Alma Mater Studiorum · Università di Bologna

SCUOLA DI SCIENZE

Corso di Laurea in Matematica

GRUPPI RISOLUBILI

Tesi di Laurea in Algebra

Relatore:
Chiar.mo Prof.
LIBERO VERARDI

Presentata da:
MICHELE PAOLIZZI

III Sessione
Anno Accademico 2013/2014

"Crede Lei
che io pensi al suo stupido violino,
quando lo Spirito mi parla?"

(Ludwig van Beethoven,
ad un violinista che si lamentava
di alcuni passaggi "insuonabili"
da lui scritti)

Ai miei amici,
che mi aiutano a non pensare sempre
al mio "stupido violino".

Indice

Introduzione

Questa tesi si prefigge l'obiettivo di presentare i *gruppi risolubili*, argomento che esula da quelli usualmente trattati nei corsi fondamentali, ma che diventa fondamentale in altri argomenti quali la teoria delle equazioni.

Perché si chiamano "risolubili"?

Il nome di tale classe di gruppi deriva infatti dalla loro correlazione con la risolubilità delle equazioni generali di n-esimo grado. Se f è un polinomio di grado n a coefficienti complessi, si dice che l'equazione $f(x) = 0$ è *risolubile per radicali* se le radici di f si ottengono attraverso un algoritmo che coinvolge *solo* i coefficienti del polinomio, le operazioni aritmetiche e le estrazioni di radici.
Per i gradi fino a 4 esistono formule generali; la più nota è quella per le equazioni di secondo grado $ax^2 + bx + c = 0$, insegnata fin dalle scuole secondarie:

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Le formule per $n = 3$ e $n = 4$ sono le cosiddette *formule di Cardano*, che fu il primo a divulgarle, ma furono trovate dai bolognesi Dal Ferro e Ferrari, e dal bresciano Tartaglia.
Per i gradi superiori a 4, come afferma il *teorema di Ruffini-Abel*, non esiste una formula risolutiva generale; tuttavia potrebbero esistere formule particolari per ogni equazione. Ma quali di queste equazioni hanno una formula risolutiva?
Qui entra in gioco la *teoria di Galois*; il gruppo di Galois è definito tramite una estensione di campi $\mathbb{F} \subset \mathbb{L}$:

$$Gal(\mathbb{L}/\mathbb{F}) = \{\psi \in Aut(\mathbb{L}) \mid \psi(c) = c \quad \forall\, c \in \mathbb{F}\}$$

In particolare se $\mathbb{L}$ è il campo di spezzamento del polinomio f a coefficienti in $\mathbb{F}$, poniamo $Gal(f) = Gal(\mathbb{L}/\mathbb{F})$.
Galois dunque affermò che *l'equazione algebrica $f(x) = 0$ di grado $n \geq 1$ è risolubile per radicali se e solo se il gruppo di Galois $Gal(f)$ di f è risolubile.*
Pertanto, se si trova che un polinomio f di grado $n \geq 5$ ha come gruppo di Galois il gruppo simmetrico S_n (che, come mostrerò nel capitolo 1, *non è risolubile*), automaticamente non esiste una formula risolutiva per radicali dell'equazione $f(x) = 0$.

Da questo spunto di prima e grande utilità, la teoria dei gruppi risolubili ha preso una propria strada, tanto da poter caratterizzare tali gruppi senza aver bisogno di passare dalla teoria di Galois.

Questa tesi infatti presenta la teoria dei gruppi risolubili senza far uso delle intuizioni di Galois: nel primo capitolo esporrò le definizioni fondamentali necessarie per lo studio dei gruppi risolubili, la chiusura del loro insieme rispetto a sottogruppi, quozienti, estensioni e prodotti, e la loro caratterizzazione attraverso la *serie derivata*.
Nel secondo capitolo sono riportati alcuni esempi di gruppi risolubili (e non risolubili) non finiti, tra i quali vi sono il gruppo delle isometrie del piano, e i *gruppi liberi*.
Infine nel terzo capitolo viene approfondito il caso dei gruppi risolubili finiti, con alcuni esempi, uno su tutti i *p-gruppi* (gruppi con ordine potenza di un primo), con un'analisi della risolubilità dei gruppi finiti con ordine minore o uguale a 100.

Nelle parti teoriche, per snellirne le notazioni, sarà utilizzata la notazione moltiplicativa:

$(G, \cdot)$ gruppo, con 1 elemento neutro.

Capitolo 1

Teoria generale sui gruppi risolubili

1.1 Serie di sottogruppi

Elemento fondamentale per la definizione dei gruppi risolubili sono le *serie di sottogruppi*. Vado dunque a definire una particolare serie di sottogruppi, detta *subnormale*:

Definizione 1.1 (**Serie subnormale**)**.** Si definisce *serie subnormale* una sequenza finita di sottogruppi di G $(G_0, G_1, \cdots, G_n)$, con $n \geq 1$, tale che:

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

I sottogruppi $G_0, \ldots, G_n$ si dicono *termini* della serie, i quozienti G_{i+1}/G_i *fattori* della serie e il numero n *lunghezza* della serie.
Inoltre, se i G_i sono tutti distinti, la serie si dice *ridotta*.

Una serie subnormale $(G_0, G_1, \ldots, G_n)$ si dice poi *abeliana* quando i suoi fattori G_{i+1}/G_i sono abeliani $\forall\, i = 0, 1, \ldots, n-1$.

1.2 Definizione di gruppi risolubili

Possiamo dunque ora definire i gruppi risolubili:

Definizione 1.2. Un gruppo G si dice *risolubile* se possiede una serie abeliana.

La lunghezza minima delle serie abeliane di G è detta *lunghezza di risolubilità* o *lunghezza derivata* di G, e la denotiamo con $dl(G)$.

Osservazione 1.1. Ogni gruppo abeliano è risolubile.

Dimostrazione. Segue dal fatto che ogni sottogruppo di un gruppo abeliano è normale. Considero dunque la serie banale $(\{1\}, G)$: abbiamo ovviamente che $\{1\} \lhd G$, e $G/\{1\} \cong G$ è abeliano. □

La serie considerata nella dimostrazione di 1.1 è anche la serie minima. Si ha dunque:

Proposizione 1.1. *Un gruppo G è abeliano se e solo se è risolubile, con $dl(G) = 1$.*

Un gruppo risolubile ha lunghezza derivata 0 se e solo se ha ordine 1; un gruppo risolubile con lunghezza derivata 2 si dice invece *metabeliano*.
Un gruppo G non banale si dice *semplice* quando i suoi unici sottogruppi normali sono $\{1\}$ e G. Banalmente si ha il seguente risultato:

Osservazione 1.2. I gruppi semplici non abeliani *non sono risolubili*.

Dimostrazione. Se G è un gruppo semplice non avendo; non avendo altri sottogruppi normali al di fuori di $\{1\}$ e se stesso, possiamo costruire soltanto la serie subnormale $\{1\} \lhd G$, nella quale $G/\{1\} \cong G$ non è abeliano. □

Esempio 1.1 (Gruppo simmetrico)**.** Andiamo a vedere la risolubilità del gruppo simmetrico S_n, con $n > 1$:

- Il gruppo S_2 è banalmente risolubile (essendo di ordine 2, è abeliano).
- S_3 è invece metabeliano: contiene difatti la serie abeliana $\{id\} \lhd A_3 \lhd S_3$, dove A_3 è il gruppo alterno di S_3, e questa serie ha lunghezza 2.
- Anche il gruppo S_4 è risolubile: la serie $(\{id\}, K, A_4, S_4)$, dove K è il *gruppo di Klein* ($K = \{id, (1\,2)(3\,4), (1\,3)(2\,4)(1\,4)(2\,3)\}$), è a fattori abeliani:
  - K è abeliano, essendo isomorfo al gruppo $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$;
  - $K \lhd A_4$: infatti in S_n due permutazioni sono coniugate se hanno la stessa successione caratteristica. K, poiché contiene tutte le permutazioni di successione caratteristica $(2, 2)$ di S_4, è dunque normale in ogni sua estensione entro S_4, quindi, in particolare, è normale in A_4 (nel quale è contenuto, poiché A_n contiene le permutazioni pari, cioè scomponibili in un numero pari di cicli disgiunti, $\forall\, n$).
    Abbiamo inoltre che, per il teorema di Lagrange, $|A_4/K| = 3$, che è primo, dunque questo fattore è ciclico e perciò abeliano;
  - Analogamente, avendo $A_4 \lhd S_4$ e $|S_4/A_4| = 2$, si ottiene che anche questo fattore è abeliano.

  Dunque la serie è subnormale; inoltre, è la serie abeliana di S_4 più breve (dato che $S_4/K \cong S_3$ non abeliano, e $A_4/\{1\} \cong A_4$ non abeliano), perciò $dl(S_4) = 3$.

