Corso:Algebra IV I1/Risoluzione di radicali/Gruppi risolubili

Considerata un'equazione di secondo grado della forma $x^2 + bx + c = 0$, le sue soluzioni sono date da

$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Esistono formule risolutive anche per equazioni di terzo e quarto grado.

1 Commutatore e gruppi derivati

Definizione 3.1

Siano G un gruppo, e $a, b \in G$. Si definisce il *commutatore* di a e b , indicato con $[a, b]$, l'elemento $a^{-1}b^{-1}ab \in G$.

Si osserva che

$$ab = ba * [a, b]$$

e che $ab = ba$ se e solo se $[a, b] = 1$.

Definizione 3.2

Sia G un gruppo, il *derivato* di G , indicato con G' , è il sottogruppo di G generato dai commutatori $[a, b]$, al variare di $a, b \in G$.

Più in generale, definisco

$$\begin{gathered} G^{(0)} = G \\ G^{(1)} = G' \\ \dots \\ G^{(i+1)} = (G^{(i)})' \end{gathered}$$

Segue quindi che $G = G^{(0)} \supseteq G^{(1)} \supseteq \cdots \supseteq G^{(i)} \supseteq G^{(i+1)}$.

Questi sottogruppi sono normali in G e addirittura caratteristici (invarianti per automorfismi): infatti se α è un automorfismo di G , dati $a, b \in G$, allora

$$\alpha([a,b]) = \alpha(a^{-1}b^{-1}ab) = \alpha(a^{-1})\alpha(b^{-1})\alpha(a)\alpha(b) = [\alpha(a), \alpha(b)],$$

cioè l'immagine mediante α di un commutatore è il commutatore delle immagini degli elementi.

Segue subito che G' e' caratteristico in G .

In generale, si vede facilmente che $G^{(i)}$ è caratteristico in G , usando il fatto che, dati tre sottogruppi A, B, C di G , con A caratteristico in B e B caratteristico in C , allora A è caratteristico in C .

2 Gruppi risolubili

Definizione 3.3

Un gruppo G si dice *risolubile* se esiste $n \geq 0$ tale che $G^{(n)} = 1 = \{1_G\}$.

Esempio 3.1

Tutti i gruppi abeliani sono risolubili, perché se G è abeliano, $[a, b] = 1 \forall a, b \in G$, allora $G^{(0)} = G$ e $G^{(1)} = 1$.

Lemma 3.1

Sia G un gruppo e N un sottogruppo di G . Se $G' \subseteq N$, allora N è normale in G , e il quoziente G/N è abeliano. Viceversa, se N è normale in G e il quoziente G/N è abeliano, allora G' è contenuto in N .

Dimostrazione

PARTE 1: Sia $G' \subseteq N$. **Mostriamo che N è normale**, cioè che N contiene i coniugati dei suoi elementi, cioè per $g \in G, n \in N$, $g^{-1}ng \in N$. Osservo che

$$g^{-1}ng = n * (n^{-1}g^{-1}ng) = n[n, g]$$

e siccome per ipotesi $G' \subseteq N$, allora $[n, g] \in N$, e quindi $g^{-1}ng = n[n, g] \in N$.

Inoltre siano Nx, Ny laterali destri in G/N . **Mostro che il quoziente è abeliano**:

$$[Nx, Ny] = (Nx)^{-1}\,(Ny)^{-1}\,Nx\,Ny = Nx^{-1}\,Ny^{-1}\,Nx\,Ny$$

e per definizione di prodotto di laterali:

$$= N(x^{-1}y^{-1}xy) = N[x, y] = N$$

dove l'ultimo passaggio vale perché i commutatori stanno in N poiché stanno in $G' \subseteq N$. Segue quindi che il commutatore di due laterali è l'identità del quoziente, e quindi il quoziente è abeliano.

