תזכורת:

תהי G חבורה ו- $H\leq G$. H משרה שני סוגים של יחסי שקילות על G. ולכן שני חלוקות של G / מחלקות שקילות/קבוצת מנה

מחלקות שמאליות וימניות:

- מחלקות שמאליות של G ביחס ל- H: הקבוצות מהצורה aH
- מחלקות ימניות של G ביחס ל- H: הקבוצות מהצורה Ha

הערות:

1. $aH = H \iff a\in H$
2. $aH = bH \iff a\in bH \iff b\in aH$

קוג מאות:

1) $H = \langle(1,2)\rangle = \{(1,2), e\}$ $\qquad$ $G = S_3$

מחלקות שמאליות:

$eH = H = \{(1,2), e\}$

$(1,3)H = \{(1,3), (1,2,3)\}$

$(2,3)H = \{(2,3), (1,3,2)\}$

מחלקות ימניות:

$He = H = \{(1,2), e\}$

$H(1,3) = \{(1,3), (1,3,2)\}$

$H(2,3) = \{(2,3), (1,2,3)\}$

הערה מחלקה ימנית לא בהכרח שווה למחלקה שמאלית

$(1,3)H \neq H(1,3)$

סימון:

1) יהי קבוצת המנה מסמנים

G/H -קבוצת המחלקות השמאליות

$H \backslash G$ - קבוצת המחלקות הימניות

2. $|G/H| = |H \backslash G| = [G:H]$ האינדקס של H ב- G

$|G| = |H| \cdot [G:H]$

מסקנה:

יהי H תת חבורה של G אז $|H| \mid |G|$

מסקנה:

לכל $a \in G$ $o(a) \mid |G|$

לכן לכל $a \in G$ כאשר G סופית $a^{|G|} = e$

דוגמאות למחלקות:

1) $G = \mathbb{Z}$ $H = 5\mathbb{Z}$

$0 + H = H = 5\mathbb{Z} = \{0, \pm 5, \pm 10, \ldots\}$

$1 + H = 1 + 5\mathbb{Z} = \{1, 6, -4, 11, -9, \ldots\}$

סה"כ יש 5 מחלקות.

2) תנו דוגמא לחבורה G ו- $H \leq G$ כך ש $[G:H] = \infty$

לכל חבורה אינסופית G, $H = \{e\}$, $[G:\{e\}] = |G|$

3) $G = GL_2(\mathbb{R})$ - יש א איברים

$H = \langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$ - 2 איברים

לכן $[G:H] = א$

תרגיל:

תהי G חבורה מסדר 8

1) הוכיחו שאם G ציקלית, אז קיימת לה תת חבורה ציקלית מסדר 4

ב) הוכיחו שאם G לא אבלית, אז קיימת לה תת חבורה ציקלית מסדר 4

ג) מצאו דוגמא נגדית לסעיף הקודם כאשר G אבלית

פתרון:

א) $G=\langle a\rangle$ $\quad H=\langle a^2\rangle=\{a^2,a^4,a^6,e\}$

ב) $|G|=8$ הסדרים האפשריים לאיברים $1,2,4,8$

לא קיים איבר מסדר 8, כי אז G הייתה ציקלית ולכן אבלית בסתירה.

לא יתכן שכל שאר האיברים מסדר 2, כי הוכחנו שאם לכל $a\in G$ מתקיים $a^2=e$ אז G אבלית. לכן קיים איבר מסדר 4

ג) $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$

זאת חבורה אבלית עם 8 איברים אבל כל איבר בריבוע שווה ל- e

תרגיל: (הכללה)

הוכיחו שאם $t\geq 3$, $|G|=2^t$, לא אבלית, אז יש ב-G איבר מסדר 4.

פתרון:

הסדרים האפשריים לאיברים $\underbrace{1}_{\text{רק איבר היחידה}},2,4,\dots,2^k$. $k\leq t$

לא יתכן איבר מסדר 2^t כי אז G ציקלית $\Leftarrow$ אבלית

לא יכול להיות שכל האיברים רחוק מ-e מסדר 2 כי אז G אבלית

קיים איבר מסדר 2^k $2 \le k < t$:

$$O(a) = 2^k \Rightarrow O(a^2) = \frac{2^k}{(2^k, 2^{k-2})} = 2^2 = 4$$

תרגיל:

הוכיחו שכל חבורה מסדר 4 היא אבלית

פתרון:

הסדרים האפשריים: 1,2,4

אם יש איבר מסדר $4 \Leftarrow$ המבורה ציקלית ולכן אבלית

אחרת כל האיברים מסדר $2 \Leftarrow G$ אבלית

משפט אוילר:

עבור $G = U_n$, (נשתמש בכך ש $a^{|G|} = e$ ומקבלים לכל איבר מצא

שזר ל-n $a^{\varphi(n)} \equiv 1 \mod n$

בפרט עבור p ראשוני, לכל $(x,p)=1$:

$e^{p-1} = 1 \mod p$ (המשפט הקטן של פרמה)

תרגיל:

מצאו את 2 הספרות האחרונות של $88211^{4039} + 2020$

פתרון:

