Algebra 2

Alberto Canonaco
alberto.canonaco@unipv.it

Università di Pavia
Corso di Laurea in Matematica

Anno Accademico 2019/2020
Lezione del 22-04-2020

Dimostrazione della Proposizione

$n \geq 5$, $\{1\} \neq H \triangleleft A_n \implies H$ contiene un 3-ciclo.

Dimostrazione della Proposizione

$n \geq 5$, $\{1\} \neq H \triangleleft A_n \implies H$ contiene un 3-ciclo.

$M(\sigma) := \{i = 1, \dots, n : \sigma(i) \neq i\}$ e $l(\sigma) := \#M(\sigma)\ \forall\, \sigma \in S_n$.

- $\sigma \neq 1 \implies l(\sigma) \geq 2$.
- $l(\sigma) = 2 \iff \sigma$ è un 2-ciclo e $l(\sigma) = 3 \iff \sigma$ è un 3-ciclo.
- Basta dimostrare che $m := \min\{l(\sigma) : 1 \neq \sigma \in H\} = 3$.
- Per assurdo sia $m > 3$ e sia $\sigma \in H \setminus \{1\}$ tale che $l(\sigma) = m$.
- σ può essere di una di queste due forme:
  1. $\sigma = (i_1, i_2, i_3, \dots) \dots$ e $\sigma \neq (i_1, i_2, i_3)$;
  2. $\sigma = (i_1, i_2)(i_3, i_4) \cdots$ prodotto di trasposizioni disgiunte.
- Nel caso 1 $l(\sigma) \geq 5 \implies \exists\, i_4, i_5 \in M(\sigma) \setminus \{i_1, i_2, i_3\}$ distinti.
- Nel caso 2 $\exists\, i_5 \notin \{i_1, i_2, i_3, i_4\}$.
- $\tau := (i_3, i_4, i_5) \implies \tilde{\sigma} := \tau\sigma\tau^{-1} \in H$ e $\tilde{\sigma} \neq \sigma$ (nel caso 1 $\tilde{\sigma}(i_2) = i_4 \neq i_3 = \sigma(i_2)$ e nel caso 2 $\tilde{\sigma}(i_4) = i_5 \neq i_3 = \sigma(i_4)$).
- $\sigma' := \tilde{\sigma}\sigma^{-1} \in H \setminus \{1\}$ tale che $M(\sigma') \subseteq M(\sigma) \cup \{i_5\}$, $\sigma'(i_2) = i_2$ e nel caso 2 $\sigma'(i_1) = i_1$.
- $l(\sigma') < l(\sigma) = m$, assurdo.

Esercizio

Per un gruppo semplice non abeliano G sono equivalenti:

1. $\exists\, H < G$ tale che $[G : H] = 5$;
2. $G \cong A_5$;
3. $\#G = 60$.

Esercizio

Per un gruppo semplice non abeliano G sono equivalenti:

1. $\exists\, H < G$ tale che $[G : H] = 5$;
2. $G \cong A_5$;
3. $\#G = 60$.

1 $\implies$ 2 L'omomorfismo $L\colon G \to S(G/H) \cong S_5$ è iniettivo (perché G è semplice e $\ker(L) \subseteq H \subsetneq G$) $\implies$ $\exists\, G' < S_5$ tale che $G' \cong G$ semplice non abeliano $\implies$

$$n := \#G = \#G' \mid 120 = \#S_5 \quad \text{e} \quad \#G' \geq 60$$

$\implies$ $n = 60$ o $n = 120$. Non può essere $n = 120$ (se no $G \cong G' = S_5$ non semplice) $\implies$ $n = 60$ $\implies$ $[S_5 : G'] = 2$ $\implies$ $G' \triangleleft S_5$ $\implies$ $G \cong G' = A_5$.

2 $\implies$ 3 Ovvio.

