Alma Mater Studiorum · Università di Bologna

DIPARTIMENTO DI MATEMATICA
Corso di Laurea in Matematica

INTEGRALE DI UN GRUPPO

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
FABRIZIO CASELLI

Presentata da:
LAURA GIOVANNUCCI

Anno Accademico 2024-2025

Al coraggio di cambiare
e di essere sé stessi, sempre.

Introduzione

Teoria dei Gruppi e integrazione sono in matematica ambiti di studio differenti. L'uno riguarda l'algebra, l'altro l'analisi funzionale. In effetti l'integrale di un gruppo non ha nulla a che vedere con l'integrale di una funzione. Tuttavia la terminologia scelta per trattare l'argomento trova ragione d'essere in alcune proprietà dell'integrale di un gruppo, che permettono di fare un'analogia con la teoria classica di integrazione. In questa tesi si andrà a definire l'integrale di un gruppo e si vedranno alcuni esempi di gruppi integrabili e non integrabili.

Il Capitolo 1 è dedicato a definire il sottogruppo *derivato*. Per un gruppo G non abeliano, in generale due elementi $x,\ y$ non commutano. Viene allora naturale definire il commutatore di $x,\ y$ come $[x,y] := x^{-1}y^{-1}xy$. Dalla definizione segue che $xy = yx[x,y]$ e che due elementi commutano se e solo se il commutatore è banale. Il derivato di G, indicato con G', è il sottogruppo generato dai commutatori. Naturalmente per un gruppo abeliano il derivato è il gruppo banale.
Il derivato di G è caratteristico, cioè è fissato da ogni automorfismo di G , ed è il più piccolo sottogruppo normale che rende il quoziente G/G' abeliano. L'operatore di derivazione si comporta bene con il prodotto diretto: se $A,\ B$ sono due gruppi, il derivato di $A \times B$ è $A' \times B'$. Inoltre se $\varphi : G \longrightarrow K$ è un omomorfismo tra gruppi, l'immagine di un commutatore è ancora un commutatore, e $\varphi(G)' = \varphi(G')$.
Si determinerà il derivato dei gruppi diedrali D_n e dei gruppi simmetrici $\mathcal{S}_n$,

considerando $n > 2$ per escludere i casi che ricadono nei gruppi abeliani. Per i gruppi diedrali si ha che $D'_n \cong C_n$ se n è dispari, $D'_n \cong C_{\frac{n}{2}}$ se n è pari. Per i gruppi simmetrici il derivato è il gruppo alterno: $\mathcal{S}'_n = \mathcal{A}_n$. Inoltre si vedrà che se $n \geq 5$, $\mathcal{A}'_n = \mathcal{A}_n$. Questo risultato ha come corollario la non risolubilità del gruppo simmetrico $\mathcal{S}_n$ per $n \geq 5$. Si mostrerà infatti che condizione necessaria e sufficiente per la risolubilità di un gruppo è la possibilità di ricadere nel gruppo banale $\{e\}$ iterando un numero finito di volte il procedimento di derivazione.

Nel Capitolo 2 si introduce l'*integrale* di un gruppo G. La definizione ricalca il concetto di primitiva: l'integrale di G è un gruppo il cui derivato coincida con G stesso, o gli sia isomorfo. Proprio come l'integrale di una funzione, l'integrale di un gruppo, se esiste, non è unico. In particolare, se H è un integrale di G, allora anche $H \times A$ è un integrale di G, dove A è un qualsiasi gruppo abeliano. Inoltre se G è un gruppo finito e H è un suo integrale, è possibile costruire un integrale finito partendo da H.
Si vedranno tre classi di gruppi integrabili: i gruppi perfetti, i gruppi abeliani e i gruppi semplici finiti. I gruppi perfetti coincidono con il proprio derivato, dunque sono un integrale di sé stessi. Per un gruppo abeliano A si costruirà esplicitamente un integrale: questo è il prodotto intrecciato con C_2, ovvero $A \wr C_2$. I gruppi semplici finiti non hanno sottogruppi normali non banali. Se hanno ordine primo sono ciclici, e quindi integrabili come gruppi abeliani. Se hanno ordine non primo sono non abeliani e perfetti, quindi integrabili.
Infine si vedrà la relazione tra integrabilità e prodotto di gruppi. Sia $G = G_1 \times G_2$; se entrambi i fattori sono integrabili, allora lo è anche G. Il viceversa non è vero in generale: $C_2 \times D_4$ è integrabile ma D_4 non lo è. Tuttavia se aggiungiamo delle ipotesi la condizione si può invertire. In particolare se G è integrabile e $G_1,\ G_2$ sono finiti e tali che $MCD(|G_1|, |G_2|) = 1$, allora G_1 e G_2 sono integrabili. Inoltre se G_1 è senza centro e G_2 è abeliano, l'integrabilità di G è equivalente all'integrabilità di G_1.

Nel Capitolo 3 si mostrano alcuni esempi di gruppi non integrabili. In generale non è semplice decidere l'integrabilità di un gruppo, e non esiste un criterio universale. Abbiamo un criterio di non integrabilità: un gruppo G che possiede un sottogruppo ciclico caratteristico non centrale non è integrabile. Con questo criterio si dimostra che i gruppi diedrali e i gruppi non abeliani di ordine pq, con p, q primi e $q \mid p-1$ non sono integrabili. In tutti gli altri casi i gruppi di ordine pq sono integrabili.
Infine si analizzano i gruppi completi, che sono gruppi senza centro in cui tutti gli automorfismi sono interni. Per i gruppi completi essere integrabili è equivalente all'essere perfetti. Se $n > 2,\ n \neq 6$, allora $\mathcal{S}_n$ è completo e non perfetto: dunque non è integrabile. Anche per $\mathcal{S}_6$ si può dimostrare che non è integrabile.

Indice

Capitolo 1

Il sottogruppo derivato

In questo capitolo vedremo come, dato un gruppo G, è possibile definire il sottogruppo derivato. Mostreremo che questo è il più piccolo sottogruppo normale di G tale per cui il quoziente G/G' è abeliano. Una proprietà importante del derivato è di essere fissato da ogni automorfismo di G, cioè di essere un sottogruppo caratteristico.

1.1 Sottogruppo caratteristico

Definizione 1.1. Sia G un gruppo e $H \leq G$. H è caratteristico in G se è invariante sotto ogni automorfismo di G, cioè se:

$$\forall\ \phi \in \mathrm{Aut}(G), \quad \phi(H) = H.$$

Osservazione 1.2. In particolare un sottogruppo caratteristico è normale. Infatti basta considerare gli automorfismi interni di G:

$$\begin{aligned} \varphi_g : G &\longrightarrow G \\ a &\longmapsto g^{-1}ag \end{aligned}$$

Poiché H è caratteristico vale:

$$\varphi_g(H) = H \quad \forall g \in G \iff H = g^{-1}Hg \quad \forall g \in G \iff H \trianglelefteq G.$$

□

Un primo esempio di sottogruppo caratteristico è il centro di un gruppo. Richiamiamo la definizione.

Definizione 1.3. Sia G un gruppo. Chiamiamo centro di G l'insieme:

$$Z(G) \coloneqq \{z \in G \quad | \quad zg = gz \quad \forall g \in G\}.$$

Se $Z(G) = \{e\}$ diciamo che G è senza centro.

Dalla definizione segue che il centro è un gruppo abeliano e normale. Inoltre $Z(G)$ coincide con G se e solo se G è un gruppo abeliano.
Mostriamo che $Z(G)$ è un sottogruppo caratteristico.

Proposizione 1.4. *Z(G) è un sottogruppo caratteristico.*

Dimostrazione. Sia $\phi \in \mathrm{Aut}(G)$, $z \in Z(G)$, e $g, g' \in G$ tali che $\phi(g') = g$.

$$\begin{aligned} &\phi(z)g = \phi(z)\phi(g') = \phi(zg') = \phi(g'z) = \phi(g')\phi(z) = g\phi(z) \\ &\implies \phi(z) \in Z(G) \implies \phi(Z(G)) \subseteq Z(G). \end{aligned}$$

Per l'altro contenimento basta considerare l'automorfismo ϕ^{-1}. Per il ragionamento fatto sopra $\phi^{-1}(Z(G)) \subseteq Z(G)$ e poi si applica ϕ :

$$\phi(\phi^{-1}(Z(G)) \subseteq \phi(Z(G)) \implies Z(G) \subseteq \phi(Z(G)).$$

Dunque $Z(G) = \phi(Z(G))\ \forall\ \phi \in Aut(G)$, cioè il centro è un sottogruppo caratteristico. □

I prossimi risultati saranno utili per le dimostrazioni future.

Lemma 1.5. *Sia G un gruppo e siano $K, H \leq G$ tali che $K \leq H \leq G$. Se K è caratteristico in H e H è caratteristico in G, allora K è caratteristico in G.*

Dimostrazione. Sia $\varphi \in Aut(G)$. H è caratteristico in $G \implies \varphi(H) = H$, dunque $\varphi \in Aut(H)$. Poiché K è caratteristico in H $\implies \varphi(K) = K$ e vale la tesi. □

Lemma 1.6. *Sia G un gruppo e N un suo sottogruppo normale. Se K è un sottogruppo caratteristico di N allora K è un sottogruppo normale di K.*

Dimostrazione. N è normale in G. Allora $\varphi_g(N) = g^{-1}Ng = N \quad \forall\ g \in G$. Questo implica che $\varphi_g \in Aut(N)$. K è caratteristico in N, cioè $\psi(K) = K \ \ \forall\ \psi \in Aut(N)$. Quindi vale:

$$\varphi_g(K) = K \quad \forall\ g \in G \iff g^{-1}Kg = K \quad \forall\ g \in G \iff K \trianglelefteq G.$$

□

1.2 Il sottogruppo derivato

In generale l'operazione di un gruppo non è commutativa. Infatti, per un gruppo non abeliano, prendendo due elementi a e b in generale si ha $ab \neq ba$. Si introduce dunque il concetto di commutatore.

