-1}(H') \end{aligned}$$

Bastera' dimostrare che

$$\begin{aligned} f \circ g &= \text{id}_N \\ g \circ f &= \text{id}_M \end{aligned}$$

in questo modo, f, g saranno biettive e l'una l'inversa dell'altra.

1.1. Dim $f \circ g = \text{id}_N$

1.1.1. $g(H') = \varphi^{-1}(H') \supseteq \ker \varphi$

Infatti,

$$h \in \ker \varphi \Rightarrow \varphi(h) = \mathbf{e} \quad \underbrace{\in}_{H' \text{ e' un gruppo}} \quad H' \Rightarrow \varphi(h) \in H' \Rightarrow h \in \varphi^{-1}(H')$$

$$\varphi^{-1}(H') \supseteq \ker \varphi \Rightarrow \varphi^{-1}(H') \in M$$

$$f \circ g(H') = \varphi(\varphi^{-1}(H'))$$

$$\varphi \text{ surriettiva} \quad \underbrace{\Rightarrow}_{\text{prop. delle funzioni [AI, 2.1.3, pg. 9]}} \quad \varphi(\varphi^{-1}(H')) = H'$$

Quindi

$$f \circ g = \text{id}_N$$

1.2. Dim $g \circ f = \text{id}_M$

Prendiamo un $H \in M$ ovvero $H \leq G$: $H \supseteq \ker \varphi$
 $g \circ f(H) = \varphi^{-1}(\varphi(H))$

1.2.1. Dim $\varphi^{-1}(\varphi(H)) = H$

1.2.1.1. Dim $\subseteq$

Sia $h \in \varphi^{-1}(\varphi(H))$, ovvero

$$\varphi(h) \in \varphi(H) \Leftrightarrow \varphi(h) = \varphi(\bar{h})$$

$$H \leq G \quad \underbrace{\Rightarrow}_{[1.141, \text{pg. 57}]} \quad \varphi(H) \leq G'$$

$$\begin{cases} \varphi(h), \varphi(\bar{h}) \in \varphi(H) \\ \varphi(h) = \varphi(\bar{h}) \end{cases} \Rightarrow \varphi(h)\varphi(\bar{h})^{-1} = \mathbf{e}' \Leftrightarrow \varphi(h\bar{h}^{-1}) = \mathbf{e}'$$

$$\Leftrightarrow h\bar{h}^{-1} \in \ker \varphi \Leftrightarrow h\bar{h}^{-1} = k \in \ker \varphi \subseteq H \Rightarrow h\bar{h}^{-1} = h' \in H \Leftrightarrow h = \underbrace{h'}_{\in H} \underbrace{\bar{h}}_{\in H} \in H \Rightarrow h \in H$$

1.2.1.2. Dim $\supseteq$

Sia $h \in H$

$$\varphi(h) \in \varphi(H) \Leftrightarrow h \in \varphi^{-1}(\varphi(H))$$

□

Corollary 1.158. *Se consideriamo solo i sottogruppi normali di G e G' , il thm di corrispondenza vale ancora, ovvero*

$$|\{H' \leq G' \text{ normale}\}| = |\{H \leq G \text{ normale} \mid H \supseteq \ker \varphi\}|$$

Proof:

Se consideriamo la stessa funzione biettiva f vista nella dimostrazione del thm di corrispondenza [1.157,pg.65], avremo

$$\begin{array}{ccc} \left\{ \begin{array}{l} H \text{ normale} \leq G \\ \varphi \text{ surriettiva} \end{array} \right. & \xRightarrow{\text{prop. [1.142,pg.58]}} & \varphi(H) = f(H) \text{ normale} \\ H' \leq G' \text{ normale} & \xRightarrow{\text{prop. [1.143,pg.58]}} & \varphi^{-1}(H) = f^{-1}(H) \text{ normale} \end{array}$$

Quindi f e' la funzione biettiva cercata.

□

Example 1.159. Se $|G'| = p$, dove p primo,

$$|G'| = p \text{ primo} \xLeftrightarrow{\text{[1.55,pg.20]}} (H' \leq G' \Rightarrow H' = \{\mathbf{e}\} \vee H' = G') \Leftrightarrow N = \{\{\mathbf{e}\}, G'\}$$

Allora, per il thm di corrispondenza [1.157,pg.65],

$$|M| = |N| = 2 \Rightarrow M = \{\ker \varphi, G\}$$

1.8.1 Teorema di Cayley

Theorem 1.160. *teorema di Cayley.*

$$\exists f : G \longrightarrow S(G) \text{ immersione}$$

Un'immersione e' un omomorfismo iniettivo.

Equivalentemente, possiamo dire che $f : G \longrightarrow \text{Im } f$ e' un isomorfismo, con $\text{Im } f \leq S(G)$.

Inoltre, una tale immersione e'

$$\begin{aligned} f(a) &= T_a \\ T_a(x) &= ax \end{aligned}$$

T_a si chiama *traslazione sinistra tramite a* .

Proof:

1. Consideriamo una sequenza di tutti gli elementi di G . E' possibile permutarla?

Per permutare la sequenza e ottenerne una nuova, basta moltiplicare tutti i suoi elementi per uno stesso elemento $a \in G$: preso $a \in G$ costruiamo la seguente funzione

$$T_a : G \longrightarrow G$$

$$T_a(x) = ax$$

T_a e' una permutazione, ovvero $T_a \in S(G)$, infatti,

1.1. T_a e' iniettiva

$$T_a(x) = T_a(y) \Leftrightarrow ax = ay \Leftrightarrow x = y$$

1.2. T_a e' surriettiva

Preso $x \in G$, la sua controimmagine e' $a^{-1}x$, infatti,

$$T_a(a^{-1}x) = aa^{-1}x = x$$

2. Quindi, per ogni elemento $a \in G$ nasce una permutazione $T_a \in S(G)$. Questa associazione e' l'omomorfismo cercato.

Consideriamo la seguente funzione

$$f : G \longrightarrow S(G)$$

$$f(a) = T_a$$

2.1. f e' un omeomorfismo

$$f(ab) = T_{ab}$$

$$T_{ab}(x) = (ab)x = a(bx) = aT_b(x) = T_a(T_b(x)) = T_a \circ T_b(x) \quad \forall x \in G$$

$$T_{ab} = T_a \circ T_b$$

2.2. f e' iniettiva

$$f(a) = f(b) \Leftrightarrow T_a = T_b \Rightarrow T_a(e) = T_b(e) \Leftrightarrow ae = be \Leftrightarrow a = b$$

□

Example 1.161. Sia $|G| = 8$, allora

$$G \xrightarrow{f} S(G) \simeq S_8$$

Theorem 1.162. *teorema di Cayley generalizzato.*

Sia $(G, \cdot)$ un gruppo. Preso un $H \leq G$, sia $G/_sH = \{aH\}_{a \in G}$ l'insieme quoziente su G indotto dalla relazione d'equivalenza $\equiv_s(H)$ (vedi [1.48, pg. 18]). Allora,

$$\exists f : G \longrightarrow S(G/_sH) \text{ omomorfismo}$$

Valgono inoltre le seguenti proprieta':

1. f potrebbe non essere iniettivo.
2. $K = \ker f \subseteq H$
3. K e' il piu' grande sottogruppo normale in G , contenuto in H :

$$N \subseteq H \text{ normale in } G \Rightarrow N \subseteq K$$

$$4. \ker f = \{a \in G \mid \forall x \in G \quad axH = xH\}$$

Proof:

La dimostrazione e' simile a quella del thm [1.160, pg. 67].

Intanto, per comodita' poniamo $M = G/_sH$. Sia

$$T_a : M \longrightarrow M$$

$$T_a(xH) = axH$$

0.1. $T_a \in S(M)$

E' iniettiva:

$$T_a(xH) = T_a(yH) \Leftrightarrow axH = ayH$$

dimostriamo che $xH = yH$

0.1.1. $\text{Dim} \subseteq$

$$xh \in xH$$

$$axh \in axH = ayH \Rightarrow axh = ayh' \Leftrightarrow xh = yh' \Leftrightarrow xh \in yH$$

0.1.2. $\text{Dim} \supseteq$

$$yh \in yH$$

$$ayh \in ayH = axH \Rightarrow ayh = axh' \Leftrightarrow yh = xh' \Leftrightarrow yh \in xH$$

E' surriettiva: preso $yH \in M$, la sua controimmagine e' $a^{-1}yH$, infatti

$$T_a(a^{-1}yH) = aa^{-1}yH = yH$$

0.2. f e' un omomorfismo

A questo punto consideriamo

$$f : G \longrightarrow S(M)$$

$$f(a) = T_a$$

e' un omomorfismo.

$$f(ab) = T_{ab}$$

$$T_{ab}(xH) = abxH = aT_b(xH) = T_a(T_b(xH)) = T_a \circ T_b(xH) \quad \forall xH \in M$$

$$T_{ab} = T_a \circ T_b$$

0.3. f puo' non essere iniettivo.

Portiamo un esempio. Consideriamo G con $|G| = 35$.

E sia $H \leq G$ con $|H| = 7$. Per il thm di Lagrange (vedi [1.53,pg.19]),

$$i_G(H) = \frac{|G|}{|H|} = 5$$

Ricordiamoci che $i_G(H) = |G/_sH| = |M|$, quindi
 $|S(M)| = 5! = 120$

Se per assurdo f fosse iniettiva,

$$|\text{Im } f| = |G| = 35$$

, ma poiche'

$$\text{Im } f \leq S(M)$$

risulta, sempre per Lagrange, che $|\text{Im } f|$ e' un divisore di $|S(M)|$. Ma questo e' assurdo dato che $35 \nmid 120$.

0.4. $K = \ker f = \{a \in G \mid \forall xH \in M \quad axH = xH\}$

$$\ker f = \{a \in G \mid f(a) = \mathbf{e}' = \text{id}_M\}$$

$$f(a) = \text{id}_M \Leftrightarrow T_a = \text{id}_M \Leftrightarrow$$

$$\Leftrightarrow T_a(xH) = \text{id}_M(xH) \Leftrightarrow axH = xH \quad \forall xH \in M$$

0.5. $K = \ker f \subseteq H$

$$k \in \ker f \Rightarrow kxH = xH \quad \forall xH \in M \quad \underbrace{\Rightarrow}_{\text{per } x=\mathbf{e}} kH = H \Rightarrow k \in H$$

0.6. Dimostriamo che

$$N \subseteq H \text{ normale in } G \Rightarrow N \subseteq K$$

Che $\ker f$ sia normale lo sappiamo gia' (vedi [1.144,pg.58]).

Supponiamo che $N \leq H$ normale. Dimostriamo che $N \subseteq K$

$$n \in N, \quad x \in G$$

$$nx \in Nx \quad \underbrace{=}_{N \text{ e' normale}} \quad xN \Rightarrow nx = xn'$$

$$nxH = xn'H \quad \underbrace{=}_{N \subseteq H} \quad xH \quad \forall x \in G \Leftrightarrow n \in K$$

□

Corollary 1.163.

$$\begin{cases} H \leq G, & |H| = p \text{ primo} \\ |G| \not\mid i_G(H)! \end{cases} \Rightarrow H \text{ e' normale}$$

Proof:

Sia $i = i_G(H)$ e sia $|G| = n$. L'ipotesi dice che n non divide $i!$

Per il thm di Cayley [1.162,pg.68],

$$\exists f : G \longrightarrow S(G/_sH) \text{ omomorfismo}$$

0.1. f non e' iniettivo

Se per assurdo lo fosse, si avrebbe $|\text{Im } f| = n$, ma

$$|\text{Im } f| \leq |S(G/_sH)| \Rightarrow |\text{Im } f| = n \text{ divide } |S(G/_sH)| = |G/_sH|! = i_G(H)!$$

$$n \not\mid i_G(H)!$$

assurdo contro ipotesi.

Analizziamo il $\ker f$:

$$f \text{ non iniettivo} \Rightarrow \{\mathbf{e}\} \subset \ker f \quad (1)$$

Sempre per il thm di Cayley, $\ker f = K$ e' il piu' grande sottogruppo normale di H ,

Per la prop [1.55,pg.20], gli unici sottogruppi di H sono quelli banali, quindi

$$K \leq H \Rightarrow K = \{\mathbf{e}\} \vee K = H \underset{(1)}{\Rightarrow} K = H$$

In conclusione, $H = \ker f$, ed e' quindi normale.

□

Corollary 1.164.

$$\begin{cases} |G| = pq, & p \geq q, & p \text{ primo} \\ H \leq G, & |H| = p \end{cases} \Rightarrow H \text{ normale}$$

Proof:

$$\frac{q!}{pq} = \frac{(q-1) \cdot (q-2) \dots 3 \cdot 2 \cdot 1}{p}$$

ma $p \geq q$, quindi $p \neq (q-i)$ $i = 1, 2, \dots, q$, percio'

$$pq \not\mid q!$$

Poiche'

$$i_G(H) \underset{\text{lagrange}[1.53,pg.19]}{=} \frac{|G|}{|H|} = \frac{pq}{p} = q$$

$$pq \not\mid q! \Leftrightarrow |G| \not\mid i_G(H)!$$

quindi, le ipotesi del cor [1.163,pg.70] sono rispettate, quindi H e' normale.

□

Example 1.165. $|G| = 5 \cdot 4 = 20$, $|H| = 5 \Rightarrow H$ normale

Example 1.166. G gruppo, $|G| = 2n$, allora

$$\exists H \leq G : |H| = 2$$

Se inoltre n e' dispari, si ha

$$\exists H \leq G : |H| = n$$

Proof:

1. Dim 1.

Un sottogruppo di ordine 2 e' del tipo $\{e, a\}$, con $a \neq e$, $a^2 = e$, o equivalentemente, con $a \neq e$, $a = a^{-1}$.

Supponiamo per assurdo che non ne esistano, ovvero che

$$\forall a \in G : a \neq e \quad a^2 \neq e \Leftrightarrow a \neq a^{-1}$$

allora, riusciamo a disporre gli elementi di G in questa maniera:

$$G = \begin{cases} e \\ a_1 \neq a_1^{-1} \\ a_2 \neq a_2^{-1} \\ \dots \end{cases}$$

ma allora il numero di elementi di G e' dispari. Assurdo contro $|G| = 2n$

2. Dim 2.

Per Cayley [1.160,pg.67], abbiamo la seguente immersione f :

$$f : G \longrightarrow S(G) \simeq S_{2n}$$

$$f(a) = T_a$$

2.1. $\text{Im } f \not\subseteq A_{2n}$

Basta che troviamo una $f(a)$ che non e' una permutazione pari.

Come a prendiamo lo stesso a di prima, ovvero, $a \in G : a \neq e$, $a^2 = e$.

$f(a) = T_a$ non lascia fisso alcun elemento: se per assurdo $T_a(x) = x$,

$$T_a(x) = x \Leftrightarrow ax = x \Leftrightarrow a = e$$

assurdo contro $a \neq e$.

$$f(a^2) = f(aa) \underbrace{=}_{f \text{ e' un omo}} f(a)f(a) = T_a T_a$$

$$a^2 = e \Leftrightarrow f(a^2) = f(e) \Leftrightarrow T_a T_a = \text{id} \Leftrightarrow T_a^2 = \text{id}$$

Quindi T_a^2 e' la permutazione identica.

$$T_a \neq \text{id}, \quad T_a^2 = \text{id} \Leftrightarrow o(T_a) = 2 \underbrace{=}_{\text{thm}[1.69,pg.25]} = \text{mcm}(l(c_1), l(c_2), \dots, l(c_k))$$

dove $c_1, c_2, \dots, c_k$ sono i cicli che compongono T_a .

Poiche' T_a non lascia fisso alcun elemento, non esiste un ciclo c_i di ordine 1 (a parte il ciclo identita'), quindi

$$\text{mcm}(l(c_1), l(c_2), \dots, l(c_k)) = 2, \quad l(c_i) > 1 \Rightarrow l(c_i) = 2 \quad \forall i = 1, 2, \dots, k$$

Percio', sara' del tipo

$$T_a = (a_1 a'_1)(a_2 a'_2) \dots (a_n a'_n)$$

dove gli a_i, a'_i sono tutti distinti fra loro

allora, T_a e' formata da n trasposizioni. n e' dispari. Quindi $T_a \notin A_{2n}$

2.2. $\text{Im } f$ ha meta' permutazioni pari e meta' dispari

Sia $H = A_{2n} \cap \text{Im } f$. H e' l'insieme di tutte le permutazioni pari di $\text{Im } f$. Sia $T_a = g \notin A_{2n}$ la permutazione dispari che abbiamo trovato prima.

