

Algebra II

AlpT (@freaknet.org)

June 12, 2008

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.

Saro' ben lieto di correggere ogni eventuale errore che mi comunicherai.

Buon lettura.

~ ~

Copyright ©2007 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	3
1.2	Laterali modulo H	7
1.2.1	Teorema di Lagrange	8
1.3	Gruppo simmetrico	9
1.4	Gruppi diedrali	14
1.5	Sottogruppi normali	15
1.6	Gruppo quoziente	16
1.7	Gruppo prodotto	17
1.7.1	Prodotto interno ed esterno	17
1.7.2	Prodotto a piu' fattori	18
1.8	Omomorfismo tra gruppi	20
1.8.1	Teorema di Cayley	23
1.9	Azione di un gruppo	24
1.9.1	Azione di coniugio	26
2	p-gruppo	26
2.1	Teorema di Sylow	27
3	Classificazione degli abeliani	28
4	Proposizioni varie	29
5	Studio dei gruppi	30

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

$$\begin{aligned} M &\neq \emptyset \\ \cdot : M \times M &\longrightarrow M \end{aligned}$$

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., $(ab)cd = a(bc)d$)

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

$$\begin{aligned} a^0 &= 1 \\ a^n &= a \cdot a^{n-1}, \quad n \in \mathbb{N} \end{aligned}$$

Proposition 1.5. Valgono le seguenti proprieta':

$$\begin{aligned} a^m \cdot a^n &= a^{m+n} \\ (a^m)^n &= a^{mn} \end{aligned}$$

Definition 1.6. In un semigrupp puo' esistere l'**elemento unita'** e :

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

Proposition 1.7. L'elemento unita', se esiste, e' unico.

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

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

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

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:

$$\begin{aligned} \left(\frac{3}{4}, \frac{4}{1} \right) &\longrightarrow \frac{7}{5} \\ \left(\frac{6}{8}, \frac{12}{3} \right) &\longrightarrow \frac{18}{11} \end{aligned}$$

Proposition 1.9. *L'elemento inverso e' unico.*

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

$$\begin{aligned} G &\neq \emptyset \\ \cdot : G \times G &\longrightarrow G \\ \forall a, b, c \in G & \quad (ab)c = a(bc) \\ \exists e \in G : \forall a \in G & \quad ae = ea = a \\ \forall a \in G \exists a^{-1} \in G : & \quad aa^{-1} = a^{-1}a = e \end{aligned}$$

Se vale la proprieta' 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 semigruppato:

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

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

Proposition 1.12. *Valgono le seguenti proprieta':*

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

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

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

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

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': $U_n = \{x \in \mathbb{C} \mid x^n = 1\}$.

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' $(U_n, \cdot)$ ne otteniamo uno, dove

$$U_n = \{a \in \mathbb{Z}_n \mid \text{mcd}(a, n) = 1\}$$

Si ha $|U_n| = \varphi(n)$ 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, ??, pg. ??]).

Verifichiamo che $\cdot$ e' una operazione:

$$M, N \in O_n \Leftrightarrow {}^t M = M^{-1}, {}^t N = N^{-1}$$

$${}^t(MN) = {}^t N {}^t M = N^{-1} M^{-1} = (MN)^{-1} \Leftrightarrow {}^t(MN) = (MN)^{-1} \Leftrightarrow MN \in O$$

4. gruppo ortogonale speciale:

$$SO_n(\mathbb{R}) = \{M^{n \times n}(\mathbb{R}) \text{ matrice} \mid {}^t M = M^{-1}, \det M = 1\}$$

$$O_n(\mathbb{R}) \setminus SO_n(\mathbb{R}) = \{M^{n \times n}(\mathbb{R}) \text{ matrice} \mid {}^t M = M^{-1}, \det M = -1\}$$

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'

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

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

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

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

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

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

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

Proposition 1.22. Caratterizzazione dei sottogruppi finiti.