Definizione 1.7. Sia G un gruppo, e $a, b \in G$. Chiamiamo commutatore di a e b l'elemento:

$$[a, b] \coloneqq a^{-1}b^{-1}ab.$$

Osservazione 1.8. Il commutatore ha questo nome perché fa commutare due elementi del gruppo. Infatti:

$$[a, b] = a^{-1}b^{-1}ab \iff ab = ba[a, b].$$

Segue subito che due elementi a e b commutano se e solo se $[a, b] = e$, cioè il loro commutatore è l'elemento neutro del gruppo.

Definizione 1.9. Il sottogruppo generato dai commutatori di un gruppo G si chiama derivato o sottogruppo dei commutatori. Si denota con G' oppure $[G, G]$:

$$G' \coloneqq \langle [a, b] \mid a, b \in G \rangle.$$

Abbiamo osservato che a e b commutano $\iff [a,b] = e$. Da questo segue che un gruppo G è abeliano se e solo se il suo derivato è banale, cioè $G' = \{e\}$. Dunque possiamo dire che il derivato ci dà una "misura" di quanto un gruppo si discosti dall'essere abeliano.

Vediamo più nel dettaglio come è fatto il sottogruppo derivato.

Proposizione 1.10. *Il sottogruppo derivato è costituito dal prodotto di commutatori.*

Dimostrazione. Sia G un gruppo. Osserviamo innanzitutto che l'elemento neutro del gruppo è un commutatore. Infatti dato $g \in G$ si ha $[g,g] = e$. Per concludere basta mostrare che l'inverso di un commutatore è ancora un commutatore, infatti dati $a, b \in G$:

$$[a,b]^{-1} = (a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba = [b,a].$$

□

Si osservi che il prodotto di due commutatori non è necessariamente un commutatore.

Esempio 1. E' stato dimostrato computazionalmente che il più piccolo gruppo il cui derivato non coincide con l'insieme dei commutatori ha ordine 96. In [5] vengono mostrati gli unici due gruppi non isomorfi di ordine 96 che hanno questa proprietà.

Il prossimo teorema mostra le principali proprietà del sottogruppo derivato.

Teorema 1.11. *Sia G un gruppo. Allora valgono:*

(a). G' è un sottogruppo caratteristico;

(b). G/G' è abeliano;

(c). se $N \trianglelefteq G$, allora G/N è abeliano se e solo se $G' \leq N$;

(d). se $N \trianglelefteq G$, allora $N' \trianglelefteq G$.

Dimostrazione. (a) Sia $\alpha \in Aut(G)$ e siano $a, b \in G$.
$\alpha([a,b]) = \alpha(a^{-1}b^{-1}ab) = \alpha(a^{-1})\alpha(b^{-1})\alpha(a)\alpha(b) =$
$= (\alpha(a))^{-1}(\alpha(b))^{-1}\alpha(a)\alpha(b) = [\alpha(a), \alpha(b)]$.

In altre parole un automorfismo porta commutatori in commutatori. Perciò vale $\alpha(G') \subseteq (G')$.
D'altra parte $[a,b] = \alpha[\alpha^{-1}(a), \alpha^{-1}(b)]$, dunque $G' \subseteq \alpha(G')$. I due contenimenti implicano $G' = \alpha(G')\ \forall\ \alpha \in Aut(G)$ e G' è un sottogruppo caratteristico.

(b) Per (a) G è in particolare normale; consideriamo il quoziente. Se $aG', bG' \in G/G'$ si ha:
$aG'bG' = abG' = ba[a,b]G' = baG' = bG'aG'$ e dunque G/G' è abeliano.

(c) Siano $a, b \in G$. Per mostrare la tesi basta osservare che:

$$NaNb = NbNa \iff Nab = Nba \iff Naba^{-1}b^{-1} = N$$
$$\iff aba^{-1}b^{-1} \in N.$$

(d) Abbiamo la catena di sottogruppi $N' \leq N \trianglelefteq G$. Per il punto (a) N' è caratteristico in N. Allora la tesi segue subito dal Lemma 1.6, che ci assicura che i sottogruppi caratteristici di sottogruppi normali sono normali.

□

Osservazione 1.12. Il punto (c) è equivalente a dire che G' è il più piccolo sottogruppo normale di G rispetto al quale il quoziente è abeliano.

Consideriamo ora il prodotto diretto di due gruppi. L'operatore di derivazione si comporta bene con il prodotto.

Proposizione 1.13. *Siano A e B due gruppi. Allora il derivato del prodotto è il prodotto dei derivati, cioè $(A \times B)' = A' \times B'$.*

Dimostrazione. Siano $a, a' \in A,\ b, b' \in B$. Il commutatore di (a, b) e (a', b') è:

$$[(a,b),(a',b')] = (a,b)^{-1}(a',b')^{-1}(a,b)(a',b') = (a^{-1}(a')^{-1}aa', b^{-1}(b')^{-1}bb') = \\ = ([a,a'],[b,b']) \in A' \times B'.$$

$A' \times B'$, essendo un gruppo, è chiuso rispetto alla sua operazione. Dunque il prodotto di commutatori di $(A \times B)'$ appartiene a $A' \times B'$ e vale $(A \times B)' \subseteq A' \times B'$.
D'altra parte, consideriamo un generico elemento $g \in A' \times B'$. Questo elemento sarà del tipo:

$$g = (a_1 a_2 ... a_k,\ b_1 b_2 ... b_h)$$

con a_i commutatori di A e b_i commutatori di B. Possiamo riscrivere g nel seguente modo:

$$g = (a_1,\ e)(a_2,\ e)...(a_k,\ e)(e,\ b_1)(e,\ b_2)...(e,\ b_h).$$

Allora basta mostrare che $(a_i, e),\ (e, b_i) \in (A \times B)'$. Mostriamolo per (a_1, e), per $(e,\ b_i)$ è analogo. Poiché a_1 è un commutatore di A, esistono $x, y \in A$ tali che $a_1 = [x, y] = x^{-1}y^{-1}xy$. Ma allora:

$$(a_1,\ e) = (x^{-1}y^{-1}xy,\ e) = (x^{-1},\ e)(y^{-1},\ e)(x,\ e)(y,\ e) = \\ = (x,\ e)^{-1}(y,\ e)^{-1}(x,\ e)(y,\ e) = [(x,\ e)(y,\ e)] \in (A \times B)'.$$

Dunque vale la tesi. □

Vediamo come si comportano gli omomorfismi con i commutatori.

Proposizione 1.14. *Siano G, K gruppi e $\varphi : G \to K$ un omomorfismo. Allora $\forall \ \ a, b \in G$ si ha $\varphi([a,b]) = [\varphi(a), \varphi(b)]$ e $\varphi(G)' = \varphi(G')$.*

Dimostrazione. Siano $a, b \in G$. Consideriamo il loro commutatore $[a,b]$ e applichiamo φ:

$$\varphi([a,b]) = \varphi(a^{-1}b^{-1}ab) = \varphi(a^{-1})\varphi(b^{-1})\varphi(a)\varphi(b) = [\varphi(a), \varphi(b)] \in \varphi(G)'.$$

Dunque gli omomorfismi mandano commutatori in commutatori e vale $\varphi(G') \subseteq \varphi(G)'$.
D'altre parte, $\forall\ x, y \in \varphi(G)$, esistono $a,\ b \in G$ tali che $x = \varphi(a)$ e $y = \varphi(b)$. Allora per l'uguaglianza sopra $[x,y] = [\varphi(a), \varphi(b)] = \varphi([a,b]) \in \varphi(G')$ e vale la tesi. □

1.3 Il derivato del gruppo diedrale

Consideriamo ora il gruppo diedrale D_n, definito come il gruppo delle simmetrie di un poligono regolare di n lati. In quest'ottica assumiamo $n \geq 3$. D_n è un gruppo di ordine $2n$, ed è generato da una rotazione di un angolo di $2\pi/n$, che indichiamo con r, e da una riflessione rispetto a uno dei suoi assi di simmetria, che indichiamo con s. In simboli:

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

Ricordiamo come è fatto il centro di D_n.

Lemma 1.15. *Il centro di D_n è isomorfo a C_2 se n è pari, è banale se n è dispari.*

Dimostrazione. Sia $D_n = \langle r, s \rangle$ il gruppo diedrale. Più esplicitamente:

$$D_n = \{e, r, ..., r^{n-1}, s, sr, ..., sr^{n-1}\}.$$

Inoltre vale che $sr^i = r^{n-i}s \quad \forall\ i = 1, ..., n-1$. Vediamo quali elementi formano il centro. Si ha che $z \in Z(D_n) \iff (zs = sz \ \wedge \ zr = rz)$.

Sia $i = 1, ..., n-1$. Se z è una rotazione r^i si ha che la seconda condizione è sempre verificata. Infatti $r^i r = r r^i \ \forall\ i$. La prima condizione impone:

$$r^i s = s r^i \iff r^i s = r^{n-i} s \iff i = n - i \iff i = \frac{n}{2}.$$

Sia ora $i = 1, ..., n$. Ricordiamo che $r^n = e$. Se z è una riflessione sr^i la seconda condizione impone:

$$sr^i r = r s r^i \iff r^{i+1} = s r s r^i \iff r^{i+1} = r^{n-1} r^i \iff i + 1 = n - 1 + i$$
$$\iff n = 2.$$

Quindi, avendo $n \geq 3$, nessuna riflessione appartiene al centro di D_n. Dunque si ha:

- se n è pari $Z(D_n) = \{e, r^{\frac{n}{2}}\} \cong C_2$, poiché $o(r^{\frac{n}{2}}) = 2$;
- se n è dispari $Z(D_n) = \{e\}$.