Poiche' g e' dispari, gH e' un insieme di permutazioni dispari, inoltre, $gH \subseteq \text{Im } f$, infatti:

$$gH \ni gh = T_a T_{a'} \underbrace{\in}_{\text{Im } f \text{ e' un gruppo}} \text{Im } f$$

Anzi, gH e' l'insieme di tutte le permutazioni dispari di $\text{Im } f$, infatti, sia $b \in \text{Im } f$ una

permutazione dispari, allora

$$g, b \text{ dispari} \Rightarrow g^{-1}b \text{ pari}$$

$$\begin{cases} g^{-1}, b \in \text{Im } f \Rightarrow g^{-1}b \in \text{Im } f \\ g^{-1}b \text{ pari} \Leftrightarrow g^{-1}b \in A_{2n} \end{cases} \Rightarrow g^{-1}b \in H \Leftrightarrow g^{-1}b = h \Leftrightarrow b = gh \Leftrightarrow b \in gH$$

Poiche' esistono solo permutazioni pari o dispari,

$$\text{Im } f = H \cup gH$$

$$|\text{Im } f| = |H \cup gH| \underset{H \cap gH = \emptyset}{=} |H| + |gH|$$

$$2n = |\text{Im } f| = |H| + |gH|$$

Per le proprieta' dei laterali, $|gH| = |H|$, quindi

$$2|H| = 2n \Leftrightarrow |H| = n$$

$$\begin{cases} f \text{ iniettiva} \\ H \leq \text{Im } f \end{cases} \Rightarrow |f^{-1}(H)| = |H|$$

$f^{-1}(H)$ e' quindi il sottogruppo cercato, ovvero

$$|f^{-1}(H)| = n$$

□

1.9 Azione di un gruppo

Definition 1.167. Sia dato un gruppo G e un insieme X , definiamo l'*azione* $*$ del gruppo G su X come la funzione:

$$\begin{aligned} * : G \times X &\longrightarrow X \\ (g, x) &\mapsto g * x \end{aligned}$$

che rispetta le seguenti proprieta':

$$\begin{aligned} \mathbf{e} * x &= x \quad \forall x \in X \\ (a \cdot b) * x &= a * (b * x) \quad \forall a, b \in G \quad \forall x \in X \end{aligned}$$

In altre parole, ogni elemento $g \in G$ puo' essere visto come la funzione:

$$g* : X \longrightarrow X$$

che porta un elemento di X in un altro elemento di X .

Proposition 1.168. La funzione $g* : X \longrightarrow X$ e' biettiva, ovvero $g* \in S(X)$, e inoltre

$$\begin{aligned} \varphi : G &\longrightarrow S(X) \\ \varphi(g) &= g* \end{aligned}$$

e' un omomorfismo tra gruppi.

Proof:

1. $g*$ e' biettiva

Infatti, l'inversa di $g*$ e' $g^{-1}*$,

$$(g* \circ g^{-1}*)(x) = g*(g^{-1}*(x)) = g*(g^{-1}*x) = (gg^{-1})*x = \mathbf{e}*x = x$$

$$(g^{-1}* \circ g*)(x) = g^{-1}*(g*(x)) = g^{-1}*(g*x) = (g^{-1}g)*x = \mathbf{e}*x = x$$

2. φ e' un omomorfismo

$$\begin{aligned}\varphi(ab) &= (ab)* \\ \forall x \in X \quad (ab)*x &= a*(b*x) = (a* \circ b*)(x) = (\varphi(a) \circ \varphi(b))(x) \\ \varphi(ab) &= (ab)* = \varphi(a) \circ \varphi(b)\end{aligned}$$

□

Definition 1.169. Definiamo lo stabilizzatore di x :

$$\text{St}(x) = \{g \in G \mid g*x = x\}$$

certamente $e \in \text{St}(x)$.

Proposition 1.170. $\text{St}(x) \leq G$

Ovvero, lo stabilizzatore di x e' un sottogruppo di G .

Proof: Usiamo la caratterizzazione [1.21,pg.7]

$a, b \in \text{St}(x)$

$$\begin{aligned}b*x = x &\Leftrightarrow b^{-1}*(b*x) = b^{-1}*x \Leftrightarrow (b^{-1}b)*x = b^{-1}*x \Leftrightarrow e*x = b^{-1}*x \Leftrightarrow x = b^{-1}*x \Rightarrow b^{-1} \in \text{St}(x) \\ (ab^{-1})*x &= a*(b^{-1}*x) = a*x = x \Rightarrow ab^{-1} \in \text{St}(x)\end{aligned}$$

□

Definition 1.171. Definiamo l'orbita di $x \in G$:

$$\mathcal{O}(x) = \{g*x \mid \forall g \in G\}$$

ovvero e' l'insieme di tutti gli elementi di X a cui x e' associato tramite una $g*$.

Poiche' $e*x = x$, $x \in \mathcal{O}(x)$.

Se $\mathcal{O}(x) = X$, $\mathcal{O}(x)$ si dira' transitiva.

Proposition 1.172. L'insieme di tutte le orbite e' una partizione di X .

Indicheremo con X/G tale insieme.

Proof:

La tesi equivale a dire che la relazione

$$y \sim x \Leftrightarrow y \in \mathcal{O}(x)$$

e' una relazione d'equivalenza. Infatti, $\mathcal{O}(x)$ diventa la classe d'equivalenza di x , e tutte le classi di equivalenza stabiliscono una partizione in X .

Dimostriamo quindi che e' una relazione d'equivalenza.

0.1. $x \sim x$

$$x \sim x \Leftrightarrow x \in \mathcal{O}(x) \text{ vero}$$

0.2. $x \sim y \Rightarrow y \sim x$

$$x \sim y \Leftrightarrow x \in \mathcal{O}(y) \Leftrightarrow \exists g \in G : g*y = x$$

$$g^{-1}*(g*y) = g^{-1}*x$$

$$g^{-1}*(g*y) = (g^{-1} \cdot g)*y = e*y = y$$

$$y = g^{-1}*x \Rightarrow y \in \mathcal{O}(x) \Leftrightarrow y \sim x$$

0.3. $x \sim y, y \sim z \Rightarrow x \sim z$

$$\begin{aligned}
x \sim y &\Leftrightarrow x \in \mathcal{O}(y) \Rightarrow \exists g \in G : g * y = x \\
y \sim z &\Leftrightarrow y \in \mathcal{O}(z) \Rightarrow \exists g' \in G : g' * z = y \\
(g \cdot g') * z &= g * (g' * z) = g * y = x \\
(g \cdot g') * z &= x \Rightarrow x \in \mathcal{O}(z) \Leftrightarrow x \sim z
\end{aligned}$$

□

Proposition 1.173.

Per ogni $x \in X$, si ha

$$|\mathcal{O}(x)| = i_G(\text{St}(x))$$

Nota: questo vale sia nel caso finito che in quello infinito.

Proof:

1. Dimostriamo che esiste una funzione biettiva tra $\mathcal{O}(x)$ e $\{a\text{St}(x)\}_{a \in G}$.⁹⁾

Consideriamo la seguente funzione:

$$\begin{aligned}
f : \mathcal{O}(x) &\longrightarrow G/\text{St}(x) \\
f(g * x) &= g\text{St}(x)
\end{aligned}$$

- 1.1. Dimostriamo che f è ben posta, ovvero che

$$g * x = g' * x \Rightarrow g\text{St}(x) = g'\text{St}(x)$$

$$\begin{aligned}
g * x = g' * x &\Leftrightarrow g^{-1} * (g * x) = g^{-1} * (g' * x) \Leftrightarrow \\
&\Leftrightarrow (g^{-1}g) * x = (g^{-1}g') * x \Leftrightarrow \mathbf{e} * x = (g^{-1}g') * x \Leftrightarrow x = (g^{-1}g') * x \\
x = (g^{-1}g') * x &\Leftrightarrow g^{-1}g' \in \text{St}(x) \Leftrightarrow g^{-1}g' = s \Leftrightarrow g' = gs \in g\text{St}(x) \Leftrightarrow g'\text{St}(x) = g\text{St}(x)
\end{aligned}$$

Procedendo a ritroso si ha pure che:

$$g * x = g' * x \Leftarrow g\text{St}(x) = g'\text{St}(x) \Leftarrow f(g * x) = f(g' * x)$$

ovvero, f è iniettiva.

È immediato verificare che f è suriettiva.

□

Corollary 1.174. Se G è finito, dalla precedente proposizione e dal teorema di Lagrange, si ha:

$$\begin{aligned}
|G| &= |\text{St}(x)|i_G(\text{St}(x)) \\
|G| &= |\text{St}(x)||\mathcal{O}(x)|
\end{aligned}$$

Example 1.175. Con G , $X = G$ consideriamo l'azione

$$T : G \times X \longrightarrow X \qquad T(g, x) = gx$$

chiamata *traslazione* si ha

$$\begin{aligned}
\mathcal{O}(x) &= X \text{ infatti} \\
y \in X = G &\Rightarrow gx = y \Leftrightarrow g = yx^{-1} \\
\text{St}(x) &= \{\mathbf{e}\}
\end{aligned}$$

⁹⁾ricordiamoci che $i_G(\text{St}(x)) = |\{a\text{St}(x)\}_{a \in G}|$

Theorem 1.176. (*Lemma di Burnside*)

Sia X un insieme su cui agisce G , poniamo

$$X^g = \{x \in X \mid gx = x\}$$

Sia X/G l'insieme di tutte le orbite, si ha:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Questo teorema ha diverse applicazioni in combinatorica, perche' permette di contare in maniera alternativa $|X/G|$.

Proof:

$$\begin{aligned} \sum_{g \in G} |X^g| &= |\{(g, x) \in G \times X \mid gx = x\}| = \sum_{x \in X} |\text{St}(x)| \stackrel{[1.174, \text{pg. } 74]}{=} \sum_{x \in X} \frac{|G|}{|\mathcal{O}(x)|} = \\ &= |G| \sum_{x \in X} \frac{1}{|\mathcal{O}(x)|} \stackrel{[1.172, \text{pg. } 73]}{=} |G| \sum_{A \in X/G} \sum_{x \in A} \frac{1}{|A|} = |G| \sum_{A \in X/G} \frac{|A|}{|A|} = \\ &= |G| |X/G| \end{aligned}$$

□

Lemma 1.177. Dato $|G|$, con $|G| = p$ primo, si ha:

1. $\forall x \in X \quad |\mathcal{O}(x)| = 1 \vee |\mathcal{O}(x)| = p$
2. $|X| = \lambda p, \exists x \in X : |\mathcal{O}(x)| = 1 \Rightarrow |Y| = \mu p \geq p, \quad \text{dove } Y = \{y \in X \mid |\mathcal{O}(y)| = 1\}$

In sostanza, la seconda proposizione dice che se $|X|$ e' un multiplo di p e se esiste almeno un x la cui orbita ha un solo elemento, allora il numero di tutti gli $y \in Y$ la cui orbita ha un solo elemento e' un multiplo di p .
(ovviamente $\lambda, \mu \neq 0$).

Proof:

Preso $x \in X$, per il cor [1.174, pg. 74] si ha

$$|G| = |\mathcal{O}(x)| |\text{St}(x)| \Rightarrow |\mathcal{O}(x)| \mid |G| = p \stackrel{p \text{ e' primo}}{\Rightarrow} |\mathcal{O}(x)| = 1 \vee |\mathcal{O}(x)| = p \quad (1)$$

Supponiamo adesso che $|X| = \lambda p$ e che $|\mathcal{O}(x)| = 1$. Poniamo $k = |Y|$.

Poiche' le orbite formano una partizione di X , si ha che $|X|$ e' uguale alla somma delle cardinalita' di tutte le orbite. Dalla (1) sappiamo che le orbite hanno cardinalita' 1 o p . Tutte quelle con cardinalita' 1 sono in Y . Con h indichiamo il numero di orbite di cardinalita' p . Abbiamo quindi

$$|X| = |Y| + ph = k + ph \Leftrightarrow \lambda p = k + ph \Rightarrow p \mid k \Leftrightarrow k = \mu p$$

Infine, poiche' $\exists x \in X : |\mathcal{O}(x)| = 1$, si ha $k \neq 0 \Leftrightarrow \mu \geq 1$ e quindi

$$\mu \geq 1 \Rightarrow \mu p \geq p$$

□

Theorem 1.178. di Cauchy.

$$|G| = n, p \text{ primo}, p \mid n \Rightarrow \exists H \leq G : |H| = p$$

$$\exists H \leq G : |H| = p \Leftrightarrow \exists a \in G : o(a) = p \Leftrightarrow \exists a \in G : \begin{cases} a^p = e \\ a \neq e \end{cases}$$

Proof: Intanto,

$$p \nmid n \Leftrightarrow p \nmid \lambda = n \quad (*)$$

1. Dimostriamo che la tesi e' equivalente a $\exists a \in G : \begin{cases} a^p = \mathbf{e} \\ a \neq \mathbf{e} \end{cases}$

$$|H| = p \text{ primo} \quad \underbrace{\Rightarrow}_{[1.56, \text{pg.20}]} \quad \exists a \in G : H = \langle a \rangle \quad \underbrace{\Rightarrow}_{[1.34, \text{pg.11}]} \quad o(a) = |H| = p$$

dimostriamo il viceversa:

$$a \neq \mathbf{e} \Rightarrow o(a) > 1$$

$$a^p = \mathbf{e} \Rightarrow o(a) \mid p \quad \underbrace{\Rightarrow}_{o(a) > 1, \text{ } p \text{ e' primo}} \quad o(a) = p \Rightarrow |\langle a \rangle| = p \Rightarrow H = \langle a \rangle \leq G$$

2. Quindi per dimostrare il teorema di Cauchy, basta far vedere che $\exists a \neq \mathbf{e} : a^p = \mathbf{e}$
Consideriamo l'insieme

$$X = \left\{ (y_1, \dots, y_p) \mid y_i \in G, \prod_{i=1}^p y_i = \mathbf{e} \right\}$$

X non e' vuoto, perche'

$$E = (\mathbf{e}, \mathbf{e}, \dots, \mathbf{e}) \in X$$

Se consideriamo l'elemento $a \in G$ della tesi, si ha

$$a^p = \mathbf{e} \Leftrightarrow a \cdot a \cdot \dots \cdot a = \mathbf{e} \Leftrightarrow (a, a, \dots, a) \in X$$

Quindi il nostro obbiettivo e' trovare un $y \in X : y_1 = y_2 = \dots = y_p, y_1 \neq \mathbf{e}$.

Osserviamo che

$$y_1 = y_2 = \dots = y_p \Leftrightarrow (y_{1+i}, y_{2+i}, \dots, y_{p+i}) = y \quad \forall i \in \{1, 2, \dots, p\} \quad (0)$$

dove le addizioni negli indici si intendono in $\mathbb{Z}_p$. Per chiarire le idee:

$$i = 0 : (y_1, y_2, \dots, y_{p-1}, y_p) \quad (1)$$

$$i = 1 : (y_2, y_3, \dots, y_p, y_1)$$

$$i = 2 : (y_3, y_4, \dots, y_1, y_2)$$

...

Quindi per ogni i stiamo permutando in modo particolare la p -upla y .

Possiamo intendere queste permutazioni, come l'azione di $(\mathbb{Z}_p, +)$ su X secondo la seguente legge:

$$i * (y_1, y_2, \dots, y_p) = (y_{1+i}, y_{2+i}, \dots, y_{p+i})$$

2.1. $*$ e' una azione

infatti,

$$0 * (y_1, y_2, \dots, y_p) = \underbrace{(y_1, y_2, \dots, y_p)}_{(1)}$$

$$(i + j) * (y_1, y_2, \dots, y_p) = (y_{1+i+j}, y_{2+i+j}, \dots, y_{p+i+j}) = i * (j * (y_1, y_2, \dots, y_p))$$

Con l'azione possiamo riscrivere la (0) in questo modo:

$$(y_{1+i}, y_{2+i}, \dots, y_{p+i}) = y \quad \forall i \in \{1, 2, \dots, p\} \Leftrightarrow i * y = y \quad \forall i \in \mathbb{Z}_p \Leftrightarrow \text{St}(y) = \mathbb{Z}_p, \quad \mathcal{O}(y) = \{y\}$$

Quindi, il nostro obbiettivo e' stato rifinito:

$$\text{dobbiamo trovare un } y \in X : |\mathcal{O}(y)| = 1, y \neq E$$

Contiamo innanzitutto gli elementi di X .

