תזכורת:

G פועלת על A. ויהי לכל $a\in A$ הגדרנו מייצב $G_a=\{g\in G: g*a=a\}$

תמיד $G_a\leq G$ תת חבורה.

המסלול של a: $G*a=\{g*a \mid g\in G\}=\{x\in A: \exists g\in G\ g*a=x\}$

משפט מסלול מייצב:

$$|G*a|=[G:G_a]=\frac{|G|}{|G_a|}$$

$|G|$ אינו סופי

$Fix(A)=\{a\in A: g*a=a \ \ g\in G \text{ לכל}\}$

אם p ראשוני, G סופית אזי G נקראת p-חבורה

אם $|G|=p^k$, $k\geq 1$

הוכחנו שאם G היא p-חבורה שפועלת על קבוצה סופית A

אזי $|Fix(A)|\equiv|A| \bmod p$

משפט: (קושי)

תהי G חבורה סופית, יהי p ראשוני כך ש $p\,||G|$. אזי קיים $g\in G$

כך ש $o(g)=p$.

הוכחה:

נגדיר $A=\{(g_1,\dots,g_p)\in G^p \mid g_1\cdot\ldots\cdot g_p=e\}$. אזי $|A|=|G|^{p-1}$

אכן את $g_1,\dots,g_{p-1}$ נוכל לקבוע באופן חופשי

ואת g_p נבחר להיות ההופכי של $g_1\cdot\ldots\cdot g_{p-1}$

הנחנו ש $p\,||G|$, לכן $p\,||A|$

החבורה $\mathbb{Z}_p$ פועלת על A: $[n]*(g_1,\dots,g_p)=(g_{n+1},g_{n+2},\dots,g_p,g_1,\dots,g_n)$

מזיזים הכל n מקומות שמאלה

נבדוק שלכל $(g_1,\dots,g_p)\in A$ גם $[n]*(g_1,\dots,g_p)\in A$.

מספיק לבדוק עבור $[1]\cdot(g_1,\dots,g_p)$. אבל, $(g_1,\dots,g_p)\in A$

אומר e $\quad g_1\cdot\ldots\cdot g_p=e$

$$g_1^{-1}(g_1\cdot\ldots\cdot g_p)\cdot g_1=g_1^{-1}e\,g_1 \Rightarrow g_2\cdot\ldots\cdot g_p\cdot g_1=e$$

ולכן $[1]\cdot(g_1,\dots,g_p)=(g_2,\dots,g_p,g_1)\in A$

ברור כי $|\mathbb{Z}_p|=p$, לכן $\mathbb{Z}_p$ הינה p-חבורה, ולפי הטענה מן הפעם שעברה, $|Fix(A)|=|A| \bmod p$

אך הוכחנו כי $|A|\equiv 0 \bmod p$

לכן $|Fix(A)|\equiv 0 \bmod p$

אם $(g_1,\dots,g_p)\in Fix(A)$ אז

$$[1]\cdot(g_1,\dots,g_p)=(g_2,\dots,g_p,g_1)=(g_1,\dots,g_p)$$

נשווה את ה p-יות

$$g_1=g_2=\ldots=g_{p-1}=g_p=g_1$$

לכן $(g_1,\dots,g_p)\in Fix(A) \iff (g_1,\dots,g_p)=(g,\dots,g)$ עבור $g\in G$ קבוע

אבל $(g,\dots,g)\in A \iff g^p=e \iff o(g)\mid p$

לכן $|Fix(A)|=|\{g\in G: o(g)\mid p\}|$

$$(g,\dots,g)\longleftarrow g$$

אבל הקבוצה $\{g\in G: o(g)\mid p\}$ לא ריקה, כי היא מכילה e.

אבל העוצמה שלה מתחלקת ב- p, לכן העוצמה היא לפחות p ולכן גדולה מ-1

זה אומר שבקבוצה $\{g\in G: o(g)\mid p\}$ יש איברים לא-טריוויאליים

יהי g איבר כזה. אזי $o(g)\mid p$ אבל $g\neq e$ ולכן $o(g)\neq 1$

ולכן בהכרח $o(g)=p$

הגדרה: תהי G חבורה, $a\in G$. המרכז של a הינו

$C_G(a)=\{g\in G : ga=ag\}$

טענה:

תהי G חבורה, $a\in G$ אזי $C_G(a)$ תת-חבורה של G

הוכחה:

נתבונן בפעולה של G על עצמה ע"י הצמדה $g*a=gag^{-1}$

לפי הפעולה הנ"ל, המייצב של a הינו

$g\in G_a \iff g*a=a \iff gag^{-1}=a \iff ga=ag \iff g\in C_G(a)$

הוכחנו כבר שמייצב G_a הוא תמיד תת חבורה. לכן $C_G(a)$

תת-חבורה, כי הוא המייצב של a עבור פעולה מסויימת

הבחנה:

