

אלגברה ב' 1 - הרצאה 6 - 13.9.12

הגדרה: סדרה נורמלית מאורך m של חבורה סופית G היא סדרת חבורות G_0, G_1, \dots, G_m המקיימת: $\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_m = G$. אם $G_{i-1} \neq G_i$ לכל i , נאמר שבסדרה אין חזרות.

הגדרה: יהיו G_0, G_1, \dots, G_m , H_0, H_1, \dots, H_n שתי סדרות נורמליות של חבורה סופית G . סדרות אלו נקראות שקולות אם $n = m$ וחבורות המנה $G_1/G_0, G_2/G_1, \dots, G_m/G_{m-1}$ איזומורפיות לחבורות המנה $H_1/H_0, H_2/H_1, \dots, H_n/H_{n-1}$ בסדר כלשהו (כלומר, קיימת תמורה $i \mapsto j$ ב- S_n כך ש- $G_i/G_{i-1} \cong H_j/H_{j-1}$).

הגדרה: הסדרה H_i תקרא עידון של הסדרה G_i (בתנאי ההגדרה הקודמת), אם עבור כל i קיים j כך ש- $G_i = H_j$.

דוגמה: $G = S_4$, $K = \{e, (12)(34), (13)(24), (14)(23)\}$. ניתן להראות $K \triangleleft S_4$, $S_4/K \cong S_3$. התת-חבורה $N = \{e, (12)(34)\}$ מקיימת $N \triangleleft K$, $K/N \cong \mathbb{Z}_2$. קיבלנו סדרה:

$$\{e\} \triangleleft_N N \triangleleft_{\mathbb{Z}_2} K \triangleleft_{S_3} G = S_4$$

סדרה אחרת: $\{e\} \triangleleft_{A_4} A_4 \triangleleft_{\mathbb{Z}_2} S_4$. הסדרה $\{e\} \triangleleft_N N \triangleleft_{\mathbb{Z}_2} K \triangleleft_{\mathbb{Z}_3} A_4 \triangleleft_{\mathbb{Z}_2} S_4$ מהווה עידון של שתי הסדרות הקודמות.

משפט (Schreier): לכל שתי סדרות נורמליות של אותה חבורה קיימים עידונים שקולים.

הוכחה: יהיו G_0, G_1, \dots, G_m , H_0, H_1, \dots, H_n שתי סדרות נורמליות של חבורה סופית G . נסמן:

$$j = 0, 1, \dots, n-1, G_{i,j} = G_{i-1}(G_i \cap H_j) \\ j = 0, 1, \dots, m, H_{i,j} = H_{j-1}(G_i \cap H_j)$$

כעת, נשים לב שלפי הלמה של צננהאוס מתקיים $G_{i,j}/G_{i,j-1} \cong H_{i,j}/H_{i-1,j}$, ובפרט $G_{i,j-1} \triangleleft G_{i,j}$, $H_{i-1,j} \triangleleft H_{i,j}$, ולכן נקבל:

$$\begin{aligned} \{e\} = G_0 = G_{1,0} \triangleleft G_{1,1} \triangleleft \dots \triangleleft G_{1,n} = G_1 = G_{2,0} \triangleleft \dots \triangleleft G_{2,n} = \\ = G_2 = G_{3,0} \triangleleft \dots \triangleleft G_{m,0} \triangleleft \dots \triangleleft G_{m,n} = G_m = G \\ \{e\} = H_0 = H_{0,1} \triangleleft H_{1,1} \triangleleft \dots \triangleleft H_{m,1} = H_1 = H_{0,2} \triangleleft \dots \triangleleft H_{m,2} = \\ = H_2 = H_{0,3} \triangleleft \dots \triangleleft H_{0,n} \triangleleft \dots \triangleleft H_{m,n} = H_n = H \end{aligned}$$

בשתי הסדרות יש בדיוק mn חבורות (לא כולל $\{e\}$), ולפי האיזומורפיזם בין חבורות המנה, שנבע מהלמה של צננהאוס, נקבל ששתי סדרות אלו שקולות. \square

מסקנה: לשתי סדרות נורמליות של אותה חבורה יש עידונים שקולים ללא חזרות.