Questi sono gli unici gruppi simmetrici risolubili; difatti si ha:

Proposizione 1.2. *Il gruppo simmetrico S_n non è risolubile per $n \geq 5$.*

Dimostrazione. Per $n \geq 5$, si ha che A_n è un gruppo semplice, e che è l'unico sottogruppo normale proprio non banale di S_n (cfr. [4, pp. 69-70], [5, pp. 295-296] per dettagli più specifici su tali teoremi). Perciò le uniche serie subnormali di S_n sono quella banale $(\{1\}, S_n)$ e la serie col gruppo alterno $(\{1\},A_n,S_n)$, nessuna delle quali è abeliana. □

1.3 La serie derivata

1.3.1 I commutatori e i sottogruppi commutatori

Definizione 1.3 (**Commutatore**)**.** Siano $a, b \in G$. Il *commutatore* di a e b è definito come

$$[a, b] = a^{-1}b^{-1}ab \quad \forall\, a,\, b \in G$$

Per $a_1, a_2, \ldots, a_n \in G$, $n > 2$, si definisce ricorsivamente come

$$[a_1, a_2, \ldots, a_n] = [[a_1, \ldots, a_{n-1}], a_n] \quad \forall\, a_1, \ldots, a_n \in G$$

Definizione 1.4 (**Interderivato**)**.** Siano X_1, X_2 sottogruppi di G. Definiamo il *sottogruppo commutatore* (o *interderivato*) come il sottogruppo generato dai commutatori; cioè

$$[X_1, X_2] = \langle [x_1, x_2] \mid x_1 \in X_1,\, x_2 \in X_2 \rangle$$

Più generalmente, definiamo il sottogruppo commutatore di $X_1, \ldots, X_n$, $n > 2$, come

$$[X_1, \ldots, X_n] = [[X_1, \ldots, X_{n-1}], X_n]$$

Queste nozioni ci servono per definire la cosiddetta *serie derivata*, serie strettamente collegata alle serie abeliane, e dunque ai gruppi risolubili.

1.3.2 Definizione di serie derivata

Denotiamo l'interderivato del gruppo G con se stesso come $G' = [G, G]$, detto anche *(sottogruppo) derivato* di G.
Un'importante proprietà del derivato è la seguente:

Proposizione 1.3. *G' è invariante per endomorfismi, ed è il minimo dei sottogruppi normali K di G tali che G/K è abeliano.*
In altre parole $G' \lhd G$, G/G' è abeliano, e se $\exists$ K sottogruppo normale di G tale che G/K sia abeliano, allora $K \supseteq G'$.

Dimostrazione. Sia f un endomorfismo di G e siano $x,\, y \in G$; allora $f([a, b]) = [f(a), f(b)]$, quindi $f(G') \subseteq G'$. In particolare G' è normale in G.

Allora $\forall\ x,\ y \in G$, in G/G' si ha:

$$[G'x, G'y] = (G'x)^{-1}(G'y)^{-1}G'xG'y = G'x^{-1}y^{-1}xy = G'$$

in quanto $x^{-1}y^{-1}xy$ è un elemento di G'.
Poiché G' è la classe di 1 nel gruppo quoziente G/G', si ha che G/G' è abeliano.
Sia poi K sottogruppo normale di G. in G/K, si ha che $[Kx, Ky] = K[x, y] = K$, essendo K abeliano. Allora $[x, y] \in K$, da cui si ha che $K \supseteq G'$. □

Esempio 1.2. Vediamo alcuni esempi di derivati notevoli:

- $G' = \{1\} \iff G$ è abeliano. Questo perché se $ab = ba$ per ogni elemento $a,\ b$ di G, si ha che $[a, b] = 1$.

- Per il gruppo simmetrico S_n, abbiamo che $(S_n)' = A_n$.
  Innanzitutto si verifica facilmente che $A_n \lhd S_n$; quindi per la proposizione 1.3 $(S_n)' \subseteq A_n$.
  Abbiamo poi che, per $n \neq 4$, A_n è semplice (per $n < 3$ si evince dall'esempio 1.1).
  Se invece $n = 4$, il gruppo di Klein K è normale in S_4, ma S_4/K non è abeliano (e quindi per la proposizione 1.3 $(S_4)' \nsubseteq K$). Allora $(S_4)' = A_4$.
  Quindi $(S_n)' = A_n\ \forall\ n > 2$, perché S_n non è abeliano (e quindi $(S_n)' \neq \{1\}$).

- Sia $\mathbb{K}$ un campo, e sia $GL_n(\mathbb{K})$ il gruppo delle matrici invertibili $n \times n$ a coefficienti in $\mathbb{K}$. Il derivato di $GL_n(\mathbb{K})$ è $(GL_n(\mathbb{K}))' = SL_n(\mathbb{K})$, il sottogruppo formato dalle matrici a determinante 1.
  Infatti siano $M,\ N \in GL_n(\mathbb{K})$: il loro commutatore è $[M, N] = M^{-1}N^{-1}MN$, il cui determinante, per il teorema di Binet, è:

  $$det([M, N]) = det(M^{-1}N^{-1}MN) = (det(M^{-1}))(det(N^{-1}))(detM)(detN) = 1$$

  Dunque i commutatori degli elementi di $GL_n(\mathbb{K})$ hanno tutti determinante 1, quindi appartengono tutti a $SL_n(\mathbb{K})$ per cui $SL_n(\mathbb{K}) \lhd GL_n(\mathbb{K})$.
  Infine, sempre per la proposizione 1.3, abbiamo che $(GL_n(\mathbb{K}))' \subseteq SL_n(\mathbb{K})$, con $(GL_n(\mathbb{K}))' \lhd SL_n(\mathbb{K})$. Si dimostra poi che vale l'uguaglianza.

Definizione 1.5 (**Serie derivata**)**.** Sia G gruppo; la *serie derivata* di G è la sequenza

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots$$

dove $G^{(n+1)} = (G^{(n)})' \quad \forall\ n$.

Si ha allora, per la proposizione 1.3, che i quozienti $G^{(n)}/G^{(n+1)}$ sono abeliani $\forall\ n$.

Osservazione 1.3. Si noti che, per la natura induttiva della definizione di serie derivata, si ottiene la seguente proprietà, che risulterà molto utile in seguito:

$$\forall\, n,\, m \in \mathbb{N},\; n+m=k, \qquad G^{(k)} = G^{(n+m)} = \left(G^{(n)}\right)^{(m)}$$

Si comincia dunque a intuire quanto possa essere stretta la correlazione tra i gruppi risolubili e la loro serie derivata, che analizzerò nella prossima sezione.

1.4 Caratterizzazione dei gruppi risolubili tramite le serie derivate

Teorema 1.1. *Se* $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n$ *è una serie abeliana di un gruppo risolubile* G*, allora* $G^{(i)} \subseteq G_{n-i} \quad \forall\, i = 0, \ldots, n$.
In particolare, $G^{(n)} = \{1\}$*, e se* $G^{(d)}$ *è il primo derivato per cui* $G^{(d)} = \{1\}$*,* $d = dl(G)$.

Dimostrazione. Dimostriamo questo teorema per induzione: Per $i = 0$ l'inclusione è certamente vera (perché $G^{(0)} = G = G_n$).
Supponendo la validità del teorema per i, la proviamo per $i+1$. Si ha:

$$G^{(i+1)} = (G^{(i)})' \subseteq (G_{n-i})' \subseteq G_{n-(i+1)},$$

poiché $G_{n-i}/G_{n-(i+1)}$ abeliano (conseguenza della proposizione 1.3). Allora si ha:

$$G^{(i+1)} \subseteq G_{n-(i+1)}$$

Pertanto l'inclusione è provata per ogni i.
Da ciò segue che nessuna serie abeliana può essere più corta della serie derivata; dunque, se d è la lunghezza della serie derivata, $d = dl(G)$. □

Da questo teorema deriva il fatto fondamentale che *un gruppo è risolubile se e solo se la serie derivata raggiunge il sottogruppo identità in un numero finito di passi* (cioè se la serie derivata è finita); poiché calcolare la serie derivata è spesso più semplice che cercare gli elementi della serie abeliana, questo facilita notevolmente la verifica di risolubilità di un gruppo.
Inoltre tramite il calcolo della serie derivata ottengo anche la serie minima del gruppo, dunque la sua lunghezza derivata: se infatti giungo ad avere il sottogruppo identità al passo k, avrò che $dl(G) = k$.

Esempio 1.3. Calcoliamo la serie derivata di S_3: in base a quanto detto nell'esempio 1.1, dovremmo avere $dl(S_3) = 2$:

Da quanto dimostrato nell'esempio 1.2 abbiamo automaticamente che $(S_3)' = A_3$. Volendo verificarlo direttamente: $S_3 = \{id, (1\,2), (1\,3), (2\,3), (1\,2\,3), (3\,2\,1)\}$; calcolando il suo derivato si ha:

$$(S_3)' = [S_3, S_3] = \{id, (1\,2\,3), (3\,2\,1)\} = A_3,$$

come già detto. A_3 è abeliano, quindi $(A_3)' = \{id\}$. Dunque la serie derivata di S_3 è $S_3 \supset A_3 \supset \{id\}$; abbiamo quindi dimostrato che S_3 è risolubile e metabeliano, poiché abbiamo ottenuto il sottogruppo identità al secondo passo (dunque $dl(S_3) = 2$).