$Z(G)=\{g\in G : ga=ag \quad \text{לכל } a\in G\}$

$Z(G)=\bigcap_{a\in G} C_G(a)$

תזכורת:

חבורה G נקראת ציקלית אם"ם קיים $g\in G$ כך ש $G=\langle g\rangle$

טענה:

יהי p ראשוני, תהי G חבורה מסדר p. אזי G ציקלית

הוכחה:

לפי קושי קיים $g\in G$ כך ש $O(g)=p$ לכן $|G|=p=|\langle g\rangle|$

לכן $\langle g\rangle=G$

הבחנה:

חבורה מסדר p^2 לא בהכרח ציקלית. למשל:

$G = \mathbb{Z}_p \times \mathbb{Z}_p$

לכל $g=(g_1,g_2)\in G$, $g^p=(g_1^p,g_2^p)=(e,e)=e_G$

לכן $o(g)|p$

בפרט אין איברים מסדר p^2, לכן G לא ציקלית

טענה:

יהי p ראשוני, תהי G חבורה. נניח $|G|=p^2$ אזי G אבלית

הוכחה:

$|G|=p^2$ לכן G הינה p-חבורה. הוכחנו בפעם הקודמת

שהמרכז של כל p-חבורה לא טריויאלי.

הוכחנו בתרגול ש $Z(G)$ הינו תת חבורה של G

לפי לגרנג' $|Z(G)|\,\big|\,|G| \Rightarrow |Z(G)|\,\big|\,p^2$

$|Z(G)|\in\{1,p,p^2\}$ אבל $Z(G)$ לא טריוויאלית

לכן $|Z(G)|\neq 1$

נניח בשלילה ש $|Z(G)|=p$

יהי $g\in G\setminus Z(G)$ ברור כי g מתחלף עם עצמו לכן $g\in C_G(g)$

מצד שני, ראינו כי $Z(G)\subseteq C_G(g)$

לכן $|C_G(g)|\geq p+1$ (p איברים מ-$Z(G)$ וגם g)

אבל, $C_G(g)$ הינו תת-חבורה של G. לפי לגרנג' מסיקים ש

$|C_G(g)|=p^2$ כלומר $C_G(g)=G$

כלומר g מתחלף עם כל איבר ב-G. כלומר, $g\in Z(G)$

וגם $g\notin Z(G)$ בסתירה. לכן $|Z(G)|\neq p$

סה"כ $|Z(G)|=p^2$ כלומר $Z(G)=G$ כלומר G אבלית

אבחנות שעלו תוך כדי ההוכחה:

1) לכל חבורה G ולכל $g\in G$, $g\in C_G(g)$

2) $g\in Z(G) \iff C_G(g)=G$

מה לגבי חבורות מסדר p^3?

לא בהכרח אבליות.

$$H(\mathbb{Z}_p)=\left\{\begin{pmatrix}1&a&c\\0&1&b\\0&0&1\end{pmatrix} \;\middle|\; a,b,c\in\mathbb{Z}_p\right\}$$

פעולה: כפל מטריצות

תרגיל: לבדוק שזו אכן חבורה.

ברור ש $|H(\mathbb{Z}_p)|=p^3$. היא לא אבלית כי $Z(H(\mathbb{Z}_p))=\left\{\begin{pmatrix}1&\boxed{0}&c\\0&1&\boxed{0}\\0&0&1\end{pmatrix} \;\middle|\; c\in\mathbb{Z}_p\right\}$

הומומורפיזמים:

הגדרה: תהיינה G,H שתי חבורות. העתקה $f:G\to H$ נקראת הומומורפיזם אם לכל $g_1,g_2\in G$ מתקיים $f(g_1 *_G g_2)=f(g_1) *_H f(g_2)$

דוגמאות:

1) תהיינה G,H שתי חבורות. $f:G\to H$ $f(g)=e_H$ לכל $g\in G$

ההומומורפיזם הטריוויאלי

אכן הומומורפיזם $f(g_1g_2)=e_H=e_H e_H=f(g_1)f(g_2)$

e_H,e_G איבר היחידה של G ו-H בהתאמה

2) G חבורה, $H\le G$ תת חבורה. $f:H\to G$ ההכלה

$f(h)=h$ לכל $h\in H\le G$

3) G חבורה כלשהי, $g\in G$. $f:\mathbb{Z}\to G$ $f(n)=g^n$

צ.ל הומ׳:

$$f(n+m)=g^{n+m}=g^n g^m=f(n)f(m)$$

התמונה של f היא $\langle g\rangle$

4) מקרה פרטי של 3. יהי $m\in\mathbb{N}$. $f:\mathbb{Z}\to\mathbb{Z}_m$, $f(n)=[n]$