Dimostrazione di 3 $\implies$ 1

$s_2 \mid 15$, $s_2 > 4$ (perché G semplice) $\implies$ $s_2 = 5$ o $s_2 = 15$.

- $s_2 = 5 \implies [G : H] = 5$ con H normalizzatore di un 2-Sylow.
- $s_2 = 15 \implies \exists\, K_1, K_2$ 2-Sylow distinti tali che $\{1\} \subsetneq K := K_1 \cap K_2$, perché altrimenti G conterrebbe $s_2(4-1) = 45$ elementi di ordine 2 o 4 (cioè gli elementi non banali dei 2-Sylow) e $s_3(3-1) = 20$ elementi di ordine 3 ($s_3 = 10$ perché $s_3 \mid 20$, $s_3 \equiv 1 \mod 3$ e $s_3 > 4$), assurdo, dato che $45 + 20 > 60$.
- $K \triangleleft K_i$ per $i = 1, 2$ (perché $\#K_i = 4$, quindi K_i è abeliano) $\implies$ $K_i < H := N(K)$ per $i = 1, 2$ $\implies$ $K_1 \subsetneq H$ (dato che $K_2 \not\subseteq K_1$) $\implies$ $[G : H] \mid [G : K_1]$, $[G : H] < [G : K_1] = 15$ e $[G : H] > 4$ $\implies$ $[G : H] = 5$.

Osservazione

In realtà a posteriori deve essere $s_2 = 5$: $V_4 \triangleleft A_4 < A_5$ $\implies$ $A_4 \subseteq N_{A_5}(V_4)$ $\implies$ $s_2 = [A_5 : N_{A_5}(V_4)] \leq [A_5 : A_4] = 5$.

Altri gruppi semplici

K campo, $n > 1$. Ricordiamo i seguenti gruppi (moltiplicativi):

- $\mathrm{GL}_n(K) := \{A \in \mathrm{M}_n(K) \,:\, \det(A) \neq 0\}$;
- $\mathrm{SL}_n(K) := \{A \in \mathrm{M}_n(K) \,:\, \det(A) = 1\} \triangleleft \mathrm{GL}_n(K)$ tale che $\mathrm{GL}_n(K)/\mathrm{SL}_n(K) \cong K^*$;
- $\mathrm{PSL}_n(K) := \mathrm{SL}_n(K)/Z(\mathrm{SL}_n(K))$ con $Z(\mathrm{SL}_n(K)) = \{a\mathrm{I}_n \,:\, a \in K,\ a^n = 1\}$.

Teorema

$n > 2$ *o* $\#K > 3 \implies \mathrm{PSL}_n(K)$ *è semplice.*

Osservazione

$\mathrm{PSL}_n(K)$ finito $\iff$ K finito. Se $\#K = q$, allora

- $\#\mathrm{GL}_2(K) = (q^2-1)(q^2-q) = (q-1)^2 q(q+1)$;
- $\#\mathrm{SL}_2(K) = \#\mathrm{GL}_2(K)/\#K^* = (q-1)q(q+1)$;
- $\#\mathrm{PSL}_2(K) = (q-1)q(q+1)/2$ se $1_K \neq -1_K$ (perché $Z(\mathrm{SL}_2(K)) = \{\pm\mathrm{I}_2\}$). In particolare $\mathrm{PSL}_2(\mathbb{Z}/p\mathbb{Z})$ è semplice per $p \geq 5$ primo e di ordine 60 se $p = 5$, 168 se $p = 7$.

Esercizio

G non abeliano, $60 < n := \#G < 168 \implies G$ non semplice.

- Dimostrare che n è della forma p^k, pq, p^2q, pqr (con p, q e r primi distinti) o che esiste p tale che $s_p \leq 5$ per n diverso da: 90, 112, 120, 132, 144, 150. Per ciascuno di questi valori di n assumere che G sia semplice e arrivare a un assurdo.

Esercizio

G non abeliano, $60 < n := \#G < 168 \implies G$ non semplice.