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

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

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

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

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

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

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

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

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

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

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.

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

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:

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

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

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.5])).

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

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

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

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

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

$$g^i = g^j \Leftrightarrow i = j \pmod{p}$$

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

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

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

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

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

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

Theorem 1.39.

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

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

Proposition 1.40.

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

Non vale il viceversa.

Proposition 1.41. Caratterizzazione dei gruppi ciclici finiti.

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

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

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

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

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

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

Corollary 1.43. Dato G ciclico,

$$\{S \leq G\} \xleftrightarrow{f} \left\{m \in \mathbb{Z} \mid m \mid n\right\}$$

con f biunivoca

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

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

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

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

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

$$\mathbb{Z} = \langle 1 \rangle$$

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

1.2 Lateralı modulo H

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

$$aH = \{ah \mid h \in H\}$$

$$Ha = \{ha \mid h \in H\}$$

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

$$1. \bigcup_{a \in G} aH = G$$

$$2. \text{ Presi } a, b \in G$$

$$aH \neq bH \Rightarrow aH \cap bH = \emptyset$$

o equivalentemente

$$aH = bH \Leftrightarrow aH \cap bH \neq \emptyset$$

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

$$a \equiv_s b (H) \Leftrightarrow aH = bH \Leftrightarrow aH \cap bH \neq \emptyset$$

$$\Leftrightarrow \exists h_1 \in H \exists h_2 \in H : ah_1 = bh_2, \quad h = h_2h_1^{-1} \in H$$

$$\Leftrightarrow a = bh \Leftrightarrow b^{-1}a = h$$

$$a \equiv_d b (H) \Leftrightarrow Ha = Hb \Leftrightarrow Ha \cap Hb \neq \emptyset$$

$$\Leftrightarrow \exists h_1 \in H \exists h_2 \in H : h_1a = h_2b, \quad h = h_1^{-1}h_2 \in H$$

$$\Leftrightarrow a = hb \Leftrightarrow ab^{-1} = h$$

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

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

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.

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

Lemma 1.52.

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

$$\varphi : H \leftrightarrow aH$$

$$\varphi(h) = ah$$

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.

Proposition 1.54. Dato G di ordine finito,

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

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: $\{e\}, G$.

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.

Corollary 1.57.

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

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

$$(a, n) = 1 \Rightarrow a^{\varphi(n)} = 1 \quad (\mathbb{Z}_n)$$

$$p \text{ primo} \Rightarrow a^{p-1} = 1 \quad (\mathbb{Z}_p)$$

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).

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

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 $x \in X$,

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

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 $\sigma^m(x) = x$.

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:

$$\gamma : X \longrightarrow X$$

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

che indicheremo semplicemente con

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

La proposizione [1.63,pg.9] 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 ,

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

Example 1.65.

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

$$\mathcal{O}_\sigma(1) = \{1, 3, 2\}$$

$$\mathcal{O}_\sigma(4) = \{4\}$$

$$\text{cicli: } (1, 3, 2), (4)$$

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

$$(3, 1, 2) \text{ non e' un ciclo di } \sigma$$

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

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.

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

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

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.

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

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

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

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.*

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*

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

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

Proposition 1.75.

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

$$A_n \leq S_n$$

Proposition 1.76.

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

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 ,*

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

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:

$$\begin{aligned}\tau(1) &= 5 \\ \tau(3) &= 4 \\ \tau(2) &= 1 \\ \tau(5) &= 2 \\ \tau(4) &= 3\end{aligned}$$

ovvero

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

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

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

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

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

Una partizione di un intero n è 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 $p(4) = |\{(4), (3, 1), (2, 2), (2, 1, 1), (1, 1, 1, 1)\}| = 5$.

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

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

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

$$m_0 := 0$$

Proposition 1.85.

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

Proposition 1.86. *Sia $n > 2$, allora*

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

Ovvero, il centro di S_n è banale.

Da qui si capisce perché S_n non è abeliano.