הסבר: לפי משפט שרייר קיימים עידונים שקולים, מהם נסיר את החזרות. המנות המתאימות לחזרות האלו טריוויאליות, ובשני הסדרות אותו מספר מנות טריוויאליות, שכן העידונים שקולים.

דוגמה: סדרות שקולות: $\{0\} \triangleleft_{\mathbb{Z}_3} 2\mathbb{Z}_6 \triangleleft_{\mathbb{Z}_2} \mathbb{Z}_6, \{0\} \triangleleft_{\mathbb{Z}_2} 3\mathbb{Z}_6 \triangleleft_{\mathbb{Z}_3} \mathbb{Z}_6$.

הגדרה: סדרת הרכב של חבורה G היא סדרה נורמלית ללא חזרות, שלא ניתנת לעידון (כלומר, כל סדרה אחרת שהיא עידון שלה, מכילה חזרות).

מסקנה (משפט זיורדן-הלדר): כל שתי סדרות הרכב של חבורה סופית G שקולות.

למה: תהא (1) $\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_m = G$ סדרה נורמלית של G . התנאים הבאים שקולים:

- I. ז(1) סדרת הרכב.
- II. $G_{i-1} (\neq G_i)$ נורמלית מקסימלית ב- G_i (כלומר, אם $H \triangleleft G_i, H \neq G_i$ אזי $H \triangleleft G_{i-1}$).
- III. G_i/G_{i-1} פשוטה.

הוכחה: $I \Leftrightarrow II$ ברור. נראה שאם $N \triangleleft H$ אז N נורמלית מקסימלית ב- H אם H/N פשוטה.

לפי משפט האיזומורפיזם השלישי, קיימת התאמה חחעל בין אוסף תת-החבורות של H המכילות את N לאוסף כל תת החבורות של H/N , והתאמה זו משמרת נורמליות. לכן, אין תת-חבורות נורמליות של H המכילות את N (פרט ל- H, N) אם H/N פשוטה. \square שאינן טריוויאליות ל- H/N , כלומר אם H/N פשוטה. \square

הגדרה: חבורה סופית G נקראת פתירה אם כל המנות בסדרת ההרכב שלה הן אבליות.

למה: תהא G חבורה סופית, ותהא $K \triangleleft G$. פתירה אם $G/K, K$ פתירות.

הוכחה: בלי הגבלת הכלליות, $G \neq K \neq \{e\}$. די להראות שסדרת מנות ההרכב של G היא איחוד סדרת מנות ההרכב של K ושל G/K . לסדרה הנורמלית $\{e\} \triangleleft K \triangleleft G$ יש עידון לסדרת הרכב:

$$\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_k = K \triangleleft G_{k+1} \triangleleft \dots \triangleleft G_m = G$$

בפרט, $\{e\} = G_0 \triangleleft G_1 \triangleleft \dots \triangleleft G_k = K$ זו סדרת הרכב של K .

$$\{e\} = G_k/G_k \triangleleft G_{k+1}/G_k \triangleleft \dots \triangleleft G_{m-1}/G_k \triangleleft G_m/G_k = G/K$$

זו סדרת הרכב של G/K , ומנותיה הן G_i/G_{i-1} , לפי משפט האיזומורפיזם השלישי. קיבלנו שסדרת המנות של סדרת ההרכב של K היא $G_1/G_0, G_2/G_1, \dots, G_k/G_{k-1}$ וסדרת המנות של סדרת ההרכב של G/K היא $G_{k+1}/G_k, G_{k+2}/G_{k+1}, \dots, G_m/G_{m-1}$, ואיחוד סדרות אלו הוא סדרת המנות של סדרת ההרכב של G . \square

הערה: ניתן להראות שהחבורה S_n פתירה אם $n \leq 4$, וזה נובע מההוכחה בהרצאה הקודמת ש- A_n פשוטה לכל $n \geq 5$, אך לא הוכחנו טענה זו בכיתה.

