ALGO

WWW.ALGORITMOSTEM.IT

SCIENCE TECHNOLOGY ENGINEERING MATHEMATICS

Appunti di Algebra1: Teoremi di Sylow

UNI - Matematica

rev.0.1 - 05 set 2023

Draft version

Appunti in formato bozza, intesi esclusivamente di ausilio alle lezioni, che le integrano nelle descrizioni e nei ragionamenti su quanto viene riportato in queste pagine.

Licenza Creative Commons CCBYNCND.
È consentita la condivisone del documento originale a condizione che non venga modificato né utilizzato a scopi commerciali, sempre attribuendo la paternità dell'opera all'autore

Introduzione

Il teorema di Lagrange afferma che ogni sottogruppo di un gruppo finito ha ordine che divide l'ordine del gruppo stesso.
In generale non è possibile invertire il teorema, ma vale solamente in casi particolari.
Il primo teorema di Sylow pone le condizioni di tale validità

$A \subset G$ — Teorema LAGRANGE → — ← 1° Teorema di Sylow — $|A|$ divide $|G|$

G gruppo finito
$m = p^r$ divide $|G|$
p numero primo

→ ∃ sottogruppi G di ordine m

I teoremi II e III di Sylow forniscono dettagli sui sottogruppi

Se $m = p^r$ è la max potenza che divide $|G|$

→ I sottogruppi di G di ordine m sono coniugati tra loro

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it

I° Teorema di Sylow

G gruppo finito $|G|$ ordine (num. elementi)

$$\forall p, r \;/\; p^r \mid |G| \implies \exists A \subseteq G \;\; |A| = p^r$$

p: numero primo; r: intero; p^r divide $|G|$; A: sottoinsieme di G

ESEMPIO $|G| = 2^3 5^2 = 200 \implies$ $2^3 \mid 200 \;\; \exists A \subseteq G \;\; |A| = 2^3$

$5^2 \mid 200 \;\; \exists B \subseteq G \;\; |B| = 5^2$

II Teorema di Sylow

Fornisce una proprietà dei p-sylow

Def Si definisce p-sylow di G ogni sottogruppo di G di ordine p^k, con p numero primo e p^k la max potenza di p che divide $|G|$

($|G| = p^k \cdot m$ con m non divisibile per p)

ESEMPIO: $|G| = 2 \cdot 7^2 = 98 \;\; \exists$ 7-sylow $\;\; \exists$ 2-sylow

Teorema Sia G gruppo e $|G| = p^k \cdot m$ con p, m coprimi

Allora tutti i p-sylow sono coniugati

$$\forall H, K \in Syl_p(G) \;\; \exists g \in G \mid g^{-1} H g = K$$

$Syl_p(G)$: insieme dei p-sylow di G

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it

III Teoreme di Sylow

Fornisce informazioni sul numero dei p-Sylow.

Teorema Sia G gruppo e $|G| = p^k \cdot m$ con p, m coprimi

Allora: 1) $|Syl_p G| \mid m$ (divide) 2) $|Syl_p G| \equiv 1 \pmod p$

Esempio $|G| = 3 \cdot 5^2 \cdot 13 = 975$

Calcoliamo il num. di sottogruppi di G di ordine 25, ovvero la cardinalità dell'insieme dei 5-Sylow $|Syl_5(G)|$

$|G| = 5^{2} \cdot 3 \cdot 13$ (5^2: max, p; $m = 39$) $\Rightarrow$

- $|Syl_5(G)|$ divide $39 \rightarrow |Syl_5(G)| \in \{1, 3, 13, 39\}$
- $|Syl_5(G)| \equiv 1 \pmod 5$ $\longrightarrow |Syl_5(G)| = 1$

Def Un p-Sylow è NORMALE se è unico

$|Syl_p(G)| = 1 \iff p$-Sylow NORMALE

NB 1

> se G ha ordine pq, con p e q primi tali che $p < q$ e $p \nmid q - 1$ (non divide), allora G è ciclico.