1.5 Chiusura della classe dei gruppi risolubili

In questa sezione dimostro come la classe dei gruppi risolubili sia chiusa per sottogruppi, quozienti ed estensioni.
Vi sono diversi modi possibili per dimostrare queste proprietà: è possibile, per esempio, passare dal Teorema fondamentale di omomorfismo per i gruppi, oppure sfruttare la correlazione tra i risolubili e la serie derivata, in particolare la teoria dei commutatori. Visto la caratterizzazione effettuata precedentemente dei gruppi risolubili tramite le serie derivate, ho deciso di intraprendere questa seconda strada.

Proposizione 1.4 (Chiusura per sottogruppi)**.** *Se G è un gruppo risolubile e H un suo sottogruppo, allora H è risolubile.*

Dimostrazione. Sia

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(d)} = \{1\}$$

la serie derivata di G. Poiché H è sottogruppo di G, si ha che $\forall\ i \geq 0 \quad H^{(i)} \subseteq G^{(i)}$, in particolare $H^{(d)} \subseteq G^{(d)} = \{1\}$. Dunque anche H è risolubile.
Si noti inoltre che $dl(H) \leq dl(G) = d$. □

Proposizione 1.5 (Chiusura per quozienti)**.** *Se G è un gruppo risolubile, e H un suo sottogruppo tale che $H \lhd G$, allora G/H è risolubile.*

Dimostrazione. Sia sempre

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots \supseteq G^{(d)} = \{1\}$$

la serie derivata di G; analizziamo i derivati di G/H.
Siano dunque $a, b \in G$ (allora $aH, bH \in G/H$); poiché, in base alle proprietà dei sottogruppi commutatori, si ha:

$$[aH, bH] = [a, b]H \quad \forall\ aH, bH \in G/H$$

Allora $(G/H)' = G'H/H$, e per induzione $(G/H)^{(i)} = G^{(i)}H/H \quad \forall\, i \geq 0$.
In particolare, per $i = d$ si ottiene:

$$(G/H)^{(d)} = G^{(d)}H/H = H/H = \{1\}$$

Dunque G/H è risolubile.
Si noti inoltre, come nel caso della proposizione 1.4, che $dl(G/H) \leq dl(G) = d$. □

Proposizione 1.6 (Chiusura per estensioni)**.** *Sia G gruppo, E sua estensione normale (dunque $G \lhd E$); se G ed E/G sono risolubili, allora E è a sua volta risolubile.*

Dimostrazione. Per quanto osservato nella dimostrazione di 1.5, si ha: $E^{(i)}G/G = (E/G)^{(i)}$ $\forall\, i \geq 0$. Quindi, se $m = dl(E/G)$, si verifica che

$$E^{(m)}G/G = (E/G)^{(m)} = \{1\}$$

Allora $E^{(m)} \subseteq G$.
Perciò, se $n = dl(G)$, per quanto detto nell'osservazione 1.3:

$$E^{(m+n)} = \left(E^{(m)}\right)^{(n)} \subseteq G^{(n)} = \{1\}$$

Dunque E è risolubile, con $dl(E) \leq m + n$. □

Ricordiamo la definizione di *prodotto diretto* (o *prodotto cartesiano*) tra due gruppi G e H:

$$G \times H = \{(g, h) \mid g \in G,\ h \in H\}$$

Allora dai tre enunciati precedenti deriva naturalmente la seguente proposizione:

Proposizione 1.7. *Il prodotto diretto di due gruppi risolubili è risolubile.*

Ricordiamo poi la definizione di *prodotto tra sottoinsiemi* A e B di G, già implicitamente usata nelle dimostrazioni degli enunciati 1.5 e 1.6:

$$AB = \{ab \mid a \in A,\ b \in B\}$$

Se H e K sono sottogruppi di G, HK è sottogruppo se e solo se $HK = KH$. Se uno dei due sottogruppi è normale in G, l'ipotesi $HK = KH$ è verificata.

Prima di dimostrare che un prodotto di sottoinsiemi è risolubile, ricordiamo il *II Teorema di isomorfismo di gruppi*, come enunciato in [4, p. 19]:

Teorema 1.2 (II Teorema di isomorfismo di gruppi)**.** *Siano H e K sottogruppi di G, $K \lhd G$. Allora $(H \cap K) \lhd G$, e $HK/K \cong H/(H \cap K)$ tramite l'isomorfismo*

$$\begin{aligned} \varphi : HK/K &\longrightarrow H/(H \cap K) \\ Nx &\longmapsto (H \cap K)x \end{aligned}$$

Proposizione 1.8. *Siano H, K sottogruppi di un gruppo G, con $K \lhd G$; allora HK è risolubile.*

Dimostrazione. Siano H e K sottogruppi risolubili di G, con $K \lhd G$ e $H \subseteq G$. Allora, per il teorema 1.2, si ha che $HK/K \cong H/(H \cap K)$.
$H/(H \cap K)$ è risolubile perché è un quoziente di H, che è risolubile, dunque anche HK/K è risolubile. K è risolubile per ipotesi, quindi, dalla proposizione 1.6, HK è risolubile. □

La scelta di $K \lhd G$ è arbitraria: la proposizione è chiaramente ancora valida anche se $H \lhd G$ e K sottogruppo di G.

Esempio 1.4 (Controesempio)**.** Se invece né H né K sono normali, anche se HK è sottogruppo, non è detto che sia risolubile.
Consideriamo per esempio A_5: A_5 è semplice, come già accennato. Esso ha un sottogruppo $H \cong A_4$, di ordine 12, e un sottogruppo $K = \langle (1\,2\,3\,4\,5) \rangle$, di ordine 5. Dato che $MCD(|H|, |K|) = 1$, si ha che $H \cap K = \{1\}$, per cui $|HK| = 12 \cdot 5 = 60 = |A_5|$; quindi $HK = A_5$.
H è risolubile (come visto nell'esempio 1.1), K è ciclico, e quindi risolubile, ma $A_5 = HK$ non lo è.

Capitolo 2

Esempi di gruppi risolubili infiniti

In questa sezione mostro alcuni esempi di gruppi risolubili di ordine infinito (il caso finito sarà più ampiamente trattato nel capitolo 3).

Chiaramente, poiché ogni gruppo abeliano è risolubile, abbiamo che i gruppi "classici" ($(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ e gli analoghi possibili per la moltiplicazione) sono risolubili. Andiamo a vedere alcuni gruppi risolubili non abeliani di ordine infinito.
Prima degli esempi, ricordo l'*azione di un gruppo su un insieme*, che ci sarà utile per alcuni esempi in questo caso e nel caso finito.

Azione di un gruppo

Sia G gruppo, X insieme. Si dice che G agisce su X come gruppo di permutazioni se esiste un morfismo di monoidi $\rho : G \to S_X$.
Siano $g \in G$, $x \in X$. Poniamo $\rho(g)(x) = x^g$; da ciò definiamo una relazione di equivalenza su X ($x,\ y \in X$):

$$x \sim y \iff \exists\ g \in G,\ x^g = y$$

Le classi di equivalenza di questa relazione sono dette *G-orbita di x*:

$$[x]_G = \{y \in X \mid \exists g \in G, \quad x^g = y\}$$

Osservazione 2.1. Poiché sono classi di equivalenza, le G-orbite sono una partizione di X.

Poniamo infine $G_x = \{g \in G \mid x^g = x\}$; G_x è un sottogruppo di X, detto *stabilizzatore* di x in G.

Dal teorema di Lagrange sull'ordine dei gruppi deriva questo teorema:

Teorema 2.1. *Se G gruppo finito, $|G_x| \cdot |[x]_G]| = |G| \quad \forall\ x \in X$.*

Caso particolare $X = G$

Se $X = G$, possiamo considerare l'azione per coniugio di G su se stesso; in questo caso, le G-orbite sono gli insiemi $[x]_G = \{g^{-1}xg \mid g \in G\}$; l'insieme degli stabilizzatori di un elemento $x \in G$ è detto *centralizzante* $C_G(x)$, e l'intersezione dei centralizzanti è detta *centro* di G:

$$Z(G) = \{g \in G \mid g^{-1}xg = x,\ \forall\, x \in G\}$$

Osservazione 2.2. Alcune note su $Z(G)$:

- Si osserva subito che $Z(G)$ è un sottogruppo normale di G.
- Notiamo che $g^{-1}xg = x \Leftrightarrow xg = gx$, dunque il centro contiene tutti gli elementi di G che commutano, per cui $Z(G)$ è abeliano.
- Inoltre, le orbite dei suoi elementi hanno tutte ordine 1, e viceversa.

