תורת החבורות 88-218-01 תשפ"א
הערות הרצאה 10

0.1 המשך ספירת מסלולים וחבורות המשולש

תזכורת 0.1. תהי G חבורה הפועלת על קבוצה X. אז

$$k = |X/G| = \frac{1}{|G|}\sum_{g\in G}|X^g| = \frac{1}{|G|}\sum_{x\in X}|\mathrm{stab}(x)|$$

כאשר

$$X^g = \{x \in X \mid g * x = x\}$$

טענה 0.2. יהיו $x, y \in X$ איברים באותו מסלול של הפעולה. אז המייצבים $\mathrm{stab}(x), \mathrm{stab}(y)$ הם תת־חבורות צמודות. כלומר קיים $g \in G$ כך ש־$\mathrm{stab}(x) = g\,\mathrm{stab}(y)g^{-1}$.

פתרון. מופיע בתרגיל בית 9.

טענה 0.3. יהיו $g, h \in G$ איברים צמודים. נניח $g = aha^{-1}$ (לכן $ga = ah$). אז

$$|X^g| = \left|X^h\right|$$

הוכחה. נגדיר העתקה

$$\begin{aligned} f\colon X^h &\to X^g \\ x &\mapsto a * x \end{aligned}$$

אז קודם נבדוק שהפונקציה מוגדרת, ואחר שהיא חח"ע ועל. לכל $x \in X^h$ מתקיים $h * x = x$. אז נחשב

$$g * (a * x) = (ga) * x = (ah) * x = a * (h * x) = a * x$$

ולכן $a * x \in X^g$. עבור חח"ע ועל, נמצא לא פונקציה הופכית:

$$\begin{aligned} f^{-1}\colon X^g &\to X^h \\ y &\mapsto a^{-1} * y \end{aligned}$$

וקל לבדוק כי $a * (a^{-1} * y) = y$ וגם $a^{-1} * (a * x) = x$ וסיימנו. □

דוגמה 0.4. ננסה לראות בכמה דרכים ניתן לצבוע קודקודי קובייה ב-d צבעים, עד כדי סיבוב הקובייה.

אנחנו רוצים לספור את מספר המסלולים של הפעולה של חבורת הסיבובים של קובייה על מספר הצביעות הכללי. נגדיר את הקבוצה

$$X = \{1, \dots, d\}^8$$

ולכן $|X| = d^8$. החבורה היא $G = S_4$ כמו שראינו פעם, ורוצים לספור את

$$k = |X/G| = \frac{1}{|S_4|} \sum_{\sigma \in S_4} |X^\sigma|$$

לפי הטענות לעיל מספיק לחשב את $|X^\sigma|$ עבור נציג מכל מחלקת צמידות של S_4, ולהכפיל בגודל מחלקת הצמידות. מחלקות הצמידות ב-S_4 הן:

$$\begin{aligned}
|[\mathrm{id}]| &= 1 \\
|[(1234)]| &= \binom{4}{4}(4-1)! = 6 \\
|[(123)]| &= \binom{4}{3}(3-1)! = 8 \\
|[(12)]| &= \binom{4}{2}(2-1)! = 6 \\
|[(12)(34)]| &= \binom{4}{2}\binom{2}{2}\frac{1}{2!} = 3
\end{aligned}$$

לכן נרצה לחשב

$$k = \frac{1}{4!}\left(1 \cdot \left|X^{\mathrm{id}}\right| + 6 \cdot \left|X^{(1234)}\right| + 8 \cdot \left|X^{(123)}\right| + 6 \cdot \left|X^{(12)}\right| + 3 \cdot \left|X^{(12)(34)}\right|\right)$$

לכן מספר הדרכים לצבוע את קודקודי הקובייה ב-d צבעים הוא

$$k = \frac{1}{24}\left(d^8 + 6d^2 + 8d^4 + 6d^4 + 3d^4\right) = \frac{1}{24}(d^8 + 17d^4 + 6d^2)$$

עבור $d = 1$ יש צביעה אחת. עבור $d = 2$ יש 23 צביעות ועבור $d = 3$ יש 333 צביעות.