2.2. $|X| = n^{p-1}$

$$y = (y_1, \dots, y_p) \in X \Leftrightarrow y_1 y_2 \dots y_p = \mathbf{e} \Leftrightarrow (y_1 \dots y_{p-1})^{-1} = y_p \quad (2)$$

Quindi, prese le prime $p - 1$ componenti di y , conosciamo l'ultima.
Consideriamo allora la seguente funzione:

$$f : G^{p-1} \longrightarrow X$$

$$(y_1, y_2, \dots, y_{p-1}) \mapsto (y_1, y_2, \dots, y_{p-1}, (y_1 y_2 \dots y_{p-1})^{-1})$$

La sua inversa e'

$$g : X \longrightarrow G^{p-1}$$

$$(y_1, \dots, y_p) \mapsto (y_1, y_2, \dots, y_{p-1})$$

infatti,

$$f \circ g(y_1, \dots, y_p) = f((y_1, y_2, \dots, y_{p-1})) = (y_1, y_2, \dots, y_{p-1}, (y_1 y_2 \dots y_{p-1})^{-1}) \underset{(2)}{=} (y_1, \dots, y_p)$$

$$g \circ f(y_1, y_2, \dots, y_{p-1}) = g(y_1, y_2, \dots, y_{p-1}, (y_1 y_2 \dots y_{p-1})^{-1}) = (y_1, y_2, \dots, y_{p-1})$$

Avendo l'inversa, f e' biettiva e quindi

$$\begin{aligned} |X| &= |G^{p-1}| = |G|^{p-1} = n^{p-1} \\ \left\{ \begin{array}{l} |X| = n^{p-1} \underset{(*)}{=} \lambda^{p-1} p^{n-1} = \mu p \\ |\mathbb{Z}_p| = p \text{ primo} \\ E \in X, |\mathcal{O}(E)| = 1 \end{array} \right. &\xRightarrow{\text{lemma [1.177, pg.75]}} |\underbrace{\{y \in X : |\mathcal{O}(x)| = 1\}}_Y| = kp > 1 \end{aligned}$$

$$E \in Y, |Y| > 1 \Rightarrow \exists \bar{y} \in X : \bar{y} \neq E, |\mathcal{O}(\bar{y})| = 1$$

che e' proprio quello che cercavamo.

□

1.9.1 Azione di coniugio

Con $G, X = G$, consideriamo la seguente azione¹⁰:

$$g * x = gxg^{-1}$$

che viene detta *azione di coniugio* o di coniugazione.

Proposition 1.179. $\text{St}(x) = C(x)$

dove $C(x)$ e' il centralizzante di x (vedi [1.24, pg.8])

Proof:

$$\text{St}(x) = \{g \in G \mid g * x = x \Leftrightarrow gxg^{-1} = x \Leftrightarrow gx = xg\} = C(x)$$

Proposition 1.180.

$$\mathcal{O}(x) = \{x\} \Leftrightarrow x \in Z(G)$$

Poiche' per la prop [1.172, pg.73] $\mathcal{O}(x)$ e' una classe, si ha che ogni elemento del centro individua una classe.

Proof:

1. Dim $\Leftrightarrow$

¹⁰e' immediato verificare che si tratta di una azione

$$\mathcal{O}(x) = \{x\} \Leftrightarrow (\forall g \in G \quad g * x = x \Leftrightarrow gxg^{-1} = x \Leftrightarrow gx = xg) \Leftrightarrow x \in Z(G)$$

□

Proposition 1.181. *Se G è finito, si ha l'equazione di classe:*

$$\begin{aligned} |G| &= |Z(G)| + \sum_{z \in F} |\mathcal{O}(z)| = |Z(G)| + \sum_{z \in F} \frac{|G|}{|C(z)|} \\ F &= f(\{\mathcal{O}(x) \mid x \notin Z(G)\}) \\ f : \{\mathcal{O}(x)\}_{x \in X} &\longrightarrow X \text{ tale che } f(\mathcal{O}(x)) \in \mathcal{O}(x) \end{aligned}$$

In altre parole, la sommatoria è estesa a tutti gli elementi esterni a $Z(G)$ e presi uno per orbita.

Proof:

Poiché le orbite formano una partizione di X , e poiché $X = G$, le orbite formano una partizione di G , perciò:

$$G = \bigcup_{x \in X} \mathcal{O}(x) = \bigcup_{z \in f(\{\mathcal{O}(x)\}_{x \in X})} \mathcal{O}(z) \Rightarrow |G| = \sum_{z \in f(\{\mathcal{O}(x)\}_{x \in X})} |\mathcal{O}(z)|$$

dobbiamo usare la funzione f perché altrimenti conteremmo più volte una stessa classe, ovvero commetteremmo un errore del tipo $|\mathcal{O}(x)| + |\mathcal{O}(x')| + \dots$, con $x, x' \in \mathcal{O}(x)$.

Per la proposizione [1.180,pg.77], ad ogni elemento del centro corrisponde una classe, quindi possiamo direttamente contare tutte queste classi contando gli elementi di $Z(G)$:

$$|G| = |Z(G)| + \sum_{z \in f(\{\mathcal{O}(x)\}_{x \notin Z(G)})} |\mathcal{O}(z)|$$

A questo punto, per il cor [1.174,pg.74] e la prop [1.179,pg.77], abbiamo

$$\begin{aligned} |\mathcal{O}(x)| &= \frac{|G|}{|\text{St}(x)|} \\ \text{St}(x) &= C(x) \\ |\mathcal{O}(x)| &= \frac{|G|}{|C(x)|} \end{aligned}$$

e quindi

$$|G| = |Z(G)| + \sum_{z \in f(\{\mathcal{O}(x)\}_{x \notin Z(G)})} \frac{|G|}{|C(z)|}$$

□

Proposition 1.182. $H \leq G$ normale $\Leftrightarrow H$ è unione di orbite.

Proof:

1. Dim $\Rightarrow$

$$H \leq G \quad \Leftrightarrow \quad \forall a \in G \quad \forall h \in H \quad aha^{-1} \in H \Leftrightarrow a * h \in H$$

[1.104,pg.42]

fissato $h \in H$ si ha allora $\forall a \in G \quad a * h \in H \Leftrightarrow \mathcal{O}(h) \subseteq H$

e quindi al variare di $h \in H$ si ha $\forall h \in H \quad \mathcal{O}(h) \subseteq H \Leftrightarrow \bigcup_{h \in H} \mathcal{O}(h) \subseteq H$

e poiché $h \in \mathcal{O}(h)$ si ha $\bigcup_{h \in H} \mathcal{O}(h) \supseteq H$

e quindi l'uguaglianza

2. Dim $\Leftarrow$

$$\begin{aligned}
 H &= \bigcup_{x \in I} \mathcal{O}(x) \quad \text{dove } I \text{ e' un qualche } I \subseteq G \\
 h \in H &\Rightarrow \exists \bar{x} \in I : h \in \mathcal{O}(\bar{x}) \quad \Leftrightarrow \quad \mathcal{O}(h) = \mathcal{O}(\bar{x}) \\
 &\quad \mathcal{O}(x) \text{ e' una classe d'equiv.} \\
 \mathcal{O}(h) &= \mathcal{O}(\bar{x}) \subseteq \bigcup_{x \in I} \mathcal{O}(x) \subseteq H \\
 h \in H &\Rightarrow \mathcal{O}(h) \subseteq H \quad (*)
 \end{aligned}$$

Dobbiamo dimostrare che

$$\forall g \in G \quad \forall h \in H \quad ghg^{-1} \in H$$

Basta usare la (*):

$$ghg^{-1} = g * h \in \mathcal{O}(h) \underset{(*)}{\subseteq} H$$

□

2 p-gruppo

Definition 2.1.

$$G \text{ e' un } p\text{-gruppo} \stackrel{\text{def}}{\Leftrightarrow} |G| = p^k, \quad p \text{ primo}, \quad k > 0$$

Proposition 2.2.

$$G \text{ e' un } p\text{-gruppo} \Leftrightarrow \forall a \in G \setminus \{e\} \quad \exists i \in \mathbb{N} : o(a) = p^i$$

Proof:

1. Dim $\Rightarrow$

I divisori di $|G| = p^k$ sono

$$1, p, p^2, \dots, p^k$$

e per Lagrange sono gli unici ordini di sottogruppi di G , allora, preso $a \in G \setminus \{e\}$, abbiamo le seguenti possibilita':

$$\langle a \rangle = p, p^2, \dots, p^k \Rightarrow o(a) = p, p^2, \dots, p^k$$

2. Dim $\Leftarrow$

Supponiamo per assurdo che $|G| = p^k q^h$, con q primo distinto da p .

$$q \nmid |G| \quad \Rightarrow \quad \exists a \in G \setminus \{e\} : o(a) = q \text{ assurdo contro Hp}$$

Cauchy [1.178, pg. 75]

□

Proposition 2.3. Sia X l'insieme su cui agisce G , si ha

$$G \text{ } p\text{-gruppo}, |G| = p^k \Rightarrow \forall x \in X \quad \exists t : |\mathcal{O}(x)| = p^t, \quad 0 \leq t \leq k$$

Proof:

Per la prop. [1.174, pg. 74],

$$|\mathcal{O}(x)| \nmid |G| = p^k \quad \Rightarrow \quad |\mathcal{O}(x)| = 1 \vee |\mathcal{O}(x)| = p^t, \quad 1 \leq t \leq k$$

p e' primo

□

Proposition 2.4.

$$G \text{ } p\text{-gruppo} \Rightarrow \{e\} \subsetneq Z(G), \quad |Z(G)| = p^t, \quad 1 \leq t \leq k$$

Proof:

0.1. Dim 1.

Consideriamo l'azione di coniugio su G .

Per l'equazione di classe (vedi [1.181,pg.78]), si ha

$$|Z(G)| = |G| - \sum_{z \in F} |\mathcal{O}(z)| = p^k - \sum_{z \in F} |\mathcal{O}(z)|$$

$$z \in F \Rightarrow |\mathcal{O}(z)| \neq 1 \quad \underbrace{\Rightarrow}_{\text{prop}[2.3,pg.79]} \quad |\mathcal{O}(z)| = p^t \Rightarrow p \nmid |\mathcal{O}(z)|$$

p divide tutto il secondo membro, e quindi anche $|Z(G)|$,

$$\begin{cases} |Z(G)| \geq 1 \\ p \nmid |Z(G)| \end{cases} \Rightarrow |Z(G)| \geq p > 1$$

0.2. Dim 2.

sia $Z = Z(G)$

$$Z \leq G \quad \underbrace{\Rightarrow}_{\text{Lagrange}} \quad |Z| \nmid |G| = p^k \Rightarrow |Z| = p^t, \quad 0 \leq t \leq k$$

$$Z \neq \{e\} \Rightarrow |Z| > 1 \Rightarrow 0 < t \leq k$$

□

Proposition 2.5. Dato G con $|G| = p^k$, p primo, allora

$\exists H_1, H_2, \dots, H_k \leq G$ normali tali che

$$\{e\} \subseteq H_1 \subseteq H_2 \subseteq \dots \subseteq H_k = G$$

$$|H_i| = p^i, \quad i = 1, 2, \dots, k$$

Si vuol dire che esiste una catena di sottogruppi normali di G , di ordine $1, p, \dots, p^k$.

Proof: Procediamo per induzione su k

1. $k = 1$

In questo caso, $|G| = p$ e quindi essendo p primo, gli unici sottogruppi di G sono $\{e\}$ e G :

$$\{e\} \subseteq G$$

$$|G| = p \text{ primo} \Rightarrow G \text{ ciclico} \Rightarrow G \text{ abeliano} \Rightarrow G \text{ normale}$$

2. $k - 1 \Rightarrow k$

Per la prop [2.4,pg.80], abbiamo che $|Z(G)| = p^t$, $0 < t \leq k$

$$|Z| = p^t, t > 0 \Rightarrow p \nmid |Z| \quad \underbrace{\Rightarrow}_{\text{thm [1.178,pg.75]}} \quad \exists H_1 \subseteq Z : |H_1| = p$$

2.1. H_1 e' normale in quanto contenuto nel centro

$$h \in H_1 \subseteq Z \Rightarrow h \text{ commuta con tutti gli elem. di } G$$

$$aha^{-1} = haa^{-1} = h \in H_1$$

quindi H_1 e' normale.

Poiche' H_1 e' normale, possiamo considerare il gruppo G/H_1 .
Per Lagrange, si ha

$$\left| \frac{G}{H_1} \right| = i_G(H_1) = \frac{|G|}{|H_1|} = \frac{p^k}{p} = p^{k-1}$$

Allora, possiamo applicare l'ipotesi induttiva su G/H_1 :

$$\exists \overline{H}_2, \overline{H}_3, \dots, \overline{H}_n \leq G/H_1 \text{ normali}$$

$$\{\overline{e}\} = \{H_1\} \subseteq \overline{H}_2 \subseteq \overline{H}_3 \subseteq \dots \subseteq \overline{H}_k = G/H_1 \quad (1)$$

$$|\overline{H}_i| = p^{i-1}, \quad i = 2, \dots, k$$

Consideriamo la suriezione naturale

$$\pi : G \longrightarrow G/H_1$$

$$\pi(g) = gH_1$$

e' facile vedere¹¹ che

$$\ker \pi = H_1$$

Inoltre, π e' un omomorfismo suriettivo, allora per il cor di corrispondenza [1.158,pg.66] π e' una biezione tra i seguenti insiemi:

$$\{\overline{H} \leq G/H_1 \text{ normale}\} \xleftrightarrow{\pi} \{H \leq G \text{ normale} \mid H \supseteq \ker \pi = H_1\}$$

Dalla (1) abbiamo allora:

$$\pi^{-1}(\{H_1\}) \subseteq \pi^{-1}(\overline{H}_2) \subseteq \pi^{-1}(\overline{H}_3) \subseteq \dots \subseteq \pi^{-1}(G/H_1)$$

$$\pi^{-1}(\{H_1\}) = \ker \pi = H_1$$

$$H_2 := \pi^{-1}(\overline{H}_2)$$

$$H_3 := \pi^{-1}(\overline{H}_3)$$

...

$$H_k := \pi^{-1}(G/H_1) = G$$

Quindi abbiamo la nostra catena di sottogruppi normali di G :

$$H_1 \subseteq H_2 \subseteq H_3 \subseteq \dots \subseteq H_k = G$$

resta da calcolare gli ordini di ogni H_i , per $i = 2, \dots, k$.

Consideriamo la restrizione di π ad H_i :

$$\pi|_{H_i} : H_i \longrightarrow \pi(H_i) = \overline{H}_i$$

$$\ker \pi|_{H_i} = \{h \in H_i \mid \pi|_{H_i}(h) = hH_1 = H_1 \Leftrightarrow h \in H_1\} = H_1 \cap H_i \underset{H_1 \subseteq H_i}{=} H_1 \quad (2)$$

essa e' ancora suriettiva, ed e' un omomorfismo, quindi per il thm dell'omomorfismo

$$\frac{H_i}{\ker \pi|_{H_i}} \simeq \overline{H}_i$$

$$\frac{H_i}{\ker \pi|_{H_i}} \underset{(2)}{=} \frac{H_i}{H_1} \simeq \overline{H}_i$$

$$\left| \frac{H_i}{H_1} \right| = |\overline{H}_i| \underset{(1)}{=} p^{i-1} \underset{Lagrange}{\Leftrightarrow} \frac{|H_i|}{|H_1|} = |\overline{H}_i| \Leftrightarrow |H_i| = p^{i-1}p = p^i$$

che e' quello che volevamo

□

Proposition 2.6. *Studiamo i p -gruppi di ordine p^k , $k = 1, 2$:*

CASE: $k=1$

G e' ciclico.

¹¹ H_1 e' l'elemento unita' in G/H_1

CASE: $k=2$

G e' abeliano

CASE: $\exists a \in G : o(a) = p^2$

G e' ciclico

CASE: $\forall a \in G \setminus \{e\} \quad o(a) = p$

$G = \langle a, b \rangle = \{a^i b^j \mid i, j = 0, 1, \dots, p-1\}$ con $o(a) = o(b)$

Proof:

1. $k = 2$

1.1. G e' abeliano

Per la prop [2.4,pg.80] $|Z(G)| > 1$ e poiche' per Lagrange $|Z(G)|$ divide $|G| = p^2$, si hanno due possibilita': $|Z(G)| = p \vee |Z(G)| = p^2$.

1.1.1. Dimostriamo che la prima non si puo' verificare

$$|Z(G)| = p \Rightarrow Z(G) \subsetneq G \Rightarrow \exists a \in G : a \notin Z(G)$$

$$\begin{cases} G \supseteq C(a) \supseteq Z(G) \\ a \in C(a), a \notin Z(G) \end{cases} \Rightarrow G \supsetneq C(a) \supsetneq Z(G) \Rightarrow |G| \geq |C(a)| > |Z(G)| \Rightarrow p^2 \geq |C(a)| > p$$

$$\begin{cases} |C(a)| \mid |G| = p^2 \text{ [per Lagrange]} \\ p \text{ e' primo} \end{cases} \Rightarrow |C(a)| = p^2 \Rightarrow C(a) = G \Rightarrow a \in Z(G) \text{ assurdo}$$

Nota: $C(a)$ e' il centralizzante di a .