נשים לב כי $[n]=[1]^n$ לכן זה מקרה פרטי של 3

כאשר $G=\mathbb{Z}_m$, $g=[1]$

5) $f:GL_n(\mathbb{R})\to\mathbb{R}^*$ $\quad f(A)=\det A$

כן

$$f(AB)=\det(AB)=\det A\cdot\det B=f(A)f(B)$$

6) $f:\mathbb{R}\to GL_2(\mathbb{R})$ ($\mathbb{R}$ עם חיבור), $f(x)=\begin{pmatrix}1&x\\0&1\end{pmatrix}$

$$f(x)f(y)=\begin{pmatrix}1&x\\0&1\end{pmatrix}\begin{pmatrix}1&y\\0&1\end{pmatrix}=\begin{pmatrix}1&x+y\\0&1\end{pmatrix}=f(x+y)$$

7) $f:\mathbb{R}\to GL_n(\mathbb{R})$, $f(x)=\begin{pmatrix}1&0&\cdots&0&*\\&\ddots&&&0\\&&\ddots&&\vdots\\&0&&\ddots&0\\&&&&1\end{pmatrix}$

8) $f:\mathbb{R}\to GL_2(\mathbb{R})$ $\quad f(x)=\begin{pmatrix}\cos x&-\sin x\\\sin x&\cos x\end{pmatrix}$

כן

$$f(x)f(y)=\begin{pmatrix}\cos x&-\sin x\\\sin x&\cos x\end{pmatrix}\begin{pmatrix}\cos y&-\sin y\\\sin y&\cos y\end{pmatrix}=$$

$$=\begin{pmatrix}\cos x\cos y-\sin x\sin y&-\cos x\sin y-\sin x\cos y\\\sin x\cos y+\cos x\sin y&\cos x\cos y-\sin x\sin y\end{pmatrix}=$$

$$=\begin{pmatrix}\cos(x+y)&-\sin(x+y)\\\sin(x+y)&\cos(x+y)\end{pmatrix}=f(x+y)$$

כי $f(x+2\pi)=f(x)$ ולכן f אינה חח"ע

9) תהי G חבורה שפועלת על הקבוצה A. לכל $g\in G$ הגדרנו $f_g:A\to A$

$f_g(a)=g*a$. הוכחנו כי f_g חח"ע ועל כי $f_{g^{-1}}$ הופכי דו-צדדי

לכן $f_g\in S_A$ $\quad$ ($S_A=\{f:A\to A$ חח"ע ועל$\}$) הרכבת פונקציות)

צב נותן לנו העתקה. $\varphi: G \to S_A$, $\varphi(g) = f_g$

צב הומומורפיזם. צריך להוכיח כי $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$

$f_{g_1 g_2} = f_1 \circ f_2$.

יהי $a \in A$ שרירותי. אזי:

$$f_{g_1 g_2}(a) = g_1 g_2 * a = g_1 * (g_2 * a) = g_1 * f_{g_2}(a) = f_{g_1}(f_{g_2}(a))$$

אכן $f_{g_1 g_2} = f_{g_1} \circ f_{g_2}$

טענה:

יהי $f: G \to H$ הומומורפיזם אזי:

1) $f(e_G) = e_H$

2) לכל $g \in G$ $f(g^{-1}) = (f(g))^{-1}$

הוכחה:

1) יהי $g \in G$, אזי $g = e_G g$ לכן $f(g) = f(e_G g) = f(e_G) f(g)$

נכפיל מימין ב- $(f(g))^{-1}$ $e_H = f(e_G)$

2) יהי $g \in G$. אזי $g g^{-1} = e_G$ לכן

$$f(g) f(g^{-1}) = f(g g^{-1}) = f(e_G) = e_H$$

לכן $f(g^{-1}) = (f(g))^{-1}$

הגדרה: יהי G חבורה. $H \leq G$ תת חבורה. H נקראות תת-חבורה נורמלית אם לכל $g \in G$, $h \in H$ מתקיים $g h g^{-1} \in H$

מסמנים $H \trianglelefteq G$

דוגמאות:

1) G כלשהי. תת-החבורה $H = \{e\}$ נורמלית

אכן לכל $g \in G$ $g e g^{-1} = e$ לכן $\{e\} \trianglelefteq G$

2) $H=G$ גם נורמלית

3) אם G אבלית אזי כל תת חבורה היא נורמלית.