נניח ששמות הקודקודים הם $\{A, B, C, D, E, F, G, H\}$ כמו בהדגמה הזו. ברור מה קורה עם תמורת הזהות. עבור מחזורים מאורך 4 נקבל בשיכון (של הפעולה):

$$(ABCD)(EFGH)$$

ולכן יש d^2 נקודות שבת. בסיבוב של 180 מעלות (כלומר תמורה כמו $(12)(34)$) נקבל

$$(AC)(BD)(EG)(FH)$$

ולכן $\left|X^{(12)(34)}\right| = d^4$. עבור סיבוב על אלכסון נקבל תמורה כמו

$$(A)(H)(BDF)(CEG)$$

ומקבלים $\left|X^{(123)}\right| = d^4$. עבור חילוף כמו (12) נקבל תמורה כמו

$$(AH)(BE)(CD)(FG)$$

הגדרה 0.5. חבורת המשולש (n, m, l) מוגדרת לפי

$$\Delta_{n,m,l} = \left\langle x, y \,\middle|\, x^n, y^m, (xy)^l \right\rangle$$

דוגמה 0.6. נשים לב כי $D_n \cong \Delta_{n,2,2}$.

דוגמה 0.7. תמורה על $\{n, m, l\}$ תוביל לחבורות איזומורפיות:

$$\begin{aligned}\Delta_{n,m,l} &= \left\langle x, y \,\middle|\, x^n, y^m, (xy)^l \right\rangle \\ &\overset{x\mapsto y^{-1}, y\mapsto x^{-1}}{=} \left\langle y, x \,\middle|\, y^n, x^m, (xy)^l \right\rangle \cong \Delta_{m,n,l}\end{aligned}$$

כי

$$(xy)^l \mapsto (y^{-1}x^{-1})^l = (xy)^{-l}$$

וגם

$$\begin{aligned}\Delta_{n,m,l} &\cong \left\langle x, y \,\middle|\, x^n, y^m, (xy)^l \right\rangle \\ &\overset{y\mapsto x^{-1}y}{=} \left\langle x, y \,\middle|\, x^n, (x^{-1}y)^m, y^l \right\rangle \\ &\overset{x\mapsto x^{-1}}{=} \left\langle x, y \,\middle|\, x^n, (xy)^m, y^l \right\rangle \cong \Delta_{n,l,m}\end{aligned}$$

וזה מספיק כדי להוכיח איזומורפיזם לשאר חבורות המשולש כי $S_3 = \langle (12), (23) \rangle$.

הערה 0.8. יש קשר למשולשים. אפשר להגדיר את "העקמומיות" של החבורה להיות

$$\kappa = \frac{1}{n} + \frac{1}{m} + \frac{1}{l} - 1$$

האיברים x, y, xy מקבילים לסיבובים ב-$\frac{2\pi}{n}, \frac{2\pi}{m}, \frac{2\pi}{l}$.

אם $\kappa > 0$, אנחנו במקרה הספרי ויש בו רק מספר סופי מעניין של מקרים, ובכולם החבורה $\Delta_{n,m,l}$ היא סופית ומסדר $\frac{2}{\kappa}$. המקרים הם $(2, 3, 4)$, $(2, 3, 3)$, $(2, 3, 5)$ ו-$(2, 2, n)$ עבור $n > 1$. נסו להוכיח כי

$$\Delta_{2,3,3} \cong A_4, \qquad \Delta_{2,3,4} \cong S_4, \qquad \Delta_{2,3,5} \cong A_5$$

ולפחות זה קל לבדוק את הסדרים.

אם $\kappa = 0$, כלומר

$$\frac{1}{n} + \frac{1}{m} + \frac{1}{l} = 1$$

זהו המקרה האוקלידי, שבו מרצפים את המישור האוקלידי (המוכר). יש רק מספר סופי של מקרים: $(2,3,6)$, את $(2,4,4)$ ואת $(3,3,3)$. לשעות הפנאי יש את המשחק הזה עם כל מיני ריצופים.

אם $\kappa < 0$, אז זה המקרה ההיפרבולי, והוא מקביל לריצופים של המישור ההיפרבולי. החבורות המתקבלות הן אינסופיות.