□

Esempio 2. Calcoliamo il derivato di D_4. Il centro di D_4 è $Z(D_4) = \{e, r^2\}$ e $D_4/Z(D_4) \cong K_4$, che è abeliano. Per il punto (c) del Teorema 1.11 si ha $D_4' \subseteq Z(D_4)$. Ma D_4' non può essere banale perchè D_4 non è abeliano. Di conseguenza $D_4' = Z(D_4) \cong C_2$.

Vediamo un risultato più generale.

Proposizione 1.16. *Il derivato di D_n è il sottogruppo generato da r^2. In particolare $D_n' \cong C_n$ se n è dispari e $D_n' \cong C_{\frac{n}{2}}$ se n è pari.*

Dimostrazione. Sia D_n il gruppo diedrale di ordine $2n$. Mostriamo innanzitutto che $\langle r^2 \rangle$ è normale in D_n. Sia $R \coloneqq \langle r \rangle$ il gruppo delle rotazioni, che è abeliano. $\langle r^2 \rangle$ è un sottogruppo di R, e dunque è normale in R. Per verificare che è normale nell'intero gruppo D_n basta coniugare r^2 con una simmetria s:

$$s r^2 s = (srs)(srs) = r^{n-1} r^{n-1} = r^{-1} r^{-1} = r^{-2} \in \langle r^2 \rangle.$$

Dunque $\langle r^2 \rangle$ è normale in D_n.
L'ordine di r^2 è $\frac{n}{2}$ se n è pari, n se n è dispari. Perciò $D_n/\langle r^2 \rangle$ ha ordine rispettivamente 4 o 2, dunque è abeliano. Da questo segue che $D_n' \subseteq \langle r^2 \rangle$. D'altra parte r^2 è un commutatore:

$$[s, r] = sr^{-1}sr = sr^{n-1}sr = ssrr = r^2.$$

Dunque $\langle r^2 \rangle \subseteq D_n'$ e vale $D_n' = \langle r^2 \rangle$. □

Esempio 3. Utilizziamo questa proposizione per calcolare il derivato di alcuni gruppi diedrali.
$D_3' \cong D_6' \cong C_3$.
$D_4' \cong C_2$ come avevamo già mostrato.

1.4 Il derivato del gruppo simmetrico

Ricordiamo alcune definizioni.

Definizione 1.17. Sia $n > 1$. Indichiamo con C_n la classe di isomorfismo del gruppo ciclico di ordine n.

Definizione 1.18. Sia $\mathcal{S}_n$ il gruppo simmetrico delle permutazioni di n elementi. Chiamiamo sottogruppo alterno $\mathcal{A}_n$ l'insieme delle permutazioni pari di $\mathcal{S}_n$, cioè l'insieme delle permutazioni che si possono scrivere con un numero pari di trasposizioni semplici.

Calcoliamo esplicitamente il sottogruppo derivato del gruppo simmetrico. Applichiamo il Teorema 1.11 per ottenere il derivato di $\mathcal{S}_3$.
In $\mathcal{S}_3$ si ha $\mathcal{A}_3 \cong C_3$. Perciò il quoziente $\mathcal{S}_3/C_3 \cong C_2$ è abeliano. Per il punto (c) del Teorema 1.11 si ha che $(\mathcal{S}_3)' \subseteq C_3$. Ci sono due possibilità:

- $(\mathcal{S}_3)' = \{1\} \iff \mathcal{S}_3$ è abeliano, che è assurdo;
- $(\mathcal{S}_3)' = \mathcal{A}_3$ rimane l'unica possibilità.

In effetti i $3-cicli$ di $\mathcal{A}_3$ si esprimono come commutatori come segue:

$$(123) = [(23), (132)]; \quad (132) = [(132), (23)].$$

Questo risultato vale in generale: il derivato di un gruppo simmetrico è il suo sottogruppo alterno.

Proposizione 1.19. *Il derivato di* $\mathcal{S}_n$ *è* $\mathcal{A}_n$ $\forall$ $n \geq 3$.

Dimostrazione. Ricordiamo che $[\mathcal{S}_n : \mathcal{A}_n] = 2$. Da questo segue che $\mathcal{A}_n$ è normale in $\mathcal{S}_n$ e $\mathcal{S}_n/\mathcal{A}_n \cong C_2$, che è abeliano. Quindi $(\mathcal{S}_n)' \subseteq \mathcal{A}_n$. Come abbiamo osservato sopra ogni $3-ciclo$ è un commutatore. Poiché $\mathcal{A}_n$ è formato dai prodotti dei $3-cicli$, si ha $\mathcal{A}_n \subseteq (\mathcal{S}_n)'$ e vale la tesi. □

Osservazione 1.20. Abbiamo visto che i $3-cicli$ sono commutatori. Tuttavia in $\mathcal{A}_3$ e $\mathcal{A}_4$ un $3-ciclo$ non è un commutatore di elementi di $\mathcal{A}_3$ e $\mathcal{A}_4$.
Se invece abbiamo a disposizione almeno 5 simboli diversi possiamo scrivere un $3-ciclo$ come commutatore di due $3-cicli$:

$$[(123), (145)] = (132)(154)(123)(145) = (142).$$

Perciò in $\mathcal{A}_5$ ogni elemento è prodotto di commutatori. Il prossimo risultato ci mostra che in realtà ogni elemento è un commutatore.

Proposizione 1.21. *Il derivato di* $\mathcal{A}_n$ *è* $\mathcal{A}_n$ $\forall$ $n \geq 5$.

Dimostrazione. Sia $n \geq 5$. $\mathcal{A}_n$ è generato da tutti i $3-cicli$ di $\mathcal{S}_n$, e come è noto non è abeliano. Per l'osservazione, a meno di scambiare i simboli, possiamo scrivere ogni $3-ciclo$ come commutatore di due $3-cicli$. Poiché il sottogruppo derivato è formato dai prodotti dei commutatori, segue che $(\mathcal{A}_n)' = \mathcal{A}_n$. □

1.5 Serie derivata e gruppi risolubili

Partendo da G' si può definire il sottogruppo derivato di G', cioè $(G')' := G^{(2)}$. Come visto nel punto (a) del Teorema 1.11 è un sottogruppo caratteristico di G' e per il punto (d) è un sottogruppo normale di G. Il procedimento di derivazione si può iterare.

Definizione 1.22. Sia G un gruppo. Si definisce sottogruppo derivato di ordine n il gruppo:

$$G^{(n)} = (G^{n-1})'.$$

Per le proprietà del derivato vale che per ogni k $G^{(k)}$ è un sottogruppo normale di G; inoltre $G^{(k-1)}/G^{(k)}$ è abeliano.

Il procedimento può terminare nel gruppo banale oppure no.

Definizione 1.23. La catena dei sottogruppi:

$$G = G^{(0)} \supseteq G' = G^{(1)} \supseteq G^{(2)} \supseteq ... \supseteq G^{(i)}...$$

è la serie derivata di G. Se $G^{(n)} = \{e\}$ per un qualche n, la serie derivata è finita.

Osservazione 1.24. I sottogruppi $G^{(i)}$ sono caratteristici in G. Mostriamolo per induzione.
Per $n = 1$ abbiamo dimostrato che è vero, infatti G' è caratteristico in G.
Sia $i < n$ e assumiamo l'ipotesi induttiva, cioè che $G^{(i)}$ sia caratteristico in G. Se consideriamo il derivato di $(G^{(i)})' = G^{(i+1)}$, questo è certamente caratteristico in $G^{(i)}$. Ma allora per il Lemma 1.5 è caratteristico anche in G. □

Introduciamo il concetto di gruppo risolubile.

Definizione 1.25. Un gruppo G si dice risolubile se esiste una catena finita di sottogruppi M_i tali che:

$$G = M_0 \supset M_1 \supset M_2 \supset ... \supset M_s = \{e\}$$

e tali che ciascuno degli M_i sia normale in M_{i-1}, e ogni quoziente M_{i-1}/M_i sia abeliano.

Esempio 4. Vediamo alcuni esempi di gruppi risolubili.

1. I gruppi abeliani sono risolubili. Infatti ci basta considerare la catena $G \supset \{e\}$.

2. Consideriamo $\mathcal{S}_3$. Abbiamo visto che $\mathcal{S}_3' = \mathcal{A}_3$. Dunque $\mathcal{A}_3 \trianglelefteq \mathcal{S}_3$ e $\mathcal{S}_3/\mathcal{A}_3$ è abeliano. Inoltre $\mathcal{A}_3 \cong C_3$ è abeliano. Allora si può considerare la catena $\mathcal{S}_3 \supset \mathcal{A}_3 \supset \{e\}$ e si conclude che $\mathcal{S}_3$ è risolubile.

3. Vediamo anche il caso di $\mathcal{S}_4$. Abbiamo dimostrato che $\mathcal{S}_4' = \mathcal{A}_4$. Dunque vale che $\mathcal{A}_4 \trianglelefteq \mathcal{S}_4$ e $\mathcal{S}_4/\mathcal{A}_3$ è abeliano. Tuttavia $\mathcal{A}_4$ non è abeliano. Infatti prendiamo $(123),\ (124) \in \mathcal{A}_4$. Si ha:

$$(123)(124) = (14)(23) \neq (124)(123) = (13)(24).$$

   Consideriamo il sottogruppo $V = \{e,\ (12)(34),\ (13)(24),\ (14)(23)\} \leq \mathcal{A}_4$. V contiene 3 elementi di ordine 2, dunque è isomorfo al gruppo di Klein, che è abeliano. Si ha che $[\mathcal{A}_4 : V] = 3$, dunque $\mathcal{A}_4/V \cong C_3$ che è abeliano. Inoltre $V \trianglelefteq \mathcal{A}_4$ perché contiene tutti gli elementi di $\mathcal{A}_4$ di ordine 2. Quindi la catena $\mathcal{S}_4 \supset \mathcal{A}_4 \supset V \supset \{e\}$ ci permette di concludere che $\mathcal{S}_4$ è risolubile.