ESEMPIO: $|G| = 7 \cdot 5 = 35$: $5 < 7$ e $5 \nmid (7-1) \Rightarrow G$ è ciclico

NB 2 $\forall$ gruppo Abeliano finito è prodotto di gruppi ciclici

NB 3 $\forall$ gruppo di ordine quadrato di un primo è Abeliano

ESEMPIO $|G| = 49 = 7^2 \Rightarrow G$ è abeliano

ESEMPIO $|G| = 64 = 8^2 \Rightarrow G$ non è abeliano

Applicazioni

Per "classificare" i gruppi di ordine n:

1) Si scompone n nel prodotto di numeri primi $n = p^k \cdot q^i$

2) Si applicano i teoremi di Sylow e si ottiene che $\exists$ i sottogruppi di Sylow: p-Sylow H, q-sylow K e sono normali (per ciascuno ne esiste uno)

3) Si deduce che G è isomorfo al prodotto diretto di H e K

4) Caratteristiche di H e K:
   ordine primo $\longrightarrow$ ciclici
   ordine quadrato di un primo $\rightarrow$ Abeliani (prodotto di ciclici)

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it

ESEMPIO:

Verificare se $\forall$ gruppo di ordine $3 \cdot 7 = 21$ è ciclico

da NB!: $|G| = p \cdot q$ primi $/ \; p < q \wedge p \nmid (q-1) \Rightarrow G$ ciclico

$|G| = 3 \cdot 7$ primi, $3 < 7 \wedge 3 \mid 6 \Rightarrow G$ non è ciclico

(o non si può dire)

ESEMPIO:

Dimostrare che $\forall$ gruppo di ordine $5 \cdot 7 = 35$ è ciclico

1) da NB!: $|G| = p \cdot q$ primi $/ \; p < q \wedge p \nmid (q-1) \Rightarrow G$ ciclico

$|G| = 5 \cdot 7$ primi, $5 < 7 \wedge 5 \nmid 6 \Rightarrow G$ è ciclico

2) altro modo:

III teor. Sylow $\rightarrow \left| Syl_5(G) \right| \mid 7 \wedge \left| Syl_5(G) \right| = 1 \pmod 5$

ovvero $\left| Syl_5(G) \right| = 1$ un sottogruppo H di ordine 5 (sottogruppo normale) ciclico (poiché $|H| = 5$ è primo)

III teor. Sylow $\rightarrow \left| Syl_7(G) \right| \mid 5 \wedge \left| Syl_7(G) \right| = 1 \pmod 5$

ovvero $\left| Syl_7(G) \right| = 1$ un sottogruppo K di ordine 7 (sottogruppo normale) ciclico (poiché $|K| = 7$ è primo)

5, 7 coprimi $\rightarrow H \cap K = 1 \quad H \cdot K = G$

ovvero G isomorfo al prodotto diretto interno $H \times K$

G ciclico poiché prodotto di $H \times K$ ciclici

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it

ESERCIZIO

Trovare un 3-Sylow di $\mathbb{Z}_{18}$

$|\mathbb{Z}_{18}| = 2 \cdot 3^2 = 18 \Rightarrow$ 3-Sylow unico sottogruppo di ordine 9 generato dall'elemento 2 (mod 18)

ESERCIZIO

Trovare i p-Sylow di S_3 (gruppo simmetrico su tre elementi) (permutazioni)

$|S_3| = 3! = 3 \cdot 2 = 6 \rightarrow$ 2-Sylow di ordine 2
3-Sylow di ordine 3

$\exists$ 3 2-Sylow, ciascuno generato da un ciclo di lunghezza 2 (disposizioni di 3 elementi a gruppi di due)

$\exists!$ 3-Sylow, ciclico, generato da un ciclo di lunghezza 3 (combinazioni di tre elementi)

LGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it

ESERCIZIO

Provare che $\forall$ gruppo con 105 elementi possiede un unico 5-Sylow oppure un unico 7-Sylow

$$|G| = 105 = 3 \cdot 5 \cdot 7$$

III Teorema Sylow $\rightarrow$ $|Syl_5(G)| \mid 21 \wedge |Syl_5(G)| = 1 \pmod 5$ (3·7)

$\in \{1,3,7,21\} \wedge 1 \pmod 5$

ovvero $|Syl_5(G)| \in \{1, 21\}$

III Teorema Sylow $\rightarrow$ $|Syl_7(G)| \mid 15 \wedge |Syl_7(G)| = 1 \pmod 7$ (3·5)

$\in \{1,5,15\} \wedge 1 \pmod 7$

ovvero $|Syl_5(G)| \in \{1, 15\}$

Poiché 5 e 7 sono coprimi, $5\text{-Sylow} \cap 7\text{-Sylow} = \{1_G\}$ quindi 5-Sylow e 7-Sylow devono essere normali, altrimenti risulterebbe un numero maggiore di elementi di G. (verificare)

$$|Syl_5(G)| = 1 \qquad |Syl_7(G)| = 1$$

ALGO - licenza d'uso creative common CCBYNCND - www.algoritmostem.it