Example 1.87. Studiamo S_3 .

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

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

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

$$|A_3| \underset{[1.76, \text{pg. 11}]}{=} \frac{3!}{2} = 3$$

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

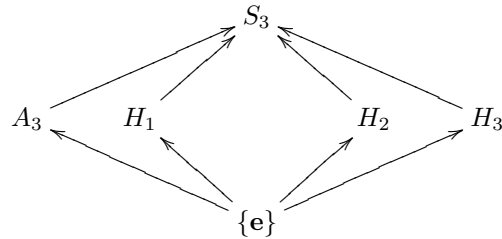
$$H_2 = \{(1), (2, 3)\}$$

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

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

Il diagramma delle inclusioni dei sottogruppi:

I laterali sinistri di H_1 :



$$|S_3| = 6 \underset{\text{Lagrange}[1.53, \text{pg. 8}]}{=} |H_1| i_G(H_1) \Rightarrow i_G(H_1) = 3$$

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

Quindi, questo e' anche un esempio di laterali destri non coincidenti con laterali sinistri.
 $\langle 0 \rangle 1. A_3 \leq S_3$ e' normale ed e' l'unico sottogruppo 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.

Lemma 1.89.

1. $\sigma \in A_n \setminus \{\text{id}\}, n \geq 3 \Rightarrow \sigma$ e' prodotto di 3-cicli
2. $n \geq 5, \sigma_1, \sigma_2$ 3-cicli di $S_n \Rightarrow \sigma_1, \sigma_2$ sono coniugati in A_n , ovvero $\exists \sigma \in A_n : \sigma_1 = \sigma \sigma_2 \sigma^{-1}$

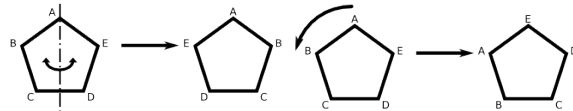
Definition 1.90. Sia G un gruppo.

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

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

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.

$$|D_n| = 2n$$

Proposition 1.94.

$$D_n \leq S_n$$

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

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

$$R \leq D_n, R = \langle r \rangle$$

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

$$o(s) = 2$$

Lemma 1.96. In D_n ,

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

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

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

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

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.

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

Proposition 1.99.

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

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.4])

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

Proposition 1.103.

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

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

Proposition 1.105. Sia $J, K \leq G$,

$$H \leq K \text{ normale} \Rightarrow H \cap J \leq K \cap J \text{ normale}$$

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.7], che in questo caso coincide sia con $\equiv_s$ che con $\equiv_d$.

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 $\equiv(H)$

Proposition 1.108. $|G| = n$

$$\begin{cases} m \mid n \\ \exists! H \leq G : |H| = m \end{cases} \Rightarrow H \text{ e' normale}$$

Nota: il viceversa vale solo se H e' un sottogruppo di Sylow normale (vedi [2.9,pg.27])

Proposition 1.109.

$$\begin{cases} H, K \leq G \text{ normali} \\ H \cap K = \{e\} \\ a \in H, b \in K \end{cases} \Rightarrow ab = ba$$

Example 1.110. $A_n \leq S_n$ e' un sottogruppo normale. (Per la def di A_n vedi [1.75,pg.11])

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:

$$aH \cdot bH = abH$$

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.6]). 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.16], 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.7], 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

$$\left| \frac{G}{H} \right| = \frac{|G|}{|H|}$$

Proposition 1.115. Dato G qualsiasi, $H, K \leq G$: $H \subseteq K$, H normale in G , si ha

$$K \text{ normale in } G \Leftrightarrow \frac{K}{H} \text{ normale in } \frac{G}{H}$$

