תורת החבורות 88-218-01 תשפ"א
הערות הרצאה 4

שלום!

תזכורת 0.1. הומומורפיזם $f\colon G \to H$ בין חבורות G, H המקיימת

$$\forall g_1, g_2 \in G : f(g_1 g_2) = f(g_1) f(g_2)$$

0.1 פעולה של חבורה על קבוצה

הגדרה 0.2. פעולה (שמאלית) של חבורה $(G, \cdot)$ על קבוצה X היא פונקציה $\varphi\colon G \times X \to X$ שנסמן $\varphi(g, x) = g * x$ שמקיימת:

1. מתקיים $g * (h * x) = (g \cdot h) * x$ לכל $g, h \in G$ ולכל $x \in X$.
2. מתקיים $e * x = x$ לכל $x \in X$.

ראינו הגדרה שקולה שפעולה היא הומומורפיזם $\varphi\colon G \to S_X$.

$$\varphi(g \cdot h) = \varphi(g)\varphi(h)$$

ובנוסף $\varphi(e) = \mathrm{id}_X$. את השקילות מוכיחים עם

$$\varphi(g)(x) = g * x$$
$$(\varphi(g^{-1})\varphi(g))(x) = \varphi(g^{-1})(g * x) = g^{-1} * (g * x) = (g^{-1}g) * x = e * x = x$$

לפעמים מסמנים $G \curvearrowright X$.

דוגמה 0.3. נבחר את $G = S_X$ שפועלת על הקבוצה X. לכל $\sigma \in S_X$ ולכן $x \in X$ הפעולה תהיה

$$\sigma * x = \sigma(x)$$

נבדוק שזו באמת פעולה: לכל $\sigma, \tau \in S_X$ ולכל $x \in X$ נבדוק

$$\sigma * (\tau * x) = \sigma * (\tau(x)) = \sigma(\tau(x)) = (\sigma \circ \tau) * x$$
$$\mathrm{id}_X * x = \mathrm{id}_X(x) = x$$

דוגמה 0.4. תהי H תת־חבורה של חבורה G, ונבחר את הקבוצה להיות $X = G$. החבורה H פועלת על G לפי כפל משמאל: $h * x = hx$ לכל $h \in H$ ולכל $x \in G$. ראינו את הפעולה הזו בהוכחה של משפט לגראנז'.

דוגמה 0.5. מקרה פרטי של הדוגמה הקודמת: החבורה G פועלת על עצמה על ידי כפל משמאל. כלומר $g * x = gx$.

מתי כפל מימין של G על עצמה הוא פעולה?

$$g * (h * x) = g * (xh) = xhg \stackrel{?}{=} xgh = (gh) * x$$

השיוויון באמצע נכון אם ורק אם g ו-h מתחלפות. לכן זו פעולה אם ורק אם G אבלית.

דוגמה 0.6. יהי F שדה. נתבונן בחבורה $G = (F^*, \cdot)$ ועל מרחב וקטורי V מעל F. נבחר את הקבוצה שלנו להיות $X = V$. נגדיר פעולה לפי זה שלכל $\alpha \in F^*$ ולכל וקטור $v \in V$:

$$\alpha * v = \alpha v$$

כלומר כפל בסקלר. קל לבדוק $\alpha * (\beta * v) = (\alpha\beta) * v$ וגם $1 * v = v$.

הכללה: נבחר $G = GL_n(F)$ ואת $X = F^n$. אז G פועלת על X לפי

$$A * v = Av$$

(כפל של מטריצה בוקטור) לכל מטריצה $A \in G$ ולכל וקטור $v \in V$. עבור $n = 2$ ו-$F = \mathbb{R}$:

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} * \begin{pmatrix} \sqrt{2} \\ -1 \end{pmatrix} = \begin{pmatrix} \sqrt{2} - 2 \\ 2\sqrt{2} - 4 \end{pmatrix}$$

דוגמה 0.7. כל חבורה G פועלת על עצמה על ידי הצמדה. כלומר לכל $g \in G$ ולכל $x \in G$ לפי

$$g * x = gxg^{-1}$$

נבדוק שזו פעולה של חבורה על קבוצה:

$$\begin{aligned} g * (h * x) &= g * (hxh^{-1}) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = (gh) * x \\ e * x &= exe^{-1} = x \end{aligned}$$

