תזכורת:

p ראשוני, G חבורה סופית $|G|=p^k m$ $(p \nmid m)$

תת חבורה $P\le G$ הינה תת חבורה p-סילו אם $|P|=p^k$

משפטי סילו:

1) לכל p, קיימת תת חבורה p-סילו. לכל p-תת חבורה H של G קיימת p-סילו $P\le G$ $P\le G$ כך ש $H\le P$

2) כל תתי חבורות p-סילו צמודות זו לזו

3) יהי n_p מספר תתי חבורות p-סילו $n_p | m$, $n_p \equiv 1 \mod p$

הוכחנו:

1) תהי G חבורה סופית $H \trianglelefteq G$ תת חבורה נורמלית. תהי $P \trianglelefteq H$ תת חבורה p-סילו נורמלית אזי $P \trianglelefteq G$

2) תהי G חבורה $|G|=30$ אזי יש ל-G תת חבורה 5 סילו נורמלית

טענה:

תהי G חבורה מסדר $|G|=12$, אזי יש לG תת חבורה 3-סילו נורמלית או תת חבורה 2-סילו נורמלית

הוכחה:

לפי סילו 3 $n_3 = 1 \mod 3, n_3 | 4 \Leftarrow n_3 = 1 \vee 4$

$12=2^2\cdot 3$, לכן $n_2 \equiv 1 \mod 2, n_2 | 3 \Leftarrow n_2 = 1 \vee 3$

אם $n_2=1$ או $n_3=1$ אז סיימנו

נניח בשלילה כי $n_2=3$, $n_3=4$

אז יש 4 תתי חבורות 3-סילו. הסדר של כל אחת הוא 3, לכן לכל אחת יש שני איברים מסדר 3. וגם ש. אבל החיתוכים טריוויאלים

סה"כ ב-G יש 8 איברים מסדר 3. בפרט, יש רק 4 איברים שאינם מסדר 3
כל תת חבורה 2-סילו, אך $n_2=3$, ולפי לגרנז' תת חבורה מסדר 4 לא
יכולה להכיל איבר מסדר 3.
לכן, תת חבורה מסדר 4 תופסת את כל האיברים מסדר $\neq 3$, אז אין
מקום לשלוש תתי חבורות כאלה. בסתירה.

תזכורת:
יהי p,q ראשוניים שונים. נניח $p<q$. לכל חבורה מסדר pq^k, $k\geq 1$, יש
תת חבורה q סילו נורמלית.

הגדרה: חבורה G נקראת פשוטה אם אין לה תתי חבורות נורמליות
מלבד $G,\{e\}$.

טענה:
תהי G חבורה מסדר $|G|=60$. נניח שתתי החבורות 5-סילו של G לא
נורמליות. אזי, G פשוטה.

הוכחה:
נניח בשלילה שיש תת חבורה נורמלית לא טריוויאלית $H \trianglelefteq G$
נניח כי $5 \mid |H|$, אזי ל-H יש תת חבורה 5-סילו. אבל $60=5\cdot 12$
ולכן כל חבורה 5-סילו של H היא מסדר 5 ולכן הינה גם תת חבורה 5-סילו של G
n_5 - מספר תתי החבורות 5-סילו של G
לפי משפט סילו השלישי $n_5 \mid 12$, $n_5 \equiv 1 \mod 5$ $\Leftarrow$ $n_5=1,6$
$n_5\neq 1$ כי תתי החבורות 5-סילו של G לא נורמליות $\Leftarrow$ $n_5=6$
לפי סילו 2, כל שתי תתי החבורות 5-סילו של G צמודות. אך $5 \mid |H|$, לכן H
מכילה אחת מהן. אבל $H\trianglelefteq G$, לכן H סגורה להצמדה, ולכן H חייבת להיות
להכיל את כל תתי החבורות 5-סילו של G. בכל אחת יש 4 איברים מסדר

5, ועם e. החיתוכים טריוויאליים. סה"כ יש 24 איברים מסדר 5. כולם

מוכלים ב-H. לכן $|H|\geq 24$. לפי לגרנז' $|H| \mid 60$. אז בהכרח $|H|=30$

אבל לפי הטענה מהשיעור הקודם, לכל חבורה מסדר 30 יש תת חבורה

5-סילו יחידה, אבל ל-H יש 6 תתי חבורות 5-סילו. בסתירה.