1.7 Gruppo prodotto

Definition 1.116. $HK = \{hk \mid h \in H, k \in K\}$

Proposition 1.117. *Siano $H, K \leq G$*

$$HK \leq G \Leftrightarrow HK = \langle H \cup K \rangle$$

Proposition 1.118. *Dati $H, K \leq G$*

$$HK \leq G \Leftrightarrow HK = KH$$

Proposition 1.119. *Siano $H, K \leq G$*

$$H \text{ normale} \vee K \text{ normale} \Rightarrow HK \leq G$$

$$H, K \text{ normali} \Rightarrow HK \leq G \text{ normale}$$

Proposition 1.120. *Dati G gruppo finito, $H, K \leq G$ sottogruppi, con K normale, si ha*

$$\begin{cases} H \cap K = \{e\} \\ |G| = |H||K| \end{cases} \Rightarrow G = HK$$

Proposition 1.121. *Dato G e $H, K \leq G$,*

$$\begin{cases} G = HK \\ H \cap K = \{e\} \end{cases} \Leftrightarrow \forall g \in G \exists!(h, k) \in H \times K : g = hk$$

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'

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. 20])

$$\begin{aligned} i_1 : G &\longrightarrow G \times G' \\ i_1(g) &= (g, e') \\ i_2 : G' &\longrightarrow G \times G' \\ i_2(g') &= (e, g') \end{aligned}$$

Inoltre, poiche' i_1, i_2 sono iniettivi, abbiamo

$$\begin{aligned} G &\simeq i_1(G) \\ G' &\simeq i_2(G') \end{aligned}$$

Proposition 1.125. Sia G prodotto interno di H, K , allora gli elementi di H, K commutano tra loro, ovvero

$$hk = kh \quad \forall h \in H \forall k \in K$$

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':

$$\begin{aligned} f : H \times K &\longrightarrow G \\ f(h, k) &= hk \end{aligned}$$

Example 1.127. Consideriamo il gruppo ciclico $G = (\mathbb{Z}_6, +)$.

$$\begin{aligned} G = \langle 1 \rangle &\Rightarrow G \text{ ciclico} \Rightarrow G \text{ abeliano} \Rightarrow \forall H \leq G \quad H \text{ normale} \\ t \mid |G| = 6 &\underbrace{\Rightarrow}_{[1.42, \text{pg.6}]} \exists! H \leq G : |H| = t \end{aligned}$$

quindi gli unici sottogruppi non banali di G sono:

$$\begin{aligned} H, K &\leq G, \quad |H| = 3, \quad |K| = 2 \\ H &= \{0, 2, 4\}, \quad K = \{0, 3\} \end{aligned}$$

abbiamo:

$$\begin{aligned} H \cap K &= \{0\} \\ |HK| &\underbrace{=}_{[1.153, \text{pg.22}]} \frac{|H||K|}{|H \cap K|} = \frac{3 \cdot 2}{1} = 6 \Rightarrow HK = G \end{aligned}$$

Quindi G e' un prodotto interno di H, K , e per il thm [1.126,pg.18], si ha

$$\mathbb{Z}_6 \simeq H \times K$$

e inoltre per la prop [1.121,pg.17], 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,

A è loro prodotto interno $\stackrel{\text{def}}{\Leftrightarrow} A$ è prodotto interno di H_i e $H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_t \quad \forall i = 1, 2, \dots, t \Leftrightarrow$

$$\Leftrightarrow \begin{cases} H_i \cap (H_1 H_2 \dots H_{i-1} H_{i+1} \dots H_t) = \{e\} & \forall i = 1, 2, \dots, t \\ A = H_1 H_2 \dots H_t \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \forall a \in A \quad \exists (h_1, h_2, \dots, h_t) \in H_1 \times H_2 \times \dots \times H_t : a = \prod_{i=1}^t h_i$$

Poiché per il thm [1.126,pg.18] sussiste un isomorfismo tra il prodotto interno ed esterno, e poiché per il thm [1.126,pg.18] 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

$$G \text{ è abeliano} \Leftrightarrow G_i \text{ è abeliano} \quad \forall i = 1, 2, \dots, t$$

