UNIVERSITÀ DEGLI STUDI DI CAGLIARI
Facoltà di Scienze
Corso di Laurea Triennale in Matematica

Sugli Ordini dei Sottogruppi di Gruppi Abeliani: Una Soluzione Elementare per un Esercizio di Herstein

Candidata
Francesca Paola Siddi

Relatore
Andrea Loi

Se un gruppo abeliano ha due sottogruppi di ordine m e n, rispettivamente, mostrare che allora ha un sottogruppo il cui ordine è il minimo comune multiplo di m e n

Esercizio 26. Topics in Algebra, Herstein

- **Lemma**: Se $a, b \epsilon \mathbb{Z}$ e non sono entrambi nulli allora $\exists\ (a, b)$ e $\exists\ s, t \epsilon \mathbb{Z}$ tali che $(a, b) = as + bt$
- **Corollario**: Se $(a, b) = 1$, allora $\exists\ s, t \epsilon \mathbb{Z}$ tali che $1 = as + bt$

- **Lemma**: $\forall\ a, b, c \epsilon \mathbb{Z}$ se $(a, b) = 1$ e $a|bc$, allora $a|c$

- **Teorema**: Ogni intero a>1 ammette un'unica fattorizzazione del tipo $a = p_1^{\alpha_1} p_2^{\alpha_2} .. p_t^{\alpha_t}$ dove $p_1 > p_2 > .. > p_t$ sono primi e $\alpha_i > 0\ \forall\ i=1,\dots,t$

- **Lemma**: Se H è un sottoinsieme finito e non vuoto di un gruppo G ed è chiuso rispetto al prodotto, allora $H \leq G$

- **Teorema di Lagrange**: Se G è un gruppo finito e $H \leq G$, allora $|H| \,\big|\, |G|$

- **Lemma**: Se $H, K \leq G$, allora $HK \leq G \iff HK = KH$
- **Corollario**: Se $H, K \leq G$ e G è abeliano, allora $HK \leq G$

- **Teorema**: Se H, K sono sottogruppi finiti di un gruppo G, allora $|HK| = \frac{|H||K|}{|H \cap K|}$

- Sia $x \epsilon G$ e $|x| = m \epsilon \mathbb{N}_+$, allora: $x^k = 1 \Leftrightarrow m|k$, $\forall k \in \mathbb{N}_+$

- Sia $x \epsilon G$ allora: $|x| = |\langle x \rangle|$

- Sia G un gruppo finito e $x \epsilon G$, allora $x^{|G|} = 1$

Sia $\boldsymbol{G}$ un gruppo abeliano e $\boldsymbol{H, K \leq G}$, con $\boldsymbol{|H| = m}$ e $\boldsymbol{|K| = n}$. Allora $\boldsymbol{\exists X \leq G}$ tale che $\boldsymbol{|X| = [m, n]}$

1) *Ogni sottogruppo di ordine finito di un gruppo abeliano può essere scritto come prodotto di sottogruppi di ordine pari a potenze di primi distinti tra loro*

Considerato H ,con $|H| = m$. Per il

Teorema: Ogni intero a>1 ammette un'unica fattorizzazione del tipo $a = p_1^{\alpha_1} p_2^{\alpha_2} .. p_t^{\alpha_t}$ dove $p_1 > p_2 > .. > p_t$ sono primi e $\alpha_i > 0$ $\forall$ *i=1,…,t*

Non è restrittivo supporre $|H| = ab$ con $(a, b) = 1$

Corollario: Se $(a, b) = 1$, allora $\exists\ s, t \in \mathbb{Z}$ tali che $1 = as + bt$

$\Rightarrow \exists\ s, t \in \mathbb{Z}$ tali che $1 = as + bt$

$$H_1 = \{x | x = h^a, h \epsilon H\}$$

$$H_2 = \{y | y = h^b, h \epsilon H\}$$

Lemma: Se H è un sottoinsieme finito e non vuoto di un gruppo G ed è chiuso rispetto al prodotto, allora $H \leq G$

$$\Rightarrow H_1, H_2 \leq H$$

$$\forall\, h \in H, \quad h = h^1 = h^{as+bt} = h^{as} h^{bt} = (h^s)^a (h^t)^b = xy \Rightarrow H = H_1\, H_2$$

$$\forall\, x \,\epsilon H_1, \quad x^b = (h^a)^b = h^{ab} = h^{|H|} = 1 \qquad \Rightarrow |x| \big| b \qquad \Rightarrow (|x|, a) = 1$$