לכן $5 \nmid H$. זה אומר ש $|H| \mid 12$. לכן $|H| \in \{2,3,4,6,12\}$. אם $|H|=12$ אזי,

לפי הטענה הראשונה של היום, יש תת חבורה 3-סילו, P, נורמלית מסדר 3 או 4.

מהטענה שהזכרנו בתחילת השיעור, $P \trianglelefteq G$. אז בהכרח יש ל-G תת חבורה

נורמלית מסדר $2,3,4,6$, נקרא לה H.

תת טענה: לחבורה המנה G/H יש תת חבורה 5-סילו נורמלית

הוכחה:

נעבור על כל האפשרויות.

$|H|=2$: אזי $|G/H|=30$, ולפי טענה מהפעם הקודמת יש ל-G/H תת חבורה 5-סילו נורמלית.

$|H|=3$: אזי $|G/H|=20$. לפי סילו 3, יהי n_5' מספר תתי החבורות 5-סילו של G/H $n_5' \mid 20,\ n_5' \equiv 1 \bmod 5 \Leftarrow n_5'=1$, לכן יש תת חבורה 5-סילו נורמלית.

$|H|=4$: אזי $|G/H|=15=5\cdot 3=pq$, לכן יש תת חבורה 5-סילו נורמלית

$|H|=5$: אזי $|G/H|=10=2\cdot 5=pq$, לכן יש תת חבורה 5-סילו נורמלית

לפי משפט האיזומורפיזם הרביעי, תת החבורה הנורמלית 5-סילו של G/H

(בכל מקרה הסדר שלה הוא 5) מתאימה לתת חבורה נורמלית $H \leq k \trianglelefteq G$

$[k:H]=[k/H : H/k]=[P:\{e_{G/H}\}]=5$. לכן $|k|=5\cdot|H|<60$

מצאנו תת חבורה נורמלית לא טריוויאלית (ואמיתית $\neq G$) $K \trianglelefteq G$ כך ש $5 \mid |K|$

בסתירה להנחה שאין תת חבורה נורמלית כזאת. בסתירה

לכן G פשוטה

תוצאה:

החבורה A_5 אינה פשוטה

הוכחה:

$|A_5| = \frac{5!}{2} = 60$ לפי הטענה הקודמת, מספיק להוכיח כי ל-A_5 אין תת חבורה 5-סילו נורמלית. נתבונן בתת החבורה

$$H = \langle (12345) \rangle = \{e, (12345), (13524), (14253), (15432)\}$$

אזי $|H| = 5$, לכן H היא תת חבורה 5-סילו של A_5. נשים לב כי

$$(12453) = (345)(12345)(345)^{-1}$$

H לא סגורה להצמדה, לכן לא נורמלית

טענה:

תהי G חבורה שפועלת על הקבוצה A. יהי $a \in A$, ויהי $b \in A$ איבר באותו מסלול, כלומר קיים $g \in G$ כך ש $b = g * a$. אזי $G_b = g G_a g^{-1}$

הוכחה:

יהי $h \in g G_a g^{-1}$. אזי, $h = gkg^{-1}$ כאשר $k \in G_a$. אזי

$$h * b = (gkg^{-1}) * (g * a) = gk * a = g * a = b$$

לכן $g G_a g^{-1} \subseteq G_b$

מצד שני, $a = g^{-1} * b$, לכן $g^{-1} G_b g \subseteq G_a \Leftarrow G_b \subseteq g G_a g^{-1}$ לכן $G_b = g G_a g^{-1}$

משפט:

החבורה A_n פשוטה לכל $n \geq 5$

הוכחה:

A_5 פשוטה

נניח ש A_{n-1} פשוטה עבור $n \geq 5$ ונוכיח כי A_n פשוטה.