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

$$o(g) = \text{mcm}(o(g_1), o(g_2), \dots, o(g_t))$$

Proposition 1.133. Sia $G = G_1 \times G_2 \times \dots \times G_t$, finito, allora

$$\begin{cases} G \text{ è ciclico} \\ G = \langle g \rangle \end{cases} \Leftrightarrow \begin{cases} G_i \text{ è ciclico} & \forall i = 1, 2, \dots, t \\ G_i = \langle g_i \rangle \\ (|G_i|, |G_j|) = (o(g_i), o(g_j)) = 1 & \forall i \neq j \end{cases}$$

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 è

$$\phi([i]_{nm}) = ([i]_n, [i]_m)$$

Proposition 1.135. Dati G_1, G_2 gruppi ciclici di ordine n, m ,

$$(n, m) = 1 \Leftrightarrow G_1 \times G_2 \text{ è ciclico}$$

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' surriettiva, 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 .

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.

$$\ker f = \{a \in G \mid f(a) = e'\}$$

di sicuro $e \in \ker f$.

Proposition 1.140. $\ker f = \{e\} \Leftrightarrow f$ e' iniettiva

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'

Proposition 1.142. Sia $f : G \longrightarrow G'$ un omomorfismo,

$$f \text{ surriettivo, } H \leq G \text{ normale} \Rightarrow f(H) \text{ e' normale}$$

Proposition 1.143. Sia $f : G \longrightarrow G'$ un omomorfismo,

$$H' \leq G' \text{ normale} \Rightarrow f^{-1}(H') \leq G \text{ normale}$$

Corollary 1.144. Sia $f : G \longrightarrow G'$ omomorfismo.

$$\ker f \leq G \text{ e' normale}$$

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 $o(f(g)) = o(g)$.

Proposition 1.146. Sia $G = \langle g \rangle$, allora

CASE: $|G| = n$

CASE: $|G| = +\infty$

Dove $\text{Hom}(G, G')$ e' l'insieme definito in [1.136, pg.20].

In altre parole, quando G e' ciclico, conosciamo esplicitamente tutti gli omomorfi da G a G' .

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,

$$f \text{ surriettiva} \Rightarrow \text{Im } f = G' \Rightarrow G/\ker f \simeq G'$$

Corollary 1.148. Se G e' finito, dato $f : G \longrightarrow G'$ omomorfismo si ha

$$\left| \frac{G}{\ker f} \right| = \frac{|G|}{|\ker f|} = |\text{Im } f|$$

o equivalentemente

$$|G| = |\ker f| |\text{Im } f| \Leftrightarrow i_G(\ker f) = |\text{Im } f|$$

Corollary 1.149. Dal cor [1.148,pg.21] segue immediatamente che

$$|\operatorname{Im} f|/|G|$$

Inoltre, se G' e' finito, per Lagrange, si ha

$$|\operatorname{Im} f|/|G'|$$

Theorem 1.150. Ogni gruppo ciclico e' 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, $G = \langle a \rangle$ e' un gruppo ciclico infinito, allora

$$(G, \cdot) \simeq (\mathbb{Z}, +)$$

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.

Theorem 1.152. teorema dell'isomorfismo I.

Dati $H, K \leq G$,

$$K \text{ normale in } G \Rightarrow \frac{H}{H \cap K} \simeq \frac{HK}{K}$$

Corollary 1.153. Dati $H, K \leq G$ finiti³, con K normale, si ha

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Corollary 1.154. Dati $H, K \leq G$, con K normale in G , si ha:

$$\psi \text{ e' surriettiva} \Leftrightarrow G = HK$$

dove

$$\begin{aligned} \psi : H &\longrightarrow \frac{G}{K} \\ \psi(h) &= hK \end{aligned}$$

Theorem 1.155. dell'isomorfismo II.

