

1. מבנים אלגבריים בסיסיים:

חבורה למחצה/אגודה → מונואיד → חבורה

U חבורת ההפיכים

$$H \leq G: Z(G) \cap H \leq Z(H)$$

בחבורה ציקלית מתקיים: $O(g^m) = \frac{n}{\gcd(n,m)}$

U_n ציקלית אם $2, 4, p > 2$, $n = p^k, 2p^k$

בחבורות p המרכז הוא לא איבר היחידה

כל חבורה מסדר p^2 היא אבלית

אם $G/Z(G)$ ציקלית אז G אבלית

2. חבורות מנה:

היח"ש שלנו הוא $g_1^{-1}g_2 \in H$ ו- $g_1 \sim_H g_2$

מח"ש הן קבוצות כל הקוסטים השמאליים

$$a^{\varphi(n)} \equiv 1 \pmod n$$

$$a^p \equiv a \pmod p$$

כל קוסט ימני הוא קוסט שמאלי

$$G/N = N \setminus G$$

נורמליות היא לא טרנזיטיבית!!

3. הומומורפיזמים:

שומר על פעולה

יחידה נשלח ליחידה

שומר על הופכי

אפי - על, תמונה אפימורפית

מונו/שיכון - חח"ע

איזו - חח"ע ועל ($G \cong H$)

אוטו - איזו ממנו לעצמו

איזו הוא יח"ש

אם G ציקלית אינסופית אז איזו ל- \mathbb{Z}

אם G ציקלית מסדר n אז איזו ל- \mathbb{Z}_n

$$U_p \cong \mathbb{Z}_{p-1}$$

$\varphi: G \rightarrow H$ אפי ציקלית/אבלי אז H גם

מונו שומר על סדר

משפטי האיזו:

$$1. G/\ker \varphi \cong \text{Im } \varphi$$

$$2. H \leq G, N \triangleleft G \Rightarrow H/N \leq HN/N \leq H/N$$

$$H/(H \cap N) \cong (HN)/N$$

$$3. M/N \triangleleft G/N \Leftrightarrow M \triangleleft G \text{ אם } N \leq M$$

$$M/N \triangleleft G/N$$

$$(G/N)/(M/N) \cong G/M$$

4. (ההתאמה) $N \triangleleft G$. אז יש התאמה חח"ע ועל בין

תת החבורות של חבורת המנה G/N לבין תת

החבורות של G המכילות את N . ההומו מוגדר

$$A_{(\leq G)} \rightarrow A/N: \text{בצורה הבאה}$$

B, A חבורות אבליות, אז אוסף ההומוי בניהם הוא

חבורה אבלית ביחס לכפל הנקודתי

אם A, B, C, D חבורות אבליות אז:

$$1. \text{Hom}(A, B \times C) \cong \text{Hom}(A, B) \times \text{Hom}(A, C)$$

$$2. \text{Hom}(A \times D, B) \cong \text{Hom}(A, B) \times \text{Hom}(D, B)$$

מסמנים ב- Aut את אוסף האוטו

אוטו פנימי הוא מצמיד את x באיבר שאיתו הוא

$$\text{Inn}(G) \cong G/Z(G), \text{Inn}$$

מוגדר, מסומן $\langle\langle S \rangle\rangle = \bigcap_{(S \subset N \triangleleft G)} N$ היא S התח"ן נוצרת על ידי S

4. יוצרים ויחסים:

$G = \langle x_1, \dots, x_n | F \rangle$ כאשר F היא קבוצת היחסים.

למשל:

$$D_n = \langle \sigma, \tau | \sigma^n = \text{id}, \tau^2 = \text{id}, \sigma\tau = \tau\sigma^{-1} \rangle$$

5. פעולות:

פעולה היא הומומורפיזם מחבורה לחבורות התמורות על קבוצה

אם $H \leq G, G \sim X$ אז $H \sim X$

אם $K \sim X$ אז הומוי $\varphi: k \rightarrow G, G \sim X$

ליבה - כל האיברים הפועלים טריוויאלית

פעולה נאמנה - ליבה טריוויאלית

הפעולה הרגולרית - החבורה פועלת על עצמה, שולחת איבר לכפל.

קייילי - כל חבורה סופית משוכנת ב- $S_{|G|}$

הליבה של H - חיתוך ההצמדות שלה

חבורה נורמלית אמ"מ היא הליבה של עצמה

העידון של קייילי - אם $H \leq G, \text{Core}(H) = \{e\}$ אז

G משוכנת ב- $S_{[G:H]}$

המסלול הוא לאן איבר נשלח, מסומן orbit

מסלול זה יח"ש

פעולה טרנזיטיבית - מסלול יחיד

מייצב של איבר - איזה איברים שולחים את האיבר לעצמו

המייצב הוא ת"ח

הליבה של פעולה היא חיתוך המייצבים

אם שני איברים באותו מסלול אז המייצבים צמודים

ההפך לא נכון!!