- Dimostrare che n è della forma p^k, pq, p^2q, pqr (con p, q e r primi distinti) o che esiste p tale che $s_p \leq 5$ per n diverso da: 90, 112, 120, 132, 144, 150. Per ciascuno di questi valori di n assumere che G sia semplice e arrivare a un assurdo.
- $n = 90, 120, 150 \implies s_5 = 6 \implies \exists\, H < G$ tale che $[G : H] = 6 \implies$ l'omomorfismo $L\colon G \to S(G/H) \cong S_6$ è iniettivo $\implies \exists\, G' < S_6$ tale che $G' \cong G$.
  Se $n = 150$ questo è impossibile perché $150 \nmid 720 = \#S_6$.
  Se $n = 90$ (risp. 120) $G' < A_6$ (altrimenti $[G' : G' \cap A_6] = 2$ $\implies G' \cap A_6 \lhd G'$, assurdo) e $[A_6 : G'] = 360/\#G' = 4$ (risp. 3), assurdo perché A_6 è semplice.

Esercizio

G non abeliano, $60 < n := \#G < 168 \implies G$ non semplice.

- Dimostrare che n è della forma p^k, pq, p^2q, pqr (con p, q e r primi distinti) o che esiste p tale che $s_p \leq 5$ per n diverso da: 90, 112, 120, 132, 144, 150. Per ciascuno di questi valori di n assumere che G sia semplice e arrivare a un assurdo.
- $n = 90, 120, 150 \implies s_5 = 6 \implies \exists\, H < G$ tale che $[G : H] = 6 \implies$ l'omomorfismo $L\colon G \to S(G/H) \cong S_6$ è iniettivo $\implies \exists\, G' < S_6$ tale che $G' \cong G$.
  Se $n = 150$ questo è impossibile perché $150 \nmid 720 = \#S_6$.
  Se $n = 90$ (risp. 120) $G' < A_6$ (altrimenti $[G' : G' \cap A_6] = 2 \implies G' \cap A_6 \lhd G'$, assurdo) e $[A_6 : G'] = 360/\#G' = 4$ (risp. 3), assurdo perché A_6 è semplice.
- $n = 112 = 2^4 \cdot 7 \implies [G : H] = 7$ (con H 2-Sylow) $\implies$ l'omomorfismo $L\colon G \to S(G/H) \cong S_7$ è iniettivo $\implies \exists\, G' < S_7$ tale che $G' \cong G \implies G' \not\subseteq A_7$ (perché $112 \nmid 2^3 \cdot 3^2 \cdot 5 \cdot 7 = \#A_7$) $\implies G' \cap A_7 \lhd G'$, assurdo.

Gruppi di ordine 132 e 144

- $n = 132 = 2^2 \cdot 3 \cdot 11 \implies s_{11} = 12$ e $s_3 = 22 \implies$ in G ci sono $s_{11}(11-1) = 120$ elementi di ordine 11 e $s_3(3-1) = 44$ di ordine 3, assurdo perché $120 + 44 > 132$.

Gruppi di ordine 132 e 144

- $n = 132 = 2^2 \cdot 3 \cdot 11 \implies s_{11} = 12$ e $s_3 = 22 \implies$ in G ci sono $s_{11}(11-1) = 120$ elementi di ordine 11 e $s_3(3-1) = 44$ di ordine 3, assurdo perché $120 + 44 > 132$.
- $n = 144 = 2^4 \cdot 3^2 \implies s_3 = 16 \implies \exists\, K_1, K_2$ 3-Sylow distinti tali che $\{1\} \subsetneq K := K_1 \cap K_2$, perché altrimenti G conterrebbe $s_3(9-1) = 128$ elementi di ordine 3 o 9 (cioè gli elementi non banali dei 3-Sylow) $\implies$ gli altri $144 - 128 = 16$ elementi formerebbero l'unico 2-Sylow, assurdo.
  $K \triangleleft K_i$ per $i = 1, 2$ (perché $\#K_i = 9$, quindi K_i è abeliano) $\implies K_i < H := N(K)$ per $i = 1, 2 \implies K_1 \subsetneq H$ (dato che $K_2 \not\subseteq K_1$) $\implies [G : H] \mid [G : K_1]$, $[G : H] < [G : K_1] = 16$ e $[G : H] > 4 \implies [G : H] = 8$ (dunque $\#H = 18$) $\implies$ $[H : K_i] = 2 \implies K_i \triangleleft H$ per $i = 1, 2$, assurdo perché K_1 e K_2 sarebbero due 3-Sylow distinti e normali di H.