Quindi l'unico caso vero e'

$$|Z(G)| = p^2$$

e quindi

$$Z(G) = G \Rightarrow G \text{ e' abeliano}$$

1.2. Esaminiamo il caso $\forall a \in G \setminus \{e\} \quad o(a) = p$

$$|\langle a \rangle| = p \Rightarrow \langle a \rangle \neq G \Rightarrow \exists b \in G \setminus \langle a \rangle$$

$$\langle a \rangle \subsetneq \langle a, b \rangle \subseteq G \Rightarrow p < |\langle a, b \rangle| \leq p^2$$

e analogamente a quanto abbiamo visto prima deduciamo che

$$|\langle a, b \rangle| = p^2 \Rightarrow \langle a, b \rangle = G$$

poiche' $o(a) = o(b)$, e poiche' G e' abeliano, si ha

$$\langle a, b \rangle = \{a^i b^j \mid i, j = 0, 1, \dots, p-1\}$$

□

Proposition 2.7. Dato G con $|G| = 2p$, con $p > 2$ primo, si hanno questi due soli casi:

CASE: G e' ciclico

CASE: $G \simeq D_p$

Proof:

$$2 \mid |G| = 2p \quad \underbrace{\Rightarrow}_{thm[1.178,pg.75]} \quad \exists a \in G : o(a) = 2$$

$$p \mid |G| = 2p \quad \underbrace{\Rightarrow}_{thm[1.178,pg.75]} \quad \exists b \in G : o(b) = p$$

Si ha che $a \notin \langle b \rangle$, infatti,

$$|\langle b \rangle| = p \text{ primo} \quad \underbrace{\Rightarrow}_{\text{prop}[1.45, \text{pg.} 16]} \quad \langle b \rangle = \langle b^i \rangle \quad \forall i = 1, 2, \dots, p-1 \Leftrightarrow \langle b \rangle = \langle \bar{b} \rangle \quad \forall \bar{b} \in \langle b \rangle \setminus \{e\}$$

quindi se per ass. $a \in \langle b \rangle \Rightarrow \langle b \rangle = \langle a \rangle$ assurdo contro $|\langle a \rangle| = 2$

CASE: G abeliano

$$G \text{ abeliano} \Rightarrow ab = ba$$

$$\begin{cases} o(a) = 2, o(b) = p, (p, 2) = 1 \\ ab = ba \end{cases} \quad \underbrace{\Rightarrow}_{\text{prop. [4.2, pg. 95]}} \quad o(ab) = 2p \Rightarrow G = \langle ab \rangle \Rightarrow G \text{ e' ciclico}$$

CASE: G non abeliano

Dimostriamo che $G \simeq D_p$. Il gruppo diedrale D_p e' caratterizzato dalle seguenti relazioni (vedi [1.93, pg. 38], [1.96, pg. 39], [1.97, pg. 40]):

$$\begin{aligned} |D_p| &= 2p \\ D_p &= \langle a, b \rangle, \quad o(b) = p, \quad o(a) = 2 \\ ab &= b^{-1}a \Leftrightarrow aba^{-1} = b^{-1} \quad \underbrace{\Leftrightarrow}_{o(a)=2} \quad aba = b^{-1} \end{aligned}$$

Le prime due condizioni sono soddisfatte:

$$\begin{aligned} |G| &= 2p \\ |\langle a, b \rangle| / |G| &\Rightarrow |\langle a, b \rangle| = 1, 2, p, 2p \quad (*) \\ \begin{cases} \langle b \rangle, \langle a \rangle \subseteq \langle a, b \rangle \\ a \notin \langle b \rangle \end{cases} &\Rightarrow |\langle a, b \rangle| \geq p+1 \quad \underbrace{\Rightarrow}_{(*)} \quad |\langle a, b \rangle| = 2p \Rightarrow G = \langle a, b \rangle \end{aligned}$$

Resta da dimostrare l'ultima condizione.

$\langle b \rangle$ e' normale perche' il suo ordine e' meta di $|G|$,

$$\langle b \rangle \text{ normale} \Rightarrow aba^{-1} \in \langle b \rangle \Leftrightarrow aba^{-1} = b^h \quad (3)$$

A questo punto basterebbe dimostrare che $h = -1$.

Prendiamo adesso i coniugati rispetto ad a di ambo i membri dell'ultima uguaglianza:

$$a(aba^{-1})a^{-1} = ab^h a^{-1}$$

$$a^2 ba^{-2} = ab^h a^{-1} = (aba^{-1})(aba^{-1}) \dots (aba^{-1}) \underbrace{(b^h)(b^h) \dots (b^h)}_{(3)} = b^{h^2}$$

$$a^2 ba^{-2} = b^{h^2} \quad \underbrace{\Leftrightarrow}_{o(a)=2 \Rightarrow a^2=e} \quad b = b^{h^2}$$

$$b^1 = b^{h^2} \quad \underbrace{\Rightarrow}_{[1.35, \text{pg.} 12]} \quad h^2 = 1 \quad (\mathbb{Z}_p) \Leftrightarrow h^2 - 1 = 0 \quad (\mathbb{Z}_p) \Leftrightarrow (h-1)(h+1) = 0 \quad (\mathbb{Z}_p) \Leftrightarrow h = 1 \vee h = -1$$

Se per assurdo $h = 1$, si avrebbe dalla (3):

$$aba^{-1} = b \Leftrightarrow ab = ba$$

e come visto nel precedente passo del caso abeliano, G sarebbe ciclico, e quindi abeliano.

Assurdo perche' per ipotesi siamo nel caso non abeliano.

Allora, l'unica possibilita' e' $h = -1$, quindi sempre dalla (3):

$$aba^{-1} = b^{-1}$$

□

2.1 Teorema di Sylow

Theorem 2.8. *di Sylow*

Sia G , $|G| = n$ e $k = \max \left\{ i \in \mathbb{N} \mid p^i \mid n \right\} \geq 1$, con p primo, allora valgono le seguenti proposizioni:

1. $\exists H \leq G : |H| = p^k$
 H viene chiamato p -sottogruppo di Sylow
2. H, H' sono due p -sottogruppi di Sylow, allora

$$\exists a \in G : H' = aHa^{-1}$$

ovvero H, H' sono coniugati

3. Sia $K \leq G$, si ha

$$|K| = p^i, i \leq k \Rightarrow \exists H \text{ } p\text{-sott. di Sylow tale che } K \subseteq H$$

4. Sia t il numero di p -sottogruppi di Sylow, allora

$$t \mid m, \quad t \equiv 1 \pmod{p}$$

dove m e' t.c.:

$$n = p^k m, \quad (m, p) = 1$$

*Nota*¹²

Proof:

1. Dim 1.

Dobbiamo trovare un sottogruppo di ordine p^k . Consideriamo l'insieme dei sottoinsiemi di G di cardinalita' p^k :

$$X = \{ S \subseteq G \mid |S| = p^k \}$$

e agiamo su di esso tramite la seguente azione:

$$* : G \times X \longrightarrow X$$

$$g * S = gS = \{ gs \mid s \in S \}$$

- 1.1. $*$ e' una azione

$$gS \subseteq G.$$

Si verifica subito che la mappa

$$s \mapsto gs$$

e' una biezione tra S e gS , e quindi $|gS| = |S|$. Percio' $gS \in X$.

Infine,

$$e * S = eS = S$$

$$(g_1 \circ g_2) * S = (g_1 \circ g_2)S = g_1(g_2S) = g_1 * (g_2 * S)$$

- 1.2. Dim. che $\forall S \in X \quad |\text{St}(S)| \leq |S| = p^k$

¹²Il numero m nasce cosi':

$$p^k \mid n \Rightarrow n = p^k m$$

se per assurdo $(m, p) > 1$, poiche' p e' primo si avrebbe: $m = p^t$, e quindi, $n = p^{k+t}$, ma questo e' assurdo perche' p^k e' il massimo delle potenze di p che dividono n .

$$\begin{aligned}\text{St}(S) &= \{g \in G \mid gS = S\} \\ g \in \text{St}(S) &\Rightarrow \forall s \in S \quad gs \in S\end{aligned}$$

Fissando s , la mappa

$$\begin{aligned}\text{St}(S) &\longrightarrow S \\ g &\mapsto gs\end{aligned}$$

e' iniettiva, infatti

$$g's = gs \Rightarrow g' = g$$

e quindi

$$|\text{St}(S)| \leq |S|$$

1.3. A questo punto cerchiamo anche un solo $\bar{S} \in X$ tale che $|\text{St}(\bar{S})| \geq p^k$, cosi' da avere

$$\begin{cases} |\text{St}(\bar{S})| \leq p^k \\ |\text{St}(\bar{S})| \geq p^k \end{cases} \Rightarrow |\text{St}(\bar{S})| = p^k$$

E cosi' $\text{St}(\bar{S})$ sarebbe il gruppo di ordine p^k cercato.

1.3.1. Si ha $|X| = \binom{n}{p^k}$

Infatti, il numero degli elementi di X e' il numero di tutti i possibili sottoinsiemi di p^k elementi che si possono formare in G .

1.3.2. $p \nmid \binom{n}{p^k}$

Considerando che $n = mp^k$ abbiamo

$$\begin{aligned}\binom{n}{p^k} &= \frac{n(n-1)(n-2)\dots(n-(p^k-1))}{p^k(p^k-1)(p^k-2)\dots 1} = \frac{mp^k(mp^k-1)(mp^k-2)\dots(mp^k-(p^k-1))}{p^k(p^k-1)(p^k-2)\dots 1} = \\ &= \frac{m(mp^k-1)(mp^k-2)\dots(mp^k-(p^k-1))}{(p^k-1)(p^k-2)\dots 1}\end{aligned}$$

1.3.2.1. Dimostriamo che

$$p^t / mp^k - i \Rightarrow p^t / p^k - i$$

con $i = 1, \dots, p^k - 1$. Cosi' facendo, avremo che tutti i fattori del tipo p^t sono sia nel numeratore che nel denominatore e quindi vengono semplificati. Non essendoci piu' fattori di tipo p^t , avremo la tesi:

$$p \nmid \binom{n}{p^k}$$

Se per assurdo $t \geq k$, allora

$$p^t / mp^k - i \xRightarrow[t \geq k]{} p^k / mp^k - i$$

$$\begin{cases} p^k / mp^k - i \\ p^k / p^k \end{cases} \Rightarrow p^k / i \text{ assurdo perche' } i < p^k$$

Quindi $t < k$, allora

$$\begin{aligned}\begin{cases} p^t / mp^k - i \\ p^t / p^k \end{cases} &\Rightarrow p^t / i \\ \begin{cases} p^t / p^k \\ p^t / i \end{cases} &\Rightarrow p^t / p^k - i\end{aligned}$$

$$1.3.3. \exists \bar{S} \in X : p \nmid |\mathcal{O}(\bar{S})| \underset{p \text{ primo}}{\Leftrightarrow} (p, |\mathcal{O}(\bar{S})|) = 1$$

Se per assurdo

$$\forall S \in X \quad p \nmid |\mathcal{O}(S)|$$

allora, essendo $|X|$ somma della cardinalita' di tutte le orbite, si avrebbe

$$p \nmid |X|$$

ma questo e' assurdo contro quanto visto in un passo precedente.

$$1.3.4. |\text{St}(\bar{S})| \geq p^k$$

Per il passo precedente, abbiamo che

$$p \nmid |\mathcal{O}(\bar{S})| \Rightarrow \begin{cases} p^k \nmid |\mathcal{O}(\bar{S})| \\ (p^k, |\mathcal{O}(\bar{S})|) = 1 \end{cases}$$

Per la prop [1.174,pg.74] abbiamo

$$|G| = |\text{St}(\bar{S})| |\mathcal{O}(\bar{S})|$$

$$\begin{cases} p^k \nmid |G| = mp^k \\ p^k \nmid |\mathcal{O}(\bar{S})| \\ (p^k, |\mathcal{O}(\bar{S})|) = 1 \end{cases} \underset{\text{prop. [AI,7.1.1,pg.29]}}{\Rightarrow} p^k \nmid |\text{St}(\bar{S})| \Rightarrow p^k \leq |\text{St}(\bar{S})|$$

2. Dim la 3.

Sia $K \leq G : |K| = p^h, 1 \leq h \leq k$.

Consideriamo l'insieme

$$P = \{H \leq G \mid |H| = p^k\}$$

ovvero l'insieme di tutti i p -sottogruppi di Sylow. Noi vogliamo far vedere che esiste un qualche $\bar{H} \in P : K \subseteq \bar{H}$.

Consideriamo la seguente azione che fa agire G su P :

$$G \times P \longrightarrow P$$

$$g * H = gHg^{-1}$$

* e' l'azione di coniugazione, ed e' ben posta: $gHg^{-1} \in P$ perche' $|gHg^{-1}| = |H| = p^k$.

Abbiamo:

$$\text{St}(H) = \{g \in G \mid gHg^{-1} = H\}$$

$$H \subseteq \text{St}(H) \Rightarrow |H| = p^k \leq |\text{St}(H)|$$

$$\begin{cases} |\text{St}(H)| \geq p^k \\ |\text{St}(H)| \leq G \Rightarrow |\text{St}(H)| \nmid |G| = p^k m \end{cases} \Rightarrow |\text{St}(H)| = p^k r, \text{ dove } r \nmid m, r \geq 1 \quad (0)$$

$$|G| \underset{[1.174,pg.74]}{=} |\text{St}(H)| |\mathcal{O}(H)| \Leftrightarrow p^k m = p^k r |\mathcal{O}(H)| \Leftrightarrow m = r |\mathcal{O}(H)| \Rightarrow |\mathcal{O}(H)| \nmid m \quad (1)$$

$$\begin{cases} |\mathcal{O}(H)| \nmid m \\ (m, p) = 1 \end{cases} \underset{p \text{ primo}}{\Leftrightarrow} p \nmid m \Rightarrow p \nmid |\mathcal{O}(H)| \Leftrightarrow (\mathcal{O}(H), p) = 1 \quad (2)$$

$$\text{piu' in generale si ha: } \lambda \nmid m \Rightarrow p \nmid \lambda \quad (2.1)$$

$$\text{infatti, se per assurdo } p \nmid \lambda \Rightarrow p \nmid \lambda, \lambda \nmid m \Rightarrow p \nmid m \text{ assurdo}$$

Prendendo un qualsiasi $H \in P$, consideriamo adesso la seguente azione di coniugazione di K

su $\mathcal{O}(H)$

$$K \times \mathcal{O}(H) \longrightarrow \mathcal{O}(H)$$

$$x \bullet T = xTx^{-1}$$

che si puo' intendere come una restrizione dell'azione di prima, perche'

$$K \subseteq G, \quad \mathcal{O}(H) \subseteq P$$

Con $\mathcal{O}_\bullet(T)$ indichiamo l'orbita di T indotta dall'azione $\bullet$.

2.1. Dim. che $\exists \bar{T} \in \mathcal{O}(H) : |\mathcal{O}_\bullet(\bar{T})| = 1$

Supponiamo per assurdo che

$$\forall \text{ orbita } \mathcal{O}_\bullet(T) \text{ si ha } |\mathcal{O}_\bullet(T)| > 1$$

Per il cor [1.174,pg.74], si ha

$$|\mathcal{O}_\bullet(T)| \mid |K| = p^h \Rightarrow |\mathcal{O}_\bullet(T)| = p^t, \quad 0 \leq t \leq h \quad (*)$$

$$|\mathcal{O}_\bullet(T)| > 1 \Rightarrow 0 < t \leq h \quad (**)$$

ma allora, poiche' le orbite creano una partizione dell'insieme su cui si agisce, abbiamo:

$$|\mathcal{O}(H)| = \sum |\mathcal{O}_\bullet(T)| \underbrace{=}_{(*)} p^{t_1} + p^{t_2} + \dots$$

$$(**) \Rightarrow p^{t_i} \neq 1$$

il secondo membro e' divisibile per p e quindi anche $|\mathcal{O}(H)|$ e' divisibile per p , assurdo contro la (2).

$$|\mathcal{O}_\bullet(\bar{T})| = 1 \Rightarrow \forall x \in K \quad x \bullet \bar{T} = x\bar{T}x^{-1} = \bar{T} \Rightarrow K \leq \text{St}(\bar{T})$$

$$\begin{cases} \bar{T} \leq \text{St}(\bar{T}) = \{x \in G \mid x\bar{T}x^{-1} = \bar{T}\} \\ \forall x \in \text{St}(\bar{T}) \quad x\bar{T}x^{-1} = \bar{T} \end{cases} \quad \underbrace{\Rightarrow}_{[1.104,pg.42]} \quad \bar{T} \text{ e' normale in } \text{St}(\bar{T})$$

$$\bar{T} \text{ normale in } \text{St}(\bar{T}), \quad K \leq \text{St}(\bar{T}) \quad \underbrace{\Rightarrow}_{[1.119,pg.49]} \quad K\bar{T} \leq \text{St}(\bar{T}) \Rightarrow \frac{K\bar{T}}{\bar{T}} \leq \frac{\text{St}(\bar{T})}{\bar{T}} \Rightarrow$$

$$\Rightarrow \left| \frac{K\bar{T}}{\bar{T}} \right| \mid \left| \frac{\text{St}(\bar{T})}{\bar{T}} \right| \quad \underbrace{=}_{[1.148,pg.61]} \quad \frac{|\text{St}(\bar{T})|}{|\bar{T}|} \underbrace{=}_{(0)} \frac{p^k r}{p^k} = r/m \Rightarrow \left| \frac{K\bar{T}}{\bar{T}} \right| \mid m \underbrace{\Rightarrow}_{(2.1)} p \nmid \left| \frac{K\bar{T}}{\bar{T}} \right| \quad (3)$$

$$K \cap \bar{T} \leq K \Rightarrow |K \cap \bar{T}| \mid |K| = p^h \Rightarrow |K \cap \bar{T}| = p^s, \quad 0 \leq s \leq h$$

$$t \text{ e' normale in } \text{St}(\bar{T}) \quad \underbrace{\Rightarrow}_{[1.152,pg.63]} \quad \frac{K}{K \cap \bar{T}} \simeq \frac{K\bar{T}}{\bar{T}} \Rightarrow \left| \frac{K\bar{T}}{\bar{T}} \right| = \left| \frac{K}{K \cap \bar{T}} \right| \quad \underbrace{=}_{[1.148,pg.61]} \quad \frac{|K|}{|K \cap \bar{T}|} = \frac{p^h}{p^s} = p^{h-s} \quad (4)$$

$$(3), (4) \Rightarrow p \nmid p^{h-s} \Rightarrow p^{h-s} = 1 \Rightarrow h-s = 0 \Leftrightarrow h = s \Rightarrow p^h = p^s \Leftrightarrow |K| = |K \cap \bar{T}|$$

$$\begin{cases} K \cap \bar{T} \subseteq K \\ |K| = |K \cap \bar{T}| \end{cases} \quad \Rightarrow \quad K \cap \bar{T} = K \Leftrightarrow K \subseteq \bar{T}$$

che e' quello che volevamo dimostrare.