2.1 Le matrici invertibili $GL_n(\mathbb{K})$

Sia $\mathbb{K}$ campo di ordine infinito; sia poi $GL_n(\mathbb{K})$ il gruppo delle matrici invertibili $n \times n$ a elementi in $\mathbb{K}$. Abbiamo quindi che $GL_n(\mathbb{K})$ *non è risolubile.*

Supponiamo che sia risolubile: allora ogni sottogruppo di $GL_n(\mathbb{K})$ dev'essere risolubile, per la proposizione 1.4; in particolare deve essere risolubile $SL_n(\mathbb{K})$, il gruppo delle matrici a determinante 1. Se questo gruppo fosse risolubile, allora anche un suo quoziente con un suo sottogruppo normale deve essere risolubile. Poniamo quindi

$$PSL_n(\mathbb{K}) = SL_n(\mathbb{K})/Z(SL_n(\mathbb{K})),$$

dove $Z(SL_n(\mathbb{K}))$ è il centro del gruppo $SL_n(\mathbb{K})$, quindi è normale, come ricordato in precedenza.
Il teorema di Jordan-Dickson però afferma:

Teorema 2.2 (Jordan-Dickson)**.** *Se* $n \geq 2$ *e* $|\mathbb{K}| > 3$*, allora* $PSL_n(\mathbb{K})$ *è semplice.*

Poiché $PSL_n(\mathbb{K})$ è semplice e non abeliano, non è risolubile. Di conseguenza non lo è $SL_n(\mathbb{K})$, quindi neppure $GL_n(\mathbb{K})$ è risolubile.

2.2 Le matrici triangolari $T_n(\mathbb{K})$

Chiamiamo $T_n(\mathbb{K})$ il sottogruppo di $GL_n(\mathbb{K})$ formato dalle matrici triangolari superiori. Più esplicitamente, se $M \in T_n(\mathbb{K})$,

$$M = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & a_{nn} \end{pmatrix}$$

con $a_{ii} \neq 0 \quad \forall\, i = 1, \ldots, n$, $a_{ij} = 0$ se a_{ij} è sotto la diagonale principale.

Abbiamo dunque che il gruppo di $T_n(\mathbb{K})$, al contrario di rispetto all'operazione di moltiplicazione riga per colonna *è risolubile*, indipendentemente da n e dal campo.

Dimostrazione. Sia infatti $D_n(\mathbb{K})$ il gruppo delle matrici diagonali:

$$D_n(\mathbb{K}) = \{M \in T_n(\mathbb{K}) \mid a_{ij} = 0, i \neq j\}$$

Sia poi $(\mathscr{N}, +)$ gruppo additivo, con $\mathscr{N}$ formato dalle matrici che hanno gli elementi della diagonale e sotto la diagonale uguali a 0; esplicitamente, se $N = (a_{ij})_{i,j=1,\ldots,n} \in \mathscr{N}$, $a_{ij} \in \mathbb{K}$, $\quad a_{ii} = 0,\ i = 1, \ldots, n$ e $a_{ij} = 0$ se a_{ij} è sotto la diagonale principale.

$$N = \begin{pmatrix} 0 & a_{12} & \cdots & a_{1n} \\ \vdots & 0 & \ddots & \vdots \\ 0 & \cdots & \ddots & a_{(n-1)n} \\ 0 & \cdots & 0 & 0 \end{pmatrix},$$

Sia infine $U = I + \mathscr{N} = \{A = I + N, \quad N \in \mathscr{N}\}$, ($I$ è la matrice identità $n \times n$). Allora abbiamo che U è un sottogruppo di $GL_n(\mathbb{K})$.

Sia poi $T \in T_n(\mathbb{K})$ e sia $diag(T) \in D_n(\mathbb{K})$ la matrice diagonale che ha gli stessi componenti della diagonale di T. Costruiamo un morfismo suriettivo:

$$\begin{aligned} \varphi : T_n(\mathbb{K}) &\xrightarrow{su} D_n(\mathbb{K}) \\ T &\longmapsto diag(T) \end{aligned}$$

Tale morfismo è ben definito, e il suo nucleo è esattamente U. Perciò $U \lhd T_n(\mathbb{K})$, e, per il Teorema fondamentale di omomorfismo sui gruppi, $T_n(\mathbb{K})/U \cong D_n(\mathbb{K}) \cong \mathbb{K}^n$, perciò $T_n(\mathbb{K})/U$ è abeliano.

Osserviamo poi che, per $r \geq 2$, l'insieme $\mathscr{N}^{r-1}$ è formato da tutte le matrici della forma:

$$N = \begin{pmatrix} 0 & \cdots & 0 & a_{1r} & \cdots & a_{1n} \\ \vdots & & & \ddots & \ddots & \vdots \\ 0 & \cdots & & \cdots & 0 & a_{(n-r+1)n} \\ 0 & \cdots & & \cdots & & 0 \\ \vdots & & & \vdots & & \vdots \\ 0 & \cdots & & \cdots & & 0 \end{pmatrix}$$

Sia allora $U_r = I + \mathscr{N}^r$. Perciò $U_1 = U$ e $U_r \supset U_{r+1}$. In particolare, U_{r+1} è normale in U_r, e il quoziente è isomorfo al gruppo additivo $(\mathbb{K}^{n-r}, +)$, tramite la seguente funzione:

$$\begin{aligned} \psi : U_{r+1}/U_r &\xrightarrow{\cong} \mathbb{K}^{n-r} \\ I + M &\mapsto (a_{1r}, \ldots, a_{(n-r+1)n}) \end{aligned}$$

Quindi, ogni U_{r+1}/U_r è abeliano. Otteniamo perciò una serie abeliana:

$$\{I\} = U_n \lhd U_{n-1} \lhd \cdots \lhd U_2 \lhd U_1 = U \lhd T_n(\mathbb{K})$$

Quindi $T_n(\mathbb{K})$ è risolubile $\forall\, n$. □

La serie sopra considerata è la cosiddetta *serie centrale discendente* di $T_n(\mathbb{K})$; essa non è in generale la serie minima, poiché si ha:

$$U_{r+1} = [U, U_r] \supseteq [U_r, U_r] = (U_r)'$$

Però essa coincide con la serie minima se $n = 2$, e in tal caso $T_2(\mathbb{K})$ è metabeliano (avendo serie $\{I\} = U_2 \lhd U_1 = U \lhd T_2(\mathbb{K})$), e nel caso $n = 3$.

2.3 Le isometrie del piano

Ricordo la definizione generale di *isometria*: si dice isometria una funzione $f : X \to Y$ tra due spazi metrici (X, d_X) e (Y, d_Y) tale che

$$\forall\, x_1,\ x_2 \in X \quad d_X(x_1, x_2) = d_Y(f(x_1), f(x_2))$$

In altre parole, una isometria è una funzione che "conserva le distanze" tra dominio e codominio.

2.3.1 Espressione analitica di una isometria piana

Considero dunque le isometrie del piano:

$$f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$$

Introduciamo nel piano un sistema di assi ortogonali: allora una retta r ha equazione

$$r : ax + by + c = 0,\ x,\ y \in \mathbb{R}^2,\ (a, b) \neq (0, 0).$$

Possiamo supporre, eventualmente dividendo i coefficienti per $a^2 + b^2$, che $a^2 + b^2 = 1$. Analizziamo le simmetrie assiali: sia $P = (x, y)$ un punto, e sia $P' = (x', y')$ il suo simmetrico rispetto alla retta r. Dunque la retta che contiene il segmento PP' è perpendicolare a r, per cui si ha

$$b(y - y') - a(x - x') = 0$$

Il punto medio di PP' poi appartiene a r, quindi:

$$a \cdot \frac{x + x'}{2} + b \cdot \frac{y + y'}{2} + c = 0$$

Otteniamo perciò il seguente sistema lineare:

$$\begin{cases} bx' - ay' = bx - ay \\ ax' + by' = -ax - by - 2c \end{cases}$$

La matrice dei coefficienti ha determinante $-a^2 - b^2 = -1$, dunque il sistema è determinato. Eseguendo i calcoli:

$$\begin{cases} x' = (b^2 - a^2)x - 2aby - 2ac \\ y' = -2abx - (b^2 - a^2)y - 2bc \end{cases} \tag{2.1}$$

Pongo $X' = \begin{pmatrix} x' \\ y' \end{pmatrix}$, $X = \begin{pmatrix} x \\ y \end{pmatrix}$, $A = \begin{pmatrix} b^2 - a^2 & -2ab \\ -2ab & a^2 - b^2 \end{pmatrix}$, $B = \begin{pmatrix} -2ac \\ -2bc \end{pmatrix}$.
Allora le equazioni (2.1) della simmetria (che chiameremo σ) in forma matriciale diventano:

$$X' = AX + B$$

Indicando con A^t la trasposta di A, si ha:

$$A^t A = \begin{pmatrix} b^2 - a^2 & -2ab \\ -2ab & a^2 - b^2 \end{pmatrix} \begin{pmatrix} b^2 - a^2 & -2ab \\ -2ab & a^2 - b^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

Quindi $A^t = A^{-1}$, cioè A è *ortogonale*.