דוגמה 0.8. יהי F שדה. נבחר שוב $G = GL_n(F)$. יהי V מרחב וקטורי ממימד n מעל F. נגדיר דגל שלם להיות שרשרת של תת־מרחבים

$$(0) = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V$$

כך שמתקיים $\dim_F V_i = i$ לכל $0 \le i \le n$. לדוגמה עבור $F = \mathbb{R}$ ו-$n = 3$ יש את הדגל

$$\left\langle \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\rangle \subseteq \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle \subseteq \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle \subseteq \mathbb{R}^3$$

שנקרא הדגל הסטנדרטי. נסמן ב-X את קבוצת הדגלים השלמים ב-V. אז הפעולה שלנו תהיה

$$A * (V_0, V_1, \dots, V_n) = (AV_0, AV_1, \dots, AV_n)$$

לכל $A \in G$ ולכל דגל $(V_0, V_1, \dots, V_n)$. לדוגמה עבור $F = \mathbb{R}$ ו-$n = 3$ נפעל על הדגל הסטנדרטי $\mathcal{V}$ עם איבר ספציפי

$$\begin{pmatrix} 2 & 3 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix} * \mathcal{V} = (AV_0, AV_1, AV_2, AV_3) =$$

$$= \left(\left\langle \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} \right\rangle, \left\langle \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 1 \end{pmatrix} \right\rangle, \mathbb{R}^3 \right)$$

0.2 מסלולים

הגדרה 0.9. תהי חבורה G הפועלת על קבוצה X. נגדיר יחס $\sim$ על X לפי

$$x_1 \sim x_2 \iff \exists g \in G,\ g * x_1 = x_2$$

טענה 0.10. היחס $\sim$ לעיל הוא יחס שקילות.

הוכחה. נוכיח את התכונות הדרושות ליחס:

רפלקסיביות: לכל $x \in X$ מתקיים $e * x = x$ ולכן $x \sim x$.

סימטריות: אם $x_1 \sim x_2$, אז קיים לפי ההגדרה $g \in G$ כך ש-$g * x_1 = x_2$. נפעיל את g^{-1} על האיברים האלו

$$x_1 = e * x_1 = (g^{-1} g) * x_1 = g^{-1} * (g * x_1) = g^{-1} * x_2$$

לכן $x_2 \sim x_1$.

טרנזיטיביות: נניח $x_1 \sim x_2$ וגם $x_2 \sim x_3$, אז קיימים $g, g' \in G$ כך ש-$g * x_1 = x_2$ וגם $g' * x_2 = x_3$. לכן

$$(g' g) * x_1 = g' * (g * x_1) = g' * x_2 = x_3$$

לכן $x_1 \sim x_3$. לכן $\sim$ יח"ש. $\square$

הגדרה 0.11. בהנתן פעולה של חבורה G על X, היחס $\sim$ מחלק את X למחלקות שקילות. למחלקת השקילות של $x \in X$ קוראים המסלול של x תחת G, ומסמנים:

$$\operatorname{orb}(x) = G * x = \{ g * x \mid g \in G \}$$

בפרט

$$X = \bigcup_{x \in X} G * x$$

.

הערה 0.12. פעולות של חבורות על קבוצות, ומרחבי המנה ביחס לפעולות האלו. בקבוק קליין, מרחב פרוייקטיבי. בוחרים $G = \mathbb{Z}_2$ ואת X להיות טורוס עבור בקבוק קליין או הספרה $\mathbb{S}^{n-1}$ עבור המרחב הפרוייקטיבי, ואת הפעולה להיות $0 * x = x$ ו-$1 * x = -x$.

0.3 טרנזיטיביות של פעולה

הגדרה 0.13. תהי G חבורה הפועלת על קבוצה X. נאמר שהפעולה היא טרנזיטיבית אם לכל שני איברים $x_1, x_2 \in X$ קיים $g \in G$ כך ש-$g * x_1 = x_2$.

טרנזיטיביות של פעולה שקולה לכך שלכל $x \in X$ מתקיים $\operatorname{orb}(x) = X$, וזה שקול לכך שקיים $x \in X$ עבורו $\operatorname{orb}(x) = X$.