3. Dim 2.

Continuiamo a usare lo stesso linguaggio del passo precedente. La nostra tesi e'

$$(\forall H \in P \forall H' \in P \Rightarrow \exists a \in G : H' = aHa^{-1}) \Leftrightarrow \forall H \in P \quad \mathcal{O}(H) = P$$

Come abbiamo visto prima, $\mathcal{O}(H) \subseteq P$. Resta da far vedere che $P \subseteq \mathcal{O}(H)$.

$$H' \in P \Rightarrow |H'| = p^k \Rightarrow H' \text{ e' un } p\text{-gruppo} \quad \underbrace{\Rightarrow}_{\text{passo precedente}} \quad H' \subseteq \bar{T} \in \mathcal{O}(H)$$

$$\begin{cases} H' \subseteq \bar{T} \\ |\bar{T}| = p^k = |H'| \end{cases} \Rightarrow \bar{T} = H' \Rightarrow H' \in \mathcal{O}(H)$$

4. Dim 4.

Osserviamo che $t = |P|$.

Nel passo precedente abbiamo dimostrato che

$$H \in P \Rightarrow \mathcal{O}(H) = P \Rightarrow |\mathcal{O}(H)| = |P| = t$$

nel passo 2, avevamo mostrato che $|\mathcal{O}(H)|/m$, quindi t/m .

Ponendo $K = H$, consideriamo l'orbita formata da un solo elemento che avevamo trovato nel passo 2: $|\mathcal{O}_\bullet(\bar{T})|$. Una tale orbita e' unica, infatti se per assurdo ne esistesse un'altra $|\mathcal{O}_\bullet(T')|$, si avrebbe

$$|\mathcal{O}_\bullet(T')| = 1 \underbrace{\Rightarrow}_{\text{passo 2}} K = H \subseteq T' \underbrace{\Rightarrow}_{|H|=|T'|} \Rightarrow H = T'$$

$$|\mathcal{O}_\bullet(\bar{T})| = 1 \underbrace{\Rightarrow}_{\text{passo 2}} K = H \subseteq \bar{T} \underbrace{\Rightarrow}_{|H|=|\bar{T}|} \Rightarrow H = \bar{T}$$

$$T = T'$$

E per quanto avevamo visto nel sottopasso <2>.1 del passo 2, abbiamo che $\exists! t_i : p^{t_i} = 1$, mentre tutte le altre sono diverse da 1, ovvero:

$$|P| = |\mathcal{O}(H)| = \sum |\mathcal{O}_\bullet(T)| = 1 + p^{t'_1} + p^{t'_2} + \dots \Rightarrow |P| = 1 \pmod{p}$$

□

Proposition 2.9. $|G| = n$, $|H| = m$, $H \leq G$ di Sylow

$$H \text{ normale} \Leftrightarrow H \text{ e' l'unico sottogruppo di ordine } m$$

Proof:

1. Dim $\Rightarrow$

$$H \text{ normale} \Leftrightarrow \forall a \in G \quad aHa^{-1} = H \quad (1)$$

Supponiamo che esista un altro $H' \leq G : |H'| = |H|$.

H p -sottogruppo di Sylow $\Rightarrow |H| = p^k$

$$|H| = |H'| = p^k \Rightarrow H, H' \text{ sono } p\text{-sottogruppi di Sylow} \quad \underbrace{\Rightarrow}_{\text{thm}[2.8, \text{pg.84}]} \quad H, H' \text{ sono coniugati} \Leftrightarrow$$

$$\Leftrightarrow \exists a \in G : H' = aHa^{-1} \underbrace{=}_{(1)} H \Rightarrow H' = H$$

2. Dim $\Leftarrow$

Segue dalla prop [1.108,pg.45]

□

Proposition 2.10.

$$\begin{cases} |G| = pq, & q > p, & \text{primi} \\ p \nmid q-1 \end{cases} \Rightarrow G = \langle ab \rangle \text{ dove, } o(a) = p, o(b) = q$$

Proof:

Per Cauchy,

$$|G| = pq \xRightarrow{[1.178, \text{pg. } 75]} \exists H, K \leq G : |H| = p, |K| = q$$

$$|H| = p, |K| = q \xRightarrow{\text{prop. } [1.56, \text{pg. } 20]} H = \langle a \rangle, K = \langle b \rangle, o(a) = p, o(b) = q$$

0.1. Dimostriamo che $\langle a \rangle \cap \langle b \rangle = \{e\}$

Per Lagrange,

$$|\langle a \rangle \cap \langle b \rangle| \mid |G| = pq \Rightarrow |\langle a \rangle \cap \langle b \rangle| = 1, p, q, pq$$

Nel caso $|\langle a \rangle \cap \langle b \rangle| = pq$ seguirebbe che

$$\langle a \rangle \cap \langle b \rangle = G$$

$$\begin{cases} \langle a \rangle \subseteq G = \langle a \rangle \cap \langle b \rangle \\ \langle a \rangle \cap \langle b \rangle \subseteq \langle a \rangle \end{cases} \Rightarrow \langle a \rangle = \langle a \rangle \cap \langle b \rangle$$

$$\text{analogamente} \Rightarrow \langle b \rangle = \langle a \rangle \cap \langle b \rangle$$

$$\langle a \rangle = \langle b \rangle$$

assurdo contro $o(a) = 3 \neq o(b) = 5$.

Anche i casi $|\langle a \rangle \cap \langle b \rangle| = p, q$ sono assurdi, infatti,

$$|\langle a \rangle \cap \langle b \rangle| = p \text{ primo} \Rightarrow \langle a \rangle \cap \langle b \rangle = \langle c \rangle, o(c) = p \Rightarrow c \in \langle a \rangle \cap \langle b \rangle$$

assurdo perche' in $\langle a \rangle$, a parte e , ci sono solo elementi di ordine p e in $\langle b \rangle$ solo elementi di ordine q .

Quindi, in definitiva,

$$|\langle a \rangle \cap \langle b \rangle| = 1 \Rightarrow \langle a \rangle \cap \langle b \rangle = \{e\}$$

0.2. $ab = ba$

Poiche' $|G| = pq = p^1 q^1$, i H e K sono rispettivamente dei p -sottogruppi, q -sottogruppi di Sylow.

Sia t il numero di p -sottogruppi di Sylow. Per il thm di Sylow [2.8,pg.84] abbiamo:

$$\begin{cases} t/q \xRightarrow{q \text{ primo}} t = 1 \vee t = q \quad (*) \\ t = 1 \pmod{p} \Rightarrow t = 1 \vee t = p + 1 \vee t = 2p + 1 \vee \dots \vee t = kp + 1 \end{cases}$$

se per assurdo esiste un $k \neq 0$ tale che $t = kp + 1 \not\equiv 1 \pmod{q}$, si ha

$$t \not\equiv 1 \pmod{q} \xRightarrow{(*)} t = q \Leftrightarrow kp + 1 = q \Leftrightarrow kp = q - 1 \Rightarrow p \mid (q - 1)$$

assurdo contro ipotesi. Quindi l'unica possibilita' e' che

$$t = 1$$

Quindi esiste un unico p -sottogruppo di Sylow, cioe' H .

Sia ora t il numero di q sottogruppi di Sylow, si ha

$$\begin{cases} t/p \\ t = 1 \pmod{q} \end{cases} \xRightarrow{q > p} t = 1$$

quindi esiste un unico q -sottogruppo di Sylow, cioe' K .

Allora, per la prop [2.9,pg.88] si ha che sia H che K sono normali.

$$\begin{cases} H = \langle a \rangle, K = \langle b \rangle \text{ normali} \\ H \cap K = \{e\} \end{cases} \xRightarrow{[1.109, \text{pg. } 45]} ab = ba$$

0.3. Q.E.D.

$$\begin{cases} o(a) = p, o(b) = q \\ ab = ba \end{cases} \underbrace{\Rightarrow}_{[4.2, \text{pg.95}]} o(ab) = pq = |G| \Rightarrow G = \langle ab \rangle$$

□

3 Classificazione degli abeliani

Lemma 3.1. *Sia G un gruppo abeliano, con $|G| = p^r$, p primo, allora*

$$G \simeq H_1 \times H_2 \times \dots \times H_t$$

dove ogni H_i e' un gruppo ciclico.

Proof: Procediamo per induzione su r .

Se $r = 0$, $|G| = 1$ e quindi $G = \{\mathbf{e}\}$.

Se $r = 1$, $|G| = p$ e quindi G e' ciclico.

Supponiamo adesso che per $r' < r$ la tesi sia vera e dimostriamo che e' vera per r .

Consideriamo $s \in G$, t.c.

$$o(s) = \max \{o(g) \mid g \in G\} \quad (1)$$

$$\text{sia } S = \langle s \rangle$$

Consideriamo un insieme massimale T , secondo l'inclusione, del seguente insieme:

$$\{T' \leq G \mid T' \cap S = \{\mathbf{e}\}\}$$

Osserviamo intanto che

$$o(s) \mid |G| = p^r \Rightarrow o(s) = p^\alpha \quad \alpha \leq r$$

1. $G = ST$

Poiche' G e' abeliano, S, T sono normali e quindi per la prop. [1.119, pg.49] si ha $ST \leq G$.

Dimostriamo allora che $G \subseteq ST$.

Sia $g \in G$, per la (1) si ha

$$o(g) \mid |G| = p^r \Rightarrow o(g) = p^\gamma$$

$$o(g) \underbrace{\leq}_{(1)} o(s) \Rightarrow \gamma \leq \alpha$$

Il gruppo $H = \langle g \rangle \cap ST$ e' tale che

$$H \leq \langle g \rangle \xRightarrow{\langle g \rangle \text{ ciclico}} H \text{ ciclico, } H = \langle b \rangle, \quad p^\beta = |H|$$

$$b \xRightarrow{[1.42, \text{pg. 14}]} g^{\frac{o(g)}{|H|}} = g^{p^{\gamma-\beta}}$$

$$b \in ST = \langle s \rangle T \Rightarrow b = s^n t$$

$$b^{p^\beta} = \mathbf{e} \xLeftrightarrow{G \text{ e' abeliano}} s^{np^\beta} t^{p^\beta} = \mathbf{e} \Leftrightarrow s^{np^\beta} = t^{-p^\beta}$$

$$\underbrace{s^{np^\beta}}_{\in S} = \underbrace{t^{-p^\beta}}_{\in T} \Rightarrow s^{np^\beta} \in S \cap T = \{\mathbf{e}\} \Rightarrow s^{np^\beta} = \mathbf{e} \Rightarrow$$

$$\Rightarrow o(s) = p^\alpha / np^\beta \Rightarrow n_1 p^\alpha = np^\beta \Rightarrow n = n_1 p^{\alpha-\beta}$$

$$b = s^n t \Leftrightarrow b = s^{n_1 p^{\alpha-\beta}} t \Leftrightarrow g^{p^{\gamma-\beta}} = s^{n_1 p^{\alpha-\beta}} t$$

$$t = g^{p^{\gamma-\beta}} s^{-n_1 p^{\alpha-\beta}} = \left(g s^{-n_1 p^{\alpha-\gamma}} \right)^{p^{\gamma-\beta}} \quad (2)$$

$$\text{Sia } c = g s^{-n_1 p^{\alpha-\gamma}}; \quad (2) \Rightarrow c^{p^{\gamma-\beta}} = t \quad (2.1)$$

1.1. Dim. che $\langle c \rangle T \cap S = \{\mathbf{e}\}$

Consideriamo $d \in S \cap \langle c \rangle T$

$$d \in S = \langle s \rangle \Rightarrow d = s^m$$

$$d \in \langle c \rangle T \Rightarrow d = c^h t_1$$

$$s^m = c^h t_1 \Leftrightarrow s^m = g^h s^{-h n_1 p^{\alpha-\gamma}} t_1 \Leftrightarrow g^h = s^u t_1^{-1}$$

$$\text{dove } u = h n_1 p^{\alpha-\gamma} + m$$

$$\underbrace{g^h}_{\in \langle g \rangle} = \underbrace{s^u t_1^{-1}}_{\in ST} \Rightarrow g^h \in H = \langle g \rangle \cap ST = \langle b \rangle = \langle g^{p^{\gamma-\beta}} \rangle \Rightarrow h = k p^{\gamma-\beta}$$

$$s^m = c^h t_1 \Leftrightarrow s^m = c^{k p^{\gamma-\beta}} t_1 \xRightarrow{(2.1)} t^k t_1$$

$$\underbrace{s^m}_{\in S} = \underbrace{t^k t_1}_{\in T} \Rightarrow s^m \in S \cap T = \{\mathbf{e}\} \Rightarrow d = s^m = \mathbf{e}$$

Ovviamente

$$T \subseteq \langle c \rangle T$$

Ma poiche' T era per definizione l'elemento massimale tra quelli che intersecati con S davano $[\mathbf{e}]$, si ha che

$$\langle c \rangle T \subseteq T$$

e quindi $T = \langle c \rangle T$, ovvero $c \in T$.

$$c \in T \Rightarrow c = t_2 \xRightarrow{(2)} g s^{-n_1 p^{\alpha-\gamma}} = t_2 \Rightarrow g = s^{n_1 p^{\alpha-\gamma}} t_2 \in ST$$

che era quello che volevamo dimostrare. Quindi,

$$G = ST$$

2. Q.E.D.

$$G = ST$$

$$p^r = |G| = |ST| \stackrel{[1.153, \text{pg.63}]}{=} \frac{|S||T|}{|S \cap T|} = p^\alpha |T| \Rightarrow |T| = p^{r-\alpha} \stackrel{r' := r-\alpha}{=} p^{r'}, \quad r' < r \quad (3)$$

$$G = ST \stackrel{[1.126, \text{pg.51}]}{\Rightarrow} G \simeq S \times T = \langle s \rangle \times T$$

e grazie alla (3), applicando l'ipotesi induttiva, si ha la tesi. □

Theorem 3.2. *Dato un gruppo abeliano finito G , tale che $|G| = n$, allora se $n = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}$ e' la fattorizzazione di n , si ha che*

$$\begin{aligned} \forall i = 1, 2, \dots, n \quad \exists! H_i \leq G : |H_i| &= p_i^{r_i} \\ G &\simeq H_1 \times H_2 \times \dots \times H_t \\ \text{dove } H_i &\simeq K_{i1} \times K_{i2} \times \dots \times K_{it_i} \quad i = 1, 2, \dots, t \\ K_{ij} &\text{ e' ciclico } \quad \forall i, j \end{aligned}$$

In altre parole, G e' isomorfo al prodotto di gruppi ciclici.

Proof: Per il thm di Sylow (vedi [2.8, pg.84]), si ha

$$\forall i \quad \exists H_i \leq G : |H_i| = p_i^{r_i}$$

e poiche' G e' abeliano, e quindi H_i normale, per la prop. [2.9, pg.88] si ha l'unicita' di H_i .