Consideriamo ora un'altra simmetria assiale σ_1: anch'essa si può quindi rappresentare in forma matriciale come $X' = A_1X + B_1$, con A_1 matrice ortogonale di determinante -1. Quindi la composizione delle due simmetrie $\sigma_1 \circ \sigma$ avrà la seguente equazione matriciale:

$$X' = A_1(AX + B) + B_1 = (A_1A)X + (A_1B + B_1)$$

A_1A è ancora ortogonale, ma ha determinante 1. Quindi un movimento (cioè una composizione di simmetrie) ha equazione $X' = MX + C$, con $M = AA_1$ ortogonale, $detM = 1$ e $C = (A_1B + B_1)$ vettore colonna.

Osservazione 2.3. Si noti che la matrice di σ non dipende da c, ma solo dai coefficienti della retta a e b. Da ciò possiamo desumere che *simmetrie con assi paralleli hanno la stessa matrice A.*

Se dunque σ_1 e σ hanno assi paralleli, allora $\sigma_1 \circ \sigma$ è una traslazione, e poiché $A_1 = A$ si ha $M = A^2 = I_2$.
Quindi l'equazione di una traslazione è $X' = X+C$, dove C è il corrispondente dell'origine $(0, 0)$ nella traslazione (il "punto di partenza" della traslazione).
Se poi componiamo una simmetria con un movimento, otteniamo di nuovo una equazione matriciale dello stesso tipo, ma con determinante -1.

Abbiamo dunque il seguente teorema:

Teorema 2.3. *Per ogni isometria f esistono una matrice ortogonale A e un vettore colonna B tali che f ha equazione $X' = AX + B$.*

Osservazione 2.4. Sia $\mathscr{M}$ l'insieme dei movimenti, $\mathscr{T}$ l'insieme delle traslazioni, $\mathscr{R}$ l'insieme delle rotazioni; si ha:

- $f \in \mathscr{M} \iff det(A) = 1$;
- $f \in \mathscr{T} \iff A = I_2$;
- $f \in \mathscr{R} \iff A \neq I_2$ e $det(A) = 1$.

2.3.2 Risolubilità del gruppo delle isometrie del piano

Le isometrie $f : X \to X$, con l'operazione di composizione, formano un gruppo, che denotiamo $Isom(X)$.
Considero quindi $X = \mathbb{R}^2$, e verifichiamo se $Isom(\mathbb{R}^2)$ è risolubile.

Sicuramente è un gruppo infinito, perché contiene il sottogruppo delle traslazioni $\mathscr{T}$ che è isomorfo a $(\mathbb{R}^2, +)$, il gruppo dei vettori del piano, quindi $Isom(\mathbb{R}^2)$ non è numerabile.

Inoltre $Isom(\mathbb{R}^2)$ non è abeliano: questo deriva dalla non commutatività della moltiplicazione riga per colonna delle matrici, tramite le quali abbiamo definito le isometrie.
Abbiamo il seguente risultato:

Lemma 2.1. *Il sottogruppo dei movimenti $\mathscr{M}$ ha indice 2 in $Isom(\mathbb{R}^2)$, quindi è un suo sottogruppo normale.*

Dimostrazione. Siano σ una simmetria assiale fissata, e f una isometria inversa. Allora $f \circ \sigma$ è un movimento, quindi esiste $\varphi \in \mathscr{M}$ tale che $f \circ \sigma = \varphi$. Ma da questo si ha che $f = \varphi \circ \sigma$, cioè $f \in \mathscr{M}\sigma$ laterale destro.
Allora $Isom(\mathbb{R}^2)/\mathscr{M} = \mathscr{M}\sigma$, pertanto gli unici laterali destri in $Isom(\mathbb{R}^2)$ sono $\mathscr{M}$ e $\mathscr{M}\sigma$, quindi $\mathscr{M}$ in $Isom(\mathbb{R}^2)$ ha indice 2. □

Ricordo ora la definizione di *prodotto semidiretto*:

Definizione 2.1. G è *prodotto semidiretto* di due suoi sottogruppi H e K se $K \lhd G$, G è prodotto di H e K (abbreviamo la notazione con $G = HK$), e $H \cap K = \{1\}$.

Sia O un punto del piano; sfruttando l'azione sui gruppi citata a pagina 9 denoto lo stabilizzatore di O rispetto al gruppo delle isometrie $Isom(\mathbb{R}^2)$ con $Isom(\mathbb{R}^2)_O$:

$$Isom(\mathbb{R}^2)_O = \{f \in Isom(\mathbb{R}^2) \mid f(O) = O\}$$

Proposizione 2.1. *Siano $\mathscr{T}$ il gruppo delle traslazioni, O un punto del piano, e $Isom(\mathbb{R}^2)_O$ lo stabilizzatore di O. Allora:*

a) $\mathscr{T}$ è normale in $Isom(\mathbb{R}^2)$.

b) $Isom(\mathbb{R}^2)$ è prodotto semidiretto di $\mathscr{T}$ per $Isom(\mathbb{R}^2)_O$.

c) $\mathscr{M}$ è prodotto semidiretto di $\mathscr{T}$ per $\mathscr{M} \cap Isom(\mathbb{R}^2)_O$.

Dimostrazione.

a) Poiché $Isom(\mathbb{R}^2)$ è generato dalle simmetrie assiali, è sufficiente provare che per ogni σ simmetria e τ traslazione, anche $\sigma^{-1} \circ \tau \circ \sigma = \sigma \circ \tau \circ \sigma$ è una traslazione.
Sia dunque s l'asse di σ e sia $\tau = \sigma_2 \circ \sigma_1$ (σ_1 simmetria di asse s_1 e σ_2 parallelo a σ_1.
Se s è parallelo a s_1 abbiamo $\sigma \circ \tau \circ \sigma = (\sigma \circ \sigma_2) \circ (\sigma_1 \circ \sigma)$, che è prodotto di due traslazioni e quindi è una traslazione.
Nel caso s non sia parallela alle altre due rette, forma con esse angoli coniugati interni supplementari, quindi le due rotazioni $\sigma \circ \sigma_2$ e $\sigma_1 \circ \sigma$ hanno ampiezze opposte. Sappiamo quindi, per un risultato della geometria, che $\sigma \circ \tau \circ \sigma = (\sigma \circ \sigma_2) \circ (\sigma_1 \circ \sigma)$ è ancora una traslazione. Dunque $\mathscr{T}$ è normale in $Isom(\mathbb{R}^2)$.

b) Siano $f \in Isom(\mathbb{R}^2)$, $O' = f(O)$ e τ la traslazione associata al vettore $\vec{OO'}$.
Allora $\tau^{-1} \circ f(O) = O$, vale a dire $\tau^{-1} \circ f \in Isom(\mathbb{R}^2)_O$. Ne segue dunque che $f \circ \tau \in Isom(\mathbb{R}^2)_O$, quindi $Isom(\mathbb{R}^2) = \mathscr{T} Isom(\mathbb{R}^2)_O$.
Inoltre, poiché l'unica traslazione con punti uniti è l'identità, si ha che $\mathscr{T} \cap Isom(\mathbb{R}^2)_O = \{id\}$. Dunque si ha il prodotto semidiretto.

c) Chiaramente $\mathscr{T}$ è normale anche in $\mathscr{M}$.
Siano μ un movimento, $O' = \mu(O)$ e τ la traslazione associata al vettore $\vec{OO'}$.
Allora $\tau^{-1} \circ \mu(O) = O$, vale a dire $\tau^{-1} \circ \mu \in \mathscr{M} \cap Isom(\mathbb{R}^2)_O$. Ne segue dunque che $\mu \circ \tau \in \mathscr{M} \cap Isom(\mathbb{R}^2)_O$, quindi $Isom(\mathbb{R}^2) = \mathscr{T}(\mathscr{M} \cap Isom(\mathbb{R}^2)_O)$. Da qui si ottiene il prodotto semidiretto. □

Gli enunciati precedenti introducono alla seguente proposizione, che dimostra la risolubilità:

Proposizione 2.2. *Il gruppo $Isom(\mathbb{R}^2)$ delle isometrie del piano è risolubile.*

Dimostrazione. La serie $\{id\} \lhd \mathscr{T} \lhd \mathscr{M} \lhd Isom(\mathbb{R}^2)$ è una serie subnormale. Inoltre, si ha:

- $\mathscr{T}/\{id\} \cong \mathscr{T} \cong (\mathbb{R}^2, +)$ che è abeliano;
- $\mathscr{M}/\mathscr{T} \cong \mathscr{M} \cap Isom(\mathbb{R}^2)_O$ per quanto detto in precedenza, e $\mathscr{M} \cap Isom(\mathbb{R}^2)_O$ è il gruppo delle rotazioni di centro O, isomorfo a $(\mathbb{R}/2\pi\mathbb{Z}, +)$ che è abeliano;
- $Isom(\mathbb{R}^2)/\mathscr{M}$ è abeliano perché ha ordine 2.

Dunque la serie è abeliana, da cui si ha che $Isom(\mathbb{R}^2)$ è risolubile. □

Osservazione 2.5. Si può notare che la serie sopra indicata è anche una serie minima: difatti $Isom(\mathbb{R}^2)/\mathscr{T}$, isomorfo al gruppo delle rotazioni e simmetrie, non è abeliano (in quanto rotazioni e simmetrie non commutano), e $\mathscr{M}$ non è abeliano. Quindi non è possibile ridurla ulteriormente. Di conseguenza $dl(Isom(\mathbb{R}^2)) = 3$.

