

(1) באגודה X סופית יש לפחות אדמ' אחד.

הוכחה: כיוון ש- X סופית קיימת לה $K \leq X$ תת-אגודה מינימלית (כך ש: $\emptyset \neq k_1 \leq k \rightarrow k_1 = k$) יהא $a \in K$ אזי $aK = \{ak : k \in K\} \leq K$ אבל K מינימלית ולכן $aK = K$.

מכאן שהקבוצה $A = \{k \in K, ak = a\}$ אינה ריקה.

נשים לב כי $A \leq K$, נראה סגירות:

$$k_1, k_2 \in A : ak_1 = a, ak_2 = a \rightarrow ak_1k_2 = ak_2 = a \rightarrow k_1 * k_2 \in K$$

שוב מתוך המינימליות נסיק כי $A=K$, מכאן שיש לפחות אדמ' אחד.

(2) מופיע בסוף.

(3) משפט ווילסון – Wilson

מספר טבעי $n > 1$ הוא מספר ראשוני אם $(n-1)! \equiv (-1) \pmod{n}$

הוכחה

בכיוון האחד: עבור $n = p > 1$ ראשוני חבורת אוילר היא: $U_p = 1, 2, \dots, p-1$. כל איבר $a \in U_p$ ההפוך לעצמו מקיים:

$$a^2 - 1 = (a-1)(a+1) \equiv 0 \pmod{p}$$

ממנו. לכן כיוון שהחבורה אבלית, במכפלת האיברים $m = (p-1)!$ האיבר היחיד שאינו מצטמצם (ע"י סידור כל איבר ליד

$$\text{ההופכי שלו) הוא: } m = p-1 \equiv (-1) \pmod{p}.$$

בכיוון ההפוך: נניח בשלילה כי n אינו ראשוני. אם $n = 4$ קל לבדוק כי: $(4-1)! = 6 \equiv 2 \pmod{4}$. סתירה.

עבור $n > 4$: כיוון ש- n אינו ראשוני, ישנו לפחות מספר אחד $1 < a \leq n-1$ שמחלק את n .

$$\text{אם: } a = \sqrt{n} \text{ אזי: } 4 < n \Leftrightarrow 2 < a \Leftrightarrow 2a < a^2 = n \Leftrightarrow 2a < a, 2a \text{ מופיעים כ"א במכפלה } (n-1)! \text{ ומכפלתם}$$

מאפסת אותה בסתירה לנתון.

אחרת (a אינו שורש של n) מתקיים: $\exists 0 < a \neq b < n : a \cdot b \equiv 0 \pmod{n}$. לכן ab מופיע במכפלה: $(n-1)!$ ושוב

מאפסת אותה בסתירה לנתון.

$$[G:H] = \frac{|G|}{|H|} \quad \text{משפט לגרנז': תהא } G \text{ חבורה סופית, אזי לכל ת"ח } H \leq G \text{ מתקיים} \quad (4)$$

הוכחה

לכל $a \in G$ נגדיר את ההעתקה $\varphi_a = H \rightarrow Ha$ לא כתבת מאיפה לאיפה ההעתקה מוגדרת

$$h_1 a = h_2 a \Rightarrow h_1 = h_2$$

וההעתקה חח"ע שכן $|H| = |Ha|$ ולכן (מעצם הגדרתו) $|H| = |Ha|$.

כיוון שהקוסטים הם מחלקות שקילות, G הוא איחוד זר שלהם ולכן $|G| = [G:H]|H|$

(5) משפט אוילר

$$\forall a \in \mathbb{Z}^*, n \in \mathbb{N} : (a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

הוכחה

$$(a, n) = 1 \Rightarrow a \equiv a' \in U_n \Rightarrow a^{\varphi(n)} \equiv a'^{|U_n|} = 1$$

(6) משפט האיזומורפיזם הראשון:

אם $\varphi: G \rightarrow H$ אפימורפיזם אז קיים איזומורפיזם $\psi: G/\ker(\varphi) \cong H$ כך ש $\varphi = \psi \circ \nu$ כאשר $\nu: G \rightarrow G/\ker(\varphi)$ הוא ההומומורפיזם הטבעי.