בעיה 0.9 (בונוס לבוחן)**.** תנו תיאור מלא של חבורת הסיבובים של תריסריון (דודקהדר), והוכיחו שהיא איזומורפית ל-A_5.

0.2 משפטי סילו

לאורך כל תת־הפרק נניח כי G היא חבורה מסדר n, ויהי p ראשוני המחלק את n. נניח כי $n = p^t m$ כאשר m זר ל-p.

טענה 0.10. תהי G חבורה, ותהי $S \subseteq G$ תת־קבוצה. אז $|S| = |gSg^{-1}|$ לכל $g \in G$.

הוכחה. מגדירים פונקציה

$$\begin{aligned} f\colon S &\to gSg^{-1} \\ s &\mapsto gsg^{-1} \end{aligned}$$

ויש פונקציה הופכית $y \mapsto g^{-1}yg$. □

תזכורת 0.11. תהי P חבורת-p סופית מסדר p^k. אם P פועלת על קבוצה X, אז

$$|\mathrm{Fix}(X)| \equiv |X| \pmod{p}$$

כי X היא איחוד זר של מסלולים, והגודל של כל מסלול מחלק את p^k.

תזכורת 0.12. תהי G חבורה, ותהי $H \leq G$. אם G פועלת על קבוצה X, אז גם H פועלת על הקבוצה X לפי צמצום הפעולה מ-G.

החבורה G פועלת על G/H לפי כפל משמאל:

$$g * xH = (gx)H$$

הגדרה 0.13. תהי G חבורה מסדר $n = p^t m$ כאשר m זר לראשוני p. תת־חבורה $P \leq G$ מסדר p^t תקרא תת־חבורת p-סילו.

כלומר היא מקסימלית בסדר שלה מבין תת־חבורות-p של G. את קבוצת כל תת־חבורות p-סילו של G נסמן ב-$\mathrm{Syl}_p(G)$.

דוגמה 0.14. אם יש חבורה מסדר $200 = 2^3 \cdot 5^2$. אז תת־חבורת 2-סילו שלה תהיה מסדר 8 ותת־חבורה 5-סילו שלה תהיה מסדר 25.

משפט 0.15 (משפטי סילו)**.** תהי G חבורה מסדר $n = p^t m$.

1. יש ל-G תת־חבורות p-סילו. כל תת־חבורה $H \leq G$ שהיא חבורת-p מוכלת בתת־חבורת p-סילו כלשהי.
2. כל שתי תת־חבורות p-סילו $P_1, P_2 \in \mathrm{Syl}_p(G)$ הן צמודות. כלומר קיים $g \in G$ כך ש-$P_1 = gP_2g^{-1}$.
3. נסמן $n_p := n_p(G) = \left|\mathrm{Syl}_p(G)\right|$. אז $n_p \equiv 1 \pmod p$ וגם $n_p | m$.

דוגמה 0.16. נבחר $G = S_4$. אז $|G| = 2^3 \cdot 3$. יש לה $n_3 = 4$ תת־חבורות מסדר 3 והן

$$\langle (123) \rangle, \langle (124) \rangle, \langle (134) \rangle, \langle (234) \rangle$$

ואכן $n_3 \equiv 1 \pmod 3$ וגם $n_3 | 2^3$.
יש לה גם $n_2 = 3$ חבורות מסדר 8. קל לחשב $n_2 \equiv 1 \pmod 2$. הבטנו גם בסריג תת־החבורות של S_4 כאן וגם בסריג עד כדי הצמדה כאן.

הוכחת משפט סילו 1. נוכיח טענה חזקה יותר: תהי $H \leq G$ מסדר p^i עבור $0 \leq i < t$, אז קיימת תת־חבורה $H \leq K \leq G$ וגם $|K| = p^{i+1}$.
הטענה הזו גוררת את המשפט באינדוקציה מתת־החבורה הטריוויאלית:

$$H \leq K_1 \leq \cdots \leq K_{t-i}$$

מעכשיו נניח $t \geq 1$. קודם נראה מה קורה אם $H \lhd G$. במקרה הזה G/H היא חבורה, והיא מסדר

$$|G/H| = \frac{|G|}{|H|} = \frac{p^t m}{p^i} = p^{t-i} m$$

והרי $i < t$, ולכן $p \,|\, |G/H|$. לפי משפט קושי קיים ב-G/H איבר מסדר p. לכן יש תת־חבורה $L/H \leq G/H$ שהיא מסדר p (תת־החבורה הציקלית שנוצרת על ידי אותו איבר). לפי משפט ההתאמה אפשר לקחת את התמונה ההפוכה של L/H תחת ההטלה $\pi : G \to G/H$, ולקבל תת־חבורה K של G שמכילה את H, ומפני שמשפט ההתאמה שומר על אינדקסים, נסיק כי $|K| = p^{i+1}$.