Gruppi risolubili

Definizione

Un gruppo G è risolubile se esistono sottogruppi

$$\{1\} = K_r \triangleleft K_{r-1} \triangleleft \cdots \triangleleft K_1 \triangleleft K_0 = G$$

tali che K_{i-1}/K_i è abeliano $\forall\, i = 1, \ldots, r$.

Esempio

G è risolubile in ciascuno dei seguenti casi:

- G è abeliano ($r = 1$);
- $G = D_n$ ($r = 2$, $K_1 = \langle R \rangle$), quindi anche $G = S_3 \cong D_3$;
- $G = S_4$ ($r = 3$, $K_1 = A_4$, $K_2 = V_4$);
- $\#G = p^n$ ($r = n$ e per induzione $\exists\, K_i \triangleleft K_{i-1}$ tale che $\#K_i = p^{n-i}$).

Un gruppo semplice non abeliano (per esempio $A_n\ \forall\, n \geq 5$) non è risolubile.

Proprietà dei gruppi risolubili

Proposizione

1. $H < G$ *e* G *risolubile* $\implies$ H *risolubile.*
2. $H \triangleleft G$ *e* G *risolubile* $\implies$ G/H *risolubile.*
3. $H \triangleleft G$, H *e* G/H *risolubili* $\implies$ G *risolubile.*

Dimostrazione.

1. $\{1\} = K_r \triangleleft \cdots \triangleleft K_0 = G \implies K_i' := K_i \cap H$ per $i = 0, \ldots, r$ tali che $\{1\} = K_r' < \cdots < K_0' = H$. Inoltre $\forall\, i = 1, \ldots, r$

$$K_{i-1}' = K_{i-1} \cap H \xrightarrow{j_i} K_{i-1} \xrightarrow{p_i} K_{i-1}/K_i$$

(con j_i l'inclusione e p_i la proiezione) è un omomorfismo tale che $\ker(p_i \circ j_i) = K_i \cap H = K_i' \triangleleft K_{i-1}'$. Per il teorema di omomorfismo esiste $K_{i-1}'/K_i' \to K_{i-1}/K_i$ omomorfismo iniettivo, dunque K_{i-1}/K_i abeliano $\implies K_{i-1}'/K_i'$ abeliano.

Dimostrazione di 2 e 3

2. $\pi\colon G \to \overline{G} := G/H$ proiezione, $\{1\} = K_r \triangleleft \cdots \triangleleft K_0 = G \implies$ $\overline{K}_i := \pi(K_i)$ per $i = 0, \ldots, r$ tali che $\{\bar{1}\} = \overline{K}_r < \cdots < \overline{K}_0 = \overline{G}$. Inoltre $\forall\, i = 1, \ldots, r$ $\overline{K}_i \triangleleft \overline{K}_{i-1}$ (perché $\pi(g)\pi(a)\pi(g)^{-1} = \pi(gag^{-1}) \in \overline{K}_i$ $\forall\, g \in K_{i-1}$ e $\forall\, a \in K_i$, dato che $gag^{-1} \in K_i$) e

$$K_{i-1} \xrightarrow{\pi_i} \pi(K_{i-1}) = \overline{K}_{i-1} \xrightarrow{\bar{p}_i} \overline{K}_{i-1}/\overline{K}_i$$

(con π_i indotto da π e $\bar{p}_i$ la proiezione) è un omomorfismo suriettivo tale che $K_i \subseteq \ker(\bar{p}_i \circ \pi_i)$. Per il teorema di omomorfismo esiste un omomorfismo suriettivo $K_{i-1}/K_i \to \overline{K}_{i-1}/\overline{K}_i$, dunque K_{i-1}/K_i abeliano $\implies$ $\overline{K}_{i-1}/\overline{K}_i$ abeliano.