Si può allora considerare S sottogruppo massimale di H_1, con $(|S|, a) = 1$

$$\Rightarrow S = H_1$$

Per assurdo: $\exists x \in H_1 \setminus S$

Corollario: Se $H, K \leq G$ e G è abeliano, allora $HK \leq G$

$\Rightarrow \langle x \rangle S < H_1$

Teorema: Se H, K sono sottogruppi finiti di un gruppo G, allora $|HK| = \frac{|H||K|}{|H \cap K|}$

$\Rightarrow |\langle x \rangle S| = \dfrac{|\langle x \rangle||S|}{|\langle x \rangle \cap S|}$ $\Rightarrow (|\langle x \rangle S|, a) = 1$ $\Rightarrow S < \langle x \rangle S < H_1$

Contraddice l'ipotesi di massimalità di S!

$$\Rightarrow S = H_1 \Rightarrow (|H_1|, a) = 1$$

Teorema di Lagrange: Se G è un gruppo finito e $H \leq G$, allora $|H|\big||G|$

$$|H_1|\big||H| = ab$$

Lemma: $\forall\ a, b, c \in \mathbb{Z}$ se $(a, b) = 1$ e $a|bc$, allora $a|c$

$$\Rightarrow |H_1|\big|b$$

$$\Rightarrow (|H_1|, |H_2|) = 1$$

$$\Rightarrow |H_2|\big|a$$

Iterando il procedimento su H_1, H_2 si ottiene che:

H può essere scritto come prodotto di sottogruppi di ordini pari a potenze di primi distinti tra loro

$\Rightarrow H, K$ possono essere scritti come prodotti di sottogruppi di ordini pari a potenze di primi distinti tra loro

2) Dati due sottogruppi di ordini finiti e primi tra loro, l'ordine del prodotto dei sottogruppi è pari al prodotto dei due ordini

Considerati di nuovo $H_1, H_2 \leq H$, $(|H_1|, |H_2|) = 1$ sappiamo che

$$|H_1 H_2| = \frac{|H_1||H_2|}{|H_1 \cap H_2|}$$

Per Lagrange:

- $H_1 \cap H_2 \leq H_1 \Rightarrow |H_1 \cap H_2| \big| |H_1|$
- $H_1 \cap H_2 \leq H_2 \Rightarrow |H_1 \cap H_2| \big| |H_2|$

$\Rightarrow |H_1 \cap H_2| = 1$

$$\Rightarrow |H_1 H_2| = |H_1||H_2|$$

Sfruttando ora il seguente

Corollario: Se $H, K \leq G$ e G è abeliano, allora $HK \leq G$

Si ottiene che inoltre $H_1 H_2 \leq H$ e, poiché questo vale per tutte le coppie di sottogruppi che fattorizzano H, si può affermare che:

Il prodotto degli ordini dei sottogruppi che fattorizzano H è pari all'ordine di H stesso

$\Rightarrow H, K$ possono essere scritti come prodotti di sottogruppi di ordini pari a potenze di primi distinti tra loro e il prodotto di tali ordini eguaglia gli ordini di H, K

3) Conclusione

Per il teorema di fattorizzazione degli interi:

$$[m,n] = p_1^{\alpha_1} p_2^{\alpha_2} .. p_t^{\alpha_t}$$

Con $p_1 > p_2 > .. > p_t$ primi e $\alpha_i > 0$ $\forall$ *i=1,…,t*

$$\Rightarrow \begin{cases} |H_i| = p_i^{\beta_i} & \text{con } 0 \le \beta_i \le \alpha_i \text{ e } \beta_i = 0 \Leftrightarrow p_i \nmid m \\ |K_i| = p_i^{\gamma_i} & \text{con } 0 \le \gamma_i \le \alpha_i \text{ e } \gamma_i = 0 \Leftrightarrow p_i \nmid n \end{cases}$$

$$\Rightarrow |H_i| = p_i^{\alpha_i} \lor |K_i| = p_i^{\alpha_i}$$

$\forall\ i=1,\dots,t\ \ \exists X_i \leq G$ tale che $|X_i| = p_i^{\alpha_i}$.

Detto allora $X = X_1X_2 \dots X_t \leq G$ si ha

$$|X| = |X_1X_2 \dots X_t| = |X_1||X_2| \dots |X_t| = p_1^{\alpha_1}p_2^{\alpha_2}..p_t^{\alpha_t} = [m,n]$$

Come dovevasi dimostrare.