פעולה ההצמדה - החבורה פועלת על עצמה, שולחת

איבר להצמדה ב- g

1. המסלול - מחלקת צמידות

2. מייצב - המרכז

3. הליבה - מרכז

מסלול מייצב (רק לסופי): $|G_x| \cdot |\text{stab}_G(x)| = |G|$

נקודת שבת - הכל שולח אותה לעצמה

משוואות המחלקות:

$$1. |G| = |Z| + \sum |g|$$

$$2. |G| = |Z| + \sum [G:C(g)]$$

אם איברים צמודים אז גודל Fix שווה

הלמה של ברנסייד (רק לסופי!) - מספר המסלולים זה

$$\frac{1}{|G|} \sum |\text{Stab}(x)| = \frac{1}{|G|} \sum |\text{fix}(g)|$$

6. S_n, A_n :

$$S_n \times S_m \mapsto S_{n+m}$$

חישוק=מסלול

עגיל=מסלול מאורך 2

תמורות הן צמודות אמ"מ בעלות אותו מבנה

מחזורים

המרכז טריוויאלי עבור $n \geq 3$

המרכז לא!

S נוצרת על ידי קבוצות החישוקים

גם על ידי קבוצת העגילים

$$s_n = \langle (1\ 2), (1\ 2 \dots n) \rangle$$

היא לא נוצרת על ידי כל עגיל וחישוק!

A_n היא קבוצת התמורות הזוגיות, תמורות מסומן 1

$$G \triangleleft N, N \triangleleft G \text{ אז } C \text{ מתפצלת ל-} \frac{[G:N]}{[C_G(x):C_N(x)]}$$

מחלקות צמידות

7. משפטי סילו:

$$|\text{Fix}(P \sim X)| \equiv |x| \pmod p$$

כאשר $H \leq G, H = p^k$

$$[N_G(H):H] \equiv [G:H] \pmod p$$

G מסדר $p^k m$ כאשר $p \nmid m$ נקראת ת"ח p -סילו

אם היא מסדר p^k

משפטי סילו:

11. נושאי העשרה:

- RSA:
 1. קיים מפתח פומבי ופרטי
 2. פומבי - $N = PQ, e \in U_N$
 3. פרטי - כך d כך $d \equiv 1 \pmod{\varphi(N)}$
 4. הצפנה - שולחים ל $X \equiv M^d \pmod{N}$
 5. פענוח - לפי אויילר והמפתחות נקבל את M
- החבורה החופשית:
 1. נחשוב על איברי קבוצה X בתור אותיות, נוסף אותיות $X^{-1} = \{x^{-1} | x \in X\}$, נסתכל על מילים ב $(X \cup X^{-1})^*$
 2. הגדרה. מילה ב $(X \cup X^{-1})^*$ נקראת מצומצמת אם היא לא מכילה אף תת מילה מהצורה $a^{-1}a$ או aa^{-1} עבור $a \in X$.
 3. הגדרה ראשונה לחבורה החופשית: היא מכילה כאיברים את כל המילים המצומצמות ב $(X \cup X^{-1})^*$ עם פעולת שרשור ואז מחיקת כל המופעים של $a^{-1}a, aa^{-1}$ באופן רקורסיבי.
 4. הגדרה שנייה לחבורה החופשית: אוסף מחלקות השקילות $(X \cup X^{-1})^* / \sim$ לפי $w_1 \sim w_2$ אם ניתן להגיע על ידי מספר סופי של הוספה או מחיקה של תת מילים מהצורה $a^{-1}a, aa^{-1}$. עם הפעולה - מחלקת השקילות של שרשור המילים (בלי צמצום) תכונת האוניברסליות של החבורה החופשית: נניח $G = \langle g_1, \dots, g_n \rangle$ קיים אפימורפיזם $\pi: F_n \rightarrow G$ החבורה המודולרית וחצי המישור העליון:
 1. $H = \{z \in \mathbb{C} | \text{Im}(z) > 0\}$
 2. פונקציית מוביוס: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} * z = \frac{az+b}{cz+d}$
 3. פעולת טרנזיטיבית
 4. המייצב הוא $SO_2(\mathbb{R})$
 5. אם עובדים עם \mathbb{Z} אז זה לא טרנזיטיבי
- חבורות פשוטות סופיות:
 1. משפט ברנסייד: לסדר של חבורה פשוטה לא אבלית יש לפחות 3 מחלקים ראשוניים.
 2. משפט פיית' תומפסון: חבורה פשוטה היא מסדר זוגי.
- חבורות לינאריות:
 1. $PSL_n(F) = SL_n(F) / Z(SL_n(F))$
 2. $PGL_n(F) = GL_n(F) / Z(GL_n(F))$
 3. $GL_n(F_q) / SL_n(F_q) \cong F_q^\times$
 4. $PGL_2(F_q) \cong S_{q+1}$.
- סדרות מדויקות:
 1. סדרה של חבורות עם הומוי ביניהם $\dots \xrightarrow{f_{i-1}} G_i \xrightarrow{f_i} G_{i+1} \xrightarrow{f_{i+1}} \dots$
 2. כך $\ker f_i = \text{Im } f_{i-1}$ באופן כללי - אם מתחיל ב 1 אז השני שיכון, אם נגמר ב 1 אז הלפני האחרון על.
 3. קצרה: $1 \rightarrow K \xrightarrow{f} G \xrightarrow{\theta} Q \rightarrow 1$
 4. הסדרה מתפצלת אם $\varphi \cdot \theta = \text{id}_Q$
- מכפלה ישרה למחצה:
 1. תהייה H, N חבורות ויהי $\varphi: H \rightarrow \text{Aut}(N)$ הומוי. נגדיר את המכפלה הישרה למחצה: $N \rtimes_\varphi H$
 2. עם הפעולה $(n_1, h_1) \cdot (n_2, h_2) = (n_1 \cdot \varphi(h_1)(n_2), h_1 h_2)$
 3. יוצא: $N \cong (N, e_H) \triangleleft N \rtimes_\varphi H$
 4. אם G חבורה $N \triangleleft G, H \leq G$ כך ש:
 - $NH = G$
 - $N \cap H = e$
 אז $G \cong N \rtimes_\varphi H$
 5. שור זסנהאוס: תהייה K, G, Q חבורות סופיות כך שהסדרה $1 \rightarrow K \rightarrow G \rightarrow Q \rightarrow 1$ מדויקת. אם $G \cong K \rtimes Q$