מסקנה: תהא G חבורת- p , $H \leq G$ תת-חבורה מירבית, אזי:

$$I. H \triangleleft G$$

$$II. [G:H] = p$$

III. ל- G יש סדרת הרכב שכל מנותיה הן ציקליות מסדר p , ובפרט G פתירה.

הוכחה:

I. לפי הלמה, $H < N_G(H) \leq G$, וממקסימליות H נובע $G = N_G(H)$, כלומר $H \triangleleft G$.
 II. G/H חבורת- p לא טריוויאלית. לפי משפט האיזומורפיזם השלישי, יש התאמה חתול בין תת-חבורות של G/H לבין תת-חבורות של G המכילות את H . לכן ל- G/H אין תת-חבורות טריוויאליות. לפיכך, G/H ציקלית מסדר p , לכן $[G:H] = p$.
 הסבר: נניח ש- H חבורה סופית בלי תת-חבורות לא-טריוויאליות. יהי $e \neq a \in H$, אזי $\langle a \rangle = H$, ולכן H ציקלית. אם $d \mid |H|$, $d \neq |H|, 1$, אזי $\langle a^d \rangle$ זו תת-חבורה מסדר d , סתירה.

III. נניח $|G| = p^n$. תהא H_1 תת-חבורה מירבית של G (ולכן מסדר p^{n-1}), אזי מהסעיפים הקודמים נובע $H_1 \triangleleft G$ ו- G/H_1 ציקלית מסדר p . תהא H_2 תת-חבורה מירבית של H_1 , ולכן מסדר p^{n-2} . שוב, מתקיים $H_2 \triangleleft G$, H_1/H_2 ציקלית מסדר p . באינדוקציה, נקבל סדרה $G \triangleleft H_1 \triangleleft H_2 \triangleleft \dots \triangleleft H_n = \{e\}$, שמנותיה ציקליות מסדר p , ולכן בפרט G פתירה. \square

הגדרה: יהיו p ראשוני ו- G סופית, כך ש- $|G| \equiv 1 \pmod{p}$. תת-חבורה $P \leq G$ נקראת (תת-)חבורת p -סילוב (Sylow) ב- G אם $|P|$ היא החזקה המקסימלית של p המחלקת את $|G|$.

למשל, אם $|G| = 3^5 \cdot 7^{28} \cdot 11$ אזי תת-חבורת-3-סילוב היא תת-חבורה מסדר 3^5 .

משפט קושי: יהיו p ראשוני ו- G סופית. אם $|G| \equiv 1 \pmod{p}$, אז יש ב- G איבר מסדר p .

הערה: בכיתה הוכחנו רק את המקרה האבלי, ואת המקרה הכללי הוכחנו בעזרת משפטי סילוב. הבאתי כאן את ההוכחה הכללית ללא משפטי סילוב, שדי מזכירה את הוכחת המשפטים.