Dati $H, K \leq G$, entrambi normali,

$$H \subseteq K \Rightarrow \frac{G/H}{K/H} \simeq \frac{G}{K}$$

Proposition 1.156. Nelle ipotesi del teorema precedente ([1.155,pg.22]), considerando

³ G non e' necessariamente finito

$$\begin{array}{ccccc}
\frac{K}{H} & \xrightarrow{i} & \frac{G}{H} & \xrightarrow{\varphi} & \frac{G}{K} \\
& & \searrow \alpha & & \swarrow \beta \\
& & \{e\} & &
\end{array}$$

con

$$\alpha(e) = H$$

$$\beta(aK) = e \quad \forall aK \in \frac{G}{K}$$

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:

$$f : M \longrightarrow N$$

$$f(H) = \varphi(H)$$

dove M, N sono i due insiemi.

Corollary 1.158. Se consideriamo solo i sottogruppi normali di G e G' , il thm di corrispondenza vale ancora, ovvero

$$|\{H' \leq G' \text{ normale}\}| = |\{H \leq G \text{ normale} \mid H \supseteq \ker \varphi\}|$$

Example 1.159. Se $|G'| = p$, dove p primo,

$$|G'| = p \text{ primo} \quad \underbrace{\Leftrightarrow}_{[1.55, \text{pg. } 8]} (H' \leq G' \Rightarrow H' = \{e\} \vee H' = G') \Leftrightarrow N = \{\{e\}, G'\}$$

Allora, per il thm di corrispondenza [1.157, pg. 23],

$$|M| = |N| = 2 \Rightarrow M = \{\ker \varphi, G\}$$

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 omomorfismo, con $\text{Im } f \leq S(G)$.

Inoltre, una tale immersione e'

$$f(a) = T_a$$

$$T_a(x) = ax$$

T_a si chiama traslazione sinistra tramite a .

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 $G/_s H = \{aH\}_{a \in G}$ l'insieme quoziente su G indotto dalla relazione d'equivalenza $\equiv_s(H)$ (vedi [1.48, pg. 7]). Allora,

$$\exists f : G \longrightarrow S(G/_s H) \text{ omomorfismo}$$

Valgono inoltre le seguenti proprietà:

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 :

$$N \subseteq H \text{ normale in } G \Rightarrow N \subseteq K$$

$$4. \ker f = \{a \in G \mid \forall x \in G \ axH = xH\}$$

Corollary 1.163.

$$\begin{cases} H \leq G, & |H| = p \text{ primo} \\ |G| \nmid i_G(H)! \end{cases} \Rightarrow H \text{ e' normale}$$

Corollary 1.164.

$$\begin{cases} |G| = pq, & p \geq q, \ p \text{ primo} \\ H \leq G, & |H| = p \end{cases} \Rightarrow H \text{ normale}$$

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

$$\exists H \leq G : |H| = n$$

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 proprietà:

$$\begin{aligned} e * x &= x \quad \forall x \in X \\ (a \cdot b) * x &= a * (b * x) \quad \forall a, b \in G \quad \forall x \in X \end{aligned}$$

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.

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 .

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 .

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.

Corollary 1.174. Se G e' 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

$$\begin{aligned}\mathcal{O}(x) &= X \text{ infatti} \\ y \in X = G &\Rightarrow gx = y \Leftrightarrow g = yx^{-1} \\ \text{St}(x) &= \{e\}\end{aligned}$$

Lemma 1.176. Dato $|G|$, con $|G| = p$ primo, si ha:

1. $\forall x \in X \quad |\mathcal{O}(x)| = 1 \vee |\mathcal{O}(x)| = p$
2. $|X| = \lambda p, \exists x \in X : |\mathcal{O}(x)| = 1 \Rightarrow |Y| = \mu p \geq p, \text{ dove } Y = \{y \in X \mid |\mathcal{O}(y)| = 1\}$

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 $\lambda, \mu \neq 0$).