הוכחה:

נסמן $K = \ker(\varphi)$ ונגדיר את ההעתקה $\psi: G/H \rightarrow H$ ע"י $\psi(Ka) = \varphi(a)$

צ"ל שההעתקה מוגדרת היטב כלומר שהתמונה של Ka לא תלויה בבחירת הנציג.

$$Ka = Kb \Leftrightarrow ab^{-1} \in K \Leftrightarrow \varphi(ab^{-1}) = 1_H \Leftrightarrow \varphi(a) = \varphi(b)$$

נבדוק ש ψ הומומורפיזם, נעזר בעובדה כי $K \triangleleft G$:

$$\psi(Ka * Kb) = \psi(Kab) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(Ka)\psi(Kb)$$

כעת נבדוק כי ψ חח"ע:

$$\ker(\psi) = \{Ka : a \in G \mid \varphi(a) = 1_H\} = \{Ka : a \in K\} = \{K\}$$

נתון כי φ על כלומר $\exists a \in G : \varphi(a) = h$ $\forall h \in H$

לכן מתוך ההגדרה של ψ המקור של h יהיה Ka תחת ψ .

(7) כל חבורה סופית G איזומורפית לתת חבורה של S_G

הוכחה

נגדיר את ההעתקה $\varphi: G \rightarrow S_G$ ע"י $a \mapsto l_a$ כאשר $l_a(x) = ax$ (תמורה של אברי G).

l_a היא אכן תמורה שכן זו העתקה חח"ע $G \rightarrow G$.

$$\forall x, y \in G : ax = ay \Rightarrow x = y$$

ומתוך סופיות זוהי גם על.

נבדוק שימור פעולה של φ , כלומר נראה כי:

$$\varphi(ab) \stackrel{?}{=} l_a \circ l_b$$

$$\forall x \in G \varphi(ab)(x) = abx = l_a(l_b(x)) = (l_a \circ l_b)(x)$$

ולכן הומו', נבדוק חח"ע

$$\ker(\varphi) = \{a \in G : l_a = id\} = \{a \in G : ax = x\} = \{e\}$$

ולכן בסה"כ φ מונו' כלומר $G \cong \varphi(G) \leq S_G$

(8) מופיע בסוף.

(9) נוסחת המחלקה

תהא G חבורה סופית, אזי:

$$|G| = |Z(G)| + \sum_{\substack{x \text{ represent} \\ \notin Z(G)}} \frac{|G|}{|C(x)|}$$

הוכחה

נתייחס לפעולת הצמדה של G לעצמה

$$\forall x \in G : Stb(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = gx\} = C(x)$$

$$\forall x \in G : |G * x| = [G : stb(x)] = \frac{|G|}{|C(x)|}$$

$$|G| = \sum_{x \text{ rep}} |G * x| = \sum_{x \text{ rep}} \frac{|G|}{|C(x)|} \stackrel{\text{במרכז כל איבר הוא}}{=} |Z(G)| + \sum_{\substack{x \text{ rep} \\ \neq Z(G)}} \frac{|G|}{|C(x)|}$$

מחלקת צמידות של עצמו כלומר באורך 1

G איחוד זר של מחלקות צמידות, ולכן

$$|G| = \sum_{x \text{ rep}} |G * x| = \sum_{x \text{ rep}} \frac{|G|}{|C(x)|} \stackrel{\substack{\text{במרכז} \\ \text{כל} \\ \text{איבר} \\ \text{הוא} \\ \text{מחלקת צמידות} \\ \text{של עצמו} \\ \text{כלומר באורך 1}}}{=} |Z(G)| + \sum_{\substack{x \text{ rep} \\ \neq Z(G)}} \frac{|G|}{|C(x)|}$$

(10) משפט (למת) Burnside

תהא G חבורה סופית הפועלת על קבוצה סופית X. מספר המסלולים ש-G יוצרת ב-X הוא

$$k = \frac{1}{|G|} \sum_{g \in G} |X_g|$$

הוכחה

הרעיון הוא לבנות "טבלת נקודות שבת" ולמלא אותה באמצעות הפונקציה:

$$T(g, x) = \begin{cases} 0 & g * x \neq x \\ 1 & g * x = x \end{cases}$$

נספור את כל ה-1 בטבלה, לא משנה לפי עמודות או שורות.

$$\sum_{g \in G} |X_g| = \sum_{x \in X} |Stb(x)| = \sum_{i=1}^k \sum_{x \in G * x_i} |Stb(x_i)| = \sum_{i=1}^k |G * x_i| \frac{|G|}{|G * x_i|} = \sum_{i=1}^k |G| = |G|k$$

(11) משפט סילו 1:

תהא G חבורה מסדר $p^n m$ כאשר p ראשוני, $n, m \in \mathbb{N}$. אזי קיימת ת"ח p -סילו, הינו ת"ח מסדר p^n .