Dimostriamo adesso che G e' prodotto interno degli H_i : dobbiamo verificare le due prop. della definizione:

$$\begin{cases} 1. H_i \cap (H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_t) = \{e\} \quad \forall i = 1, 2, \dots, t \\ 2. G = H_1 H_2 \dots H_t \end{cases}$$

1. Dim. 1.

Sia $c \in H_i \cap (H_1 \dots H_t)$, allora

$$c \in (H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_t) \Rightarrow c = h_1 h_2 \dots h_{i-1} h_{i+1} \dots h_t \quad (1)$$

$$h_j \in H_j \stackrel{[1.57, \text{pg.21}]}{\Rightarrow} h_j^{|H_j|} = h_j^{p_j^{r_j}} = e \quad \forall j = 1, 2, \dots, t \quad (2)$$

$$\text{sia } \pi_i = p_1^{r_1} \dots p_{i-1}^{r_{i-1}} p_{i+1}^{r_{i+1}} \dots p_t^{r_t}$$

$$c^{p_1^{r_1} \dots p_{i-1}^{r_{i-1}} p_{i+1}^{r_{i+1}} \dots p_t^{r_t}} \stackrel{G \text{ abel}}{=} h_1^{\pi_i} h_2^{\pi_i} \dots h_t^{\pi_i} \stackrel{(2)}{=} e \Rightarrow o(c) \mid \pi_i$$

$$c \in H_i \stackrel{[1.57, \text{pg.21}]}{\Rightarrow} c^{|H_i|} = c^{p_i^{r_i}} = e \Rightarrow o(c) \mid p_i^{r_i}$$

ma poiche' $(\pi, p_i^{r_i}) = 1$, si ha

$$\begin{cases} (\pi, p_i^{r_i}) = 1 \\ o(c) \mid \pi \\ o(c) \mid p_i^{r_i} \end{cases} \Rightarrow o(c) \mid 1 \Rightarrow o(c) = 1$$

$$o(c) = 1 \Rightarrow c = e$$

2. Dim. 2.

Consideriamo $G_1 = H_1 H_2 \dots H_t$, allora per quanto abbiamo dimostrato nel passo precedente, si ha che G_1 e' prodotto interno degli H_i .

$$G_1 \text{ prod. interno di } H_1, H_2, \dots, H_t \quad \underbrace{\Rightarrow}_{[1.126, \text{pg.} 51]} \quad G_1 \simeq H_1 \times H_2 \times \dots \times H_t$$

$$|G_1| = \prod_{i=1}^t |H_i| = \prod_{i=1}^t p_i^{r_i} = n$$

$$\begin{cases} G_1 \leq G \\ |G_1| = |G| \end{cases} \quad \underbrace{\Rightarrow}_{[1.23, \text{pg.} 8]} \quad G_1 = G$$

Quindi

$$G = G_1 \simeq H_1 \times H_2 \times \dots \times H_t \quad (*)$$

3. Q.E.D.

Ogni H_i e' un gruppo abeliano, con $|H_i| = p_i^{r_i}$, allora, per il lemma [3.1,pg.90], si ha che ogni H_i e' isomorfo al prodotto di gruppi ciclici:

$$H_i \simeq K_{i1} \times K_{i2} \times \dots \times K_{it_i}$$

Quindi dalla (*) si ha la tesi:

$$G \simeq \prod_{i=1}^t \prod_{j=1}^{t_i} K_{ij}$$

□

Example 3.3. In congiunzione con le prop. [1.134,pg.55],[1.135,pg.56], il thm [3.2,pg.92] permette di classificare tutti i gruppi abeliani.

Ad esempio, consideriamo G abeliano, con $|G| = 84$, avremo

$$\begin{aligned} |G| &= 84 = 2^2 \cdot 3 \cdot 7 \\ G &\simeq H_1 \times H_2 \times H_3, \quad |H_1| = 3, |H_2| = 7, |H_3| = 4 \\ H_1 \text{ ciclico} &\Rightarrow H \simeq \mathbb{Z}_3 \\ H_2 \text{ ciclico} &\Rightarrow J \simeq \mathbb{Z}_7 \\ H_3 \simeq \text{prod. gruppi ciclici} &\Rightarrow H_3 \simeq \mathbb{Z}_4 \vee H_3 \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \end{aligned}$$

Quindi, questi sono gli unici casi possibili:

$$\begin{aligned} G &\simeq \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_4 \simeq \mathbb{Z}_{84} \\ G &\simeq \mathbb{Z}_3 \times \mathbb{Z}_7 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \mathbb{Z}_{42} \times \mathbb{Z}_2 \end{aligned}$$

Proposition 3.4. Sia dato G abeliano, $|G| = n$, allora si ha

$$m \mid n \Rightarrow \exists H \leq G : |H| = m$$

Proof:

1. Dim. l'esistenza

Scomponiamo n :

$$n = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}$$

$$m \mid n \Rightarrow m = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}, \quad 0 \leq s_i \leq r_i$$

Per il thm [3.2,pg.92] si ha:

$$G \simeq H_1 \times H_2 \times \dots \times H_t, \quad |H_i| = p_i^{r_i}$$

Ogni H_i e' un p -gruppo, quindi per la prop. [2.5,pg.80]

$$\exists M_i \leq H_i : |M_i| = p^{s_i}$$

$$\prod_{i=1}^t M_i \leq H_1 \times H_2 \times \dots \times H_t \simeq G \Rightarrow \exists M \leq G : \prod_{i=1}^t M_i \simeq M$$

$$|M| = \left| \prod_{i=1}^t M_i \right| = \prod_{i=1}^t |M_i| = \prod_{i=1}^t p^{s_i} = m$$

2. Dim. la non unicit 

Consideriamo $|G| = 4$. Si hanno due casi: $G \simeq \mathbb{Z}_4 \vee G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Consideriamo il secondo caso, e poniamo $m = 2$. Troviamo pero' due sottogruppi di G di ordine 2:

$$\{(0, 1), (0, 0)\}, \{(1, 1), (0, 0)\}$$

□

Proposition 3.5. *Sia dato G abeliano, $|G| = n$, allora si ha*

$$\forall p \text{ primo} : p \nmid n \Rightarrow \exists! H \leq G : |H| = p \Leftrightarrow G \text{ e' ciclico}$$

Proof:

1. Dim. $\Rightarrow$

Per il thm [3.2,pg.92] si ha:

$$G \simeq H_1 \times H_2 \times \dots \times H_t, \quad |H_i| = p_i^{r_i}$$

$$H_i \simeq K_{i1} \times K_{i2} \times \dots \times K_{it_i} \quad i = 1, 2, \dots, t$$

$$K_{ij} \text{ e' ciclico}, \quad |K_{ij}| = p_i^{s_j} \quad \forall i, j$$

Fissiamo un i , e supponiamo per assurdo che $t_i \geq 2$. Per il thm di Cauchy

$$p_i \nmid p_i^{s_i} \Rightarrow \exists K'_{ij} \leq K_{ij} : |K'_{ij}| = p_i \quad \forall j = 1, \dots, t_i$$

[1.178,pg.75]

Al variare di j , possiamo allora formare i seguenti sottogruppi di G :

$$\left\{ (\mathbf{e}, \mathbf{e}, \dots, \mathbf{e}, \underbrace{k}_{\text{posizione } j}, \mathbf{e}, \dots, \mathbf{e}) \mid k \in K'_{ij} \right\}$$

che sono in numero t_i . Ma questo e' in contrasto contro l'ipotesi dell'unicita' di H , sottogruppo di ordine p .

Abbiamo cosi' visto che $t_i = 1$, e quindi che H_i e' ciclico.

Infine, poiche'

$$(|H_i|, |H_h|) = 1 \quad \forall i \neq h$$

per il thm [1.133,pg.54] si ha la tesi.

1. Dim. $\Leftarrow$

Per il thm [1.42,pg.14].

□

4 Proposizioni varie

Proposition 4.1. Dato un G con $|G| \geq 2$,

$$\forall a \in G \quad a^2 = e \Rightarrow G \text{ e' abeliano } , |G| = 2^k$$

Proof:

0.1. Dim che G e' abeliano

Nota:

$$a^2 = e \Leftrightarrow a = a^{-1}$$

Sia $a, b \in G$

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba$$

$$ab = ba$$

quindi G e' abeliano.

0.2. Dimostriamo che $|G| = 2^k$

Consideriamo n elementi distinti di G , e creiamo il sottogruppo da essi generato

$$H_n = \langle a_1, a_2, \dots, a_n \rangle \quad \underbrace{=}_{G \text{ e' abeliano}} \quad \{a_1^{i_1} a_2^{i_2} \dots a_n^{i_n} \mid i_1, i_2, \dots, i_n \in \mathbb{Z}\}$$

poiche' ogni a_i ha ordine due, $a_i^k = a_i \vee a_i^k = e$, quindi possiamo scrivere

$$\langle a_1, a_2, \dots, a_n \rangle = \{a_1^{i_1} a_2^{i_2} \dots a_n^{i_n} \mid i_1, i_2, \dots, i_n \in \{0, 1\}\}$$

Poiche' ogni esponente dei vari a_i puo' essere o zero o uno, e' chiaro che esistono 2^n possibilita'.

Poiche' $H_n \leq G$, possono verificarsi due possibilita': $H_n = G \vee H_n \neq G$.

Se $H_n = G$, abbiamo finito: $|G| = |H_n| = 2^n$. Altrimenti, basta considerare H_{n+1} .

Al massimo arriveremo fino a H_p , dove $p = |G|$. In questo caso si ha necessariamente $H_p = G$, per definizione di sottogruppo generato.

□

Proposition 4.2. Dati $a, b \in G$,

$$\begin{cases} o(a) = m, & o(b) = n, & (m, n) = 1 \\ ab = ba \end{cases} \Rightarrow o(ab) = mn$$

Proof:

$$(ab)^{mn} = a^{mn} b^{mn} \quad \underbrace{=}_{o(a)=m, o(b)=n} \quad e \quad (1)$$

Resta da dimostrare che mn e' il piu' piccolo esponente t.c. $(ab)^{mn} = \mathbf{e}$.

$$(1) \quad \underbrace{\Rightarrow}_{[1.36, \text{pg.12}]} k = o(ab) / mn \Rightarrow \exists k_1 k_2 \geq 1 : k = k_1 k_2, k_1 / m, k_2 / n$$

$$k_1 / m \Rightarrow m = \lambda_1 k_1$$

$$k_2 / n \Rightarrow n = \lambda_2 k_2$$

$$(ab)^{mk_2} = (ab)^{\lambda_1 k_1 k_2} = (ab)^{\lambda_1 k} = ((ab)^k)^{\lambda_1} = \mathbf{e}$$

$$\mathbf{e} = (ab)^{mk_2} \underbrace{=}_{ab=ba} a^{mk_2} b^{mk_2} = \mathbf{e} b^{mk_2} = b^{mk_2}$$

$$b^{mk_2} = \mathbf{e} \Rightarrow o(b) = n / mk_2$$

$$n / mk_2 \Leftrightarrow \lambda_2 k_2 / mk_2 \Leftrightarrow \lambda_2 / m$$

$$\lambda_2 / m, \lambda_2 / n \Rightarrow \lambda_2 / (m, n) = 1 \Rightarrow \lambda_2 = 1$$

Analogamente,

$$\lambda_1 / m, \lambda_1 / n \Rightarrow \lambda_1 / (m, n) \Rightarrow \lambda_1 = 1$$

In conclusione:

$$\lambda_1 = \lambda_2 = 1 \Rightarrow m = k_1, n = k_2 \Rightarrow mn = k_1 k_2 = k = o(ab)$$

□

Proposition 4.3. *Sia G abeliano, $a, b \in G$, allora*

$$\exists c \in G : o(c) = \text{mcm} \{o(a), o(b)\}$$

Proof: Siano $r = o(a)$, $s = o(b)$, $m = \text{mcm} \{r, s\}$. Scomponiamo in fattori r, s :

$$r = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}$$

$$s = p_1^{s_1} p_2^{s_2} \dots p_t^{s_t}$$

$$\text{con } 0 \leq r_i, s_i \quad \forall i$$

Per la proprieta' del mcm [AI,9.9.1,pg.41], si ha

$$m = \prod_{i=1}^t p_i^{\mu_i}$$

$$\text{con } \mu_i = \max \{r_i, s_i\} \quad \forall i \quad (1)$$

Consideriamo i seguenti elementi:

$$a_i = a^{\alpha_i}$$

$$\alpha_i = \prod_{1 \leq j \leq t, j \neq i} p_j^{r_j}$$

$$b_i = b^{\beta_i}$$

$$\beta_i = \prod_{1 \leq j \leq t, j \neq i} p_j^{s_j}$$

$$1. \quad o(a_i) = p_i^{r_i}$$

$$a_i^{p_i^{r_i}} = a^{\alpha_i p_i^{r_i}} = a^{\prod_{j=1}^t p_j^{r_j}} = a^r = \mathbf{e}$$

$$\Rightarrow o(a_i) / p_i^{r_i} \Rightarrow o(a_i) \leq p_i^{r_i}$$

Se per assurdo $r' = o(a_i) < p_i^{r_i}$, allora

$$a_i^{r'} = \mathbf{e} \Leftrightarrow a^{\alpha_i r'} = \mathbf{e} \Rightarrow o(a) = r / \alpha_i r' \Rightarrow r \leq \alpha_i r' = r' \prod_{1 \leq j \leq t, j \neq i} p_j^{r_j} \Leftrightarrow$$

$$\Leftrightarrow \prod_{j=1}^t p_j^{r_j} \leq r' \prod_{1 \leq j \leq t, j \neq i} p_j^{r_j} \underbrace{\Leftrightarrow}_{\text{semplificando}} p_i^{r_i} \leq r'$$

assurdo contro $r' < p_i^{r_i}$. Quindi $o(a_i) = p_i^{r_i}$

2. $o(b_i) = p_i^{s_i}$

Analogamente.

Siano dati i seguenti elementi:

$$c_i = \begin{cases} a_i & r_i > s_i \\ b_i & r_i \leq s_i \end{cases} \quad \forall i = 1, \dots, t$$

3. $o(c_i) = p_i^{\mu_i}$

CASE: $r_i > s_i$

$$r_i > s_i \Rightarrow \mu_i = \max\{r_i, s_i\} = r_i$$

$$c_i = a_i$$

$$o(c_i) = o(a_i) \underbrace{=}_{\text{passo 1}} p_i^{r_i} = p_i^{\mu_i}$$

CASE: $r_i \leq s_i$

$$r_i \leq s_i \Rightarrow \mu_i = \max\{r_i, s_i\} = s_i$$

$$c_i = b_i$$

$$o(c_i) = o(b_i) \underbrace{=}_{\text{passo 2}} p_i^{s_i} = p_i^{\mu_i}$$

4. Q.E.D.

$$\begin{cases} o(c_i) = p_i^{\mu_i} \quad \forall i \\ \{p_i\} \text{ sono primi distinti} \end{cases} \Rightarrow \text{MCD}(o(c_1), \dots, o(c_t)) = 1 \quad (2)$$

$$\begin{cases} G \text{ abeliano} \\ c := \prod_{i=1}^t c_i \end{cases} \underbrace{\Rightarrow}_{[4.2, \text{pg.95}]} o(c) = \prod_{i=1}^t o(c_i) = \prod_{i=1}^t p_i^{\mu_i} \underbrace{=}_{(1)} m$$

c e' quindi l'elemento cercato.

□

Proposition 4.4. *Dati $H, K \leq G$*

$$\begin{cases} |H| = p \text{ primo} \\ p \nmid |K| \end{cases} \Rightarrow H \cap K = \{\mathbf{e}\}$$

Proof:

$$|H| = p \text{ primo} \underbrace{\Leftrightarrow}_{[1.55, \text{pg.20}]} (J \leq H \Leftrightarrow J = \{\mathbf{e}\} \vee J = H) \quad (*)$$

$$H \cap K \leq H \Rightarrow H \cap K \leq H \underbrace{\Leftrightarrow}_{(*)} H \cap K = \{\mathbf{e}\} \vee H \cap K = H$$

Se per assurdo $H \cap K = H$, allora

$$H \cap K = H \Leftrightarrow H \subseteq K \xRightarrow{\text{lagrange}} |H|/|K| \Leftrightarrow p/|K|$$

assurdo contro Hp.

Quindi l'unica possibilita' e' $H \cap K = \{e\}$. □

Proposition 4.5.

$$\begin{cases} G = \langle a, b \rangle \\ o(a) = o(b) = 4 \\ a^2 = b^2 = (ab)^2 \end{cases} \Rightarrow G \simeq \mathbb{H}$$

dove $\mathbb{H}$ e' il gruppo dei quaternioni.

Nota: la condizione $(ab)^2 = b^2$ equivale a: $ba = a^{-1}b$.

Proof: PROOF SKETCH: Con la condizione $ba = a^{-1}b$, si dimostra che

$$G = \{a^r b^s \mid r = 0, 1, \dots, 3, s = 0, 1\}$$

Si osserva che

$$\mathbb{H} = \{i^r j^s \mid r = 0, 1, \dots, 3, s = 0, 1\}$$

si dimostra che la seguente funzione e' ben posta ed e' un isomorfismo

$$f(a^r b^s) = i^r j^s$$
□

5 Studio dei gruppi

In questa sezione studieremo i gruppi di ordine $1, \dots, 15$.

Proposition 5.1. $|G| = 1$ allora $G = \{e\}$, e non abbiamo molto da dire.