PARTE 2: Viceversa, se N è un sottogruppo normale di G con G/N abeliano, allora $G' \subseteq N$. G/N abeliano significa che dati due laterali $Nx, Ny \in G/N$, allora il commutatore è l'identità del quoziente, cioè

$$N = [Nx, Ny] = N[x, y],$$

per i conti precedenti, e quindi $[x, y] \in N \forall x, y \in G$; segue che, siccome N contiene i generatori di G' , allora G' è contenuto in N .

3 Proprietà dei gruppi risolubili

Proprietà 1: se G è risolubile, lo sono anche tutti i suoi sottogruppi e tutti i suoi quozienti.

Dimostrazione

RISOLUBILITÀ DEI SOTTOGRUPPI: supponiamo che G sia risolubile allora esiste $n \geq 0$ tale che $G^{(n)} = 1$. Sia H un sottogruppo di G , **affermo che** $H^{(i)} \subseteq G^{(i)} \forall i$.

- Per $i = 0$, $H^{(0)} = H \subset G^{(0)} = G$.
- Per $i = 1$, $H^{(1)} = H'$ è generato da $[x, y]$ al variare di $x, y \in H$. L'insieme di generatori di $H^{(1)}$ è contenuto nell'insieme di generatori di $G^{(1)}$ che è

  $$\{[g, h],\ g, h \in G\}$$

  allora $H^{(1)} \leq G^{(1)}$.

- In generale, se suppongo che $H^{(i)}$ sia un sottogruppo di $G^{(i)}$, allora

  $$H^{(i+1)} = (H^{(i)})' \leq (G^{(i)})' = G^{(i+1)}$$

  per il passo precedente.

RISOLUBILITÀ DEI QUOZIENTI: si verifica per induzione che se N è normale in G , allora

$$(G/N)^{(i)} = \frac{G^{(i)} * N}{N},$$

e, siccome G è risolubile, esiste n tale che $G^{(n)} = 1$, e per tale n si ha $(G/N)^{(n)} = (G^{(n)} * N)/N = 1_{G/N}$, cioè anche il quoziente è risolubile.

Proprietà 2: sia G un gruppo e N un sottogruppo normale di G , allora se N e G/N sono risolubili, anche G è risolubile.

Dimostrazione

Per ipotesi G/N è risolubile, allora esiste $t \geq 0$ tale che $(G/N)^{(t)} = N$, e questo implica $(G^{(t)} * N)/N = N$, cioè $G^{(t)} \subseteq N$. Inoltre, anche N è risolubile, quindi esiste s tale che $N^{(s)} = 1$. Allora $(G^{(t)})^{(s)} = G^{(t+s)} \subset N^{(s)} = 1$, cioè $G^{(t+s)} = 1$, e quindi G è risolubile con $n = s + t$.

Esempio 3.2

Mostriamo che S_3 è un gruppo risolubile non abeliano. Se trovo N normale in S_3 , tale che N è risolubile e S_3/N è risolubile, allora posso concludere che S_3 è risolubile. Sia N il sottogruppo di S_3 generato dal 3-ciclo $(1, 2, 3)$: allora N , essendo ciclico, è abeliano e quindi anche risolubile.

Inoltre G/N ha ordine $6/3 = 2$, quindi è anch'esso ciclico e abeliano, e quindi risolubile.

Proprietà 3: Sia G un gruppo, allora sono equivalenti:

1. G è risolubile
2. G ha una serie normale a quozienti abeliani, cioè esiste una catena di sottogruppi tale che

$$G_0 \geq G_1 \geq \cdots \geq G_i \geq G_{i+1} \geq \cdots \geq G_s = 1$$

con G_{i+1} normale in G_i e G_i/G_{i+1} abeliano, per ogni i .

Dimostrazione

$1 \longrightarrow 2$: se G è risolubile, esiste $n \geq 0$ minimo tale che $G^{(n)} = 1$. Considero la serie dei derivati (serie derivata):

$$G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(i)} \geq G^{(i+1)} \geq \cdots \geq G^{(n)} = 1$$

Siccome $G^{(i+1)}$ può essere considerato come il derivato di $G^{(i)}$, si ha che $G^{(i+1)}$ è normale in $G^{(i)}$ e che il quoziente $G^{(i)}/G^{(i+1)}$ è abeliano per la proprietà 1, e quindi la serie derivata è una serie normale a quozienti abeliani.