הוכחה: נוכיח באינדוקציה על $n = |G|$, ונפריד לשני מקרים עבור G אבלי ולא אבלי.
 נוכיח תחילה עבור המקרה האבלי. אם G פשוטה, אזי היא ציקלית מסדר ראשוני (אחרת הייתה קיימת תת-חבורה שלה, שהיא נורמלית מהאבליות), ולכן היא בהכרח מסדר p והאיבר המקיים את התנאי המבוקש הוא היוצר של חבורה. אחרת, קיימת $N \triangleleft G$ שאינה טריוויאלית. אם p מחלק את הסדר של N , אזי N מכילה איבר מסדר p לפי הנחת האינדוקציה. אחרת, p מחלק את $[G:N]$, לפי משפט לגראנז', וכמו כן חבורה זו מכילה איבר מסדר p לפי הנחת האינדוקציה. לכן, קיים $x \in G$ עבורו $(xN)^p = x^p N = N$, כלומר $x^p \in N$. קיים ל- x^p הפכי ב- N , נסמנו ב- a . $|N|, p$ זרים, לכן קיימים s, t כך ש- $s|N| + tp = 1$ (אלגוריתם אוקלידס).
 $a = a^1 = a^{tp} = (a^t)^p = b^p$, מתקיים $b = a^t$. נבחר $b = a^t$, ולכן $bx^p = (bx)^p$. אילו bx היה איבר מסדר 1, אזי $x \in N$ מסגירות להפכי, בסתירה לכך שהסדר של xN הוא p .

נראה את המקרה הלא-אבלי. מתקיים $Z(G) < G$. אם p מחלק את הסדר של $C_G(a)$ עבור $a \in G \setminus Z(G)$ כלשהו (קיים a כזה כי G לא קומוטטיבית), אז משום ש- $C_G(a)$ תת-חבורה ממש (משום ש- a אינו במרכז) של G , לפי הנחת האינדוקציה קיים איבר ב- $C_G(a)$ המקיים את תנאי המשפט. אחרת, p מחלק את $[G : C_G(a)]$ לכל $a \in G \setminus Z(G)$. נשתמש במשוואת המחלקים: $|G| = \sum_{i \in I'} \underbrace{[G : C_G(x_i)]}_{p|} + |Z(G)|$, ולכן גם $|Z(G)|$ מתחלק ב- p . לפי הנחת האינדוקציה, יש במרכז איבר מסדר p , וסיימו. \square

משפט (המשפט הראשון של סילוב): תהא G סופית, p ראשוני המחלק את הסדר של G , אזי קיימת ל- G תת-חבורה p -סילוב.

הוכחה: באינדוקציה על סדר החבורה. טריוויאלי עבור $G = \{e\}$. נניח נכונות עבור כל חבורה מסדר קטן מ- n , ונוכיח עבור $|G| = n$.

- I. נניח שקיימת חבורת- p $N < G$ שאינה טריוויאלית. לפי הנחת האינדוקציה, לחבורת המנה G/N קיימת חבורת p -סילוב. לפי משפט האיזומורפיזם השלישי, חבורה זו מהצורה P/N כאשר P היא תת-חבורה של G המכילה את N . לפי משפט לגראנז', P היא חבורת- p . לפי משפט האיזומורפיזם השלישי מתקיים $[G : P] = [G/N : P/N]$. חבורת P/N סילוב של G/N , ולכן $[G/N : P/N]$ זר ל- p . לפיכך, גם $[G : P]$ זר ל- p , ולכן הסדר של P , המחלק את G , הוא החזקה המקסימלית של p המחלקת את $|G|$, כלומר P חבורת p -סילוב.
- II. אם קיימת $H < G$ כך ש- $[G : H]$ זר ל- p , אז לפי הנחת האינדוקציה יש ל- H תת-חבורה p -סילוב, נסמנה P . מתקיים $[G : P] = [G : H][H : P]$, ולכן גם $[G : P]$ זר ל- p , ולכן P תת-חבורה p -סילוב של G .

המקרה הכללי: נניח שלכל $H < G$ מתקיים $p \mid [G : H]$. נשתמש במשוואת המחלקים:

$$|G| = \sum_{i \in I'} \underbrace{[G : C_G(x_i)]}_{p|} + |Z(G)|$$

ולכן גם $|Z(G)|$ מתחלק ב- p . לפי משפט קושי (יש צורך בחלק האבלי בלבד) יש ב- $Z(G)$ איבר g מסדר p . נתבונן ב- $N = \langle g \rangle$. מתקיים $N < G$ כי אם $n \in N, h \in G$, אזי $hnh^{-1} = n$, כי $n \in Z(G)$. לכן, לפי I, סיימו. \square

משפט: תהא G סופית, p ראשוני המחלק את הסדר של G .