$|G| = 2$ allora $G = \{e, a\} = \langle a \rangle$ e $G \simeq \mathbb{Z}_2$ per il thm [1.150, pg. 61]

$|G| = 3$ allora $G = \{e, a, b\} = \langle a \rangle = \langle b \rangle \simeq \mathbb{Z}_3$ perche' 3 e' un primo e quindi applichiamo la prop [1.56, pg. 20].

Proposition 5.2. $|G| = 4$

Si possono verificare due casi:

$$G = \langle a \rangle \simeq \mathbb{Z}_4 \vee G = \{e, a, b, c\} \text{ con } o(a) = o(b) = o(c) = 2$$

Nel secondo caso G si chiama gruppo Vier. In ogni caso, G e' abeliano.

Proof:

$$|G| = 2^2 \xRightarrow{[2.6, \text{pg. 81}]} G \text{ abeliano}$$

Consideriamo adesso il secondo caso. $o(a)$ deve dividere 4 ([1.54, pg. 19]), quindi $o(a) = 1, 2, 4$. Supponiamo $a \neq e$, allora $o(a) = 2, 4$.

$$o(a) = 4 \xRightarrow{[1.41, \text{pg. 14}]} G = \langle a \rangle$$

ma questo e' assurdo perche' siamo nell'ipotesi in cui G non e' ciclico. Abbiamo quindi dimostrato che ogni $a \in G$ diverso da e ha ordine due.

Proposition 5.3. $|G| = 5$ allora $G = \langle a \rangle \simeq \mathbb{Z}_5$ ([1.56,pg.20] e [1.150,pg.61])

Proposition 5.4. $|G| = 6$ Si possono verificare solo due casi:

$$G \simeq \mathbb{Z}_6 \vee G \simeq S_3$$

Proof:

Basta applicare la prop. [2.7,pg.82], ricordandosi che $S_3 \simeq D_3$. Qui di seguito diamo una dimostrazione alternativa che fa uso del thm di Cayley.

Consideriamo $g \in G$. $o(g)$ deve dividere 6 ([1.54,pg.19]), quindi $o(g) = 1, 2, 3, 6$

$$|G| = 6 \text{ e' pari} \quad \Rightarrow \quad \exists a \in G : o(a) = 2$$

exp.[1.166,pg.70]

0.1. $\exists b \in G : o(b) = 3$

Supponiamo per assurdo che

$$\forall b \in G \quad o(b) \neq 3 \Leftrightarrow \forall b \in G : b \neq e \quad o(b) = 2, 6$$

Se $o(b) = 6$, allora $o(b^2) = 3$, assurdo.

Se b tali che $o(b) = 6$ non ce ne sono, allora

$$\forall b \in G : b \neq e \quad o(b) = 2$$

$$\Rightarrow \quad |G| = 2^k$$

prop[4.1,pg.95]

ma questo e' assurdo perche' $|G| = 6$.

Quindi $o(a) = 2, o(b) = 3$. Distinguiamo due casi,

CASE: G abeliano

Poiche' G e' abeliano $ab = ba$, poiche' inoltre $o(a) = 2, o(b) = 3$, per la proposizione [4.2,pg.95], si ha

$$o(ab) = 2 \cdot 3 = 6 \quad \Rightarrow \quad G = \langle ab \rangle \quad \simeq \quad \mathbb{Z}_6$$

[1.41,pg.14] [1.150,pg.61]

CASE: G non abeliano

Ricordandoci che $o(a) = 2, o(b) = 3$, consideriamo i seguenti gruppi:

$$H = \{e, a\}, \quad K = \{e, b, b^2\}$$

0.1.1. K e' normale

Infatti,

$$|K| = 3 \quad \Rightarrow \quad i_G(K) = \frac{|G|}{|K|} = \frac{6}{3} = 2 \quad \Rightarrow \quad K \text{ normale}$$

Lagrange[1.53,pg.19] [1.51,pg.19]

0.1.2. H non e' normale

Supponiamo per assurdo che lo sia.

$$\begin{cases} H, K \text{ normali} \\ a^{-1} = a \in H, b \in K \\ H \cap K = \{e\} \end{cases} \quad \Rightarrow \quad ab = ba$$

prop. [1.109,pg.45]

$$\begin{cases} ab = ba \\ o(a) = 2, o(b) = 3 \end{cases} \quad \Rightarrow \quad o(ab) = 6 \Rightarrow G = \langle ab \rangle \quad \Rightarrow \quad G \text{ abeliano}$$

prop.[4.2,pg.95] prop.[1.40,pg.13]

assurdo.

0.1.3. Appliciamo il teorema di Cayley II (vedi [1.162,pg.68])

Consideriamo

$$M = \{gH\}_{g \in G}$$

$$|M| = i_G(H) \underbrace{=}_\text{lagrange} 3$$

$$S(M) \simeq S_3$$

allora per Cayley

$$\exists f : G \longrightarrow S_3 \text{ omomorfismo}$$

0.1.3.1. f e' iniettiva

Sempre per Cayley, $\ker f$ e' il piu' grande sottogruppo normale di H . Ma $H = \{\mathbf{e}, a\}$, quindi $\ker f = \{\mathbf{e}\} \vee \ker f = H$. Ma H non e' normale, quindi $\ker f = \{\mathbf{e}\}$.

0.1.3.2. f e' biettiva

Poiche' $|G| = |S_3|$ e poiche' f e' iniettiva, per le prop delle funzioni (vedi [AI,7,pg.9]), f e' anche surriettiva.

f e' quindi un isomorfismo:

$$G \simeq S_3$$

quello che volevamo dimostrare.

□

Proposition 5.5. $|G| = 7$ allora G e' ciclico e $G \simeq \mathbb{Z}_7$ ([1.56,pg.20] e [1.150,pg.61])

Proposition 5.6. $|G| = 8$, si hanno questi casi

CASE: G abeliano

1. $G = \langle a \rangle$, $G \simeq \mathbb{Z}_8$
2. $G = \langle a, b, c \rangle = \{a^i b^j c^k \mid i, j, k \in \{0, 1\}\}$,
dove $o(a) = o(b) = o(c) = 2$
3. $G = \langle a, c \rangle = \{a^i c^j \mid i = 0, 1, 2, 3, j = 0, 1\}$
dove $o(a) = 4, o(c) = 2$

CASE: G non abeliano

$$G \simeq D_4 \vee G \simeq Q$$

dove Q e' il gruppo dei Quaternioni.

Proof:

CASE: G abeliano

Applicando il thm [3.2,pg.92] si arriva subito al risultato:

$$G \simeq \mathbb{Z}_8 \vee G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \vee G \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$$

Dimostriamo adesso lo stesso risultato, senza far uso del thm [3.2,pg.92].

CASE: $\exists a \in G : G = \langle a \rangle$

In questo caso G e' ciclico e isomorfo a $\mathbb{Z}_8$

CASE: $\forall a \in G : a \neq \mathbf{e} \ o(a) = 2$

Per la prop [4.2,pg.95],

$$|G| = 2^k$$

quindi poiche' $|G| = 8$

$$|G| = 2^3$$

e

$$G = \langle a, b, c \rangle = \{a^i b^j c^k \mid i, j, k \in \{0, 1\}\}$$

CASE: $\forall a \in G \ o(a) \neq 8$, e inoltre $\exists a \in G : a \neq \mathbf{e} \ o(a) \neq 2$

Questo caso e' la negazione dei due precedenti. Poiche' $o(a)$ deve dividere $|G| = 8$, si ha $o(a) = 1, 2, 4, 8$, ma nel nostro caso, l'unica possibilita' valida e' $o(a) = 4$.

Consideriamo

$$H = \langle a \rangle = \{\mathbf{e}, a, a^2, a^3\}$$

Nota: e' facile vedere che l'unico elemento di ordine 2 e' a^2 (anche per la prop [1.44,pg.15]).

0.0.1. $\exists b \in G \setminus H : b \neq \mathbf{e} \ o(b) = 2$

Supponiamo per assurdo che preso un $b \in G \setminus H$, $o(b) \neq 2$. Considerando le ipotesi del nostro caso, l'unica possibilita' valida e' che

$$o(b) = 4$$

allora, sia $K = \langle b \rangle = \{\mathbf{e}, b, b^2, b^3\}$

Nota: e' facile vedere che l'unico elemento di ordine 2 e' b^2 (anche per la prop [1.44,pg.15]).

Consideriamo $K \cap H$.

0.0.1.1. $K \cap H \neq \{\mathbf{e}\}$

Supponiamo per assurdo che $K \cap H = \{\mathbf{e}\}$. Allora presi comunque $i, j, i', j' \in \mathbb{Z} : i \neq i', j \neq j'$ si ha

$$a^i b^j \neq a^{i'} b^{j'}$$

infatti se per assurdo

$$a^i b^j = a^{i'} b^{j'} \Leftrightarrow a^i = a^{i'} b^{j'-j} \Leftrightarrow a^{i-i'} = b^{j'-j} \Rightarrow a^{i-i'} \in K \cap H$$

assurdo contro $K \cap H = \{\mathbf{e}\}$.

Quindi l'insieme $KH = \{a^i b^j \mid i, j = 0, 1, 2, 3\}$ ha 16 elementi. Poiche' siamo nel caso abeliano $KH = HK$ e quindi per la prop [1.118,pg.48]

$$KH \leq G$$

ma questo e' assurdo perche' G ha solo 8 elementi.

In conclusione $\exists c \in K \cap H, c \neq \mathbf{e}$.

$$K \cap H \leq K, H, \quad |K| = |H| = 4 \quad \underbrace{\Rightarrow}_{\text{lagrange [1.53,pg.19]}} \quad |K \cap H| = 1, 2, 4$$

$$\begin{cases} K \neq H \\ K \cap H \neq \{\mathbf{e}\} \end{cases} \Rightarrow |K \cap H| = 2 \Leftrightarrow K \cap H = \{\mathbf{e}, c\} = \langle c \rangle$$

$$o(c) = 2$$

ma gli unici elementi di ordine 2 in K e H sono a^2, b^2 , quindi deduciamo che

$$c = a^2 = b^2$$

Consideriamo $a^{-1}b$,

$$(a^{-1}b)^2 = a^2(b^{-1})^2 \underbrace{=}_{a^2=b^2} \mathbf{e}$$

$$o(a^{-1}b) = 2$$

Se per assurdo $a^{-1}b \in H$, allora poiche' solo a^2 ha ordine 2, si ha

$$a^{-1}b = a^2 \Leftrightarrow b = a \in H$$

assurdo perche' $b \notin H$.

Allora, necessariamente $a^{-1}b \in G \setminus H$.

Ecco che abbiamo trovato un elemento di ordine 2 che sta' in $G \setminus H$. Assurdo contro la nostra ipotesi iniziale che diceva che non esistevano elementi in $G \setminus H$ di ordine due.

In definitiva, $\exists c \in G \setminus H : o(c) = 2$.

Considerando H del passo precedente, per Lagrange abbiamo

$$i_G(H) = \frac{|G|}{|H|} = \frac{8}{4} = 2$$

quindi

$$\begin{aligned} \{gH\}_{g \in G} &= \{H, G \setminus H\} \\ \Rightarrow G \setminus H &= gH \text{ con } g \notin H \end{aligned}$$

allora se come g prendiamo l'elemento $c \in G \setminus H$ del passo precedente, abbiamo

$$G \setminus H = cH$$

Adesso possiamo scrivere per intero G :

$$G = H \cup cH = \{\mathbf{e}, a, a^2, a^3\} \cup \{c, ac, a^2c, a^3c\} = \langle a, c \rangle = \{a^i c^j \mid i = 0, 1, 2, 3, \ j = 0, 1\}$$

$$G = \langle a, c \rangle = \{a^i c^j \mid i = 0, 1, 2, 3, \ j = 0, 1\}$$

$$\text{dove } o(a) = 4, o(c) = 2$$

CASE: G non abeliano

Un gruppo di 8 elementi non abeliano e' il gruppo diedrale D_4 (vedi prop. [1.98,pg.41]), il gruppo diedrale D_4 e' caratterizzato dalle seguenti relazioni (vedi [1.96,pg.39], [1.97,pg.40]):

$$D_4 = \langle r, s \rangle, \quad o(r) = 4, \quad o(s) = 2$$

$$sr = r^{-1}s$$

Il gruppo Q dei quaternioni e' cosi' definito:

$$Q = \{\pm 1, \pm i, \pm j, \pm k\}$$

$$-x = \text{inverso di } x \quad \forall x \in Q$$

$$(-1) \cdot x = x \cdot (-1) = -x \quad \forall x \in Q$$

$$i^2 = -1, \quad i^3 = -i, \quad i^4 = 1$$

$$j^2 = -1, \quad j^3 = -j, \quad j^4 = 1$$

$$k^2 = -1, \quad k^3 = -k, \quad k^4 = 1$$

$$ij = k, \quad jk = i, \quad ki = j$$

$$ji = -k, \quad kj = -i, \quad ik = -j$$

Cominciamo ad esaminare G .

Se per assurdo $\exists g \in G : o(g) = 8$ allora $G = \langle g \rangle \Rightarrow G$ abeliano . Assurdo.

Se per assurdo $\forall g \in G : g \neq \mathbf{e} \quad o(g) = 2$ allora per la prop [4.1,pg.95] G e' abeliano. Assurdo.

Allora,

$$o(g) = 1, 2, 4$$

$$\exists a \in G : a \neq \mathbf{e}, \quad o(a) \neq 2 \Rightarrow o(a) = 4$$

Consideriamo

$$H = \langle a \rangle = \{\mathbf{e}, a, a^2, a^3 = a^{-1}\}$$

gli unici elementi di ordine 4 sono a, a^{-1} (vedi [1.45,pg.16])

$$|H| = 4 = \frac{|G|}{2} \Rightarrow H \text{ normale}$$

Per quanto abbiamo detto

$$\forall y \in G \setminus H : y \neq \mathbf{e} \quad o(y) = 4 \quad \underbrace{\bigoplus}_{XOR} \quad \exists y \in G \setminus H : y \neq \mathbf{e}, \quad o(y) = 2$$

Esaminiamo questi due casi.

CASE: $\exists y \in G \setminus H : y \neq \mathbf{e}, \quad o(y) = 2$

$|H| = 4 \Rightarrow i_G(H) = 2$ ovvero, ci sono solo due laterali di H in G e poiche' $G = H \cup G \setminus H$ sono $H, G \setminus H$

$y \in G \setminus H$, $G \setminus H$ laterale di $H \Rightarrow G \setminus H = yH$

$$G \setminus H = yH = \{y, ya, ya^2, ya^3\} \quad (1)$$

$$G = H \cup G \setminus H = \{e, a, a^2, a^3, y, ya, ya^2, ya^3\}$$

0.0.1. $o(yay^{-1}) = o(a)$

Sia $p = o(a)$.

$$a^p = e$$

$$(yay^{-1})^2 = ya \underbrace{y^{-1} \cdot y}_e ay^{-1} = ya^2 y^{-1}$$

$$(yay^{-1})^3 = (yay^{-1})(ya^2 y^{-1}) = ya^3 y^{-1}$$

...

$$(yay^{-1})^p = ya^p y^{-1} = yy^{-1} = e$$

se per assurdo ci fosse un $t < p$ tale che $(yay^{-1})^t = e$ allora

$$(yay^{-1})^t = ya^t y^{-1} = e \Leftrightarrow ya^t = y \Leftrightarrow a^t = e$$

assurdo contro il fatto che $p = o(a)$.

$$H \text{ normale} \Rightarrow yay^{-1} \in H$$

$$\begin{cases} o(yay^{-1}) = o(a) = 4 \\ \text{gli unici elementi di ordine 4 di } H \text{ sono } a, a^{-1} \end{cases}$$

$$\Rightarrow yay^{-1} = a \vee yay^{-1} = a^{-1} \Leftrightarrow ya = ay \vee ya = a^{-1}y$$

CASE: $ya = ay$

$$G = H \cup G \setminus H = \{e, a, a^2, a^3, y, ya, ya^2, ya^3\}$$

$$ya^i = yaa^{i-1} = aya^{i-1} = a \cdot ya \cdot a^{i-2} = a^2 y \cdot a^{i-2} = \dots = a^i y$$

$$ya^i = a^i y \quad \forall i \Rightarrow G \text{ abeliano}$$

assurdo poiche' siamo nel caso in cui G non e' abeliano.