יש פעולה טבעית של A_n על הקבוצה $\{1,\dots,n\}$ (רואים את האיברים של A_n כתמורות). הפעולה הזאת טרנזיטיבית. אכן, יהיו $a \neq b$ איברים של $\{1,\dots,n\}$. יהי c איבר אחר, שונה מ- a,b

אזי $\sigma = (a\,b\,c) \in A_n$ וברור כי $\sigma * a = \sigma(a) = b$
תמורה זוגית

לכל $i \in \{1,\dots,n\}$ נגדיר $G_i = Stab(i) = \{\sigma \in A_n : \sigma(i) = i\}$

לפי הטענה שהוכחנו לפני ההפסקה, הפעולה טרנזיטיבית $\Leftarrow G_1,\dots,G_n$ כולם צמודים זה לזה.

<u>צעד 1:</u> לכל $i \in \{1,\dots,n\}$, $G_i \simeq A_{n-1}$

הוכחה:

כל איבר של G_i קובע את i, אז בעצם הוא תמורה זוגית של הקבוצה $\{1,\dots,i-1,i+1,\dots,n\}$

הוכחה פורמלית:

$A_{n-1} \to G_n$

$\tau \in A_{n-1} \mapsto \sigma \qquad \sigma(i) = \begin{cases} \tau(i) & i \leq n-1 \\ n & i = n \end{cases}$

קל לראות שזה איזומורפיזם. לכן $G_n \simeq A_{n-1}$. לכל $k \in \{1,\dots,n\}$ G_k, G_n צמודות וכפרט איזומורפיות. לכן $G_k \simeq G_n \simeq A_n$

מסקנה: $G_1,\dots,G_n$ כולן פשוטות (לפי הנחת האינדוקציה)

צעד ב: תת החבורות $G_1, \ldots, G_n$ יוצרות את A_n, כלומר כל איבר של A_n הינו מכפלה של איברים של $G_1 \cup G_2 \cup \ldots \cup G_n$

הוכחה:

כל איבר $\sigma \in A_n$ הוא תמורה זוגית, לכן ניתן להציג את σ כמכפלה של מספר זוגי של חילופים

$\sigma = (a_1\, a_2)(a_3\, a_4) \ldots (a_{2k-1}\, a_{2k})$ k זוגי, יהי

$\tau_1 = (a_1\, a_2)(a_3\, a_4)$

$\tau_2 = (a_5\, a_6)(a_7\, a_8)$

$\vdots$

$\tau_{\frac{k}{2}} = (a_{2k-3}\, a_{2k-2})(a_{2k-1}\, a_{2k})$

$\sigma = \tau_1 \ldots \tau_{\frac{k}{2}}$

כל τ_i הינו מכפלה של שני חילופים, לכן שייך ל-A_n. בכל $\tau_i = (a_{4i-3}\, a_{4i-2})(a_{4i-1}\, a_{4i})$ מופיעים לכל היותר 4 מספרים שונים. כיוון ש $n \geq 5$, יש $\ell \in \{1, \ldots, n\}$ שלא מופיע ב- τ_i. לכן $\tau_i(\ell) = \ell \Leftarrow \tau_i \in G_\ell$

צעד ג: תהי $H \trianglelefteq A_n$ תת חבורה (מוכלת ממש ב-A_n) אזי $H \cap G_i = \{e\}$ לכל $1 \leq i \leq n$

הוכחה:

לפי משפט האיזומורפיזם השני $H \cap G_i \trianglelefteq G_i \Leftarrow H \trianglelefteq A_n$

לפי צעד 1, ידוע כי $G_i \cong A_{n-1}$ ולכן פשוטה. זה אומר ש $H \cap G_i = \{e\}$ או $H \cap G_i = G_i$

אם $H \cap G_i = G_i$, אזי $G_i \leq H$, אך H נורמלית, לכן H סגורה להצמדה, ולכן H מכילה את כל תתי החבורות $G_1, \ldots, G_n$

כי כולן צמודות ל-G_i. ובכלל H סגורה לכפל ולפי צעד 2
$H=A_n$, בסתירה להנחה כי H מוכלת ממש ב-A_n.
לכן, $H\cap G_i=\{e\}$ לכל $1\le i\le n$