Come vedremo alla fine di questa sezione non ci sono altri gruppi simmetrici risolubili.

Un risultato importante è la caratterizzazione dei gruppi risolubili con la serie derivata. Infatti condizione necessaria e sufficiente affinché un gruppo G sia risolubile è che in un numero finito di passi il procedimento di derivazione termini nel gruppo banale. In altre parole G deve avere una serie derivata finita.

Teorema 1.26. *Un gruppo G è risolubile se e solo se esiste $m \in \mathbb{N}$ tale che $G^{(m)} = \{e\}$.*

Dimostrazione. Supponiamo $G^{(m)} = \{e\}$ per un qualche $m \in \mathbb{N}$. Posto $M_i = G^{(i)}$ consideriamo la catena di sottogruppi:

$$M_0 = G \supset M_1 \supset M_2 \supset ... \supset M_m = G^{(m)} = \{e\}.$$

Questa catena coincide proprio con la serie derivata si G. Per le proprietà del sottogruppo derivato ogni M_i è caratteristico e quindi normale nel sottogruppo precedente M_{i-1}. Inoltre il quoziente:

$$M_{i-1}/M_i = G^{(i-1)}/G^{(i)} = G^{(i-1)}/(G^{(i-1)})'$$

è abeliano. Dunque G è risolubile.
Viceversa supponiamo G risolubile. Allora esiste una catena finita di sottogruppi

$$G = M_0 \supset M_1 \supset M_2 \supset ... \supset M_s = \{e\}$$

tali che $\forall\ i = 1, ..., s \quad M_i \trianglelefteq M_{i-1}$ e M_{i-1}/M_i è abeliano. Ma allora, per il Teorema 1.11 si ha che $M'_{i-1} \subseteq M_i\ \forall\ i$. Si hanno dunque questi contenimenti:

$M_1 \supseteq M'_0 = G'$;
$M_2 \supseteq M'_1 \supseteq G^{(2)}$ dall'inclusione precedente e passando ai derivati;
...
$M_i \supseteq M'_{i-1} \supseteq G^{(i)}$;
...
$M_s = \{e\} \supseteq M'_{s-1} \supseteq G^{(s)}$.

Dall'ultima riga segue che $G^{(s)} = \{e\}$. □

Corollario 1.27. *Il gruppo simmetrico $\mathcal{S}_n$ non è risolubile $\forall\ n \geq 5$.*

Dimostrazione. Sia $n \geq 5$. Abbiamo visto che $\mathcal{S}'_n = \mathcal{A}_n$. Con la Proposizione 1.21 abbiamo dimostrato che $\mathcal{A}_n$ è perfetto, cioè $\mathcal{A}'_n = \mathcal{A}_n \neq \{e\} \quad \forall\ n \geq 5$. In altre parole $\mathcal{S}_n$ non ha una serie derivata finita e dunque per il Teorema precedente non è risolubile. □

Osservazione 1.28. Questo risultato ha un'importanza storica ed è legato alla teoria sulla risolubilità delle equazioni polinomiali. Un polinomio è risolubile per radicali se e sole se il suo *gruppo di Galois* è risolubile. Per $n \geq 5$ il gruppo di Galois associato a un generico polinomio di grado n è proprio $\mathcal{S}_n$, che come abbiamo dimostrato non è risolubile. In altre parole il suo campo di spezzamento non è contenuto in un'estensione radicale, che è un'estensione ottenuta mediante una torre di estensioni algebriche, ognuna delle quali è ottenuta aggiungendo un elemento che è la radice n-esima di un elemento del campo precedente. Conseguenza di questo importante risultato è che non esiste una formula generale risolutiva per le equazioni di grado $n \geq 5$ contenente somme, prodotti e radici n-esime.

Capitolo 2

Integrale di un gruppo

In questo capitolo andiamo a definire il cuore dell'argomento di questa tesi. Vedremo i primi esempi di gruppi integrabili. La terminologia scelta richiama apertamente l'integrabilità in senso analitico. Sebbene siano concetti differenti, vedremo alcuni risultati che permettono di fare un parallelismo tra l'integrabilità algebrica di un gruppo e l'integrabilità analitica di una funzione.

2.1 Definizione e prime proprietà

Definizione 2.1. Sia G un gruppo. Un integrale di G è un gruppo H che verifica, a meno di isomorfismo, $H' = G$.
Se G ha un integrale diremo che è integrabile o che è un gruppo realizzabile da commutatori.

Come vedremo non tutti i gruppi sono integrabili, e non esiste un test semplice per decidere l'integrabilità.

Mostriamo le prime proprietà. Innanzitutto vediamo che se un gruppo ha un integrale, allora ne ha infiniti.

Proposizione 2.2. *Sia G un gruppo e H un integrale di G. Sia A un gruppo abeliano. Allora $H \times A$ è un integrale per G.*

Dimostrazione. H è un integrale di G, dunque $H' = G$. A essendo abeliano ha derivato banale. Per la Proposizione 1.13 vale:

$$(H \times A)' = H' \times A' = G \times \{e\} \cong G.$$

Cioè $H \times A$ è un integrale di G. □

Osservazione 2.3. Facendo un parallelismo con la primitiva F di una funzione f ($F' = f$), questo risultato è l'analogo di aggiungere una costante c a F e ottenere una nuova primitiva di f.

Il prossimo teorema mostra che se un gruppo finito ha un integrale, allora è possibile costruire un integrale finito di quel gruppo. Premettiamo alcuni risultati.

Introduciamo il concetto di gruppo privo di torsione, ovvero un gruppo dove ogni potenza di un qualsiasi elemento, escluso l'elemento neutro, non è mai uguale all'unità del gruppo.

Definizione 2.4. Un gruppo G si dice privo di torsione se $\forall\ g \in G, g \neq e$, si ha $o(g) = \infty$. Equivalentemente l'unico elemento di ordine finito è l'elemento neutro.

Il prossimo risultato è un'estensione del Teorema di Lagrange sull'indice dei sottogruppi.

Proposizione 2.5 (Proprietà moltiplicativa dell'indice)**.** *Sia G un gruppo e $K \leq H \leq G$ una catena di sottogruppi. Allora:* $[G : K] = [G : H][H : K]$.

Dimostrazione. Supponiamo finiti gli indici a destra dell'uguaglianza e poniamo $[G : H] = m$ e $[H : K] = n$. Si potrebbe ragionare analogamente

se fossero infiniti. Elenchiamo le m classi laterali di H in G, scegliendo un rappresentante per ogni classe:

$$G = g_1H \sqcup g_2H \sqcup ... \sqcup g_mH.$$

Allo stesso modo scegliamo dei rappresentanti per ogni classe laterale di K in H, ottenedo la partizione:

$$H = h_1K \sqcup ... \sqcup h_nK.$$

Poiché la moltiplicazione per g_i è un'operazione invertibile, si ha che $g_iH = g_ih_1H \sqcup ... \sqcup g_ih_nH$ è una partizione della classe laterale g_iH. Mettendo insieme le due partizioni si ottiene una partizione di G in $m \cdot n$ classi laterali del tipo g_ih_jK.

□

Infine diamo per buono questo risultato: un gruppo G abeliano finitamente generato si può scrivere in modo unico come prodotto $A \times B$, dove A è un gruppo finito, in particolare è il sottogruppo di torsione di G e B è il prodotto di r copie di $\mathbb{Z}$. B quindi è privo di torsione.

A questo punto possiamo dimostrare il seguente teorema.

Teorema 2.6. *Sia G un gruppo finito. Se G ha un integrale allora G ha un integrale che è un gruppo finito.*

Dimostrazione. Sia H un integrale di G. Riconduciamoci al caso in cui H è finitamente generato.
Poiché $G = H'$ e G è un gruppo finito, esiste un numero finito di commutatori $[h_1, k_1], ..., [h_r, k_r]$ che generano G, con $h_i, k_i \in H$. Se consideriamo $\tilde{H} = \langle h_i, k_i \rangle$ si ha che $\tilde{H} \leq H$, $\tilde{H}$ è un integrale di G ed è finitamente generato. Dunque senza perdita di generalità assumiamo H finitamente generato.
Mostriamo che ogni classe di coniugio di H è contenuta in una classe laterale di $H' = G$. Infatti siano $h, x \in H$. Poiché G è il derivato di H:

$$Gx^{-1}hxh^{-1} = G \implies Gx^{-1}hx = Gh.$$

Poiché G è finito, le classi di coniugio di H sono di ordine limitato.
Mostriamo che il centro di H ha indice finito. Sia $H = \langle h_1, ..., h_k \rangle$. Sappiamo che la cardinalità di una classe di coniugio di un elemento h uguaglia l'indice del suo centralizzante nel gruppo. Per quanto appena visto il centralizzante di ogni generatore $C_H(h_i)$ ha indice finito in H (al massimo $|G|$). In generale il centro di un gruppo è dato dall'intersezione dei centralizzanti di tutti i suoi elementi. Se il gruppo è finitamente generato, basta prendere l'intersezione dei centralizzanti dei generatori. Nel nostro caso:

$$Z(H) = \bigcap_{i=1}^{k} C_H(h_i)$$

e per quanto osservato ha indice finito in H.
$Z(H)$ è un gruppo abeliano ed è finitamente generato: lo possiamo scrivere come $Z(H) = A \times B$, dove A è finito e B è finitamente generato e privo di torsione.
Poiché $B \leq Z(H)$, B è un sottogruppo normale di H. Consideriamo la catena di sottogruppi $B \leq Z(H) \leq H$. Abbiamo visto che $[H : Z(H)]$ è finito. Inoltre $[Z(H) : B] = |A| < \infty$. Ma allora per la Proposizione 2.5 il quoziente $H/B = \bar{H}$ è un gruppo finito.
Poiché B è privo di torsione e G è finito, si ha $B \cap G = \{e\}$. Segue che la proiezione al quoziente ristretta a G è iniettiva:

$$\pi|_G : G \hookrightarrow H/B.$$

Allora unendo questo alla Proposizione 1.14 si ha:

$$\bar{H}' = \pi(H)' = \pi(H') = \pi(G) \cong G$$

Cioè $\bar{H}$ è un integrale finito di G. □

2.2 Primi esempi di gruppi integrabili

Il gruppo integrabile più semplice è il gruppo banale. Infatti un qualsiasi gruppo abeliano ha derivato banale. Si può anche osservare che $\{e\}' = \{e\}$. Ci sono altri gruppi con la proprietà di coincidere con il proprio derivato: li chiamiamo *gruppi perfetti*.