אכן, $ghg^{-1}=gg^{-1}h=h\in H$

4) G חבורה כלשהי. אזי $Z(G)\trianglelefteq G$. אכן, ראינו בתרגול ש $Z(G)$ תת-חבורה. יהי $h\in Z(G)$, יהי $g\in G$. אזי $gh=hg$

$$ghg^{-1}=h\in Z(G)$$

5) יהי $f:G\to H$ הומ׳. (H לא בהכרח תת-חבורה של G)

הגרעין של f הינו המקור של e_H

$$\ker(f)=f^{-1}(e_H)=\{g\in G: f(g)=e_H\}$$

טענה: $\ker f\trianglelefteq G$

הוכחה:

אם $g_1,g_2\in\ker f$ אזי $f(g_1g_2)=f(g_1)f(g_2)=e_He_H=e_H$

לכן $g_1g_2\in\ker f$

אם $g\in\ker f$, הוכחנו (בטענה הקודמת) $f(g^{-1})=(f(g))^{-1}=e_H^{-1}=e_H$

לכן $g^{-1}\in\ker f$.

$\ker f$ סגור לכפל ולהפכיים, כלומר $\ker f$ תת-חבורה של G

יהי $h\in\ker f$, $g\in G$

$$f(ghg^{-1})=f(g)f(h)f(g^{-1})=f(g)f(g^{-1})=e_H$$

לכן $ghg^{-1}\in\ker f$ $\Leftarrow$ $\ker f\trianglelefteq G$

טענה:

G חבורה, $H \leq G$ תת-חבורה.

אז: $H \trianglelefteq G \iff gH = Hg$ לכל $g \in G$

(המחלקות מימין הן המחלקות משמאל)

הוכחה:

($\Rightarrow$) יהי $h \in H$, $g \in G$. אז $gh \in gH = Hg = \{xg : x \in H\}$

לכן קיים $x \in H$ כך ש $gh = xg \Leftarrow ghg^{-1} = x \in H$

לכן $H \trianglelefteq G$

($\Leftarrow$) נניח $H \trianglelefteq G$. יהי $g \in G$, $h \in H$

$$gh = \underbrace{(ghg^{-1})}_{\in H} g \in Hg$$

לכן $gH \subseteq Hg$

באותו אופן,

$$hg = g\underbrace{(g^{-1}h(g^{-1})^{-1})}_{\in H} \in gH$$

לכן $Hg \subseteq gH$ וסה"כ $gH = Hg$

בחזרה להומומורפיזמים:

הגדרה: $f: G \to H$ הומ'. $Im(f) = f(G) = \{f(g) : g \in G\} \leq H$

טענה:

יהי $f: G \to H$ הומ'

1) $\ker(f) \trianglelefteq G$

2) $f(G) \leq H$ תת חבורה (לאו בהכרח נורמלי)

הוכחה:

1) הוכחנו בדוגמא 5

2) נבדוק סגירות לכפל ולהפכיים. יהיו $h_1, h_2 \in f(G)$. צ"ל קיימים $g_1, g_2 \in G$

כך ש $f(g_1)=h_1$, $f(g_2)=h_2$. לכן:

$f(g_1 g_2) = f(g_1) f(g_2) = h_1 h_2$

לכן $h_1 h_2 \in f(G)$

כמו כן, אם $h \in f(G)$, קיים $g \in G$ כך ש $f(g)=h$ הוכחנו

כי $f(g^{-1}) = (f(g))^{-1} = h^{-1}$ ולכן $h^{-1} \in f(G)$

לכן $f(G)$ תת-חבורה של H

הכללה:

יהי $f: G \to H$ הומ'. יהי $h \in f(G)$. קיים $g \in G$ כך ש $f(g)=h$

המקור של h $f^{-1}(h) = \{x \in G : f(x)=h\}$

נשים לב ש:

$x \in f^{-1}(h) \iff f(x) = h = f(g) \iff f(x)^{-1} f(g) = e_H \iff f(x^{-1}) f(g) = e_H$

$\iff f(x^{-1} g) = e_H \iff x^{-1} g \in \ker f$

הוכחנו $x \in f^{-1}(h) \iff x, g$ שייכים לאותה מחלקה של $\ker f$

(לא חשוב אם מחלקה ימין או משמאל כי $\ker f \trianglelefteq G$)

הוכחנו:

טענה:

יהי $f: G \to H$ הומ'. יהי $h \in f(G)$. המקור $f^{-1}(h)$ הינו מחלקה

אחת של $\ker f$, כלומר $g(\ker f) = (\ker f) g$

כאשר $g \in f^{-1}(h)$

תוצאה:

יהי $f:G\to H$ הומ׳. אזי f חח״ע $\iff$ $\ker f=\{e_G\}$

הוכחה:

f חח״ע $\iff$ לכל מקור יש רק איבר אחד $\iff$

$\iff$ לכל מחלקה של $\ker f$ יש איבר 1 $\iff$ $|\ker f|=1$ $\iff$

הוכחנו $|gH|=|H|$

$\iff$ $\ker f=\{e_G\}$