צעד 4: תהי H כנ"ל. יהיו $\sigma,\tau\in H$. אם קיים $1\le k\le n$ כך ש $\sigma(k)=\tau(k)$
אזי $\sigma=\tau$

הוכחה:

נתבונן באיבר $\sigma^{-1}\tau\in H$. אזי, $\sigma^{-1}(\tau(k))=\sigma^{-1}(\sigma(k))=k$
לכן, $\sigma^{-1}\tau\in G_k\cap H\underset{\text{צעד 3}}{=}\{e\}$. לכן, $\sigma=\tau \Leftarrow \sigma^{-1}\tau=e$

צעד 5: יהי $\sigma\in H$. נרשום את σ כמכפלה של מחזורים זרים.
ב-σ לא מופיעים מחזורים מאורך 3 או יותר. כלומר, σ הינו
מכפלה של חילופים זרים.

הוכחה:

נניח בשלילה כי יש ב-σ מחזור באורך 3 או יותר
$\sigma=(a\,b\,c\,\dots)(\text{מחזורים זרים})$
יהי $1\le d,e\le n$ שונים מ-a,b,c ($n\ge 5$ ולכן קיימים כאלה)
אזי $\tau=(c\,d\,e)\in A_n$. אך H נורמלית, לכן
$\rho=\tau\sigma\tau^{-1}=(a\,b\,d\dots)(\text{מחזורים זרים})\in H$

נשים לב כי $\sigma(a)=\rho(a)=b$, לכן $\sigma=\rho$ לפי הצעד הקודם.
מצד שני, $\rho(b)=d\ne c=\sigma(b)$ ולכן $\sigma\ne\rho$.

צעד 6: תהי $H\trianglelefteq A_n$ תת חבורה נורמלית (ומוכלת ממש ב-A_n)
אזי $H=\{e\}$. כלומר A_n פשוטה

הוכחה:

תהי $H \trianglelefteq A_n$ תת חבורה נורמלית ואמיתית (מוכלת ממש)

נניח בשלילה שקיים $e \neq \sigma \in H$. לפי הצעד הקודם, σ הינו מכפלה של שיקופים (חילופים) זרים.

מצד שני, $\sigma \in A_n$, לכן σ הינו מכפלה של לפחות שני שיקופים זרים. כלומר ש- $\sigma = (a\,b)(c\,d)$ (מכפלה של שיקופים זרים אולי)

שוב, יהי $1 \le f \le n$ שונה מ a,b,c,d אזי $\tau = (c\,d\,f) \in A_n$

$\rho = \tau\sigma\tau^{-1} = (a\,b)(d\,f)(\text{שיקופים זרים}) \in H$

אזי $\sigma(a) = b = \rho(a) \Leftarrow \sigma = \rho$ לפי 4

אבל $\rho(d) = f \neq c = \sigma(d)$, לכן $\rho \neq \sigma$ בסתירה. לכן H טריוויאלית

מסקנה:

יהי $n \in \mathbb{N}$. אזי A_n פשוטה $\iff n \neq 4$

הוכחה:

$|A_4| = 12$ והוכחנו היום שבהכרח יש תת חבורה 2-סילו או 3-סילו נורמלית. הוכחנו גם $\{e,(1\,2)(3\,4),(1\,3)(2\,4),(1\,4)(2\,3)\} \trianglelefteq A_4$

לכן A_4 אינה פשוטה

אם $n \ge 5$, הוכחנו כי A_n פשוטה.

אם $n = 3$ אזי $|A_3| = 3$, הסדר שלה ראשוני, לכן לפי לגרנז' אין תתי חבורות מלבד A_3 ו- $\{e\}$

אם $n = 1$ או 2 אזי $A_n = \{e\}$, ברור שפשוטה.

טענה:

יהי $n\geq 5$. אזי תתי החבורות הנורמליות היחידות של S_n הינן $S_n, A_n, \{e\}$

הוכחה:

$A_n = \ker(sgn: S_n \to \{\pm 1\})$, לכן $A_n \trianglelefteq S_n$.