Definizione 2.7. Un gruppo G è perfetto se coincide con il proprio sottogruppo derivato, cioè $G' = G$.

Un gruppo perfetto è dunque integrabile per definizione ed è l'integrale di sé stesso. Con la Proposizione 1.21 abbiamo dimostrato che i gruppi alterni sono gruppi perfetti $\forall\ n \geq 5$.

2.3 Gruppi abeliani

Una classe importante di gruppi integrabili sono i gruppi abeliani, sia finiti che infiniti. In questa sezione vedremo come si può costruire un integrale di un gruppo abeliano. Dimostreremo che per ogni gruppo abeliano il prodotto intrecciato con C_2 è un integrale. La struttura del prodotto intrecciato è un tipo particolare di prodotto semidiretto.

Definizione 2.8. Siano G_1, G_2 gruppi e sia ϕ un omomorfismo da G_2 a $Aut(G_1)$:

$$\phi : G_2 \longrightarrow Aut(G_1)$$
$$g \longmapsto \varphi_g$$

Nel prodotto cartesiano $G_1 \times G_2$ si può definire l'operazione:

$$(g_1, g_2) \cdot (g_1', g_2') \coloneqq (g_1 \phi(g_2)(g_1'), g_2 g_2').$$

$G_1 \times G_2$ con questa operazione è un gruppo che prende il nome di prodotto semidiretto. Lo indichiamo con il simbolo: $G_1 \rtimes_\phi G_2$.

Osservazione 2.9. Dalla definizione segue che il prodotto semidiretto è un gruppo. L'elemento neutro è (e_1, e_2), cioè la coppia degli elementi neutri dei due gruppi. Infatti, se $(g_1, g_2) \in G_1 \rtimes_\phi G_2$ si ha:

$$(g_1, g_2) \cdot (e_1, e_2) = (g_1\phi(g_2)(e_1), g_2e_2) = (g_1e_1, g_2) = (g_1, g_2);$$
$$(e_1, e_2) \cdot (g_1, g_2) = (e_1\phi(e_2)(g_1), e_2g_2) = (id_{G_1}(g_1), g_2) = (g_1, g_2).$$

Vediamo come determinare l'inverso di un elemento (g_1, g_2). Poiché ϕ è un omomorfismo, dato $g_2 \in G_2$, l'automorfismo inverso di $\phi(g_2)$ è $(\phi(g_2))^{-1} = \phi(g_2^{-1})$. Sia $(x, y) = (g_1, g_2)^{-1}$. L'elemento x deve soddisfare:

$$g_1\phi(g_2)(x) = e_1 \iff \phi(g_2)(x) = g_1^{-1} \iff x = (\phi(g_2))^{-1}(g_1^{-1}) = \phi(g_2^{-1})(g_1^{-1}).$$

La condizione su y è invece: $g_2y = e_2 \iff y = g_2^{-1}$.
Per l'unicità dell'inverso abbiamo quindi che:

$$(g_1, g_2)^{-1} = (\phi(g_2^{-1})(g_1^{-1}), g_2^{-1}).$$

□

Osservazione 2.10. Inoltre osserviamo che $G_1 \rtimes_\phi G_2 = G_1 \times G_2$ se e solo se ϕ è l'omomorfismo nullo.

Con il prodotto semideretto possiamo costruire un'altra struttura algebrica: il prodotto intrecciato.

Definizione 2.11. Dati due gruppi N e H e un'azione di H su un insieme finito di indici $\Omega = \{1, ..., d\}$ definiamo il prodotto intrecciato:

$$N \wr_\Omega H \coloneqq B \rtimes H.$$

Dove B, detta base del prodotto intrecciato, è:

$$B = \prod_{i \in \Omega} N = \underbrace{N \times N \times ... \times N}_{d \text{ volte}}.$$

L'azione di H su B consiste nel permutare le componenti del prodotto diretto secondo l'azione di H su Ω.

Esempio 5. Sia A un gruppo e consideriamo $A \wr C_2$, il prodotto intrecciato con il gruppo ciclico di ordine 2. $H = C_2 = \{id, \sigma\}$ agisce su $\Omega = \{1, 2\}$ permutando i due elementi. La base è $B = A \times A$, mentre l'azione di C_2 sul generico elemento (a_1, a_2) è la seguente:

$$id(a_1, a_2) = (a_1, a_2); \quad \sigma(a_1, a_2) = (a_2, a_1).$$

Vediamo come si moltiplicano due elementi:

$$((a_1, a_2),\ \sigma) \cdot ((a_1', a_2'),\ id) = ((a_1, a_2)\sigma(a_1', a_2'),\ \sigma\ id) = ((a_1 a_2', a_2 a_1'),\ \sigma)$$
$$((a_1, a_2),\ id) \cdot ((a_1', a_2'),\ id) = ((a_1, a_2)id(a_1', a_2'),\ id\ id) = ((a_1 a_1', a_2 a_2'),\ id).$$

Infine osserviamo che se A è un gruppo finito e $|A| = n$, allora $|A \wr C_2| = 2n^2$.

A questo punto siamo pronti per dimostrare che i gruppi abeliani sono integrabili.

Teorema 2.12. *Sia A un gruppo abeliano. Allora $A \wr C_2$ è un integrale per A.*

Dimostrazione. Poniamo $W \coloneqq A \wr C_2$ e mostriamo che $W' \cong A$.
Siano $x, y \in W$. Andiamo a vedere quando questi due elementi commutano, e in caso contrario calcoliamo il loro commutatore $[x, y] = x^{-1}y^{-1}xy$. Otteniamo poi W', che è generato per definizione dai commutatori.
Siano $a_1, a_2, b_1, b_2 \in A$ tali che $(a_1, a_2) \neq (e_A, e_A) \neq (b_1, b_2)$. Per l'Osservazione 2.9 si ha che:

$$((a_1, a_2),\ id)^{-1} = (id(a_1^{-1}, a_2^{-1}),\ id) = ((a_1^{-1}, a_2^{-1}),\ id);$$
$$((a_1, a_2),\ \sigma)^{-1} = (\sigma(a_1^{-1}, a_2^{-1}),\ \sigma) = ((a_2^{-1}, a_1^{-1}),\ \sigma).$$

Analizziamo i quattro possibili casi.

Caso 1 Siano $x = ((a_1, a_2),\ id)$ e $y = ((b_1, b_2),\ id)$. Se li moltiplichiamo:

$$xy = ((a_1, a_2),\ id)((b_1, b_2),\ id) = ((a_1 b_1, a_2 b_2),\ id) =$$
$$= ((b_1 a_1, b_2 a_2),\ id) = ((b_1, b_2),\ id)((a_1, a_2)\ id) = yx$$

Dunque in questo caso x e y commutano, e il loro commutatore è banale. Si noti che nella serie di uguaglianze la commutatività di A è essenziale.

Caso 2 Siano $x = ((a_1, a_2),\ id)$ e $y = ((b_1, b_2),\ \sigma)$. Il loro commutatore è:

$$\begin{aligned}[xy] &= ((a_1^{-1}, a_2^{-1}),\ id)((b_2^{-1}, b_1^{-1}),\ \sigma)((a_1, a_2),\ id)((b_1, b_2),\ \sigma) = \\ &= ((a_1^{-1}b_2^{-1}, a_2^{-1}b_1^{-1}),\ \sigma)((a_1b_1, a_2b_2),\ \sigma) = \\ &= ((a_1^{-1}b_2^{-1}a_2b_2, a_2^{-1}b_1^{-1}a_1b_1),\ id) = ((a_1^{-1}a_2, a_2^{-1}a_1),\ id)\end{aligned}$$

Per le ipotesi su a_1 e a_2 il commutatore non è banale: x e y non commutano.

Caso 3 Siano $x = ((a_1, a_2),\ \sigma)$ e $y = ((b_1, b_2),\ id)$. Il loro commutatore è:

$$\begin{aligned}[xy] &= ((a_2^{-1}, a_1^{-1}),\ \sigma)((b_1^{-1}, b_2^{-1},\ id)((a_1, a_2),\ \sigma)((b_1, b_2),\ id) = \\ &= ((a_2^{-1}b_2^{-1}, a_1^{-1}b_1^{-1}),\ \sigma)((a_1b_2, a_2b_1),\ \sigma) = \\ &= ((a_2^{-1}b_2^{-1}a_2b_1, a_1^{-1}b_1^{-1}a_1b_2),\ id) = ((b_2^{-1}b_1, b_1^{-1}b_2),\ id)\end{aligned}$$

Anche in questo caso x e y non commutano.