הוכחה

נראה באינדוקציה על $|G|$.

בדיקת התחלה: $|G| = p$ אז G עצמה p -סילו.

הנחה: הטענה נכונה עבור כל G מסדר $|G| < p^n m$

צ"ל: נכונה עבור $|G| = p^n m$

ישנם שני מקרים בלבד:

(א) קיימת ת"ח $H \leq G$ כך ש: $|H| = p^n m_1$, $m_1 < m$. לפי הנחת האינדוקציה יש בתוך H ת"ח p -סילו ב- G .

(ב) לא קיימת ת"ח $H \leq G$ מסדר $p^n m_1$, $m_1 < m$.

כלומר כל ת"ח היא מסדר $p^{n_1} m$ עם $n_1 < n$. באופן כללי יתכן גם: $m_1 \leq m$

$$\forall H \leq G : p \mid [G:H] = \frac{|G|}{|H|}$$

מכאן ע"פ נוסחת המחלקה:

$$p^n m = \underbrace{|G|}_{\substack{\text{מתחלק} \\ \text{ב} \\ p}} = |Z(G)| + \underbrace{\sum_{\substack{x \in G \\ x \neq e \\ \notin Z(G)}}}_{\substack{\text{מתחלק} \\ \text{ב} \\ p}} [G:C(x)] \Rightarrow p \mid |Z(G)| \Rightarrow Z(G) \neq \{e\}$$

כעת כיוון $Z(G)$ אבלית ו $|Z(G)| \mid p$ קיים איבר מסדר p (טענה קודמת), נשים לב כי:

$$(a \in Z(G)) \quad H = \langle a \rangle \triangleleft G$$

$$|G/H| = \frac{p^n m}{p} = p^{n-1} m$$

ע"פ הנחת האינדוקציה, יש ל G/H תת-חבורה p -סילו, כלומר $\exists A \leq G/H$ כך ש: $|A| = p^{n-1}$

$$H \triangleleft G \Rightarrow \text{קיים אפי } \nu: G \rightarrow G/H, \quad g \mapsto gH$$

נסמן: $A^* = \nu^{-1}(A) \leq G$. נמצא את ν ל:

$$\nu_0: A^* \rightarrow A$$

$$e \in A \Rightarrow \ker(\nu) = \ker(\nu_0) = H$$

לפי משפט איז'ר 1:

$$A^*/\ker(\nu_0) = A^*/H \cong A$$

$$|A^*| = |H||A| = p p^{n-1} = p^n$$

(12) משפט סילו 2:

תחת התנאים של משפט סילו 1 $((p, m) = 1, |G| = p^n m)$:

- (א) כל ת"ח $H \leq G$ מסדר p^k כאשר $1 \leq k \leq n$ מוכלת באיזשהי ת"ח p -סילו.
 (ב) כל שני ת"ח p -סילו הם צמודות.

הוכחה

תהא $H \leq G$ עם $|H| = p^k$.

קבוצת ת"ח p -סילו $Syl_p =$

ע"פ משפט סילו 1:

$$Syl_p \neq \phi$$

תהא $P \in Syl_p$ ונגדיר פעולה $H \times G/p \rightarrow G/p$ ע"י $(h, xP) \mapsto hxP$

פעולת H מחלקת את איברי G/p למסלולים זרים. נזכר כי H היא חבורת p , ולכן:

$$m = |G/p| = \sum_{x \text{ rep}} |H * xp| = \sum_{x \text{ rep}} [H:Stb(xp)] = \sum_{x \text{ rep}} p^{r_x}$$