Theorem 1.177. *di Cauchy.*

$$|G| = n, \ p \text{ primo}, p \nmid n \Rightarrow \exists H \leq G : |H| = p$$

$$\exists H \leq G : |H| = p \Leftrightarrow \exists a \in G : o(a) = p \Leftrightarrow \exists a \in G : \begin{cases} a^p = e \\ a \neq e \end{cases}$$

1.9.1 Azione di coniugio

Con G , $X = G$, consideriamo la seguente azione⁴:

$$g * x = gxg^{-1}$$

che viene detta *azione di coniugio* o di coniugazione.

Proposition 1.178. $\text{St}(x) = C(x)$

dove $C(x)$ e' il centralizzante di x (vedi [1.24,pg.4])

Proposition 1.179.

$$\mathcal{O}(x) = \{x\} \Leftrightarrow x \in Z(G)$$

Poiche' per la prop [1.172,pg.25] $\mathcal{O}(x)$ e' una classe, si ha che ogni elemento del centro individua una classe.

Proposition 1.180. Se G e' finito, si ha l'equazione di classe:

$$|G| = |Z(G)| + \sum_{z \in F} |\mathcal{O}(z)| = |Z(G)| + \sum_{z \in F} \frac{|G|}{|C(z)|}$$

$$F = f(\{\mathcal{O}(x) \mid x \notin Z(G)\})$$

$$f : \{\mathcal{O}(x)\}_{x \in X} \longrightarrow X \text{ tale che } f(\mathcal{O}(x)) \in \mathcal{O}(x)$$

In altre parole, la sommatoria e' estesa a tutti gli elementi esterni a $Z(G)$ e presi uno per orbita.

Proposition 1.181. $H \leq G$ normale $\Leftrightarrow H$ e' unione di orbite.

2 p-gruppo

Definition 2.1.

$$G \text{ e' un } p\text{-gruppo} \stackrel{\text{def}}{\Leftrightarrow} |G| = p^k, \ p \text{ primo}, \ k > 0$$

Proposition 2.2.

$$G \text{ e' un } p\text{-gruppo} \Leftrightarrow \forall a \in G \setminus \{e\} \exists i \in \mathbb{N} : o(a) = p^i$$

Proposition 2.3. Sia X l'insieme su cui agisce G , si ha

$$G \text{ } p\text{-gruppo}, |G| = p^k \Rightarrow \forall x \in X \exists t : |\mathcal{O}(x)| = p^t, \ 0 \leq t \leq k$$

⁴e' immediato verificare che si tratta di una azione

Proposition 2.4.

$$G \text{ p-gruppo} \Rightarrow \{e\} \subsetneq Z(G), \quad |Z(G)| = p^t, \quad 1 \leq t \leq k$$

Proposition 2.5. Dato G con $|G| = p^k$, p primo, allora

$$\begin{aligned} \exists H_1, H_2, \dots, H_k \leq G \text{ normali tali che} \\ \{e\} \subseteq H_1 \subseteq H_2 \subseteq \dots \subseteq H_k = G \\ |H_i| = p^i, \quad i = 1, 2, \dots, k \end{aligned}$$

Si vuol dire che esiste una catena di sottogruppi normali di G , di ordine $1, p, \dots, p^k$.

Proposition 2.6. Studiamo i p -gruppi di ordine p^k , $k = 1, 2$:

Proposition 2.7. Dato G con $|G| = 2p$, con $p > 2$ primo, si hanno questi due soli casi:

CASE: G e' ciclico

CASE: $G \simeq D_p$

2.1 Teorema di Sylow

Theorem 2.8. di Sylow

Sia G , $|G| = n$ e $k = \max \left\{ i \in \mathbb{N} \mid p^i \mid n \right\}$, 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

$$|K| = p^i, \quad i \leq k \Rightarrow \exists H \text{ p-sott. di Sylow tale che } K \subseteq H$$