- I. אם $G \leq H$ חבורת- p , אזי H מוכלת בתת-חבורת p -סילוב של G (הרחבה של המשפט הראשון).
- II. כל שתי תת-חבורות p -סילוב, צמודות זו לזו (המשפט השני של סילוב).
- III. מספר חבורות p -סילוב, שנסמנו n_p , מקיים $n_p \equiv 1 \pmod{p}$. לכן, אם P חבורת p -סילוב, אזי $n_p \equiv 1 \pmod{p} \mid [G : P]$ (המשפט השלישי של סילוב).

הוכחה:

- I. נראה קצת יותר: תהי P חבורת p -סילוב ב- G . נראה שיש $g \in G$ כך ש- $H \leq gPg^{-1}$.
 א. G פועלת על $X = \{gPg^{-1} \mid g \in G\}$ על ידי הצמדה. ברור ש- X היא מסלול ב- G (המסלול של P). לכן: $|X| = [G : G_p]$, $G_p = \{g \in G \mid gPg^{-1} = P\} = N_G(P)$. מצד שני, $P \leq G_p \leq G$, ולכן p זר ל- $X = [G : G_p]$ (כי P -סילוב).
- ב. אם H חבורת- p אז H פועלת על X על ידי הצמדה, ולכן $X = \bigcup_{i \in I} X_i$, כאשר $\{X_i\}_{i \in I}$ מסלולים ב- H . אם $P_i \in X_i$, אזי $|X_i| = [H : H_{P_i}]$, ולכן $|X_i|$ חזקה של p . אבל $|X| = \sum_{i \in I} |X_i|$, לכן לפי אי יש $i \in I$ כך ש- $|X_i| = 1$.
- ג. $H \leq P_i \Leftrightarrow |X_i| = 1$: אם $H \leq P_i$ אז $hP_ih^{-1} = P_i$ לכל $h \in H$, ולכן $X_i = \{P_i\}$. להיפך, אם $|X_i| = 1$, אזי:

$$H = H_{P_i} = \{h \in H \mid hP_ih^{-1} = P_i\} \leq \{g \in G \mid gP_i g^{-1} = P_i\} = N_G(P_i)$$

- אבל $P_i < N_G(P_i)$, ולכן $HP_i \leq G$. כעת $|HP_i| = \frac{|H| \cdot |P_i|}{|H \cap P_i|}$ חזקה של p , ולכן P_i חבורת p -סילוב ב- G ו- $P_i \leq HP_i$, ולכן בהכרח $P_i = HP_i$, כלומר $H \leq P_i$. לכן, לפי ב', קיים i עבורו $H \leq P_i$, וסיימנו.

- II. נניח כי H, P חבורות p -סילוב ב- G . לפי I, $H \leq gPg^{-1}$ עבור $g \in G$ כלשהו.
 $H = gPg^{-1} \Leftrightarrow |H| = |P| = |gPg^{-1}|$

- III. אם H חבורת p -סילוב ב- G , אזי לפי I: $H = P_i \Leftrightarrow |X_i| = 1$. לכן, יש i_0 יחיד כך ש- $|X_{i_0}| = 1$ (הזה המתאים ל- H). אבל, $|X_i|$ הוא חזקה של p , לכן $|X_i| = 1$ לכל $i \neq i_0$. לכן $|X| = \sum_{i \neq i_0} |X_i| + 1$, ולכן $|X| \equiv 1 \pmod{p}$, אבל X זו קבוצת כל התת-חבורות p -סילוב, לכן $n_p \equiv 1 \pmod{p}$.

בהוכחת I ראינו $n_p = |X| = [G : G_p]$, ולכן בפרט $n_p \mid [G : P]$. \square