$$K = \pi^{-1}(L/H)$$

ואז

$$\begin{aligned} [L/H : H/H] &= [\pi^{-1}(L/H) : H] \\ |K| = [K : \{e\}] &= [K : H][H : \{e\}] \end{aligned}$$

אם H לא נורמלית, אז G/H לא חבורה. אבל נוכל להזכר במנרמל

$$N_G(H) = \{g \in G \,|\, gH = Hg\} = \left\{g \in G \,\middle|\, g^{-1}Hg = H\right\}$$

וכבר הזכרנו כי $H \lhd N_G(H) \leq G$. אם p מחלק את $|N_G(H)/H|$, אז עושים את אותו נימוק עם משפט קושי לגבי חבורת המנה $N_G(H)/H$. כעת נותר להוכיח כי p מחלק את הסדר $|N_G(H)/H|$.

נתבונן בפעולה של H על קבוצת המחלקות G/H על ידי כפל משמאל. נמצא את נקודות השבת של הפעולה:

$$\begin{aligned} gH \in \mathrm{Fix}(G/H) &\iff \forall h \in H : h * gH = gH \\ &\iff \forall h \in H : hgH = gH \\ &\iff \forall h \in H : g^{-1}hgH = H \\ &\iff \forall h \in H : g^{-1}hg \in H \\ &\iff g \in N_G(H) \end{aligned}$$

לכן $\mathrm{Fix}(G/H) = N_G(H)/H$.

אם $i = 0$, אז $H = \{e\}$, ואז $N_G(H) = G$, ולכן $N_G(H)/H \cong G$. במקרה זה ברור כי p מחלק את $|N_G(H)/H|$. אחרת, $i \geq 1$ ולכן p מחלק את $|H|$. לפי הטענה בתזכורת:

$$|N_G(H)/H| = |\mathrm{Fix}(G/H)| \equiv |G/H| \pmod{p}$$

אבל p מחלק את $|G/H| = p^{t-i}m$. לכן $|N_G(H)/H| \equiv 0 \pmod{p}$, כלומר p מחלק את הסדר שרצינו, וסיימנו. □

הערה 0.17. במהלך ההוכחה של משפט סילו 1 הוכחנו שאם G חבורה ו-$H \leq G$ היא תת־חבורה מסדר p^i, ונניח $p|[G : H]$, אז $H \subsetneq N_G(H)$.

הוכחת משפט סילו 2. יהיו $P_1, P_2 \in \mathrm{Syl}_p(G)$. לכן

$$|P_1| = |P_2| = p^t$$

ואנחנו צריכים להוכיח שהן צמודות. שימו לב שתת־חבורות מאותו סדר (אפילו איזומורפיות) הן לא בהכרח צמודות כמו ב-S_4:

$$\langle (12)(34), (13)(24) \rangle \cong \langle (12), (34) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

נתבונן בפעולה של P_1 על קבוצת המחלקות G/P_2 לפי כפל משמאל. מפני ש-P_1 היא חבורת-p, אז

$$|\mathrm{Fix}(G/P_2)| \equiv |G/P_2| \equiv \frac{|G|}{|P_2|} \equiv \frac{p^t m}{p^t} \equiv m \pmod{p}$$

ושימו לב כי m זר ל-p. לכן p לא מחלק את $|\mathrm{Fix}(G/P_2)|$. בפרט $\mathrm{Fix}(G/P_2) \neq \varnothing$. כלומר קיימת לפחות נקודת שבת אחת $gP_2 \in \mathrm{Fix}(G/P_2)$.