$2 \longrightarrow 1$: Sia $G = G_0 \geq G_1 \geq \cdots \geq G_i \geq G_{i+1} \geq \cdots \geq G_s = 1$ una serie normale a quozienti abeliani, che esiste per ipotesi. **Mostro che per ogni i ,** $G^{(i)} \subseteq G_i$. Se questo vale si ha in particolare che $G^{(s)} \subseteq G_s = 1$, quindi $G^{(s)} = 1$ e G è risolubile.
Per $i = 0$, $G^{(0)} = G = G_0$; suppongo vero l'asserto per i e lo mostro per $i + 1$, cioè, supponendo che $G^{(i)} \subseteq G_i$, mostro che $G^{(i+1)} \subseteq G_{i+1}$.

Per definizione di serie normale a quozienti abeliani, G_{i+1} è normale in G_i e G_i/G_{i+1} è abeliano, allora per il primo lemma sui gruppi risolubili, $G_i' \subseteq G_{i+1}$. D'altra parte, siccome $G^{(i)}$ è un sottogruppo di G_i , $(G^{(i)})' \subseteq G_i'$, allora, in conclusione

$$G^{(i+1)} = (G^{(i)})' \subseteq G_i' \subseteq G_{i+1}$$

Quindi vale la tesi.

Esempio 3.3

Mostro che S_4 è un gruppo risolubile applicando quest'ultima proprietà. Osservo che A_4 è normale in S_4 . Inoltre,

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

è un sottogruppo normale in A_4 . Il quoziente A_4/V ha ordine $\frac{o(A_3)}{o(V)} = 12/4 = 3$, e quindi è ciclico e abeliano. Allora $S_4 \geq A_4 \geq V \geq 1$ è una serie normale a quozienti abeliani.

Affinché un gruppo finito non sia risolubile, deve esistere un certo indice i tale che $G^{(i)} = G^{(s)}$ per ogni $s \geq i$, cioè a partire da un certo indice il gruppo $G^{(i)}$ non deve più ridursi quando viene derivato.

Sia G un gruppo semplice, cioè un gruppo che non ha sottogruppi normali non banali. Allora, se considero la serie dei derivati si ha: $G^{(0)} = G$, e $G^{(1)} = G'$, e siccome G' è normale in G , si hanno solo due possibilità:

1. $G' = G$ e in questo caso la serie dei derivati non si arresta, infatti si avrà $G^{(i)} = G, \ \forall i$;
2. $G' = 1$, e siccome quoziente G/G' dev'essere abeliano, e in questo caso $G/G' = G$, segue che G è abeliano, allora G è un gruppo ciclico di ordine p , con p primo (perche' G e' privo di sottogruppi non banali).

Esempio 3.4

Da queste osservazioni segue che S_5 non è risolubile perché ha come sottogruppo A_5 che è semplice (da dimostrare).

Osservazione 3.1

Dato un gruppo G che agisce su un insieme Ω transitivamente, e dati $\alpha, \beta \in \Omega$, esiste un elemento $g \in G$ tale che $\alpha^g = \beta$. Allora tra gli stabilizzatori vale la relazione $G_\beta = G_{\alpha^g}$, cioè gli stabilizzatori $(G_\alpha)_{\alpha \in \Omega}$ sono tutti coniugati.

Proposizione 3.1

A_5 è semplice.