2.4 Gruppi con serie derivata non finita

Esistono gruppi infiniti la cui serie derivata, sebbene strettamente decrescente, non è finita.

Definiamo, per $n > 1$, il cosiddetto *gruppo libero* F_n generato dagli elementi $a_1, \ldots, a_n$ e $a_1^{-1}, \ldots, a_n^{-1}$ (l'elemento neutro è rappresentato da 1), per il quale le uniche relazioni concesse sono l'associatività e $xx^{-1} = 1 \ \forall\, x \in F_n$.

Esempio 2.1. Per capire meglio possiamo ragionare, prendendo $n = 21$, come se:

- $\{a_i,\ i = 1, \ldots, 21\}$ fosse formato dalle lettere minuscole dell'alfabeto italiano;
- $\{a_i^{-1},\ i = 1, \ldots, 21\}$ fosse formato dalle lettere maiuscole dell'alfabeto italiano;
- 1 fosse la "parola vuota".

In questo caso F_{21} è formato da tutte le parole componibili con tali lettere (chiaramente anche quelle che nella lingua italiana non hanno senso).
La relazione $xx^{-1} = 1$ equivale dunque a eliminare due parole, o due successioni di lettere, consecutive che siano una l'inverso dell'altra (a livello semantico, un palindromo; a livello grafico, successioni opposte di lettere). Per esempio:

$$\text{MIo niPOTe ha OtTo Anni} \longrightarrow \text{MIo niPOTe h nni}$$
$$\text{AmMarare} \longrightarrow \text{rare}$$

Considerando i commutatori degli elementi di tali gruppi liberi F_n, si ha che nessun commutatore può essere uguale a uno degli a_i, altrimenti avremmo una relazione aggiuntiva, non concessa.
Pertanto $(F_n)' \subset F_n$. Per induzione si ha quindi che $(F_n)^{(k+1)} \subset (F_n)^{(k)} \quad \forall k > 0$. Si ottiene perciò una serie derivata infinita:

$$F_n \supset (F_n)' \supset (F_n)^{(2)} \supset \cdots \supset (F_n)^{(k)} \supset \cdots$$

Perciò F_n non è risolubile per $n > 1$ (F_1 invece è risolubile, in quanto $F_1 \cong (\mathbb{Z}, +)$, quindi è abeliano). Tuttavia, se noi quozientiamo F_n con un suo k-esimo derivato, otteniamo per qualsiasi k un gruppo con una serie abeliana di lunghezza k.

Dunque $F_n/(F_n)^{(k)}$ è risolubile $\forall\ k \geq 0$, con $dl\left(F_n/(F_n)^{(k)}\right) = k$.
Oppure, in generale, $(F_n)^{(j)}/(F_n)^{(k)}$ risolubile $\forall\ k \geq j \geq 0$, con $dl\left((F_n)^{(j)}/(F_n)^{(k)}\right) = k - j$.

Osservazione 2.6. Il prodotto diretto di una infinità numerabile di gruppi risolubili non è detto sia risolubile: è sicuramente vera se ogni gruppo è abeliano (prodotto diretto di abeliani è ancora abeliano, e dunque risolubile); se non tutti i gruppi sono risolubili, il prodotto diretto è risolubile se *la lunghezza derivata è limitata superiormente.*

Consideriamo un esempio: posto $G_k = F_n/F_n^{(k)}$, si ha $dl(G_k) = k$. Allora il prodotto $G = \prod_{k\in\mathbb{N}} G_k$ non è risolubile, perché $G^{(r)} = \prod_{k\in\mathbb{N}} (G_k)^{(r)}$, e $(G_k)^{(r)} \neq \{1\} \quad \forall\ k > r$.

Capitolo 3

Gruppi risolubili finiti

Nel capitolo 1 ho enunciato proprietà valide per un generico gruppo risolubile. In questo capitolo invece approfondisco l'argomento per i gruppi finiti, per evidenziare quali tra questi possa essere risolubile, scoprendo ulteriori proprietà.

3.1 Teoria preliminare

Per fare questo approfondiamo la teoria relativa alle serie di sottogruppi. Ricordiamo alcune definizioni particolari relative ai gruppi:

- Un sottogruppo H di G si dice *proprio* se $H \subsetneq G$;
- Un sottogruppo H si dice *massimale* se per ogni K sottogruppo di G per cui $H \subseteq K \subseteq G$, si ha $H = K$ o $K = G$;
- Un sottogruppo J si dice *normale minimo* se è normale non banale e se, per ogni K sottogruppo di G per cui $\{1\} \subseteq K \subseteq J$, con $K \lhd G$, si ha $K = 1$ oppure $K = J$;
- Un gruppo abeliano finito si dice *abeliano elementare* se i suoi elementi, ad eccezione dell'unità, hanno tutti lo stesso ordine p; da ciò deriva che l'ordine del gruppo è p.

Definizione 3.1 (**Raffinamento di serie**)**.** Siano $A = (A_0, \ldots, A_n)$ e $B = (B_0, \ldots, B_m)$ due serie subnormali; B si dice *raffinamento* di A se esiste una funzione iniettiva

$$T : \{0, 1, \ldots, n\} \xrightarrow{1-1} \{0, 1, \ldots, m\}$$

tale che $A_i = B_{T(i)} \ \forall\, i$.
Se A è ridotta, equivale a dire che ogni elemento di A deve essere contenuto in B.

Sull'insieme delle serie subnormali posso inoltre definire una relazione di equivalenza:

Definizione 3.2. Due serie subnormali $(G_0, G_1, \ldots, G_r)$ e $(H_0, H_1, \ldots, H_s)$ si dicono *equivalenti* se esiste una biezione tra i loro fattori che rende isomorfi i fattori corrispondenti.

Vale a dire: $(G_0, G_1, \ldots, G_r) \sim (H_0, H_1, \ldots, H_s) \iff r = s$ e se $\exists\ \sigma \in S_r$ gruppo simmetrico tale che

$$G_{i+1}/G_i \cong H_{\sigma(i+1)}/H_{\sigma(i)} \ \ \forall\, i = 0, 1, \ldots, r-1$$

Sull'equivalenza tra serie abbiamo questo importante teorema, di cui riporto solo l'enunciato:

Teorema 3.1 (Schreier)**.** *Due serie subnormali di G possiedono sempre raffinamenti equivalenti.*

Può succedere che in una serie subnormale $(\{1\} = G_0, G_1, \ldots, G_n = G)$ ogni G_i con $0 \leq i < n$ sia normale in G. Allora la serie si dice *serie normale*.

Esempio 3.1. Un esempio di serie normale è la serie derivata.

Se ogni G_i è un sottogruppo normale, proprio e massimale di G, chiamiamo la serie *serie principale*.

L'analogo della serie principale per una serie subnormale è la cosiddetta *serie di composizione*:

Definizione 3.3 (**Serie di composizione**)**.** Una *serie di composizione* di G è una serie subnormale ridotta i cui fattori sono tutti semplici.
In altre parole, una serie di composizione è una serie subnormale $(G_0, G_1, \ldots, G_n)$ in cui ogni G_i è un sottogruppo normale, proprio e massimale di G_{i+1}.

Un teorema molto importante relativo alle serie di composizione è il seguente:

Teorema 3.2 (Jordan, Hölder, Dedekind)**.** *Sia G gruppo con una serie di composizione S. Allora:*

a) Ogni serie subnormale T si può raffinare ad una serie di composizione.

b) Tutte le serie di composizioni sono equivalenti.

Dimostrazione. a) Le serie S e T hanno dei raffinamenti equivalenti (dal teorema di Schreier), tuttavia, il raffinamento di S, eliminati i termini ripetuti, coincide con S, dunque anche il raffinamento di T, eliminati i termini ripetuti, è una serie di composizione.

b) Se anche T è una serie di composizione, allora coincide con il suo raffinamento; dunque S e T sono equivalenti. □

Osservazione 3.1. Il teorema precedente è analogo nel caso di serie normali, sostituendo alle serie di composizione le serie principali:

a) Ogni serie normale T si può raffinare con una serie principale.

b) Tutte le serie principali sono equivalenti.

Questo teorema ci interessa particolarmente per i gruppi finiti a causa del seguente teorema, dimostrabile per induzione:

Teorema 3.3. *Un gruppo finito ha* sempre *una serie di composizione.*

Dunque, nel caso di un gruppo finito, il teorema di Jordan, Hölder e Dedekind vale sempre.

3.2 Caratterizzazione dei gruppi risolubili finiti

Osservate tutte queste proprietà, abbiamo il seguente teorema:

Teorema 3.4. *Sia G un gruppo finito. Sono allora equivalenti:*

1. *G è risolubile;*
2. *G ha una serie di composizione i cui fattori sono ciclici di ordine primo;*
3. *G ha una serie principale a fattori abeliani elementari.*

Dimostrazione. La dimostrazione di questo teorema, viste le premesse, diventa molto semplice:

1. $\Rightarrow$ 2. Se G è finito e risolubile, raffinando la sua serie abeliana si ottiene una serie a fattori abeliani e semplici (la semplicità è data dal fatto che il raffinamento è una serie di composizione, derivato dal teorema 3.2), perciò ciclici di ordine primo.