מציאת שתי ספרות אחרונות של מספר זה פשוט $\mod 100$

$$88211^{4039} + 2020 \mod 100 = 11^{4029} \mod 100 + 20 \mod 100$$

$$11^{\varphi(100)} = 11^{40} \equiv 1 \mod n$$

$$11^{4039} = \underbrace{11^{4040}}_{1 \mod 100} \cdot 11^{-1}.$$

נמצא את ההופכי של 11 ב-$\mathbb{Z}_{100}$ כפלי

$$100 = 9 \cdot 11 + 1 \Rightarrow 1 = 100 - 9 \cdot 11 \Rightarrow 11^{-1} \equiv 91 \mod 100$$

$91+20 \mod 100 = 111 \mod 100 = 11 \mod 100$ לכן

שתי הספרות האחרונות: 11

פעולות של חבורה על קבוצה:

G חבורה, X קבוצה. G פועלת על X אם קיימת פו'

$G \times X \to X$
$(g,x) \mapsto g*x$

שמקיימת

1) $\forall x \in X, \quad e*x = x$

2) $\forall g,h \in G, x \in X \quad g*(h*x) = (gh)*x$

דוגמאות:

1) $G = S_n$ פועלת על $X = \{1,...,n\}$ $\quad (1,2)*2 = 1$

2) S_n פועלת על $X = \mathbb{F}[x_1,...,x_n]$

למשל $n=4$

$x_1x_2 - x_3$

$x_2^4 + x_4^3 - x_1$

מפעילים את התמורה על האינדקסים

3) $G = GL_n(\mathbb{F})$ פועלת על $\mathbb{F}^n$. מכפילים את המטריצה בוקטור

4) G פועלת על עצמה $g*x = gx$

5) G פועלת על עצמה $g*x = g^{-1}xg$

הגדרה: תהי G חבורה. שפועלת על X. נגיד שG פועלת

"נאמנה" על X אם $\forall \underset{e \neq}{g} \in G \; \exists x \in X: \; gx \neq x$

דוגמאות:

1) S_n על $\{1,...,n\}$ נאמנה

2) S_n על $\mathbb{F}[x_1,...,x_n]$ אם σ מזיזה איפשהו j אז היא מזיזה את הפולינום x_j ולכן זו פעולה נאמנה

3) $GL_n(\mathbb{F})$ על $\mathbb{F}^n$ פועלת נאמנה. תהי $A\neq I\in G$ כך ש $c_i(A)\neq e_i$

$Ae_i = c_i(A)$

4) פעולה נאמנה יהי $g\neq e$ $\forall x\in G\ \ gx\neq x$

5) לא בהכרח, למשל אם G אבלית $\forall g,x\ \ g*x=x$

הגדרה: תהי G חבורה שפועלת על X. לכל $x\in X$ נגדיר:

1) המסלול של x $\{gx|g\in G\}=orb(x)\subseteq X$

2) המייצב של x, $\{g\in G|gx=x\}=Stab(x)\leq G$

דוגמאות:

1) $GL_n(\mathbb{F})$ פועלת על $\mathbb{F}^n$ $orb\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}=\left\{\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}\right\}$

כל שאר הווקטורים במסלול 1

הסבר: יהי $u,v\neq 0$ את כל אחד מהם נשלים לבסיס ל- $\mathbb{F}^n$

$B=\{u=u_1,...,u_n\}$ בסיס $C=\{v=v_1,...,v_n\}$ בסיס

נגדיר $T:\mathbb{F}^n\to\mathbb{F}^n$ $T(u)=v$ $(T(u_i)=v_i)$

לפי משפט ההגדרה זה נותן העתקה לינארית

היא הפיכה. נוכיח שהיא חח"ע:

$$T\left(\sum\alpha_i u_i\right)=\sum\alpha_i v_i=0 \Rightarrow \alpha_i=0$$

העתקה לינארית חח"ע ממרחב לעצמו היא הפיכה

ניקח $A=[T]_S^S$ $Au=[T(u)]=v$

ב) מי המייצב של וקטור v?
כאשר קיים וקטור שהמייצב שלו טריוויאלי?

תשובה:

ל.ו. לכל וקטור v נוכל למצוא $A \neq I$ הפיך כך ש $Av=v$

הוכחה:

אם $v=0$ $stab(v) = GL_n(\mathbb{F})$

אם $v \neq 0$ נרחיב לשני בסיסים שונים:

$$\mathcal{B} = \{v, v_2 .. v_n\} \quad C = \{v, u_2, \dots, u_n\}$$

ושם מגדיר העתקה לינארית הפיכה, לפי משפט ההגדרה

$$A = [T]_S^S \quad T(v) = v \quad T \neq I$$

תרגיל:

S_n פועלת על $\mathbb{F}[x_1, x_2, x_3, x_4]$ מצאו מסלול ומייצב ל- $x_1x_2 + x_3x_4$

פתרון:

$$orb = \{x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3\}$$

$$Stab = \{e, (1,2), (3,4), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3), (1,3,2,4), (1,4,2,3)\}$$

תרגיל:

G פועלת על עצמו ע"י כפל משמאל. לכל איבר $x \in G$ מצאו מסלול ומייצב.

פתרון:

$$stab(x) = \{e\}$$

כי אם $gx = x$
$\Downarrow$
$g = e$

$$orb(x) = G$$

כי לכל $y \in G$ $yx^{-1} \in G$ ולכן $yx^{-1} * x = y$