Quindi l'unico caso lecito e' $ya = a^{-1}y$. Allora, considerando anche che $o(a) = 4, o(y) = 2$, procedendo come nella dimostrazione del thm [1.97,pg.40] giungiamo a:

$$G = \langle a, y \rangle$$

Quindi, sempre per il thm [1.97,pg.40], l'isomorfismo cercato e' definito da:

$$a^i y^j \mapsto r^i s^j \quad i = 0, 1, \dots, 3, \quad j = 0, 1$$

CASE: $\forall y \in G \setminus H : y \neq e \quad o(y) = 4$

0.0.1. Dim. che $y \in G \setminus H, y \neq e \Rightarrow y^2 = a^2, ay \in G \setminus H$

Fissato $y \in G \setminus H, y \neq e$ sia

$$K = \langle y \rangle = \{e, y, y^2, y^3\}$$

K e H sono normali

$$\Rightarrow$$

$$HK \leq G$$

prop [1.119,pg.49]

Procedendo come nel passo <4>.1 del caso G abeliano, si conclude che

$$H \cap K \neq \{e\}$$

$$H \cap K = \langle c \rangle \quad \text{con } o(c) = 2$$

gli unici elementi di ordine 2 di H e K sono a^2, y^2 quindi $c = a^2 = y^2$

$$H \cap K = \{e, a^2 = y^2\}$$

$$y \in G \setminus H \Rightarrow ay \notin H$$

infatti, se per assurdo $ay \in H \Leftrightarrow ay = a^i \Leftrightarrow y = a^{i-1} \Rightarrow y \in H$ assurdo

sia $t = ay$

$$t \notin H \Leftrightarrow t \in G \setminus H$$

Applicando ripetutamente la proposizione

$$y \in G \setminus H, y \neq e \Rightarrow y^2 = a^2, \quad ay \in G \setminus H$$

che e' stata appena dimostrata, otteniamo:

$$y^2 = a^2, \quad z := ay \in G \setminus H$$

$$z^2 = a^2, \quad t := az = a^2y \in G \setminus H$$

$$t^2 = a^2, \quad x := at = a^3y \in G \setminus H$$

$$x^2 = a^2, \quad ax = a^4y \underbrace{=}_{o(a)=4} y \in G \setminus H$$

$$a^2 = y^2 = x^2 = t^2 = z^2$$

Osservando che $x, y, z, t \in G \setminus H \Rightarrow o(x) = o(y) = o(z) = o(t) = 4 \Rightarrow x^{-1} = x^3, \dots$,
abbiamo

$$a^2z = z^3 = z^{-1}$$

$$a^2t = t^3 = t^{-1}$$

$$a^2x = x^3 = x^{-1}$$

$$a^2y = y^3 = y^{-1}$$

poiche' x, y, z, t, a sono di ordine 4, abbiamo anche

$$x^4 = z^4 = t^4 = y^4 = a^4 = e$$

Si ha pure

$$\alpha\beta = \beta^{-1}\alpha \quad \forall \alpha \neq \beta \in \{a, x, y, z, t\} \quad (*)$$

infatti

$$o(\beta) = 4 \Rightarrow |\langle \beta \rangle| = 4 \Rightarrow \langle \beta \rangle \text{ normale}$$

$$\begin{cases} \langle \beta \rangle \text{ normale} \\ G \text{ non abeliano} \end{cases} \xRightarrow{\text{come nel passo 3.1 del caso precedente}} \alpha\beta = \beta^{-1}\alpha \quad (*)$$

Calcoliamo gli inversi dei vari elementi:

$$\begin{cases} zx = ayx \underbrace{=}_{y=ax} a^2x^2 = a^4 = e \\ xz = a^3yz = a^2ayz = a^2z^2 = a^4 = e \end{cases} \Rightarrow x = z^{-1}$$

$$\begin{cases} ty = a^2y^2 = a^4 = e \\ yt = ya^2y = y^4 = e \end{cases} \Rightarrow y = t^{-1}$$

$$a^3 = a^{-1}$$

Infine, calcoliamo i vari prodotti:

$$yz \underset{(*)}{=} z^{-1}y = xy = a^3y^2 = aa^2y^2 = aa^4 = a$$

$$za = a^{-1}z = a^3z = a^4y = y$$

$$ay = z$$

$$zy = ay^2 = a^3 = a^{-1}$$

$$az = a^2y = t$$

$$ya = a^{-1}y = a^3y = x$$

Ecco che possiamo definire il seguente isomorfismo tra G e Q :

$$\mathbf{e} \mapsto 1$$

$$a^2 \mapsto -1$$

$$y \mapsto i$$

$$z \mapsto j$$

$$a \mapsto k$$

$$t \mapsto -i$$

$$x \mapsto -j$$

$$a^3 \mapsto -k$$

infatti, con queste associazioni ritroviamo proprio Q . □

Proposition 5.7. $|G| = 9$.

G e' abeliano, e si hanno questi casi:

CASE: G e' ciclico

CASE: $G = \langle a, b \rangle, \quad o(a) = o(b) = 3$

Proof: $|G| = 9 = 3^2$ e quindi basta applica la prop [2.6,pg.81]

Proposition 5.8. $|G| = 10$, si hanno questi due soli casi:

CASE: G e' ciclico

CASE: $G \simeq D_5$

Proof: $|G| = 2 \cdot 5 = 10$ e quindi basta usare la prop [2.7,pg.82].

Proposition 5.9. $|G| = 11$ e' ciclico poiche' 11 e' primo.

Proposition 5.10. $|G| = 12$

CASE: G abeliano

$$1. G \simeq \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \simeq \mathbb{Z}_6 \times \mathbb{Z}_2$$

$$2. G \simeq \mathbb{Z}_3 \times \mathbb{Z}_4 \simeq \mathbb{Z}_{12}$$

CASE: G non abeliano

$$1. G \simeq A_4$$

$$2. G \simeq D_6 \text{ (!da verificare!)}$$

Proof: Per il caso abeliano basta applicare il thm [3.2,pg.92] e la prop [1.134,pg.55].
 Supponiamo G non abeliano. Per il thm di Sylow (vedi [2.8,pg.84]), abbiamo

$$\begin{aligned} \exists H_1, H_2, \dots, H_t \text{ 3-sottogruppi di sylow, } & \begin{cases} t/4 \\ t = 1 \quad \mathbb{Z}_3 \end{cases} \\ \exists K_1, K_2, \dots, K_u \text{ 2-sottogruppi di sylow, } & \begin{cases} u/3 \\ t = 1 \quad \mathbb{Z}_2 \end{cases} \end{aligned}$$

Abbiamo allora i seguenti casi:

CASE: $t = u = 1$

In questo caso H_1 e' l'unico sottogruppo di sylow di ordine 3 e K_1 e' l'unico di ordine 4. Allora, per la prop [2.9,pg.88], H_1, K_1 sono normali.

0.1. $H_1 \cap K_1 = \{e\}$

$$H_1 \cap K_1 \leq H_1 \Rightarrow |H_1 \cap K_1| / |H_1| \Rightarrow |H_1 \cap K_1| = 1, 3$$

se per assurdo $|H_1 \cap K_1| = 3$, allora

$$|H_1 \cap K_1| = 3 \quad \underbrace{\Rightarrow}_{\text{unicita' di } H_1} \quad H_1 \cap K_1 = H_1 \Leftrightarrow H_1 \subseteq K_1 \quad \underbrace{\Leftrightarrow}_{H_1 \text{ e' un gruppo}} \quad H_1 \leq K_1 \Rightarrow |H_1| / |K_1| \Leftrightarrow 3/4$$

assurdo

0.2. $H_1 K_1 = G$

$$\begin{aligned} H_1, K_1 \text{ normali} & \quad \underbrace{\Rightarrow}_{[1.119, \text{pg.49}]} \quad H_1 K_1 \leq G \\ |H_1 K_1| & \quad \underbrace{=}_{[1.153, \text{pg.63}]} \quad \frac{|H_1| |K_1|}{|H_1 \cap K_1|} = |H_1| |K_1| = |G| \\ \begin{cases} H_1 K_1 \leq G \\ |H_1 K_1| = G \end{cases} & \Rightarrow H_1 K_1 = G \end{aligned}$$

0.3. $G \simeq H_1 \times K_1$

$$\begin{cases} H_1, K_1 \text{ normali} \\ H_1 \cap K_1 = \{e\} \\ G = H_1 K_1 \end{cases} \xrightarrow{\text{def}} G \text{ prodotto interno di } H_1, K_1 \quad \underbrace{\Rightarrow}_{[1.126, \text{pg.51}]} \quad G \simeq H_1 \times K_1$$

H_1 e' ciclico ($|H_1| = 3$ che e' primo) e quindi e' abeliano.

K_1 e' abeliano perche' e' un 2-gruppo di ordine 2 (vedi [2.6,pg.81])

$$H_1, K_1 \text{ abeliani} \quad \underbrace{\Rightarrow}_{[1.130, \text{pg.53}]} \quad H_1 \times K_1 \text{ abeliano} \Rightarrow G \text{ abeliano}$$

assurdo.

In definitiva, il caso $u = t = 1$ non si puo' realizzare.

CASE: $t = 4, u = 3$

0.1. $H_i \cap K_j = \{e\}$

$$h \in H_i \cap K_j \Rightarrow \begin{cases} h \in H_i \Rightarrow o(h) / |H_i| \Rightarrow o(h) = 1, 3 \\ h \in K_j \Rightarrow o(h) / |K_j| \Rightarrow o(h) = 1, 2, 4 \end{cases} \Rightarrow h = 1$$

Gli H_i sono 4 sottogruppi distinti di ordine 3, i K_j sono 3 distinti e di ordine 4, inoltre, poiche' $H_i \cap K_j = \{e\}$, gli H_i sono distinti dai K_j . In totale abbiamo quindi il seguente numero di

elementi distinti:

$$1 + (|H_1| - 1) + \cdots + (|H_4| - 1) + (|K_1| - 1) + \cdots + (|K_3| - 1) = 1 + 8 + 9 = 18$$

(i vari $+1, -1$ sono stati aggiunti per considerare l'elemento $\mathbf{e}$ che e' comune a tutti i sottogruppi).

Questo pero' e' in contrasto con $|G| = 12$. In definitiva, anche questo caso $t = 4, u = 3$ non si puo' verificare.

CASE: $t = 4, u = 1$

Sia $H = H_i$ con un i qualsiasi.

$$\begin{aligned} G/_s H &= \{gH \mid g \in G\} \\ |G/_s H| &\stackrel{[1.53, \text{pg. 19}]}{=} \frac{|G|}{|H|} = 4 \quad (1) \\ H \leq G &\stackrel{[1.162, \text{pg. 68}]}{\Rightarrow} \exists \text{ omomorfismo } f : G \longrightarrow S(G/_s H) \stackrel{(1)}{\simeq} S_4 \end{aligned}$$

0.1. $\{\mathbf{e}\}$ e' il piu' grande sottogruppo normale di H

$$J \leq H \Rightarrow |J| \mid |H| = 3 \Rightarrow |J| = 1, 3 \Rightarrow J = [\mathbf{e}] \vee J = H$$

$$\left\{ |H_1| = |H_2| = \cdots = |H_4| = 3 \Rightarrow H \text{ non e' l'unico sottogruppo di ordine 3} \right.$$

$$\stackrel{[2.9, \text{pg. 88}]}{\Rightarrow} H \text{ non e' normale}$$

quindi l'unico sottogruppo normale di H e' $\{\mathbf{e}\}$.

Sempre per il thm [1.162, pg. 68], $\ker f$ e' il piu' grande sottogruppo normale di H , e quindi $\ker f = \{\mathbf{e}\}$, ovvero f e' iniettiva.

Infine,

l'unico sottogruppo di ordine 12 di S_4 e' $A_4 \Rightarrow \text{Im } f = A_4$ il gruppo alterno quindi

$$G \simeq A_4$$

□

Proposition 5.11. $|G| = 13$ e' ciclico poiche' 13 e' primo.

Proposition 5.12. $|G| = 15 \Rightarrow G$ e' ciclico.

Proof: $|G| = 15 = 3 \cdot 5$

La tesi e' diretta conseguenza della proposizione [2.10, pg. 88]

□

6 Esercizi

Example 6.1. Sia G un p -gruppo di ordine p^3 . Provare che:

1. $\forall g \in G \quad g^{p^2} \in Z(G)$
2. $\forall a, b \in G, \quad aba^{-1}b^{-1} \in Z(G)$
3. $\exists g \in G : g^p \notin Z(G) \Rightarrow \frac{G}{Z(G)}$ e' ciclico
4. Supponendo che $\forall g \in G \quad o(g) = p$, trovare quanti sottogruppi distinti di ordine p esistono in G

Proof:

1. Dim 1.

$$o(g) = 1, p, p^2, p^3$$

$$g^{|G|} = \underbrace{\quad}_{\text{Lagrange [1.53,pg.19]}} \quad g^{p^3} = \mathbf{e} \Rightarrow o(g) \mid p^3 \Rightarrow o(g) = 1, p, p^2, p^3$$

Nei casi $o(g) = 1, p, p^2$, si ha $g^{p^2} = \mathbf{e}$, e quindi la tesi e' vera.

Nel caso $o(g) = p^3$, G e' ciclico, quindi abeliano, e quindi la tesi e' vera.

2. Dim 2.

Sia $Z = Z(G)$

$$Z \leq G \quad \underbrace{\Rightarrow}_{\text{Lagrange [1.53,pg.19]}} \quad |Z| \mid |G| = p^3 \Rightarrow |Z| = 1, p, p^2, p^3 \quad (*)$$

$$G \text{ p-gruppo} \quad \underbrace{\Rightarrow}_{[2.4, \text{pg.80}]} \quad |Z| > 1 \Rightarrow \underbrace{|Z| = p, p^2, p^3}_{(*)}$$

Se $|Z| = p^3$, G sarebbe abeliano e quindi non ci sarebbe nulla da dimostrare.

- 2.1. Dimostriamo che se $|Z| = p, p^2$ allora G/Z e' un gruppo abeliano

CASE: $|Z| = p$

$$|G/Z| = |G|/|Z| = p^2$$

$$|G/Z| = p^2 \Rightarrow G/Z \text{ e' abeliano}$$

CASE: $|Z| = p^2$

$$|G/Z| = p \Rightarrow G/Z \text{ e' ciclico} \Rightarrow G/Z \text{ e' abeliano}$$

Consideriamo la suriezione naturale π :

$$\pi : G \longrightarrow G/Z$$

$$\pi(g) = \bar{g} = gZ$$

$$\bar{a}\bar{b} \quad \underbrace{=}_{G/Z \text{ e' abeliano}} \quad \bar{b}\bar{a} \Leftrightarrow \bar{a}\bar{b}\bar{a}^{-1}\bar{b}^{-1} = \bar{\mathbf{e}} \Leftrightarrow \overline{aba^{-1}b^{-1}} = \bar{\mathbf{e}}$$

$$\Rightarrow aba^{-1}b^{-1} \in \ker \pi = Z$$

3. Dim 3.

Si ha che $o(\bar{g}) = p^2$, infatti,

$$g^p \notin Z = \ker \pi \Rightarrow \bar{g}^p = \bar{g}^p \neq \bar{e}$$

se per assurdo $o(\bar{g}) = 1, p \Rightarrow \bar{g}^p = \bar{e}$ assurdo

se per assurdo $o(\bar{g}) = p^3 \Rightarrow |G/Z| = p^3 \Rightarrow |Z| = 1$ assurdo, perche' Z e' non banale

Consideriamo i vari casi:

$$|Z| = p, p^2, p^3$$

Se per assurdo $|Z| = p^3$, allora $Z = G$ e $g^p \in Z$. Assurdo.

Se $|Z| = p$, allora

$$|Z| = p \Rightarrow |G/Z| = p^2$$

$$o(\bar{g}) = p^2 \Rightarrow G/Z \text{ e' ciclico}$$

Se $|Z| = p^2$, allora

$$|Z| = p \Rightarrow |G/Z| = p \Rightarrow G/Z \text{ e' ciclico}$$

4. Dim. 4

Preso $\alpha \in G \setminus \{e\}$ consideriamo $\langle \alpha \rangle$.

Preso $\alpha_1 \in G \setminus \{\langle \alpha \rangle\}$ consideriamo $\langle \alpha_1 \rangle$.

4.1. Si ha che $\langle \alpha \rangle \cap \langle \alpha_1 \rangle = \{e\}$

Infatti, se per assurdo cosi' non fosse, si avrebbe $|\langle \alpha \rangle \cap \langle \alpha_1 \rangle| \neq 1$, e allora

$$|\langle \alpha \rangle \cap \langle \alpha_1 \rangle| \leq |\langle \alpha \rangle| \Rightarrow |\langle \alpha \rangle \cap \langle \alpha_1 \rangle| \Big/ |\langle \alpha \rangle| = p \Rightarrow |\langle \alpha \rangle \cap \langle \alpha_1 \rangle| = p$$

assurdo, perche' $\alpha_1 \notin \langle \alpha \rangle$.

Cosi' procedendo, avremo

$$\langle a \rangle, \langle \alpha_1 \rangle, \langle \alpha_2 \rangle, \dots$$

tutti disgiunti tra loro. Poiche' ognuno di loro e' di ordine p , abbiamo

$$|G| = x(p-1) + 1 \Leftrightarrow x = \frac{|G| - 1}{p-1} = \frac{p^3 - 1}{p-1} = \frac{(p-1)(p^2 + 1 + p)}{p-1} = p^2 + 1 + p$$

e x e' il numero cercato.

□