4. Sia t il numero di p -sottogruppi di Sylow, allora

$$t \equiv 1 \pmod{p}, \quad t \equiv 1 \pmod{p}$$

dove m e' t.c.:

$$n = p^k m, \quad (m, p) = 1$$

Nota⁵

Proposition 2.9. $|G| = n$, $|H| = m$, $H \leq G$ di Sylow

$$H \text{ normale} \Leftrightarrow H \text{ e' l'unico sottogruppo di ordine } m$$

Proposition 2.10.

$$\begin{cases} |G| = pq, & q > p, & \text{primi} \\ p \nmid q-1 \end{cases} \Rightarrow G = \langle ab \rangle \text{ dove, } o(a) = p, o(b) = q$$

⁵Il numero m nasce cosi':

$$p^k \nmid n \Rightarrow n = p^k m$$

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 .

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.

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*

$$\begin{aligned} \forall i = 1, 2, \dots, t \quad \exists! H_i \leq G : |H_i| &= p_i^{r_i} \\ G &\simeq H_1 \times H_2 \times \dots \times H_t \\ \text{dove } H_i &\simeq K_{i1} \times K_{i2} \times \dots \times K_{it_i} \quad i = 1, 2, \dots, t \\ K_{ij} &\text{ e' ciclico } \quad \forall i, j \end{aligned}$$

In altre parole, G e' isomorfo al prodotto di gruppi ciclici.

Example 3.3. In congiunzione con le prop. [1.134,pg.19],[1.135,pg.19], il thm [3.2,pg.28] 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*

$$m \mid n \Rightarrow \exists H \leq G : |H| = m$$

Proposition 3.5. *Sia dato G abeliano, $|G| = n$, allora si ha*

$$\forall p \text{ primo} : p \mid n \quad \exists! H \leq G : |H| = p \Leftrightarrow G \text{ e' ciclico}$$

4 Proposizioni varie

Proposition 4.1. *Dato un G con $|G| \geq 2$,*

$$\forall a \in G \quad a^2 = e \Rightarrow G \text{ e' abeliano, } |G| = 2^k$$

Proposition 4.2. *Dati $a, b \in G$,*

$$\begin{cases} o(a) = m, & o(b) = n, & (m, n) = 1 \\ ab = ba \end{cases} \Rightarrow o(ab) = mn$$

Proposition 4.3. *Sia G abeliano, $a, b \in G$, allora*

$$\exists c \in G : o(c) = \text{mcm} \{o(a), o(b)\}$$

Proposition 4.4. *Dati $H, K \leq G$*

$$\begin{cases} |H| = p \text{ primo} \\ p \nmid |K| \end{cases} \Rightarrow H \cap K = \{e\}$$

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: $ba = a^{-1}b$.

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.22]
 $|G| = 3$ 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.8].

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.

Proposition 5.3. $|G| = 5$ allora $G = \langle a \rangle \simeq \mathbb{Z}_5$ ([1.56,pg.8] e [1.150,pg.22])

Proposition 5.4. $|G| = 6$ Si possono verificare solo due casi:

$$G \simeq \mathbb{Z}_6 \vee G \simeq S_3$$

Proposition 5.5. $|G| = 7$ allora G e' ciclico e $G \simeq \mathbb{Z}_7$ ([1.56,pg.8] e [1.150,pg.22])

Proposition 5.6. $|G| = 8$, si hanno questi casi

CASE: G abeliano

CASE: G non abeliano

Proposition 5.7. $|G| = 9$.

G e' abeliano, e si hanno questi casi:

CASE: G e' ciclico

CASE: $G = \langle a, b \rangle$, $o(a) = o(b) = 3$

Proposition 5.8. $|G| = 10$, si hanno questi due soli casi:

CASE: G e' ciclico

CASE: $G \simeq D_5$

Proposition 5.9. $|G| = 11$ e' ciclico poiche' 11 e' primo.

Proposition 5.10. $|G| = 12$

Proposition 5.11. $|G| = 13$ e' ciclico poiche' 13 e' primo.

Proposition 5.12. $|G| = 15 \Rightarrow G$ e' ciclico.