1. G מסדר $p^t m, p \nmid m$, כל תת חבורה מסדר p^i מוכלת בחבורה מסדר p^{i+1} לכל i בין 0 ל- $t-1$
 2. כל ת"ח p -סילו צמודות זו לזו (אם קיימת אחת היא נורמלית)
 3. $n_p = [G : N_G(P)], n_p \equiv 1 \pmod{p}, n_p | m$
- G פשוטה שפועלת לא טריוויאלית על קבוצה מגודל n אזי G משוכנת ב S_n
8. חבורות פתירות:
- סדרה נורמלית אם כל האיברים נורמליים ב G
 - סדרה היא תת נורמלית אם כל איבר נורמלי באיבר הבא
 - המנות נקראות מנות הסדרה
 - כל סדרה נורמלית היא תת נורמלית אבל לא הפוך!!
 - עידון זה כשאנחנו דוחפים חבורה לתוך הסדרה
 - ניתן לעדן שלב אמ"מ למנה שלו יש תח"ן
 - סדרת הרכב - סדרה תת נורמלית מקסימלית, סדרה תת נורמלית עם מנות פשוטות
 - אם חבורה סופית תמיד אפשר לעדן לסדרה תת נורמלית
 - בהינתן סדרה לכל תח"ן קיימת סדרה תת נורמלית שעוברת בה וגם המנות של החדשה מנות של המקורית או תח"ן שלה
 - $C(N \cap B) = (CN) \cap B, C \subseteq B, N, B, C \leq G$
 - זיורדן הולדר - כל סדרות ההרכב באותו אורך עם מנות איזומורפיות עד כדי סדר
 - המנות של סדרת הרכב הם גורמי ההרכב חבורה פתירה אם:
 1. כל גורמי ההרכב ציקליים
 2. יש סדרה תת נורמלית עם מנות אבליות
 3. יש סדרה תת נורמלית עם מנות ציקליות מסדר ראשוני.
 4. יש סדרת הרכב עם מנות ציקליות מסדר ראשוני.
9. קומוטטורים:
- הקומוטטור של x, y הוא $[x, y] = xyx^{-1}y^{-1}$
 - $xy = yx \Leftrightarrow [x, y] = 1$
 - הנוצרת על ידי הקומוטטורים. $G' = [G, G] = \langle [x, y] | x, y \in G \rangle$ תת החבורה $G' \triangleleft G$
 - G אבלית אמ"מ הנגזרת שלה היא 1
 - $(G/N)' = (G'N)/N: N \triangleleft G$
 - G'/G נקראת האבליזציה של G .
 - חבורה הסופית G פתירה אמ"מ הנגזרת שלה מתאפסת לבסוף
 - פתירה אם מתקיים אחד מהתנאים הבאים:
 1. יש סדרה תת נורמלית עם מנות אבליות.
 2. הסדרה הנגזרת מגיעה ל 1 .
 3. יש סדרה נורמלית עם מנות אבליות.
 - נאמר ש G היא הרחבה של Q ע"י K אם $G/K \cong Q: K \triangleleft G$
10. מיון חבורות אבליות:
- טענה. תהא G חבורה סופית ותהייה $P_1, \dots, P_m \leq G$ כל ת"ח p -סילו שלה (הראשוניים לאו דווקא שונים). אזי $G = \langle P_1, \dots, P_m \rangle$.
 - פירוק פרימרי: תהא G חבורה אבלית סופית ותהא $P_1 \leq G$ ת"ח p_1 -סילו, אזי: $G \cong P_1 \times G_1$ לאיזושהי $G_1 \leq G$.
 - נובע באינדוקציה כי חבורה אבלית סופית היא מכפלה ישרה של ת"ח p -סילו שלה.
 - חבורת p -אבלית סופית איזומורפית למכפלה ישרה של חבורות p -ציקליות.
 - כל חבורה אבלית סופית הינה מכפלה ישרה של חבורות ציקליות