דוגמה 0.14. תהי X קבוצה, ונתבונן בפעולה של $G = S_X$ על X שראינו (כלומר $\sigma * x = \sigma(x)$). יהיו $x_1, x_2 \in X$. ונסמן פונקציה בסימון (x_1, x_2) להיות הפונקציה שמחליפה בין x_1 לבין x_2 ואת שאר איברי X משאירה במקום. כלומר

$$(x_1, x_2)(x) = \begin{cases} x_2 & x = x_1 \\ x_1 & x = x_2 \\ x & x \neq x_1, x_2 \end{cases}$$

ברור כי $(x_1, x_2) \in S_X$. פונקציה כזו נקראת חילוף. ברור כי $(x_1, x_2) * x_1 = x_2$ ולכן הפעולה טרנזיטיבית.

דוגמה 0.15. חבורה G פועלת על עצמה על ידי הצמדה. אז

$$g * e = geg^{-1} = e$$

ולכן אם $|G| > 1$, אז הפעולה היא לא טרנזיטיבית, שהרי $\operatorname{orb}(e) = \{e\}$.

דוגמה 0.16. הפעולה של $GL_n(F)$ על F^n על ידי כפל מטריצה בוקטור אינה טרנזיטיבית, שהרי לכל $A \in GL_n(F)$:

$$A * \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

שימו לב שאם $v, w \in F^n$ אינם וקטור האפס, אז קיימת מטריצה $B \in GL_n(F)$ כך ש-$B * v = w$. כלומר תחת הפעולה הזו יש בדיוק שני מסלולים.

דוגמה 0.17. הפעולה של $GL_n(F)$ על קבוצת הדגלים השלמים ב-V היא טרנזיטיבית. תרגיל לבית.

0.4 משפט מסלול־מייצב

הגדרה 0.18. תהי חבורה G הפועלת על קבוצה X, ויהי $x \in X$. המייצב של x הוא הקבוצה

$$\mathrm{stab}(x) = G_x = \{g \in G \,|\, g * x = x\}$$

לרוב אנחנו נשתמש בסימון $\mathrm{stab}(x)$.

הגדרה 0.19. באופן כללי, המייצב של תת־קבוצה $Y \subseteq X$ הוא

$$\mathrm{stab}(Y) = \{g \in G \,|\, g * Y = Y\}$$

שימו לב כי $g * Y = Y$ הוא שיוויון של קבוצות. יש הגדרה נוספת שבו כל איבר של Y נשמר בפני עצמו, הנקראת תת־חבורת האיזוטרופיה של Y שהיא

$$\{g \in G \,|\, \forall x \in Y,\ g * x = x\} \leq \mathrm{stab}(Y)$$

טענה 0.20. לכל $x \in X$ המייצב $\mathrm{stab}(x)$ ובאופן יותר כללי לכל תת־קבוצה $Y \subseteq X$, המייצב $\mathrm{stab}(Y)$, ותת־חבורת האיזוטרופיה הן כולן תת־חבורות של G.

הוכחה מלאה לבית. נוכיח רק שהמייצב $\mathrm{stab}(Y)$ תת־חבורה.
המייצב $\mathrm{stab}(Y)$ לא ריק כי $e \in \mathrm{stab}(Y)$ לפי הגדרה של פעולה של חבורה על קבוצה.
יהיו $g_1, g_2 \in \mathrm{stab}(Y)$. אז נראה סגירות להופכי. מתקיים $g_1 * Y = Y$, ואז

$$g_1^{-1} * Y = g_1^{-1} * (g_1 * Y) = (g_1^{-1} g_1) * Y = e * Y = Y$$

ולכן גם $g_1^{-1} \in \mathrm{stab}(Y)$. סגירות לפעולה (המצומצמת מ-G) גם קל להוכיח:

$$(g_1 g_2) * Y = g_1 * (g_2 * Y) = g_1 * Y = Y$$

ולכן $g_1 g_2 \in \mathrm{stab}(Y)$. □

דוגמה 0.21. תהי X קבוצה, אז הפעולה שראינו של החבורה S_X על X מקבלים את המייצבים שראינו בעבר.

