UNIVERSITÀ DEGLI STUDI DI CAGLIARI
FACOLTÀ DI SCIENZE

IL TEOREMA DI JORDAN-HÖLDER E IL GRUPPO MOSTRO

CORSO DI LAUREA IN MATEMATICA
ANNO ACCADEMICO 2019/2020

RELATORE: PROF. ANDREA LOI

GIADA MELIS

INDICE:

DEFINIZIONE:

Un sottogruppo K di un gruppo G è *normale* ($K \triangleleft G$) se i laterali sinistro e destro di ogni elemento g di G coincidono, ovvero: $gK = Kg$.
Equivalentemente, se vale: $\forall g \in G,\ k \in K \quad gkg^{-1} \in K$.

DEFINIZIONE:

Un gruppo G non banale è *semplice* se l'unico sottogruppo normale proprio è quello banale.

ESEMPIO:

- Un gruppo ciclico $G = \mathbf{Z}/m\mathbf{Z}$ è semplice se e solo se *m* è primo: infatti tutti i sottogruppi di G sono normali, e corrispondono ai divisori di *m*.
- Il gruppo alterno A_n per $n \geq 5$ è semplice e in particolare A_5 è il più piccolo gruppo semplice non abeliano.

DEFINIZIONE:

Dato un gruppo G, una *serie subnormale* è una sequenza finita di sottogruppi A_i, ognuno dei quali sottogruppo normale del successivo ($A_{i+1} \lhd A_i \;\; i = 0,1,\ldots,n$) e si indica:

$$1 = A_n \lhd \cdots \lhd A_1 \lhd A_0 = G\,.$$

I gruppi quoziente A_i/A_{i+1} sono detti *fattori della serie* e la lunghezza di una serie corrisponde al numero di inclusioni strette nella sequenza.

In particolare si dice che due serie subnormali sono *equivalenti* se esiste una corrispondenza biunivoca tra i gruppi quoziente tale che i corrispondenti fattori siano isomorfi.

ESEMPIO:

$G = A_4 \quad K = \{id, (12)(34), (13)(24), (14)(23)\} \quad H = \{id, (12)(34)\}$

È facilmente dimostrabile che $K \lhd G$ e poiché K è abeliano, ogni sottogruppo di un gruppo abeliano è normale, quindi vale $H \lhd K$.

H non è sottogruppo normale di G, infatti esiste un elemento $h = (12)(34) \in H$ e $g = (123) \in G$ tale che $ghg^{-1} \notin H$.

La serie $\{id\} \lhd H \lhd K \lhd G$ è una serie subnormale.

DEFINIZIONE:

Dato un gruppo G, una *serie subnormale* è una sequenza di sottogruppi A_i, ognuno dei quali sottogruppo normale del successivo ($A_{i+1} \lhd A_i \;\; i = 0,1,\ldots,n$) e si indica:

$$1 = A_n \lhd \cdots \lhd A_1 \lhd A_0 = G\,.$$

I gruppi quoziente A_{i+1}/A_i sono detti *fattori della serie* e la lunghezza di una serie corrisponde al numero di inclusioni strette nella sequenza.

In particolare si dice che due serie subnormali sono *equivalenti* se esiste una corrispondenza biunivoca tra i gruppi quoziente tale che i corrispondenti fattori siano isomorfi.

ESEMPIO:

$G = A_4 \quad K = \{id, (12)(34), (13)(24), (14)(23)\} \quad H = \{id, (12)(34)\}$

È facilmente dimostrabile che $K \lhd G$ e poiché K è abeliano, ogni sottogruppo di un gruppo abeliano è normale, quindi vale $H \lhd K$.

H non è sottogruppo normale di G, infatti esiste un elemento $h = (12)(34) \in H$ e $g = (123) \in G$ tale che $ghg^{-1} \notin H$.

La serie $\{id\} \lhd H \lhd K \lhd G$ è una serie subnormale.

DEFINIZIONE:

Una *serie normale* è una serie subnormale i cui sottogruppi sono normali in G.

ESEMPIO: $G = S_n \quad H = A_n = \{\sigma \in S_n : sgn(\sigma) = 1\}$

A_n coincide con il kernel dell'omomorfismo di gruppi $segno: S_n \longrightarrow \{+1, -1\}$ dunque è un sottogruppo normale di S_n.

La serie $\{id\} \lhd H \lhd G$ è una serie normale.

DEFINIZIONE:

Una *serie di composizione* è una serie normale $1 = H_n \lhd \ldots \lhd H_1 \lhd H_0 = G$, tale che ogni H_{i+1} è un sottogruppo normale massimale di H_i.