אבל $(m, p) = 1$ ולכן בהכרח לפחות $r_x = 0$ עבור x אחד, כלומר קיימת לפחות נקודת שבת אחת, כלומר קיים xP כל שלכל $h \in H$

$$hxP = xP \Leftrightarrow x^{-1}hxP = x^{-1}xP = P \Leftrightarrow x^{-1}hx \in P \Leftrightarrow h \in xPx^{-1} \Rightarrow H \subseteq xPx^{-1}$$

$$|xPx^{-1}| = |P| = p^n$$

(ב)

ע"פ סעיף קודם בפרט לכל $P_1 \in Syl_p(G)$ (מסדר p^n) ולכל בחירה התחלתית של $P_2 \in Syl_p(G)$ קיים כך x כלשהו כך ש: $P_1 \subseteq xP_2x^{-1}$.

אבל $|P_1| = p^n = |P_2| = |xP_2x^{-1}|$ ולכן $P_1 = xP_2x^{-1}$.

(ההצמדה לא משנה את גודל הקבוצה!).

עבור חבורה G נסמן $n_p = |Syl_p(G)|$

(א) $n_p = [G : N_G(P)]$

(ב) $n_p \equiv 1 \pmod{p}$

(ג) $k \in \mathbb{N} \cup \{0\}, (m, p) = 1, m = \frac{|G|}{p^n}$ כאשר $n_p = (1 + kp)|_m$

הוכחה

(א) נגדיר את הפעולה $G \times Syl_p(G) \rightarrow Syl_p(G)$ ע"י $(g, P) \mapsto g * P = gPg^{-1}$.

ע"פ משפט סילו 2 הפעולה היא הומוגנית (יש מסלול אחד).

לכן $n_p = |G * P| = [G : Stb(P)] = [G : N_G(P)]$

כי $Stb(P) = \{g \in G : gPg^{-1} = P\} = N_G(P)$

(ב) תהא $P \in Syl_p(G)$ ונתייחס לצמצום של פעולת ההצמדה לפעולת P בלבד. כעת הפעולה כבר לא בהכרח הומוגנית!

$P \times Syl_p(G) \rightarrow Syl_p(G) : (p, P_1) \mapsto pP_1p^{-1}$

גודל כל מסלול: $[P : Stb(Q)] = |P * Q| = [P : Stb(Q)] \forall Q \in Syl_p(G)$ מחלק את $|P| = p^n$, כלומר אורך כל מסלול הוא

מאורך 1 או חזקה של p .

ומכאן ע"פ נוסחת המחלקה הכללית:

$$|Syl_p(G)| = |X| = |F| + \sum_{\substack{Q \text{ rep} \\ \notin F}} [P : Stb(Q)] = \frac{p^n}{p^{r < n}}$$

ונקבל כי $|F| \equiv n_p \pmod{p}$

אנו נראה כי $F = \{P\}$ היא נקודת השבת היחידה.

מצד אחד $P \in F$ שכן: $P * P = \{pPp^{-1} : p \in P\} = \{P\}$

מצד שני, יהי $Q \in Syl_p(G)$ כך ש $Q \in F$ אזי $P \leq N_G(Q)$ שכן Q היא נקודת שבת תחת הצמדה של P :

$P, Q \leq N_G(Q)$ ולכן $\forall p \in P : pQp^{-1} = Q$

קבלנו שתי ת"ח p -סילו ב $N_G(Q)$. אבל $Q < N_G(Q)$ ולכן היא היחידה, כלומר $P = Q$.

מסקנה:

$|F| = 1 \Rightarrow n_p \equiv |F| \pmod{p} = 1$

(ג) ע"פ לגראנז':

$$[G : P] = \frac{|G|}{|P|} = \frac{|G|}{|N_G(P)|} \frac{|N_G(P)|}{|P|} = [G : N_G(P)][N_G(P) : P]$$

$$\Rightarrow n_p \mid \frac{|G|}{|P|} = m$$

צריך להזכיר שעפ"י סעיף א': $n_p = [G : N_G(P)]$

טענת עזר

תהא G חבורת p מסדר p^n (p ראשוני), אזי לכל $1 \leq k \leq n$ קיימת ת"ח נורמלית ב- G מסדר p^k .

הוכחת טענת העזר

באינדוקציה על $|G| = p^n$

התחלה: אם $|G| = p$ אז ניקח את G עצמה.