Caso 4 Infine siano $x = ((a_1, a_2),\ \sigma)$ e $y = ((b_1, b_2),\ \sigma)$. Il commutatore è:

$$\begin{aligned}[xy] &= ((a_2^{-1}, a_1^{-1}),\ \sigma)((b_2^{-1}, b_1^{-1},\ \sigma)((a_1, a_2),\ \sigma)((b_1, b_2),\ \sigma) = \\ &= ((a_2^{-1}b_1^{-1}, a_1^{-1}b_2^{-1}),\ id)((a_1b_2, a_2b_1),\ id) = \\ &= ((a_2^{-1}b_1^{-1}a_1b_2, a_1^{-1}b_2^{-1}a_2b_1),\ id)\end{aligned}$$

Dunque l'unico caso in cui x e y commutano è il primo. Facendo variare x e y dentro W e riscrivendo in modo più comodo i commutatori trovati nei casi sopra, possiamo scrivere l'insieme dei commutatori S:

$$S = \{[x, y] | x, y \in W\} = \{((a, a^{-1}),\ id) | a \in A\} \cong \{(a, a^{-1}) | a \in A\} \subseteq A \times A.$$

Chiaramente $S \subseteq W'$. Mostriamo che in questo caso il prodotto di due commutatori è ancora un commutatore. Infatti, dati $(a, a^{-1}), (b, b^{-1}) \in S$:

$$(a, a^{-1})(b, b^{-1}) = (ab, a^{-1}b^{-1}) = (ab, b^{-1}a^{-1}) = (ab, (ab)^{-1}) \in S.$$

Dunque $S = W'$. Ci resta da mostrare che $W' \cong A$. Consideriamo:

$$\psi : A \longrightarrow S$$
$$a \longmapsto (a, a^{-1})$$

ψ è ben posta, suriettiva e iniettiva; è un omomorfismo di gruppi:

$$\psi(ab) = (ab, b^{-1}a^{-1}) = (ab, a^{-1}b^{-1)} = (a, a^{-1})(b, b^{-1}) = \psi(a)\psi(b).$$

ψ è quindi un isomorfismo di gruppi e vale $(A \wr C_2)' \cong A$. A è quindi integrabile. □

Questo risultato ci assicura che $\forall\ n \in \mathbb{N}$ esiste un gruppo integrabile di ordine n.

2.4 Gruppi semplici

I gruppi semplici finiti costituiscono un'altra classe di gruppi integrabili.

Definizione 2.13. Un gruppo G è semplice se gli unici sottogruppi normali sono $\{e\}$ e G stesso. In altre parole un gruppo semplice non ha sottogruppi normali non banali.

Esempio 6. Se p è un numero primo, $\mathbb{Z}_p$ è un gruppo semplice. Infatti gli unici divisori di p sono p e 1, dunque per il Teorema di Lagrange gli unici sottogruppi sono quelli banali, e sono normali perché è un gruppo abeliano.

Lemma 2.14. *Un gruppo semplice non abeliano è perfetto.*

Dimostrazione. Sia G un gruppo semplice, cioè i suoi sottogruppi normali sono $\{e\}$ e G. Se $G' = \{e\}$ avremmo che G è abeliano, contro le ipotesi. Perciò necessariamente $G' = G$. □

Quindi i gruppi semplici non abeliani sono integrabili.

Esempio 7. Un esempio di gruppo semplice non abeliano è $\mathcal{A}_5$. In effetti è stato dimostrato che è il più piccolo gruppo semplice non abeliano.

Proposizione 2.15. *I gruppi semplici finiti sono integrabili.*

Dimostrazione. Sia $n \in \mathbb{N},\ n > 1$. Consideriamo un gruppo semplice S di ordine n.

- Se n è un numero primo allora $S \cong C_n$, che è abeliano e per il Teorema 2.12 è integrabile.
- Se n non è primo, S non è abeliano. Infatti in un gruppo abeliano tutti i sottogruppi sono normali. Per il Teorema di Cauchy, per un qualsiasi divisore primo p di n esiste un sottogruppo di ordine p di S, che non è normale poiché S è semplice. Dunque S non è abeliano e per il Lemma 2.14 è perfetto. Concludiamo che anche in questo caso S è integrabile.

□

Esempio 8. Sia p un numero primo. Consideriamo il gruppo semplice C_p. Siamo in grado di costruire due integrali differenti. Essendo abeliano abbiamo che $C_p \wr C_2$ è un integrale. Inoltre sappiamo che il derivato del gruppo diedrale di ordine $2p$ è isomorfo a $C_p : D'_p \cong C_p$. Dunque anche D_p è un integrale di C_p.

2.5 Integrale e prodotto di gruppi

Se riusciamo a scrivere un gruppo G come prodotto diretto $G_1 \times G_2$ abbiamo una condizione sufficiente per decidere l'integrabilità. In particolare dimostreremo che il prodotto di due gruppi integrabili è integrabile. Inoltre avendo come ipotesi l'integrabilità di G abbiamo anche delle condizioni per decidere l'integrabilità dei singoli fattori.
Per dimostrare questi risultati occorrono alcune proprietà del prodotto diretto. Introduciamo una notazione che ci sarà utile. Se $G = G_1 \times G_2$, siano $\bar{G_1}, \bar{G_2}$ i seguenti sottogruppi:

$$\bar{G_1} = G_1 \times \{e_2\} \cong G_1$$
$$\bar{G_2} = \{e_1\} \times G_2 \cong G_2$$

Lemma 2.16. *Siano G_1, G_2 due gruppi. Allora il quoziente di $G_1 \times G_2$ rispetto al sottogruppo $\bar{G}_i$ isomorfo a un fattore è isomorfo all'altro fattore.*

Dimostrazione. Vediamo solo un caso, l'altro si mostra in modo analogo. Sia $\bar{G}_1 = G_1 \times \{e_2\} \cong G_1$. Mostriamo che $G_1 \times G_2/\bar{G}_1 \cong G_2$. Consideriamo la proiezione al secondo fattore:

$$p_2 : G_1 \times G_2 \longrightarrow G_2$$
$$(g_1, g_2) \longmapsto g_2$$

Si ha che $Ker(p_2) = G_1 \times \{e_2\} \cong G_1$. Per il Teorema fondamentale di omomorfismo tra gruppi vale che:

$$G_1 \times G_2/Ker\ (p_2) \cong G_2.$$

□

Se G_1 e G_2 sono gruppi finiti e le loro cardinalità sono coprime, il gruppo degli automorfismi è isomorfo al prodotto dei gruppi degli automorfismi. Il lemma successivo potrebbe dimostrarsi come corollario di questo fatto. Mostriamo invece direttamente che sotto questa ipotesi $\bar{G}_1$ e $\bar{G}_2$ sono sottogruppi caratteristici di $G_1 \times G_2$.

Lemma 2.17. *Siano G_1, G_2 due gruppi finiti tali che $MCD(|G_1|, |G_2|) = 1$. Allora $\bar{G}_1$ e $\bar{G}_2$ sono sottogruppi caratteristici di $G_1 \times G_2$.*

Dimostrazione. Mostriamolo per $\bar{G}_1 = G_1 \times \{e_2\}$. La dimostrazione per $\bar{G}_2$ è del tutto analoga. Sia $\phi \in Aut(G_1 \times G_2)$ e sia $(g_1, e_2) \in \bar{G}_1$. Sia $(g_1', g_2') = \phi((g_1, e_2))$. Poiché ϕ è un automorfismo preserva gli ordini degli elementi:

$$o((g_1', g_2')) = o((g_1, e_2)) = o(g_1).$$

Inoltre vale che :

$$o((g_1', g_2')) = mcm(o(g_1'), o(g_2')) = \frac{o(g_1')o(g_2')}{MCD(o(g_1'), o(g_2'))} = o(g_1')o(g_2').$$

L'ultima uguaglianza deriva dal Teorema di Lagrange: l'ordine di ogni elemento divide la cardinalità del gruppo, ed essendo $|G_1|, |G_2|$ coprime per ipotesi, saranno coprimi anche tutti i loro rispettivi divisori. Questo implica anche che $o(g_2') \mid o(g_1)$ se e solo se $o(g_2') = 1$. Mettiamo insieme le due uguaglianze e questa ultima osservazione:

$$o(g_1) = o(g_1')o(g_2') \implies o(g_2') \mid o(g_1) \implies o(g_2') = 1 \implies g_2' = e_2.$$

Dunque $\phi(\bar{G_1}) \subseteq \bar{G_1}$. Inoltre essendo ϕ in particolare iniettiva vale l'uguaglianza $\phi(\bar{G_1}) = \bar{G_1}$, cioè $\bar{G_1}$ è un sottogruppo caratteristico di $G_1 \times G_2$. □

Infine vediamo come si determina il centro del prodotto.

Lemma 2.18. *Siano G_1, G_2 due gruppi. Il centro del prodotto è il prodotto dei centri, cioè $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.*

Dimostrazione. Basta osservare che:

$$\begin{aligned}(x,y) \in Z(G_1 \times G_2) &\iff (x,y)(g_1,g_2) = (g_1,g_2)(x,y) \ \forall\ (g_1,g_2) \in G_1 \times G_2 \\ &\iff (xg_1, yg_2) = (g_1x, g_2y) \quad \forall\ (g_1,g_2) \in G_1 \times G_2 \\ &\iff (x \in Z(G_1) \wedge y \in Z(G_2)) \iff (x,y) \in Z(G_1) \times Z(G_2).\end{aligned}$$

Dunque vale la tesi. □

A questo punto possiamo dimostrare il teorema seguente.