Una serie normale è una serie di composizione se ogni fattore di composizione è un gruppo semplice. Un'ulteriore caratterizzazione è che una serie normale è una serie di composizione se e solo se è di lunghezza massimale.

PROPRIETÀ:

Ogni gruppo finito ha una serie di composizione: infatti per induzione sull'ordine del gruppo G, il gruppo è semplice (e quindi la serie di composizione è $1 \triangleleft G$) oppure ha un sottogruppo normale massimale di cardinalità minore di $|G|$. Al contrario non tutti i gruppi infiniti ne posseggono una.

ESEMPIO:

$G = \mathbf{Z_6} \quad H = <3>$

$\mathbf{Z}_6$ è gruppo ciclico di ordine 6 e i suoi sottogruppi sono:

$$<0> = \{0\} \quad <3> = \{0,3\} \quad <2> = \{0,2,4\} \quad <1> = \mathbf{Z_6}$$

Essendo G abeliano, tali sottogruppi sono normali.

Inoltre H è massimale in G e $\{0\}$ è massimale in H.

La serie $\{0\} \triangleleft H \triangleleft G$ è una serie di composizione.

PRIMO TEOREMA DI ISOMORFISMO (teorema fondamentale di isomorfismo):

Siano G e H gruppi e sia $f: G \to H$ un omomorfismo, allora il nucleo di f è un sottogruppo normale di G, ed il gruppo quoziente $G/Ker(f)$ è isomorfo all'immagine di f.

$$\mathrm{Ker}(f) \lhd G, \quad G/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$$

SECONDO TEOREMA DI ISOMORFISMO (teorema del diamante):

Sia G un gruppo, H un sottogruppo di G e N un sottogruppo normale di G. Allora il sottoinsieme prodotto

$$HN = \{hn \,|\, h \in H, n \in N\}$$

è anch'esso un sottogruppo di G, e inoltre:

- $H \cap N$ *è normale in H;*
- $H/(H \cap N) \cong HN/N.$

LEMMA:

Sia G un gruppo con $A \neq B$ normali in G tali che G/A, G/B sono semplici, allora:

$$G/A \simeq B/(A \cap B) \qquad G/B \simeq A/(A \cap B)$$

DIMOSTRAZIONE:

Sia $A \subset B$ allora B/A è normale nel gruppo semplice G/A. Essendo $A \neq B$ il quoziente è non banale, e per ipotesi anche G/B è semplice dunque non è il gruppo stesso. Si ha una contraddizione, dunque $A \not\subset B$ e per simmetria $B \not\subset A$. Consideriamo ora il sottogruppo normale AB di G, la sua immagine attraverso la mappa quoziente, AB/A è un sottogruppo normale di G/A.

Poiché $B \not\subset A$ risulta che AB/A è diverso da $\{e\}$ e poiché G/A è semplice avremo $AB/A = G/A$. Infine dal secondo teorema di isomorfismo concludiamo:

$B/(A \cap B) \simeq AB/A = G/A$ e per simmetria $G/B \simeq A/(A \cap B)$.

∎

TEOREMA DI JORDAN-HÖLDER:

Sia G un gruppo e supponiamo che G abbia una serie di composizione, siano

$$\{e\} = G_r \lhd \cdots \lhd G_1 \lhd G_0 = G$$
$$\{e\} = H_s \lhd \cdots \lhd H_1 \lhd H_0 = G$$

due qualsiasi serie di composizione per G allora $r = s$ e esiste $\sigma \in S_r$ tale che $\forall k$:

$$G_k / G_{k+1} \simeq H_{\sigma(k)} / H_{\sigma(k)+1}$$

1

DIMOSTRAZIONE:

Usiamo l'induzione sulla lunghezza della serie di composizione più corta per G.

È sufficiente dimostrare che qualsiasi serie di composizione è equivalente ad una serie minimale, e dunque che qualsiasi due serie sono equivalenti.

2

Se G è semplice allora ha un'unica serie di composizione: $\{e\} \lhd G$.

Per il caso induttivo supponiamo che

$\{e\} = G_r \lhd \cdots \lhd G_1 \lhd G_0 = G$ sia la serie minimale per G.

Se $G_1 = H_1$, allora per induzione la serie che inizia da G_1 sarà equivalente alla serie che inizia da H_1, dunque anche l'intera serie lo sarà.

Consideriamo, quindi, il caso $G_1 \neq H_1$ e definiamo $K = (H_1 \cap G_1)$ che è normale in G; per il lemma risulta che $G_1/K \simeq G/H_1$ e $H_1/K \simeq G/G_1$ sono semplici.