לפי הגדרה $h * gP_2 = gP_2$ לכל $h \in P_1$. לכן $g^{-1}hgP_2 = P_2$ לכל $h \in P_1$. כלומר $g^{-1}hg \in P_2$ לכל $h \in P_1$, או בקיצור $g^{-1}P_1g \subseteq P_2$. אבל P_1 ו-P_2 הן קבוצות סופיות מאותו גודל, ולכן מההכלה נקבל שיוויון. כלומר $P_1 = gP_2g^{-1}$, כמו שרצינו. □

מסקנה 0.18. תהי $P \leq G$ תת־חבורת p-סילו. אז $P \lhd G$ אם ורק אם $n_p = 1$.

הוכחה. נניח כי $n_p = 1$. כלומר $\mathrm{Syl}_p(G) = \{P\}$. לכל $g \in G$ מתקיים $gPg^{-1} \in \mathrm{Syl}_p(G)$, שהרי $|gPg^{-1}| = |P|$. לכן $gPg^{-1} = P$ לכל $g \in G$. כלומר $P \lhd G$.
בכיוון השני, נניח כי $P \lhd G$. תהי $Q \in \mathrm{Syl}_p(G)$ תת־חבורת p-סילו כלשהי. אז $Q = gPg^{-1}$ עבור $g \in G$ כלשהו לפי משפט סילו 2. מהנורמליות של P נקבל כי $Q = P$. לכן $n_p = 1$. □

הוכחת משפט סילו 3. החבורה G פועלת על $X = \mathrm{Syl}_p(G)$ על ידי הצמדה:

$$g * P = gPg^{-1}$$

לכל $g \in G$ ולכל $P \in X$. לפי משפט סילו 2 הפעולה היא טרנזיטיבית. כלומר יש לה מסלול אחד וגודלו הוא $|X| = n_p$. תהי $P \in X$ ולפי משפט מסלול־מייצב נקבל

$$n_p = |X| = |G * P| = [G : \mathrm{stab}(P)]$$

בנוסף $g \in \mathrm{stab}(P)$ אם ורק אם $gPg^{-1} = P$. כלומר אם ורק אם $g \in N_G(P)$. לכן

$$n_p = [G : N_G(P)]$$

מפני ש־$P \leq N_G(P) \leq G$, אז $|N_G(P)|$ מחלק את p^t לפי משפט לגראנז'. אז $|N_G(P)| = p^t m'$ עבור m' שזר ל־p. לכן

$$n_p = [G : N_G(P)] = \frac{|G|}{|N_G(P)|} = \frac{p^t m}{p^t m'} = \frac{m}{m'}$$

בפרט $n_p | m$. נותר להוכיח $n_p \equiv 1 \pmod{p}$.
כעת נתבונן בפעולה של P על X על ידי הצמדה (זו הפעולה שמצומצמת מהפעולה של G על X):

$$h * Q = hQh^{-1}$$

לכל $h \in P$ ולכל $Q \in X$. נשים לב כי P היא נקודת שבת של הפעולה (כי $hPh^{-1} = P$ לכל $h \in P$). נבחר $Q \in X$ נקודת שבת כלשהי. אז

$$h * Q = hQh^{-1} = Q$$

לכל $h \in P$. לכן $h \in N_G(Q)$ לכל $h \in P$, ונסיק $P \leq N_G(Q)$. לכן P היא גם תת־חבורת p-סילו של $N_G(Q)$, שהרי $|N_G(Q)|$ מחלק את $|G|$ לפי משפט לגראנז' ולא תתכן חזקה גבוהה יותר מ־p^t שמחלקת את $|N_G(Q)|$.
אבל גם $Q \leq N_G(Q)$, ואפילו $Q \lhd N_G(Q)$. לפי המסקנה הקודמת של משפט סילו 2, זו חייבת להיות תת־חבורת p-סילו היחידה של $N_G(Q)$. לכן $Q = P$. כלומר $\mathrm{Fix}(X) = \{P\}$. אז לפי הטענה מהתזכורת

$$n_p = \left|\mathrm{Syl}_p(G)\right| = |X| \equiv |\mathrm{Fix}(X)| \pmod{p}$$

ולכן $n_p \equiv 1 \pmod{p}$. □