Dimostrazione (dimostrazione dettagliata)

Fattorizzo l'ordine di A_5 : $o(A_5) = 5!/2 = 60 = 4 * 3 * 5$. **Mostro che** A_5 **non ha sottogruppi normali non banali**. Considero un sottogruppo normale N in A_5 , con $N \neq A_5$, e mostro che $N = 1$. Indico con $\mathrm{Syl}_3(\mathrm{A}_5)$ l'insieme dei sottogruppi di Sylow di A_5 che sono ciclici e hanno ordine 3, e con $\mathrm{Syl}_5(\mathrm{A}_5)$ l'insieme dei sottogruppi di Sylow di A_5 che hanno ordine 5 e sono ciclici.

Considero i casi possibili:

- Supponiamo che $3 \mid o(N)$, allora N contiene un elemento di ordine 3. Siccome i 3-sylow di A_5 sono ciclici di ordine 3, esiste $P \in \mathrm{Syl}_3(\mathrm{A}_5)$ con $P \leq N$. Siccome N è normale, N coincide con i suoi (sottogruppi) coniugati

$g^{-1}Ng$ al variare di $g \in A_5$. Ora, per ogni $g \in A_5$, $g^{-1}Pg \subset g^{-1}Ng = N$ (con $g^{-1}Pg$ indico il coniugato di P mediante g).

Siccome i 3-sylow sono tutti coniugati tra loro, N li contiene tutti. Allora contiene tutti gli elementi di ordine 3 di A_5 , che sono i 3-cicli e sono $5 * 4 * 3/3 = 20$ (5 possibilità di scelta per il primo elemento, 4 per il secondo, 3 per il terzo e divido per 3 perché lo stesso 3-ciclo può essere scritto in 3 modi distinti).

Allora, siccome N deve contenere tutti i 3-sylow e anche l'unità, si ha $|N| > 20$ e $|N| \mid 60$. Allora l'unica possibilità è che N abbia ordine 30 . In particolare, $5 \mid o(N)$.

- Se $5 \mid o(N)$, allora esiste $P \in \mathrm{Syl}_5(\mathrm{A}_5)$ con $P \leq N$. Come prima, N è normale e deve coincidere con i suoi coniugati. E quindi contiene tutti i coniugati di P mediante gli elementi di A_5 . Siccome i 5-sylow sono tutti coniugati tra loro, N li contiene tutti; allora N contiene tutti gli elementi di A_5 di ordine 5, che sono i 5-cicli e sono $5*4*3*2/5 = 24$. In particolare

abbiamo che $3 \mid o(N)$.

In conclusione, se $3 \mid o(N)$, anche $5 \mid o(N)$ e, viceversa, se $5 \mid o(N)$, anche $3 \mid o(N)$. Ma allora N ha $20 + 24 + 1 = 45$ elementi, ma $45 \nmid 60$, e questo è assurdo perché si deve avere $o(N) \mid o(A_5)$.

- Rimane da valutare la possibilità $o(N) \mid 4$, si può avere $o(N) = 4$ oppure $o(N) = 2$.

Se $o(N) = 4$, allora N è un 2-Sylow in A_5 , ed è normale, allora è l'unico 2-sylow di A_5 (infatti un sottogruppo di Sylow normale in G è sempre unico del suo ordine perché coincide con i suoi coniugati). Allora N contiene tutti gli elementi di ordine 2 di A_5 , che sono i prodotti di due scambi e sono $5 * 4 * 3 * 2/8 = 15$ (divido per 8 perché un prodotto di due scambi può essere scritto in $2^3 = 8$ modi distinti, posso invertire l'ordine dei due scambi e l'ordine degli elementi in ogni scambio). Ma $15 > o(N) = 4$, assurdo!

- Se $o(N) = 2$, allora $N = \{1, x\}$, dove x è il prodotto di due scambi, e fissa una sola tra le cinque cifre dell'insieme $\Omega = \{1, 2, 3, 4, 5\}$, diciamo α . Allora x , e quindi N , sta nello stabilizzatore G_α della cifra fissata.

A_5 agisce in modo transitivo sull'insieme Ω , allora gli stabilizzatori degli elementi di Ω sono tutti coniugati. Segue che N che è normale è contenuto in ogni coniugato dello stabilizzatore G_α , e quindi sta nello stabilizzatore di ogni cifra. Ma questo non può avvenire perché x è il prodotto di due scambi, assurdo.