תרגיל 0.22 (לבית)**.** בפעולה של $GL_n(\mathbb{R})$ על קבוצת הדגלים השלמים, המייצב של הדגל הסטנדרטי הוא קבוצת המטריצות ההפיכות שהן המשולשיות עליונות.

משפט 0.23 (מסלול־מייצב)**.** תהי G חבורה הפועלת על קבוצה X, ויהי $x \in X$. אז

$$[G : \mathrm{stab}(x)] = |G * x|$$

במילים, עוצמת המסלול של x שווה לעוצמת קבוצת המחלקות השמאליות של $\mathrm{stab}(x)$.

הוכחה. נגדיר פונקציה

$$\begin{aligned}\Phi\colon G/\operatorname{stab}(x) &\to G*x\\ g\operatorname{stab}(x) &\mapsto g*x\end{aligned}$$

נוכיח שהפונקציה הזו מוגדרת היטב, חח"ע ועל. מכאן שנקבל שיוויון בין עוצמות שדרוש לטענה.

תחילה נוכיח ש-Φ מוגדרת היטב. אם $g_1\operatorname{stab}(x) = g_2\operatorname{stab}(x)$, אז $g_2^{-1}g_1 \in \operatorname{stab}(x)$. לכן קיים $h \in \operatorname{stab}(x)$ כך ש-$g_1 = g_2h$. א

$$g_1 * x = (g_2h) * x = g_2 * (h * x) = g_2 * x$$

כמו שרצינו, ולכן Φ מוגדרת היטב.

נראה כי Φ היא על. יהי $y \in G * x$. לפי הגדרת מסלול, זה אומר שקיים $g \in G$ כך ש-$y = g * x$. אז

$$\Phi(g\operatorname{stab}(x)) = g * x = y$$

ולכן Φ היא על. כעת נראה שהיא חח"ע. נניח $\Phi(g_1\operatorname{stab}(x)) = \Phi(g_2\operatorname{stab}(x))$. לכן $g_1 * x = g_2 * x$. נפעיל את g_1^{-1} על המשוואה האחרונה ונקבל

$$x = e * x = (g_1^{-1}g_2) * x = g_1^{-1} * (g_1 * x) = g_1^{-1} * (g_2 * x) = (g_1^{-1}g_2) * x$$

כלומר $g_1^{-1}g_2 \in \operatorname{stab}(x)$. כלומר $g_1\operatorname{stab}(x) = g_2\operatorname{stab}(x)$, כמו שרצינו. לכן Φ חח"ע ועל. □

מסקנה 0.24. תהי G חבורה סופית הפועלת על קבוצה X. אז העוצמה של כל מסלול מחלקת את הסדר של G.

הוכחה. יהי $x \in X$. המייצב $\operatorname{stab}(x)$ הוא תת־חבורה של G, ולפי משפט לגראנז' $|G| = |\operatorname{stab}(x)|\,[G : \operatorname{stab}(x)]$. אז לפי משפט מסלול מייצב

$$|G| = |\operatorname{stab}(x)|\,|G * x|$$

ולכן $|G * x|$ מחלקת את $|G|$. □

דוגמה 0.25. אם יודעים שתיים מבין שלוש העוצמות $|\operatorname{stab}(x)|$, $|G * x|$ ו-$|G|$, אז יודעים גם את השלישית. למשל נתבונן בקובייה (חלקה בצבע אחיד), ועל הפעולה של חבורת הסיבובים שלה על קבוצת הפאות של הקובייה. המייצב של פאה הוא בגודל 4, ומפני שהפעולה טרנזיטיבית המסלול של כל פאה הוא בגודל 6. לכן הסדר של חבורת הסיבובים הוא $6 \cdot 4 = 24$. קצת יותר קשה להוכיח שהחבורה הזו איזומורפית ל-S_4.

חבורת השיקופים והסיבובים של הקובייה היא מסדר 48, וכמובן שחבורת הסיבובים היא תת־חבורה שלה מאינדקס 2.