Sia $K_i = (K \cap G_i)$, allora $K_i \lhd G_i$ e $K_{i+1} \lhd K_i$.

Consideriamo l'omomorfismo $K_i \longrightarrow G_i/G_{i+1}$ dato dalla mappa quoziente.

L'immagine è normale e il nucleo corrisponde a K_{i+1}, quindi per il primo teorema di isomorfismo K_i/K_{i+1} è un sottogruppo normale di G_i/G_{i+1}.

Inoltre poiché G_i/G_{i+1} è semplice, per ogni coppia di sottogruppi $K_i, K_{i+1},\ K_i = K_{i+1}$ oppure K_i/K_{i+1} è semplice.

Rimuovendo gli elementi uguali otteniamo due serie per G_1:

$$\{e\} = G_r \lhd \cdots \lhd G_2 \lhd G_1$$
$$\{e\} = K_r \lhd \cdots \lhd K_1 \lhd G_1$$

Per induzione su G_1 le due serie sono equivalenti, e in particolare devono avere la stessa lunghezza, $r-1$, dunque esattamente uno dei gruppi K_i/K_{i+1} è banale.

Sapendo che $K_1 \lhd H_{1,}$ dunque abbiamo due serie per H_1:

$$\{e\} = H_s \lhd \cdots \lhd H_2 \lhd H_1$$

$$\{e\} = K_r \lhd \cdots \lhd K_1 \lhd H_1$$

Dal momento che esattamente uno dei gruppi K_i/K_{i+1} è banale, concludiamo che H_1 possiede una serie di composizione di lunghezza $r-1$ che è minore della lunghezza della serie minimale per G. Quindi per induzione queste serie sono equivalenti e $s-1 = r-1$.

È sufficiente mostrare che le serie

$$\{e\} = K_r \lhd \cdots \lhd K_1 \lhd G_1 \lhd G$$

$$\{e\} = K_r \lhd \cdots \lhd K_1 \lhd H_1 \lhd G$$

sono equivalenti.

Per il lemma $G/G_1 \simeq H_1/K_{1,}\ G/H_1 \simeq G_1/K_1$ e chiaramente $K_i/K_{i+1} \simeq K_i/K_{i+1}$.

∎

TEOREMA (CLASSIFICAZIONE DEI GRUPPI SEMPLICI FINITI):

Ogni gruppo semplice finito è isomorfo a uno dei seguenti gruppi:

- un membro di una delle tre classi infinite:
  - i gruppi ciclici di ordine primo,
  - i gruppi alterni A_n con $n \geq 5$,
  - i gruppi di tipo Lie
- uno dei 26 gruppi chiamati “gruppi sporadici”.

Per quanto riguarda la dimostrazione del teorema di classificazione, attualmente esistono due “versioni” chiamate: dimostrazione di prima generazione, risalente attorno al 1985, e dimostrazione di seconda generazione, di creazione più recente. I problemi che accomunano entrambe le versioni sono la complessità e la lunghezza, infatti la dimostrazione consiste di decine di migliaia di pagine tratte da diverse centinaia di articoli di giornale scritti da circa 100 autori diversi, pubblicate tra il 1955 e il 2004 circa.

DEFINIZIONE:

Un gruppo G è *ciclico* se esiste un elemento g del gruppo (detto generatore) tale che

$G = \{g^n : n \in \mathbf{Z}\}$ (notazione moltiplicativa) $G = \{ng : n \in \mathbf{Z}\}$ (notazione additiva).

Ovvero G coincide con il sottogruppo generato da g e si usa scrivere $G = \langle g \rangle$ oppure $G = [g]$.

ESEMPIO: i gruppi quoziente $\mathbf{Z}/n\mathbf{Z}$.

DEFINIZIONE:

Sia S_n l'insieme delle permutazioni di {1,2,3,...,*n*}, è detto *gruppo alterno* il sottogruppo A_n di S_n contenente le permutazioni pari.

DEFINIZIONE:

Un gruppo G munito di una struttura di varietà differenziabile tale che le operazioni moltiplicazione e inversione

$$\begin{aligned} G \times G &\longrightarrow G \\ (a,b) &\mapsto a \cdot b \end{aligned} \qquad\qquad \begin{aligned} G &\longrightarrow G \\ a &\mapsto a^{-1} \end{aligned}$$

sono entrambe differenziabili, è detto *gruppo di Lie*.