- L'unica possibilità rimanente è quindi $N = 1$.

4 Semplicità di A_n n ge 5

Teorema 3.1

A_n è semplice per $n \geq 5$.

Dimostrazione

CASO BASE: per $n = 5$, A_5 ha ordine $60 = 4 * 3 * 5$, in particolare i 3-sylow di A_5 sono ciclici di ordine 3, e i 5-sylow di A_5 sono ciclici di ordine 5.

Consideriamo $N \neq 1$ sottogruppo normale di A_5 , e **mostriamo che** $N = A_5$.

Considero i casi possibili:

- $3 \mid o(N)$. Allora esiste un $P \in \mathrm{Syl}_3(\mathrm{A}_5)$ con $P \subseteq N$.

Nota: per indicare $g^{-1}Pg$ scrivo P^g .

Dato $g \in A_5$, $P^g \subseteq N^g = N$, allora $P^g \subseteq N$ per ogni g . Siccome i 3-sylow di A_5 sono tutti coniugati, segue che N contiene tutti i 3-sylow di A_5 . Equivalentemente, N contiene tutti i 3-cicli di A_5 che sono $5 * 4 * 3/3 = 20$. Questo significa che $o(N) > 20$ (infatti N contiene anche l'unità), inoltre $o(N) \mid o(A_5) = 60$, e quindi, oltre alla possibilità $o(N) = 60$, l'unica altra alternativa è che $o(N) = 30$, cioè $5 \mid o(N)$.

- $5 \mid o(N)$. Allora esiste $P \in \mathrm{Syl}_5(A_5)$ con $P \subseteq N$. Allora per ogni $g \in A_5$, $P^g \subseteq N^g = N$, e come prima N contiene tutti i 5-sylow di A_5 che sono tutti coniugati tra di loro; equivalentemene N contiene tutti i 5-cicli, che sono $5!/5 = 24$. Allora, oltre al caso $o(N) = 60$, l'unica alternativa è che $o(N) = 30$, quindi $3 \mid o(N)$.

Da questi due casi segue che $5 \mid o(N)$ se e solo se $3 \mid o(N)$. In ciascun caso N ha almeno $20 + 24 + 1 = 45$ elementi, e contemporaneamente $o(N) \mid 60$, quindi in questi casi l'unica possibilità è $o(N) = 60$ e quindi $N = A_5$.

- $3 \nmid o(N) \land 5 \nmid o(N)$: segue che $o(N) \mid 4$ e ci sono due sottocasi:

-
  - Se $o(N) = 4$, N è un 2-sylow di A_5 , e siccome N è normale, è l'unico 2-sylow di A_5 , e quindi contiene gli elementi di A_5 che hanno ordine 2, ovvero contiene tutti i prodotti di due trasposizioni, chesono $5 * 4 * 3 * 2/8 = 15$, assurdo.
  - Se $o(N) = 2$, allora si avrà $N = \{1, x\}$ dove x è prodotto di due trasposizioni. Segue che $x \in G_\alpha$ ($G = A_5$), dove G_α è lo stabilizzatore di una delle cifre nell'insieme $\{1, 2, 3, 4, 5\}$, cioè $N \subseteq G_\alpha$. Per $g \in A_5$, $N \subseteq (G_\alpha)^g = G_{\alpha^g}$. D'altra parte, A_5 opera transitivamente sull'insieme delle cifre, e quindi gli stabilizzatori sono tutti coniugati. Allora N è contenuto in ciascuno stabilizzatore, cioè x fissa ogni cifra di Ω , assurdo!

PASSO INDUTTIVO: sia $n \geq 6$ e supponiamo A_{n-1} semplice, **mostriamo allora che** A_n **è semplice**.

Considero N sottogruppo normale di A_n , e vogliamo mostrare che $N = A_n$.