Teorema 2.19. *Siano G_1, G_2 due gruppi e $G = G_1 \times G_2$ il prodotto diretto. Allora valgono:*

(a). Se G_1 e G_2 sono integrabili allora G è integrabile;

(b). Se G è integrabile e finito e $MCD(|G_1|, |G_2|) = 1$ allora G_1 e G_2 sono integrabili;

(c). Se G_1 è senza centro e G_2 è abeliano allora G è integrabile se e solo se G_1 è integrabile.

Dimostrazione. (a) Siano H_1 e H_2 due gruppi tali che $H_1' = G_1$ e $H_2' = G_2$. Sia $H \coloneqq H_1 \times H_2$. Per la Proposizione 1.13 vale:

$$H' = (H_1 \times H_2)' = H_1' \times H_2' = G_1 \times G_2 = G.$$

Dunque G è integrabile.

(b) Sia H un integrale di $G_1 \times G_2$, cioè $H' = G_1 \times G_2$. Poiché $MCD(|G_1|, |G_2|) = 1$, allora $\bar{G_1}$ è un sottogruppo caratteristico di $G_1 \times G_2$. Ciò implica che $\bar{G_1}$ è un sottogruppo caratteristico di H e in particolare è normale in H. Inoltre $\bar{G_1}$ è contenuto in H'. Allora, indicando con π la proiezione al quoziente:

$$(H/\bar{G_1})' = \pi(H)' = \pi(H') = H'/\bar{G_1} = (G_1 \times G_2)/\bar{G_1} \cong G_2.$$

Segue che G_2 è integrabile e analogamente anche G_1 è integrabile.

(c) Sia $G = G_1 \times G_2$ integrabile e sia H tale che $H' = G_1 \times G_2$. Per il Lemma 2.18 e poichè G_1 è senza centro:

$$Z(G_1 \times G_2) = Z(G_1) \times Z(G_2) = \{e_1\} \times G_2 \cong G_2.$$

Allora $\bar{G_2}$ è un sottogruppo caratteristico di G e dunque è normale in H. Derivando il quoziente e utilizzando il Lemma 2.16:

$$(H/\bar{G_2})' = H'/\bar{G_2} = (G_1 \times G_2)/\bar{G_2} \cong G_1.$$

Dunque G_1 è integrabile.
D'altra parte sia G_1 integrabile. G_2 è abeliano per ipotesi e per il Teorema 2.12 è integrabile. Allora per il punto (a) si ha che $G_1 \times G_2$ è prodotto di gruppi integrabili e quindi è integrabile.

□

Osservazione 2.20. L'ipotesi su G_1 di essere senza centro che si è usata nel punto (c) è essenziale. Per esempio consideriamo $C_2 \times D_4$, che ha un integrale di ordine 128. D_4 ha centro non banale e come vedremo non è integrabile. Questo esempio ci dice anche che in generale il punto (a) non si può invertire: un gruppo integrabile può avere nella sua fattorizzazione diretta gruppi non integrabili. Rimane una questione aperta l'esistenza di un gruppo $G = G_1 \times G_2$ integrabile in cui entrambi i fattori sono non integrabili.

Esempio 9. Il gruppo di Klein $K_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ è integrabile. Vediamo quali integrali di K_4 possiamo costruire grazie ai risultati di questo capitolo.
Innanzitutto, essendo abeliano un suo integrale è $K_4 \wr C_2$.
Adesso sfruttiamo il fatto che è isomorfo al prodotto di $C_2 \times C_2$. Come abbiamo visto nella Capitolo 1, $D_4' \cong C_2$. Possiamo allora considerare $D_4 \times D_4$ come integrale di K_4.

Capitolo 3

Gruppi non integrabili

Non esiste un test semplice per decidere l'integrabilità di un gruppo. In questo capitolo vedremo un criterio che, sotto particolari ipotesi, ci permette di stabilire se un gruppo non è integrabile. Inoltre vedremo una condizione necessaria e sufficiente per l'integrabilità dei gruppi completi.

3.1 Criterio di non integrabilità

Vediamo un criterio che ci permette di concludere che i gruppi diedrali non sono integrabili.

Lemma 3.1. *Se C è un gruppo ciclico allora $Aut(C)$ è abeliano.*

Dimostrazione. Sia $C = \langle c \rangle$. Sia $g = c^k$ un generico elemento di C, $\alpha, \beta \in Aut(C)$. Allora:

$$\alpha \circ \beta(g) = \alpha\beta(c^k) = \alpha(\beta(c))^k = (\alpha \circ \beta(c))^k.$$

Quindi ci basta mostrare che due automorfismi commutano sul generatore. Siano $\alpha(c) = c^l,\ \beta(c) = c^m$:

$$\alpha \circ \beta(c) = \alpha(c^m) = (\alpha(c))^m = (c^l)^m = c^{m \cdot l} = (c^m)^l = (\beta(c))^l = \beta(c^l) = \\ = \beta(\alpha(c)) = \beta \circ \alpha(c).$$

□

Proposizione 3.2. *Sia G un gruppo con un sottogruppo ciclico caratteristico C non contenuto in $Z(G)$. Allora G non ha integrale.*

Dimostrazione. Per assurdo sia H un integrale di G, cioè $H' = G$. Si ha la catena di sottogrupppi $C \leq G \leq H$, dove C è caratteristico in G, G è caratteristico in H e quindi C è caratteristico in H. In particolare C è normale in H e da questo deriva che H, agendo per coniugio, induce un gruppo di automorfismi di C:

$$\begin{aligned} \varphi_h : C &\longrightarrow C \\ c &\longmapsto h^{-1}ch \end{aligned}$$

Il gruppo degli automorfismi di un gruppo ciclico è abeliano. Allora $G = H'$ agisce banalmente su C. Infatti sia $g \in G$, e $h, k \in H$ tali che $g = h^{-1}k^{-1}hk$. Allora si ha:

$$\varphi_g = \varphi_{h^{-1}}\varphi_{k^{-1}}\varphi_h\varphi_k = \varphi_h^{-1}\varphi_k^{-1}\varphi_h\varphi_k = id_C.$$

L'ultima uguaglianza deriva dalla commutatività delle φ_i considerate come automorfismi di C. Segue che per ogni $c \in C$ si ha che:

$$g^{-1}cg = c \quad \forall\ g \in G \iff cg = gc \quad \forall\ g \in G \iff c \in Z(G).$$

Dunque $C \leq Z(G)$ che contraddice le ipotesi.

□

Corollario 3.3. *I gruppi diedrali non sono integrabili.*

Dimostrazione. Sia D_n un gruppo diedrale con $n > 2$. Sia $R = \langle r \rangle$ il sottogruppo ciclico di ordine n generato dalla rotazione r. Sia $\phi \in Aut(D_n)$. $\phi(r)$ ha ordine n e appartiene a R perché tutti gli elementi fuori da R, cioè le riflessioni, hanno ordine 2. Dunque R è caratteristico e per quanto visto nella Proposizione 1.15 è non centrale. Allora D_n non è integrabile. □

3.2 Gruppi di ordine pq

In questa sezione analizziamo i gruppi di ordine pq, dove p, q sono primi distinti. Distinguiamo due casi, in base alla divisibilità di $p-1$ rispetto a q. Il criterio di non integrabilità può essere applicato quando $q \mid p-1$. Sotto queste ipotesi il gruppo non abeliano di ordine pq non è integrabile.

Innanzitutto mostriamo che esiste un tale gruppo non abeliano.

Lemma 3.4. *Siano p, q numeri primi tali che $p > q$ e $q \mid p-1$. Allora esiste un gruppo non abeliano di ordine pq.*

Dimostrazione. Sia $\varphi : \mathbb{Z}_q \longrightarrow Aut(\mathbb{Z}_p)$. Se φ è l'omomorfismo banale allora $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q = \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$, che è abeliano. Se invece φ è non banale allora $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ non è abeliano.
Mostriamo che effetivamente esiste un tale omomorfismo non banale. Si ha che $Aut(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}\ \forall\ p$ primo. Per ogni $n \mid p-1$ c'è un unico sottogruppo ciclico $H \leq Aut(\mathbb{Z}_p)$ di ordine n. Questo deriva dal fatto che $Aut(\mathbb{Z}_p)$ è ciclico. Sia $n = q$, che divide $p-1$ per ipotesi.
Sia $\varphi : \mathbb{Z}_q \longrightarrow Aut(\mathbb{Z}_p)$ un omomorfismo tale che $Im(\varphi) = H$. Dunque φ è non banale e $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ è non abeliano. □

Sotto queste ipotesi si può dimostrare un fatto più forte. Se p, q sono numeri primi tali che $p > q$ e $q \mid p-1$, allora, a meno di isomorfismo, esistono solo due gruppi di ordine pq :

- il gruppo abeliano $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$
- il gruppo non abeliano $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$, dove $\varphi : \mathbb{Z}_q \longrightarrow Aut(\mathbb{Z}_p)$ è un qualsiaisi omomorfismo non banale.

Ricordiamo la definizione di $p-$sottogruppo di Sylow.

Definizione 3.5. Sia p un numero primo e sia G un gruppo tale che $p \mid |G|$. P è un $p-$ sottogruppo di Sylow di G se la cardinalità di P è uguale alla potenza massima di p che divide $|G|$.