Un *sottogruppo di Lie* H di un gruppo di Lie G è un gruppo di Lie, sottogruppo di G e tale che la funzione inclusione da H a G è un'immersione iniettiva e omomorfismo di gruppi.

ESEMPIO:

- le matrici invertibili reali $n \times n$ con il prodotto formano un gruppo, denotato $GL(n, \mathbf{R})$ oppure $GL_n(\mathbf{R})$:

$$GL(n, \mathbf{R}) = \{A \in M(n, \mathbf{R}): detA \neq 0\}.$$

  Tale gruppo è un gruppo reale non compatto di Lie. É sconnesso e ha due componenti connesse.

- le matrici reali ortogonali $n \times n$ formano un gruppo, denotato $O(n)$: $O(n, \mathbf{R}) = \{A \in GL(n, \mathbf{R}) \mid A^t A = I\}$

  queste soddisfano $det(A) = \pm 1$.

  $O(n)$ è un sottogruppo di $GL(n)$, compatto, sconnesso e sottogruppo di Lie di $GL(n)$.
  In particolare si può dimostrare che qualsiasi sottogruppo chiuso di $GL(n, \mathbf{R})$ è un gruppo di Lie.

- tra i gruppi semplici finiti di Lie troviamo:
  - i gruppi di Chevalley, $A_n(q)$, $B_n(q)$ $n > 1$, $C_n(q)$ $n > 2$, $D_n(q)$ $n > 3$, $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$;
  - i gruppi di Steinberg, ${}^2A_n(q^2)$ $n > 1$, ${}^2D_n(q^2)$ $n > 3$, ${}^2E_6(q^2)$, ${}^3D_4(q^3)$;
  - i gruppi di Suzuki, ${}^2B_2(2^{2n+1})$;
  - i gruppi di Ree e di Tits, ${}^2F_4(2^{2n+1})$, ${}^2G_2(3^{2n+1})$.

DEFINIZIONE:

Si chiama *gruppo sporadico* un gruppo semplice finito che è uno dei 26 casi eccezionali del teorema di classificazione dei gruppi semplici finiti.

I primi cinque gruppi sporadici furono scoperti da Emile Léonard Mathieu nel 1861 e nel 1873. Gli altri 21 furono scoperti tra il 1965 ed il 1975, generalmente prendono il nome dai loro scopritori.

Il più grande gruppo semplice sporadico è il *gruppo mostro*.
Chiamato in questo modo per la sua dimensione: il numero di elementi è pari a

8 · 1053

oppure

246 · 320 · 59 · 76 · 112 · 133 · 17 · 19 · 23 · 29 · 31 · 41 · 47 · 59 · 71

oppure 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000

circa uguale al numero di particelle elementari nel pianeta Giove.

- Scoperta nel 1973 (Griess e Fischer)
- Costruzione nel 1980 (Griess)
- Nuovi gruppi sporadici (Fischer, Conway, Norton e Thompson)

Griess lo costruì nel 1980 come gruppo di automorfismi dell'algebra di Griess, un'algebra di 196 884 dimensioni, commutativa e non associativa sui numeri reali.

DEFINIZIONE:

Si dice *algebra su un campo* K (K-algebra), uno spazio vettoriale munito di un prodotto bilineare.

DEFINIZIONE:

Sia G un gruppo, un *sottoquoziente* di G è un gruppo della forma H/N dove H è un sottogruppo di G e N è un sottogruppo normale di H.

Il mostro M contiene 20, incluso se stesso, dei 26 gruppi sporadici come sottoquozienti, chiamati “famiglia felice” da Robert Griess.

Il diagramma a lato, basato su uno presente nel libro “Il mostro e la simmetria” di Mark Ronan, mostra come sono legati.

I gruppi in bianco sono i 6 gruppi sporadici non collegati ad M e sono chiamati *pariahs.*

Per esempio, gli ordini di J_4 e del Gruppo Lyons *Ly* sono divisibili per 37. Poiché 37 non divide l’ordine del mostro, non possono essere suoi sottoquozienti; dunque J_4 e *Ly* sono pariahs.
Infatti 37 è uno dei primi non-supersingolari, di cui fanno parte anche: 43, 53, 61, 67 e qualsiasi numero primo maggiore o uguale a 73.

Un numero primo si dice *primo supersingolare* se divide l’ordine di M. Esistono esattamente 15 numeri primi supersingolari: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59 e 71.

Il mostro possiede almeno 44 classi di coniugio di sottogruppi massimali. Sono stati trovati gruppi semplici non-abeliani di 60 tipi di isomorfismo come sottogruppi o quozienti di sottogruppi.