3. $\{1\} = K'_r \triangleleft \cdots \triangleleft K'_0 = H$ e $\{\bar{1}\} = \overline{K}_s \triangleleft \cdots \triangleleft \overline{K}_0 = \overline{G}$ (dove $\overline{K}_i = K_i/H$ con $H < K_i < G$ per $i = 0, \ldots, s$) $\implies$ $\{1\} = K'_r \triangleleft \cdots \triangleleft K'_0 = K_s \triangleleft \cdots \triangleleft K_0 = G$. Inoltre $\forall\, i = 1, \ldots, s$ $K_{i-1}/K_i \cong \overline{K}_{i-1}/\overline{K}_i$ per il terzo teorema di isomorfismo.

Conseguenze

- $G \cong H < S_4 \implies G$ risolubile.
- $n \geq 5 \implies S_n$ non risolubile:
  $A_n < S_n$ e A_n non è risolubile.
- $\#G = pq$ o p^2q (con p e q primi distinti) $\implies G$ risolubile:
  $\exists\, H \triangleleft G$ con H di Sylow, quindi H e G/H sono abeliani e pertanto risolubili.
- $\#G = pqr$ (con p, q e r primi distinti) $\implies G$ risolubile:
  $\exists\, H \triangleleft G$ con H di Sylow, quindi H è abeliano e G/H è risolubile per il punto precedente.
- $\#G < 60 \implies G$ risolubile:
  se G non è abeliano, $\exists\, H \triangleleft G$ non banale $\implies$ induttivamente H e G/H sono risolubili.
- $G = G_1 \times G_2$ risolubile $\iff G_1$ e G_2 risolubili:
  $G_1' := G_1 \times \{1\} \triangleleft G$ tale che $G_1' \cong G_1$ e $G/G_1' \cong G_2$.

Caratterizzazione dei gruppi risolubili

Ricordiamo che il sottogruppo dei commutatori di un gruppo G è

$$[G, G] := \langle aba^{-1}b^{-1} \ : \ a, b \in G \rangle \lhd G$$

tale che, se $H \lhd G$, allora G/H è abeliano $\iff [G, G] \subseteq H$.
Definendo $G^{(0)} := G$ e induttivamente $G^{(i)} := [G^{(i-1)}, G^{(i-1)}]$
$\forall\, i > 0$, si ha allora $G^{(i)} \lhd G^{(i-1)}$ e $G^{(i-1)}/G^{(i)}$ è abeliano $\forall\, i > 0$.

Proposizione

G è risolubile $\iff \exists\, r \in \mathbb{N}$ *tale che* $G^{(r)} = \{1\}$.

Dimostrazione.

$\Longleftarrow$ Chiaro.

$\Longrightarrow$ $\{1\} = K_r \lhd \cdots \lhd K_0 = G$ con K_{i-1}/K_i abeliano $\forall\, i = 1, \ldots, r$
$\Longrightarrow$ $G^{(i)} \subseteq K_i \ \forall\, i = 0, \ldots, r$ per induzione su i: vero se $i = 0$; se $i > 0$ per induzione $G^{(i-1)} \subseteq K_{i-1} \Longrightarrow$
$G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \subseteq [K_{i-1}, K_{i-1}] \subseteq K_i$
perché K_{i-1}/K_i è abeliano. Dunque $G^{(r)} = \{1\}$.