1. $\Rightarrow$ 3. Raffinando invece la serie derivata di G, che è una serie normale, per quanto detto nell'osservazione 3.1 si ottiene una serie principale a fattori abeliani.
Sappiamo poi che, se K è un sottogruppo di L, con $L \lhd G$, e K è caratteristico in L (cioè è invariante per autormorfismi di L), allora $K \lhd G$; i fattori di una serie principale non possono avere sottogruppi caratteristici, altrimenti sarebbe possibile raffinare la serie, e i soli gruppi abeliani privi di sottogruppi caratteristici propri sono i gruppi abeliani elementari. Quindi i fattori principali di un gruppo risolubile sono abeliani elementari.

2., 3. $\Rightarrow$ 1. L'inverso è praticamente automatico, poiché sia le serie di composizione a fattori ciclici d'ordine primo, sia le serie principali a fattori abeliani elementari, sono serie abeliane. □

Esempio 3.2. Consideriamo il gruppo simmetrico S_3. Ricordo che è un gruppo risolubile metabeliano, con serie abeliana minima $S = (\{id\}, A_3, S_3)$. Verifico se ha una serie di composizione a fattori ciclici di ordine primo (per il teorema precedente, essendo S_3 finito e risolubile, ce l'ha sicuramente).
Si può osservare, come già mostrato nell'esempio 1.1, che S è già ridotta a fattori ciclici di ordine primo; inoltre $\{id\}$ è sottogruppo normale massimale in A_3, che è normale massimale in S_3. Dunque S è anche serie di composizione a fattori ciclici di ordine primo di S_3.

Sulla risolubilità dei gruppi finiti ci sono alcuni teoremi importanti e molto noti; uno di questi è il teorema di Feit-Thompson:

Teorema 3.5 (Feit-Thompson)**.** *Tutti i gruppi di ordine dispari sono risolubili.*

La dimostrazione di tale teorema nella versione originale è lunga oltre 300 pagine e estremamente complicata, quindi non la riporterò qua.

Nella prossima sezione vedremo esempi di gruppi finiti risolubili, dimostrandone la risolubilità senza fare uso di questi due teoremi. Il caso più noto, quello del gruppo simmetrico, è già stato ampiamente trattato nel capitolo 1.

3.3 Esempi di gruppi risolubili finiti

3.3.1 I diedrali

Come abbiamo già notato nel capitolo 2, esistono 3 tipologie naturali di isometrie in $\mathbb{R}^2$: le rotazioni, le simmetrie e le traslazioni.
Se X è un sottospazio di $\mathbb{R}^2$, è intuitivamente comprensibile che una isometria che lascia X immutato non può essere una traslazione, ma può essere o una rotazione o una simmetria.
Sia dunque X un poligono regolare con un numero $n \geq 3$ di lati; definiamo:

$$S_{\mathbb{R}^2}(X) = \{f : \mathbb{R}^2 \to \mathbb{R}^2 \text{ isometria} \mid f(X) = X\}$$

Guardiamo gli elementi di $S_{\mathbb{R}^2}(X)$:

- Le rotazioni che preservano X sono le rotazioni di angolo $2\pi k/n,\ k = 0, 1, \ldots, n-1$, e che hanno per centro il centro di X;
- Le simmetrie che lasciano X immutato sono quelle rispetto agli *assi di simmetria* del poligono: per n pari essi corrispondono alle rette passanti per vertici opposti; se n è invece dispari essi sono le rette passatti per un vertice e il punto medio del lato opposto.

Gli elementi di $S_{\mathbb{R}^2}(X)$ sono quindi n rotazioni e n simmetrie: in totale $n+n=2n$ elementi.
$S_{\mathbb{R}^2}(X)$ forma un gruppo, detto anche *gruppo diedrale*, che denotiamo D_n.

Essendo un gruppo ed essendo formato da isometrie di $\mathbb{R}^2$, D_n è un sottogruppo di $Isom(\mathbb{R}^2)$, che è risolubile, come visto nel capitolo 2.
Pertanto, dalla proposizione 1.4 sui sottogruppi di gruppi risolubili, si conclude che D_n è risolubile.

3.3.2 Il caso di $GL_n(\mathbb{K})$ finito

Come mostrato a pagina 10, il gruppo delle matrici invertibili $GL_n(\mathbb{K})$, con $\mathbb{K}$ di ordine infinito, non è risolubile.
Esistono invece alcuni piccoli casi finiti nei quali $GL_n(\mathbb{K})$ è risolubile: quando $n=2$ e $|\mathbb{K}| \leq 3$. Siano dunque $\mathbf{2}$ e $\mathbf{3}$ campi generici rispettivamente di ordine 2 e 3.

- $GL_2(\mathbf{2})$: esso ha ordine $(2^2-1)\cdot(2^2-2)=6$, quindi è isomorfo a S_3, perciò è risolubile.
- $GL_2(\mathbf{3})$: questo ha invece ordine $(3^2-1)\cdot(3^2-3)=8\cdot 6=2^4\cdot 3$. Quindi, per un teorema che mostrerò più avanti, il *teorema di Burnside*, è risolubile.

3.3.3 I gruppi di ordine p^k

Un ruolo importante nei gruppi finiti è coperto dai gruppi di ordine p^k, con p primo, detti *p-gruppi*.
Chiaramente, se $k=1$ (in generale, se il gruppo è abeliano, come ad esempio $\mathbb{Z}_{p^k}$) la risolubilità di tali gruppi è banale, poiché ogni gruppo abeliano è risolubile. Considererò dunque il caso:

$$G \text{ gruppo non abeliano, } |G|=p^k, \text{ con } k>1.$$

L'importanza dei p-gruppi nella teoria generale dei gruppi risolubili finiti si deduce dal seguente enunciato:

Proposizione 3.1. *Sia G un gruppo finito risolubile.*

a) Sia P un sottogruppo normale minimo. Allora P è un p-gruppo abeliano elementare.

b) Sia M un sottogruppo massimale. Allora $[G:M]$ è la potenza di un primo.

Dimostrazione. a) La serie normale $1 \lhd P \lhd G$, come affermato nell'osservazione 3.1 sul teorema di Jordan-Hölder-Dedekind, si raffina ad una serie principale, ed essendo G risolubile, per il teorema 3.4 essa ha tutti i fattori che sono p-gruppi abeliani elementari, in particolare $P \cong P/\{1\}$.

b) Procediamo per induzione sull'ordine di G.
Per $|G| = 1$ il risultato è vero; sia poi P un sottogruppo normale minimo di G. Per a) P è abeliano elementare di ordine p^k, con p primo, $k \in \mathbb{N}$.
Se $P \subseteq M$ allora, per ipotesi induttiva, $[G : M] = [G/P : M/P]$ è potenza di un primo.
Se invece $P \nsubseteq M$, allora $M \subset PM$, quindi $PM = G$. Sia poi $L = P \cap M$: si ha che $L \subset P$, perché P è abeliano, e $L \subset M$, perché $P \subset G$. Ne segue, per la teoria dell'azione di un gruppo, che $G = PM \subseteq N_G(L)$, dove $N_G(L)$ è il *gruppo normalizzante* di L in G, definito come $N_G(L) = \{x \in G \mid x^{-1}Lx = L\}$. Si ha quindi che $L \lhd G$.
Poiché P è minimale, L deve essere di conseguenza costituito solo dall'identità ($L = \{1\}$). Ma allora $|G| = |P| \cdot |M|$, cioè $[G : M] = |G|/|M| = |P| = p^k$. □

Dimostriamo dunque ora la risolubilità dei p-gruppi.

Teorema 3.6. *Sia G un p-gruppo non abeliano, $|G| = p^k$, $k > 1$. Allora G è risolubile.*

Dimostrazione. Per dimostrare la risolubilità di G sfruttiamo l'azione dei gruppi: consideriamo perciò l'azione per coniugio di G su se stesso.
Dimostriamo dunque che G ha centro non banale, cioè che $Z(G) \neq \{1\}$.
Dal teorema 2.1 risulta che $|[x]_G|$ è un divisore dell'ordine di $|G| - = p^k$, quindi è del tipo $|[x]_G| = p^h$, $h \leq k$. Dato che le classi $[x]_G$ generano una partizione di G, abbiamo:

$$p^k = |G| = \sum_{i=1}^{n} |[x_i]_G| = |[1]_G| + |[x_2]_G| + \ldots + |[x_n]_G| = 1 + p^{h_2} + \ldots + p^{h_n}$$

con $1 = p^{h_0}$, $h_i \leq k$, $i = 0, \ldots, n$.
Dunque, abbiamo che $p^k = 1 + c$, con $c = p^{h_2} + \ldots + p^{h_n} \equiv 0 \; mod\, p$; e questo è assurdo.
Dunque esiste qualche altra classe di lunghezza 1 oltre a quella dell'elemento neutro, da cui $Z(G) \neq \{1\}$.
Abbiamo quindi che $|G/Z(G)| < p^k = |G|$. $G/Z(G)$.
Iterando il procedimento su $G/Z(G)$, otteniamo una serie abeliana per $G/Z(G)$, dunque $G/Z(G)$ è risolubile; poiché $Z(G)$ è abeliano (quindi risolubile, dall'osservazione 1.1) e normale in G, per la proposizione 1.6 sulla risolubilità delle estensioni normali di gruppi risolubili, G è risolubile. □

Purtroppo non si hanno informazioni generali sulle serie minime o di composizione dei p-gruppi.