Sia $\alpha \in \{1, \dots, n\}$, e chiamo H lo stabilizzatore di α . $H \cong A_{n-1}$ e quindi H è semplice per induzione.

Considero l'intersezione $N \cap H$: siccome N è normale, $N \cap H$ è normale in H . H è semplice, allora $N \cap H = H$ oppure $N \cap H = 1$. Considero i due casi:

- $N \cap H = H$. Allora $H \subseteq N$, e per $g \in A_n$, $H^g = G_{\alpha^g} \subseteq N^g = N$. Inoltre A_n agisce in modo transitivo su $\Omega = \{1, \dots, n\}$, allora $G_\beta \subseteq N$ per ogni $\beta \in \Omega$, perché i G_β sono tutti coniugati.

Allora N contiene tutti gli elementi di A_n che fissano la cifra β per ogni $\beta \in \Omega$, in particolare tra questi ci sono tutti i prodotti di due trasposizioni. Siccome essi generano A_n (infatti ogni permutazione pari è scritta come il prodotto di un numero pari di scambi), segue che $A_n = N$.

- $H \cap N = 1$. Per ogni $g \in A_n$ tale che $\alpha^g = \beta$, $(N \cap H)^g = N \cap H^g = N \cap G_\beta = 1$, quindi, per ogni β , l'unico elemento di N che fissa tale cifra è l'identità.

Sia $x \in N$ con $x \neq 1$, e ne considero la struttura ciclica. Allora possono verificarsi due casi:

Caso 1: x contiene un n -ciclo con $n \geq 3$

Caso 2: x è prodotto di trasposizioni.

A meno di riordinare le cifre possiamo supporre, considerando i due casi, che

Caso 1: nella scrittura di x come prodotto di trasposizioni compare il ciclo $(1, 2, 3, \dots)$, cioè $x = (1, 2, 3, \dots, m) * \dots$;

Caso 2: $x = (1, 2)(3, 4) * \dots$.

Chiamo y il coniugato di x mediante il 3-ciclo $(3, 5, 6)$, che è contenuto in N e si ottiene applicando $(3, 5, 6)$ alle cifre di x , quindi:

Caso 1: $y = (1, 2, 5, \dots, m) * \dots$

Caso 2: $(1, 2)(5, 4) * \dots$ Allora $y \neq x$ in entrambi i casi. Osservo poi che l'elemento xy^{-1} fissa la cifra 1, infatti:

Caso 1: $1^{xy^{-1}} = (1^x)^{y^{-1}} = 2^{y^{-1}} = 1$;

Caso 2: $1^{xy^{-1}} = 2^{y^{-1}} = 1$.

Concludo che xy^{-1} , essendo prodotto di elementi di N , sta in N , e fissa la cifra 1, quindi sta in $N \cap G_1$ ma è diverso dall'identità, assurdo!

Osservazione 3.2

Sia G risolubile e semplice: allora, per la risolubilità, G' non può essere tutto G ; inoltre per la semplicità l'unica possibilità è che $G' = 1$, allora G è abeliano. Segue che G non può avere sottogruppi (tutti i sottogruppi di un gruppo abeliano infatti sono normali in G) e quindi G dev'essere ciclico di ordine p con p primo.

Il fatto che A_n per $n \geq 5$ è semplice implica che S_n non è risolubile per $n \geq 5$.

5 Fonti per testo e immagini; autori; licenze

5.1 Testo

- **Corso:Algebra IV I1/Risoluzione di radicali/Gruppi risolubili** *Fonte:* https://it.wikitolearn.org/Corso%3AAlgebra_IV_I1/Risoluzione_di_radicali/Gruppi_risolubili?oldid=48395 *Contributori:* Toma.luca95, ScimmiaSpaziale e Mmontrasio

5.2 Immagini

5.3 Licenza dell'opera

- [Project:Copyright Creative Commons Attribution Share Alike 3.0 & GNU FDL]
- Creative Commons Attribution-Share Alike 3.0