תהי $H \trianglelefteq S_n$ תת חבורה נורמלית. נניח כי $H \neq S_n$ אזי $H\cap A_n \trianglelefteq A_n$

ובגלל A_n פשוטה, לכן $H\cap A_n = A_n$ או $H\cap A_n = \{e\}$

אם $H\cap A_n = A_n$, זה אומר $A_n \leq H \Leftarrow [S_n : H] \leq 2$ אבל $H \neq S_n \Leftarrow$

$[S_n : H] = 2 \Leftarrow H = A_n$

אז נניח $H\cap A_n = \{e\}$. לכן כל איבר לא טריוויאלי של H הוא תמורה

אי זוגית. יהיו $h_1, h_2 \in H$ לא טריוויאלים. אזי הם אי זוגיים. המכפלה

$h_1 h_2$ היא זוגית, לכן $h_1 h_2 = e$. אם h_1, h_2 איברים לא טריוויאליים

של H אזי $h_1 h_2 = h_1 h_1 = e \Leftarrow h_2 = h_1$

זה אומר שב-H יש לכל היותר איבר לא טריוויאלי 1, כלומר $|H| = 1$

או $|H| = 2$.

אם $|H| = 2$, אז $H = \{e, \sigma\}$, כאשר σ הוא מכפלה של שיקופים זרים

$\sigma = (a\ b)$ (שיקופים זרים)

$\tau = (b\,c)\sigma(b\,c)^{-1} = (a\ c)$ (שיקופים זרים) $\in H$

כי $H \trianglelefteq S_n$. ובגלל $c \neq a \Leftarrow \tau \neq e$

$c \neq b \Leftarrow \tau \neq \sigma$

לכן $\tau \in H$ בסתירה. לכן $|H| = 1$, כלומר $H = \{e\}$

הגדרה: תהי G חבורה (לאו דווקא סופית) סדרה תת-נורמלית של G

היא סדרה סופית של תת חבורות

$\{e\} = G_0 \leq G_1 \leq \dots \leq G_r = G$

כך ש $G_i \trianglelefteq G_{i+1}$ לכל $0 \le i \le r-1$

דוגמא:

$$\underbrace{\{e\}}_{G_0} \trianglelefteq \underbrace{\{e,(12)(34)\}}_{G_1} \trianglelefteq \underbrace{\{e,(12)(34),(13)(24),(14)(23)\}}_{G_2} \trianglelefteq \underbrace{A_4}_{G_3} \trianglelefteq \underbrace{S_4}_{G_4}$$

זו סדרה תת נורמלית של S_4. נשים לב כי $G_1 \ntrianglelefteq S_4$

הגדרה: סדרה תת נורמלית של G נקראת סדרת הרכב אם כל מנה G_{i+1}/G_i היא חבורה פשוטה (במילים אחרות, סדרה תת נורמלית מקסימלית)

הערה: לא לכל חבורה G יש סדרת הרכב. לדוגמא לחבורה $\mathbb{Z}$ אין סדרת הרכב

אכן, נניח $\{e\} \trianglelefteq G_1 \dots \trianglelefteq G_r = \mathbb{Z}$ היא סדרת הרכב

אז G_1 תת חבורה לא טריוויאלית של $\mathbb{Z}$.

זה אומר שקיים $n \in \mathbb{N}$ כך ש $G_1 = n\mathbb{Z}$ אבל $G_1/G_0 = n\mathbb{Z}$ לא פשוטה

כי $2n\mathbb{Z} \trianglelefteq G_1/G_0$

משפט (ז'ורדן-הלדר):

תה"נ $\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_s = G$

$\{e\} = \tilde{G}_0 \trianglelefteq \tilde{G}_1 \trianglelefteq \dots \trianglelefteq \tilde{G}_s = G$

שתי סדרות הרכב של G (אם קיימות כאלה) אז $r=s$ ויש לכן את

אותן המנות עד כדי תמורה

$$\{G_1/G_0, \dots, G_r/G_{r-1}\} = \{\tilde{G}_1/\tilde{G}_0, \dots, \tilde{G}_r/\tilde{G}_{r-1}\}$$