הערה 0.26. גם את העוצמה של $|X|$ אפשר לחשב עם מייצבים ומסלולים. נסמן ב-$\mathcal{O}$ את קבוצת המסלולים תחת הפעולה, ולכל מסלול $O \in \mathcal{O}$ נבחר נציג x_O. אז

$$X = \bigcup_{O \in \mathcal{O}} O$$

וזהו איחוד זר. לכן

$$|X| = \sum_{O \in \mathcal{O}} |O| = \sum_{O \in \mathcal{O}} [G : \mathrm{stab}(x_O)]$$

הגדרה 0.27. תהי חבורה G הפועלת על קבוצה X, ויהי $x \in X$. נאמר כי x הוא נקודת שבת של הפעולה אם $g * x = x$ לכל $g \in G$. זה קורה אם ורק אם $G * x = \{x\}$, וזה קורה אם ורק אם $|G * x| = 1$.

נסמן את קבוצת נקודות השבת של X תחת הפעולה בסימון $\mathrm{Fix}(X)$.

דוגמה 0.28. תהי G חבורה הפועלת על עצמה על ידי הצמדה. מתי $x \in \mathrm{Fix}(G)$? זה אם ורק אם $x = g * x = gxg^{-1}$ לכל $g \in G$. כלומר $gx = xg$ לכל $g \in G$. זה קורה אם ורק אם $x \in Z(G)$. לכן $\mathrm{Fix}(G) = Z(G)$.

0.5 חבורות-p

נראה קצת תורת מבנה של חבורות סופיות.

הגדרה 0.29. יהי p מספר ראשוני. חבורה G תקרא חבורת-p אם הסדר של כל איבר הוא חזקה של p.

משפט 0.30 (קושי)**.** תהי G חבורה סופית, ויהי p מספר המחלק את הסדר שלה. אז קיים איבר ב-G מסדר p.

הוכחה בהמשך, אבל קודם מסקנות ודוגמאות.

טענה 0.31. תהי G חבורה סופית. אז G היא חבורת-p אם ורק אם $|G| = p^n$ עבור n כלשהו.

הוכחה. אם G היא מסדר p^n, אז ראינו מסקנה ממשפט לגראנז' שהסדר של כל איבר מחלק את הסדר של החבורה. לכן הסדר של כל איבר הוא p^i עבור $0 \leq i \leq n$ כלשהו, וסיימנו.

בכיוון השני, נניח כי G חבורת-p סופית. נניח בשלילה שיש ראשוני $q \neq p$ המחלק את הסדר של G. אז לפי משפט קושי, קיים איבר מסדר q ב-G. זו סתירה לכך ש-G היא חבורת-p. לכן רק p מחלק את $|G|$. $\square$

טענה 0.32. תהי G מסדר p^n הפועלת על קבוצה סופית X. אז

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

הוכחה. נניח כי $|G| = p^n$ לפי הטענה הקודמת. לפי המסקנה ממשפט מסלול־מייצב, העוצמה של כל מסלול מחלקת את $|G| = p^n$. לכן העוצמה של כל מסלול שייכת לקבוצה $\{1, p, p^2, \ldots, p^n\}$.

איבר $x \in X$ הוא נקודת שבת אם ורק אם $|G * x| = 1$. לכן המסלולים של האיברים ב-$X \setminus \mathrm{Fix}(X)$ הם מעוצמה ששייכת לקבוצה $\{p, p^2, \ldots, p^n\}$. כלומר p מחלק את הגודל של המסלולים האלו. כלומר מודולו p הגודל שלהם שקול ל-0.

מפני ש-X היא איחוד זר של מסלולים, אז

$$|X| = \bigcup_{x \in X} |G * x| = |\mathrm{Fix}(X)| \cdot 1 + \sum_{i=1}^{n} C_i \left| X \setminus \mathrm{Fix}(X) \right| \cdot p^i$$

אז מפני ש-$p^i \equiv 0 \pmod p$ לכל $1 \leq i \leq n$ נקבל את הדרוש. □

תרגיל 0.33. הוכיחו שהמרכז של חבורת-p סופית (שאינה טריוויאלית) אינו טריוויאלי.

פתרון. תהי G חבורת-p מסדר p^n, עבור $n \geq 1$. היא פועלת על עצמה על ידי הצמדה, וראינו ש-$Z(G) = \mathrm{Fix}(G)$ תחת הפעולה הזו. אז לפי הטענה הקודמת

$$|Z(G)| \equiv |G| \pmod p$$

לכן $|Z(G)| \equiv 0 \pmod p$. ידוע כי $e \in Z(G)$. כלומר $|Z(G)| > 0$, ומפני ש-$p|\,|Z(G)|$, נסיק כי $|Z(G)| \geq p$. בפרט $Z(G) \neq \{e\}$.