הנחה: נניח שהטענה נכונה לכל G כך ש- $|G| < p^n$, צ"ל עבור $|G| = p^n$.

בחבורת p המרכז $Z(G)$ לא טריוויאלי.

כחבורה אבלית ב- $Z(G)$ יש איבר a מסדר p .

נסמן $\langle a \rangle = H$. כיוון ש- $H \leq Z(G)$, $H \triangleleft G$. נתבונן באפימורפיזם הטבעי $v: G \rightarrow G/H, g \mapsto gH$.

ע"פ לגראנז' $|G/H| = p^{n-1}$ ולכן עפ"י ההנחה לכל $1 \leq k \leq n$ קיימת ת"ח נורמלית $A \triangleleft G/H$, $|A| = p^{k-1}$.

נתבונן ב- $\tilde{A} = v^{-1}(A)$. כיוון ש- v הומו', $\tilde{A} \triangleleft G$. ע"פ משפט איזו' $I: \tilde{A}/_{H=\ker v} \cong A$ (גם בצמצום של v ל- \tilde{A} הגרעין נשאר H).

ולכן $|\tilde{A}| = |H||A| = pp^{k-1} = p^k$ ■

הוכחת המשפט

ע"פ טענת העזר נוכל לבנות סדרה נורמלית

$$G \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright \{e\}$$

כך שאם $|G| = p^n$ אז $|G_1| = p^{n-1}$, $|G_2| = p^{n-2}$,

ונקבל $G_k/G_{k+1} \cong \mathbb{Z}_p$ ולכן צקלית ולכן אבלית.

משפט (מיון תת-חבורות של חבורה ציקלית סופית): תהא $G = \langle a \rangle$ חבורה ציקלית מסדר n אזי:

1. $|H| \mid n \iff H \leq G$

2. לכל k טבעי: $k \mid n$, קיימת ת"ח יחידה $H \leq G$ כך ש: $|H| = k$.

הוכחה:

1. עפ"י משפט לגרנז'.

2. כל ת"ח של חבורה ציקלית היא ציקלית. כמו כן לכל $k \mid n$:

$$o(a^j) = k \iff k = \frac{n}{(j, n)} \iff (j, n) = \frac{n}{k}$$

עבור $j = \frac{n}{k}$ מקבלים קינום. באופן כללי אם: $j = \frac{n}{k}t$ אז ממילא: $a^j \in \langle a^{n/k} \rangle$ ומכאן היחידות. □

משפט (מתי מכפלה ישרה של שתי חבורות ציקליות היא חבורה ציקלית):

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm} \iff (n, m) = 1 \quad n, m \in \mathbb{N}$$

הוכחה:

בכיוון \Leftarrow נגדיר: $\varphi: \mathbb{Z}_{nm} \rightarrow \mathbb{Z}_n \times \mathbb{Z}_m$ ע"י: $\varphi(x \pmod{nm}) = (x \pmod{n}, x \pmod{m})$.

כיוון ש: $(n, m) = 1$ תכונת העל וחח"ע נובעות ממשפט השאריות הסיני. נראה שימור פעולה:

$$\begin{aligned} \varphi((x+y) \pmod{nm}) &= ((x+y) \pmod{n}, (x+y) \pmod{m}) \\ &= (x \pmod{n}, x \pmod{m}) + (y \pmod{n}, y \pmod{m}) \\ &= \varphi(x \pmod{nm}) + \varphi(y \pmod{nm}) \end{aligned}$$

מכאן שזהו איזומורפיזם.

בכיוון \Rightarrow : נתון כי: $\mathbb{Z}_n \times \mathbb{Z}_m$ ציקלית, כלומר: $o((a, b)) = nm$. $\exists (a, b) \in \mathbb{Z}_n \times \mathbb{Z}_m$:

$$(a, b)^{[n, m]} = ([n, m]a, [n, m]b) = (nu, mv) = (0, 0)$$

נשים לב כי: $(a, b)^{[n, m]} = (0, 0)$

אם כן: $nm = o((a, b)) \leq [n, m]$ אבל זה יתכן רק כאשר: $nm = [n, m]$ ומכאן ש: $(n, m) = 1$. □