Un'altro enunciato generalizza il teorema precedente (ne riporto solo l'enunciato):

Proposizione 3.2. *Se p, q, r sono primi, tutti i gruppi di ordine p^k, p^kq, p^2q^2 o pqr sono risolubili.*

Parte di questo teorema è estremamente generalizzata dal *Teorema di Burnside* e, insieme al teorema di Feit-Thompson, fa parte dei teoremi più noti della teoria dei gruppi risolubili finiti:

Teorema 3.7 (Burnside)**.** *Ogni gruppo di ordine $p^m q^n$ è risolubile (p, q primi).*

Anche questo teorema ha una dimostrazione estremamente complicata, che non riporterò.

Un altro curioso teorema di tipo numerico è il seguente:

Teorema 3.8 (Burnside, Feit-Thompson)**.** *Se G è un gruppo finito semplice, allora o 12 o 8 dividono $|G|$.*

Osservazione 3.2. Da questo teorema si deduce che, se $|G|$ non è multiplo né di 12 né di 8, non è semplice.
Sia dunque $K \neq \{1\}$ un sottogruppo normale proprio di G; allora per il teorema di Lagrange neanche $|K|$ e $|G/K|$ sono multipli né di 12 né di 8. Perciò, per induzione, otteniamo che sia K che G/K sono risolubili; dunque, per la proposizione 1.4 sulla estensione di gruppi risolubili, anche G è risolubile.

A questo punto, considerando i teoremi sui p-gruppi, insieme ai teoremi di Feit-Thompson e Burnside e al teorema precedente, si sono ridotti tantissimo gli interi k per cui un gruppo con ordine k non è risolubile.
Consideriamo gli ordini da 1 a 100: escludendo automaticamente i dispari, le potenze di 2 e i prodotti di potenza di 2 soli primi, rimangono solo 30, 42, 60, 66, 70, 78, 84 e 90.

- 30, 42, 66, 70, 78 sono multipli di 3 primi, quindi per la proposizione 3.2 i gruppi con tali ordini sono risolubili;

- Abbiamo che $90 = 2 \cdot 3^2 \cdot 5$, quindi 12 né 8 dividono questi numeri, pertanto un gruppo con ordine 90 non è semplice, e per quanto visto nell'osservazione precedente è risolubile.

- Poiché $|A_5| = 60$, non tutti i gruppi di ordine 60 sono risolubili, perché A_5, come visto nella proposizione 1.2, non è risolubile.
  Un esempio di gruppo risolubile di ordine 60 è il gruppo diedrale D_{30} del poligono a 30 facce (come abbiamo visto, il gruppo diedrale D_n è sempre risolubile e ha ordine $2n$), oltre chiaramente a tutti i gruppi finiti abeliani di ordine 60, come $\mathbb{Z}_{60}$.

- Rimane solo 84: esso però è divisibile per 12, e la sua scomposizione in fattori primi è $2^2 \cdot 3 \cdot 7$, quindi non possiamo usare nessuno dei risultati precedenti.
  Ciononostante, grazie alla teoria sui *p-sottogruppi di Sylow* e al relativo *Teorema di Sylow*, non esposti in questa tesi, possiamo dire che i gruppi di ordine 84 sono risolubili.

Conclusione

Già dalla ridotta presentazione che questa tesi porta dei gruppi risolubili, si intuisce quanto tale argomento sia importante nella teoria algebrica e quanto si sia espanso dall'intuizione di Galois per la teoria delle equazioni.

La loro classe infatti, insieme a quella dei gruppi abeliani, è probabilmente tra le classi di gruppi più studiate, per la ricchezza di proprietà possedute. Una su tutte: tutti i gruppi risolubili finiti hanno π-sottogruppi di Hall. Un sottogruppo H di un gruppo finito G si dice π-sottogruppo di Hall di G se, per $|G| = \prod_{i=1}^{n} p_i^{a_i}$ esiste un sottoinsieme $\pi = \{p_{i_1}, \ldots, p_{i_r}\} \subseteq \pi(G) = \{p_1, \ldots, p_n\}$ tale che $|H| = \prod_{j=1}^{r} p_{i_j}^{a_{i_j}}$.
Il Teorema di Hall afferma infatti che *se G è finito e risolubile, per ogni $\pi \subseteq \pi(G)$ esiste un π-sottogruppo di Hall, ogni altro π-sottogruppo è incluso in uno di essi, e due π-sottogruppi di Hall sono coniugati.*

Nello studio dei gruppi risolubili sono poi entrati in gioco tantissimi strumenti, alcuni dei quali, più o meno implicitamente, sono stati anche utilizzati in questa tesi, come la *nilpotenza* di un gruppo e la *teoria di Sylow*.
La teoria di Sylow è una teoria sui p-sottogruppi di un gruppo finito G che, come accennato nell'ultimo esempio del capitolo precedente, favorisce l'analisi della risolubilità dei gruppi finiti. Se $|G|$ è $p^a m$ (p primo, $MCD(p, m) = 1$), ogni sottogruppo di ordine p^a si dice *p-sottogruppo di Sylow di G*.
Il teorema di Sylow afferma che *un gruppo di ordine $p^a m$ (p primo, $MCD(p, m) = 1$) possiede p-sottogruppi di Sylow; ogni suo p-sottogruppo è incluso in un p-sottogruppo di Sylow, e tutti i p-sottogruppi di Sylow sono coniugati; infine, detto n_p il loro numero, si ha $n_p \equiv 1 \ (mod\, p)$ e $n_p \mid m$.*
Intuitivamente, questo teorema consente di riportare l'ordine di un gruppo a uno dei casi noti per il quale un gruppo con tale ordine è sempre risolubile.
Un gruppo poi si dice nilpotente se possiede una *serie centrale*, cioè una serie normale $\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$ tale che $G_{i+1}/G_i \subseteq Z(G/G_i)$ per ogni i.
Si ha che *ogni gruppo nilpotente è risolubile*, e molto spesso per dimostrare la risolubilità di un gruppo si passa dalla nilpotenza. Così abbiamo implicitamente fatto noi, nel caso delle matrici triangolari $T_n(\mathbb{K})$ negli esempi del capitolo 2 (avevamo infatti trovato

una *serie centrale discendente*), oppure nel caso stesso dei p-gruppi del capitolo 3 dove, dimostrando che i p-gruppi hanno centro non banale, ne abbiamo dimostrato la nilpotenza.

Questa ricchezza di strumenti per studiare i gruppi risolubili fa sì che spesso, nello studio avanzato della teoria dei gruppi, per il medesimo studio vengano analizzati separatamente i gruppi risolubili e i non risolubili: sui gruppi risolubili è infatti possibile, come abbiamo visto, usare tantissimi strumenti che non sono utilizzabili negli altri casi; per esempio possiamo ragionarvi per induzione sulla sua serie abeliana, semplificando i ragionamenti.

Chiaramente lo studio non si è esteso solo in funzione dei gruppi risolubili: si è arrivato a parlare di *gruppi supersolubili*, cioè gruppi con una serie normale a fattori ciclici: si ha, per esempio, che se G è un gruppo finito e tutti i suoi sottogruppi sono supersolubili, allora è risolubile (cfr. [5, p. 397]); o addirittura si è arrivati a definire generalizzazioni della risolubilità (si veda a tal proposito le classi di Kuroš-Černikov, descritte in [2, par. 22]).

Questa tesi quindi non ha inteso esaurire l'argomento, in quanto così enormemente vasto, ma ha voluto riguardare ad alcuni argomenti di studio affrontati precedentemente con uno strumento in più, quale è quello dei gruppi risolubili.

Bibliografia

[1] M. Idà, Dispense del corso di Algebra II, a.a. 2014-2015.

[2] M. I. Kargapolov, Ju. I. Merzljakov, "Fundamentals of the Theory of Groups", Springer-Verlag, New York, 1979.

[3] S. Lang, "Algebra", Springer-Verlag, New York, 2002.

[4] Derek J. S. Robinson, "A Course in the Theory of Groups", Springer-Verlag, New York, 1982.

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

[6] L. Verardi, Dispense del corso di Algebra Superiore, a.a. 2004-2005.

[7] L. Verardi, Dispense del corso di Elementi di Algebra da un punto di vista superiore, a.a. 2012-2013.

[8] L. Verardi, Dispense del corso di Teoria dei Numeri, a.a. 2013-2014.