הוכחת משפט קושי. תהי G חבורה סופית, ונניח $p|\,|G|$ ראשוני. נגדיר

$$X = \{(g_0, g_1, \ldots, g_{p-1}) \mid g_i \in G, g_0 g_1 \ldots g_{p-1} = e\}$$

במילים, אלו הן ה-p-יות הסדורות של איברי G שמכפלתן היא e. קל לחשב $|X| = |G|^{p-1}$ כי

$$g_0 = (g_1 \ldots g_{p-1})^{-1}$$

החבורה $\mathbb{Z}_p$ פועלת על X בעזרת הזזה סיבובית של האינדקסים בכל p-יה. לכל $\overline{n} \in \mathbb{Z}_p$ נזיז את האינדקסים n מקומות שמאלה:

$$\overline{n} * (g_0, g_1, \ldots, g_{p-1}) = (g_{n+0}, g_{n+1}, \ldots, g_{n+p-1})$$

כאשר האינדקסים מחושבים מודולו p.

צריך לבדוק שלכל $(g_0, g_1, \ldots, g_{p-1}) \in X$ גם $\overline{n} * (g_0, g_1, \ldots, g_{p-1}) \in X$. מספיק לבדוק זאת עבור $\overline{1}$, ולהשתמש באינדוקציה. כלומר נתון כי $g_0 g_1 \ldots g_{p-1} = e$ ורוצים להראות שגם

$$\overline{1} * (g_0, g_1, \ldots, g_{p-1}) = (g_1, \ldots, g_{p-1}, g_0) \in X$$

נצמיד ב-g_0^{-1} ונקבל

$$g_0^{-1}g_0g_1\dots g_{p-1}g_0=g_0^{-1}eg_0$$
$$g_1\dots g_{p-1}g_0=e$$

כמו שרצינו. קל לראות כי $\bar{0}*(g_0,g_1,\dots,g_{p-1})=(g_0,g_1,\dots,g_{p-1})$.
בנוסף ידוע לנו כי $|\mathbb{Z}_p|=p$, ולכן $\mathbb{Z}_p$ היא חבורת-p סופית. לפי הטענה הקודמת

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

מפני ש-$|X|=|G|^{p-1}$ וידוע לנו כי p מחלק את $|G|$,אז $p||X|$. לכן $|\mathrm{Fix}(X)|\equiv 0 \pmod p$. יהי איבר $(g_0,\dots,g_{p-1})\in\mathrm{Fix}(X)$. אז

$$(g_0,g_1,\dots,g_{p-1})=\bar{1}*(g_0,g_1,\dots,g_{p-1})=(g_1,g_2,\dots,g_{p-1},g_0)$$

אז מהשוואה בכל קואורדינטה של ה-p-יות נקבל $g_0=g_1=g_2=\dots=g_{p-1}$. כלומר אם $(g_0,\dots,g_{p-1})\in\mathrm{Fix}(X)$, אז $g_{p-1}=\dots=g_0=g$ עבור $g\in G$ קבוע. אם $(g,\dots,g)\in X$, אז $g^p=e$. לכן $o(g)|p$ לפי טענה מהרצאה קודמת.
אז יש התאמה חח"ע ועל בין קבוצת נקודות השבת ב-X תחת הפעולה לעיל, לבין קבוצת האיברים ב-G שהסדר שלהם מחלק את p.

$$|\mathrm{Fix}(X)|=|\{g\in G\,|\,o(g)|p\}|$$
$$(g,\dots,g)\hookleftarrow g$$

אבל ידוע לנו על לפחות איבר אחד שהוא נקודת שבת, והוא $(e,\dots,e)$, כי $o(e)=1|p$. לכן $|\{g\in G\,|\,o(g)|p\}|>1$, ולכן יש לפחות $p-1$ איברים מסדר p בחבורה, כי איבר היחידה הוא היחיד מסדר p. □

תרגיל 0.34. יהי p ראשוני, ותהי חבורה G מסדר p^2. אז G אבלית.

פתרון. אולי בהרצאה הבאה.