Proposizione 3.6. *Siano p, q numeri primi tali che $p > q$ e $q \mid p-1$. Allora il gruppo non abeliano di ordine pq è senza centro e non integrabile.*

Dimostrazione. Sia $\varphi : \mathbb{Z}_q \longrightarrow Aut(\mathbb{Z}_p)$, φ non banale. Allora $\varphi(\mathbb{Z}_q) \cong C_q$ e $G \coloneqq \mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ è non abeliano. Mostriamo che è senza centro. Siano $(z_1,\ z_2) \in Z(G)$ e $(g_1,\ g_2) \neq (e_1,\ e_2) \in G$. Vale che:

$$(z_1,\ z_2)(g_1,\ g_2) = (g_1,\ g_2)(z_1,\ z_2) \iff (z_1\varphi(z_2)g_1,\ z_2g_2) = (g_1\varphi(g_2)z_1,\ g_2z_2).$$

$z_2g_2 = g_2z_2$ è sempre vero perché $\mathbb{Z}_q$ è abeliano.
Se $g_1 = e \ \wedge \ g_2 \neq e$ la condizione sulla prima coordinata impone:

$$z_1e = e\varphi(g_2)z_1 \quad \forall\ g_2 \in \mathbb{Z}_q,\ g_2 \neq e \iff z_1 = \varphi(g_2)(z_1) \quad \forall\ g_2 \in \mathbb{Z}_q,\ g_2 \neq e$$
$$\iff z_1 = e.$$

L'ultima implicazione deriva dal fatto che l'azione di $\mathbb{Z}_q$ su $\mathbb{Z}_p$ è libera: poiché φ è non banale nessun elemento di $\mathbb{Z}_p$ viene fissato. Se $g_1 \neq e$, usando la condizione appena trovata, si ha:

$$\varphi(z_2)g_1 = g_1 \quad \forall\ g_1 \in \mathbb{Z}_p,\ g_1 \neq e \iff \varphi(z_2) = id_{\mathbb{Z}_p} \iff z_2 = e$$

per iniettività di φ. Dunque $Z(G)$ è banale.
Mostriamo che G ha un unico $p-$sottogruppo di Sylow. Sia s_p il numero di $p-$sottogruppi di Sylow di G. Dai Teoremi di Sylow si ha che:

$$s_p \mid q \quad \wedge \quad (s_p \equiv 1 \pmod p \iff s_p = 1 + kp, \quad k \in \mathbb{N}).$$

Poiché q è primo, la prima condizione implica $s_p = 1 \ \vee \ s_p = q$. Ma $p > q$, quindi la seconda condizione implica $s_p = 1$. Chiamiamo P questo sottogruppo, che ha ordine p. P è ciclico perché ha ordine primo. Poiché è l'unico sottogruppo di ordine p, per ogni automorfismo σ di G si ha $\sigma(P) = P$. Dunque P è caratteristico in G.
Abbiamo trovato un sottogruppo ciclico caratteristico di G non centrale. Siamo nelle ipotesi della Proposizione 3.2 e possiamo concludere che G non è integrabile. □

Se invece $q \nmid p-1$, il gruppo di ordine pq è isomorfo a C_{pq}.

Proposizione 3.7. *Siano p, q numeri primi tali che $p > q$ e $q \nmid p-1$. Se G è un gruppo di ordine pq, allora $G \cong C_{pq}$.*

Dimostrazione. Siano p, q due primi tali che $p > q$, $q \nmid p-1$, e sia G un gruppo di ordine pq. Per il Teorema di caratterizzazione dei gruppi ciclici ci basta mostrare che G ha un unico sottogruppo di ordine p e un unico sottogruppo di ordine q. Infatti p e q, essendo primi distinti, sono gli unici divisori di pq.
Usiamo i Teoremi di Sylow. Siano s_p e s_q il numero, rispettivamente, di $p-$sottogruppi di Sylow e di $q-$sottogruppi di Sylow di G. Questi sono sottogruppi di ordine p e q. Allora si ha che:

$$s_p \mid q \quad \wedge \quad (s_p \equiv 1 \pmod{p} \iff s_p = 1 + kp, \quad k \in \mathbb{N}).$$

Come abbiamo già visto, poiché $p > q$, queste due condizioni implicano $s_p = 1$. Ragioniamo analogamente per s_q. Per s_q valgono le condizioni:

$$s_q \mid p \quad \wedge \quad s_q \equiv 1 \pmod{q}.$$

La prima condizione implica $s_q = 1 \ \vee \ s_q = p$. Se fosse $s_q = p$, allora la seconda condizione implicherebbe $p \equiv 1 \pmod{q} \iff q \mid p-1$ che è contro le nostre ipotesi. Necessariamente anche $s_q = 1$.
Dunque G è un gruppo ciclico di ordine pq. □

Corollario 3.8. *Siano p, q numeri primi tali che $p > q$ e $q \nmid p-1$. Se G è un gruppo di ordine pq, allora G è integrabile.*

3.3 Gruppi completi

I gruppi completi sono una classe speciale di gruppi senza centro. Per questi gruppi abbiamo una condizione necessaria e sufficiente per l'integrabilità.

Definizione 3.9. Un gruppo è completo se il suo centro è banale e ogni automorfismo è interno, cioè $Aut(G) = Inn(G)$.

Vediamo una proprietà utile dei gruppi completi.

Proposizione 3.10. *Sia G un gruppo completo e sia H un gruppo tale che $G \trianglelefteq H$. Allora $H = G \times C_H(G)$.*

Dimostrazione. Ricordiamo che $C_H(G) = \{h \in H \mid gh = hg \quad \forall g \in G\}$ è il centralizzante del sottogruppo G in H.
Sia $h \in H$. $\varphi_h(g) = h^{-1}gh$ è un automorfismo di G, poiché la normalità di G implica $\varphi_h(G) = G$. Poiché G è completo $\varphi_h \in Inn(G)$, cioè esiste $g_1 \in G$ tale che:

$$h^{-1}gh = g_1^{-1}gg_1 \quad \forall\, g \in G \iff (g_1h^{-1})g = g(g_1h^{-1}) \quad \forall\, g \in G.$$

Allora $g_1h^{-1} \in C_H(G)$. Questo implica che $h \in GC_H(G)$, da cui segue che $H = GC_H(G)$.
Inoltre $C_H(G) \cap G = Z(G) = \{e\}$ perché G è senza centro. Infine si ha che $C_H(G) \trianglelefteq H$. Infatti sia $x \in C_H(G),\ h \in H$. Mostriamo che $h^{-1}xh \in C_H(G)$.

$$\begin{aligned} h^{-1}xh \in C_H(G) &\iff h^{-1}xhg = gh^{-1}xh \quad \forall\, g \in G \\ &\iff xhgh^{-1} = hgh^{-1}x \quad \forall\, g \in G. \end{aligned}$$

L'ultima uguaglianza è sempre vera perché $hgh^{-1} \in G$ per normalità e $x \in C_H(G)$.
Allora per la caratterizzazione del prodotto diretto vale $H \cong G \times C_H(G)$.

□

Proposizione 3.11. *Sia G un gruppo completo. Allora G è integrabile se e solo se è perfetto.*

Dimostrazione. Sia G un gruppo completo e integrabile. Allora esiste un gruppo H tale che $H' = G$. In particolare $G \trianglelefteq H$. Posto $T = C_H(G)$, per la proposizione precedente vale $H \cong G \times T$, con $T \trianglelefteq H$ e $G \cap T = \{e\}$. Si ha che $T \cong GT/G \cong H/H'$ è abeliano. Ma allora:

$$G = H' \cong (G \times T)' = G' \times T' = G' \times e_T \cong G'.$$

Cioè G è un gruppo perfetto.
L'altra implicazione è banalmente verificata poiché ogni gruppo perfetto è integrabile. □

Diamo per buono questo risultato, senza dimostrarlo. Se $n \geq 3,\ n \neq 6$, allora il gruppo degli automorfismi di $\mathcal{S}_n$ è costituito solo da automorfismi interni, cioè $Aut(\mathcal{S}_n) = Inn(\mathcal{S}_n)$.

Lemma 3.12. *Sia $n \geq 3$. Allora $\mathcal{S}_n$ è senza centro.*

Dimostrazione. Sia $n \geq 3$ e sia $\sigma \in Z(\mathcal{S}_n),\ \sigma \neq id$. Allora esistono $a, b \in \{1, ..., n\},\ a \neq b$ tali che $\sigma(a) = b$. Sia $c \in \{1, ..., n\},\ c \neq a,\ c \neq b$. Allora $(bc)\sigma \neq \sigma(bc)$. Infatti $(bc)\sigma$ porta a in b, mentre $\sigma(bc)$ porta a in c. Perciò $\sigma = id$ e $Z(\mathcal{S}_n)$ è banale. □

Osservazione 3.13. Quindi nel caso in cui $n \geq 3,\ n \neq 6$, $\mathcal{S}_n$ è completo. Usiamo la Proposizione 3.11 per concludere che non è integrabile.

Corollario 3.14. *Sia $n \geq 3,\ n \neq 6$. Allora il gruppo simmetrico $\mathcal{S}_n$ non è integrabile.*

Dimostrazione. Sia $n \geq 3,\ n \neq 6$. Come osservato, sotto queste ipotesi $\mathcal{S}_n$ è completo. Inoltre il suo derivato è $\mathcal{A}_n \neq \mathcal{S}_n$, cioè non è un gruppo perfetto. Allora, per la Proposizione 3.11 $\mathcal{S}_n$ non è integrabile.

□

Osservazione 3.15. In realtà è stato dimostrato in [4] che anche $\mathcal{S}_6$ non è integrabile.

Bibliografia

[1] G.M. Piacentini Cattaneo. *Algebra, un approccio algoritmico*. Decibel editrice, Padova, 1996.

[2] A. Machì. *Gruppi. Una introduzione a idee e metodi della Teoria dei Gruppi*. Springer-Verlag Italia, Milano, 2007.

[3] M. Artin. *Algebra*. Bollati Boringhieri, 1997.

[4] J. Araùjo, P.J. Cameron, C. Casolo, F. Mattucci. *Integrals of groups*. Israel Journal of Mathematics, 2019.

[5] L.C. Kappe, R.F. Morse. *On commutators in groups*. Journal of Group Theory, January 2005.