חבורות

בעצם הדבר שמגיעים ל- $1=(a,1)$ או $a=(a,0)$

משפט

(a,b) הוא הצ"ל המינימלי של a,b.

$(a,b)=\min\{au+bv \mid u,v\in\mathbb{Z}\setminus\{0\}\}$ | $(180,125)=(135,45)=(45,0)=45$

משפט $(a,b)=au+bv$

אלגוריתם אוקלידס המורחב

$61=1\cdot51+10$

$(237,61)=(61,51)=(51,10)=(10,1)=1$

$237=61\cdot3+51$ $\qquad$ $51=10\cdot5+1$

$1=51-10\cdot5=61-10-(61-51)\cdot5=$

$=61-(61-51)-(61-51)\cdot5=$

$=61-6(61-(237-3\cdot61))=61-6(61-237+3\cdot61)=$

$=61-6\cdot61+6\cdot237-18\cdot61=6\cdot237-23\cdot61$

תרגיל

אם $(a,b)=1$ ו- $a|bc$ אז $a|c$

פתרון

$au+bv=1 \Rightarrow cau+cbv=c$

כעת a מחלק את שני המחוברים, לכן הוא מחלק את אגף ימין כנדרש.

תכונות של gcd, lcm

1. נסמן $d=\gcd(m,n)$ ויהי e אשר $e|m$ וגם $e|n$ אזי $e|d$.

הוכחה: $d=mu+nv$ וכעת $e|m \Rightarrow e|mu \Rightarrow e|(mu+nv) \Rightarrow e|d$

$e|n \Rightarrow e|nv$

2. $\gcd(am,an)=a\cdot\gcd(m,n)$

3. אם $m|a$ ו- $n|a$ אז $[a,b]|a$

חבורות

הגדרות

1) תהי S קבוצה. $*: S\times S\to S$ נקראת פעולה דו מקומית או בינארית. ונסמן
$$a*b=*(a,b)$$
2) תהי S קב' ו-$*$ פעולה בינארית עליה. אם $*$ אסוציאטיבית, כלומר
$$\forall a,b,c\in S:\ (a*b)*c=a*(b*c)$$
אזי S תקרא חבורה למחצה או אגודה.

3) נאמר $(S,*)$ חבורה למחצה. אם קיים $e\in S$ כך שלכל $a\in S$
$$a*e=e*a=a$$
אזי e יקרא האיבר הניטרלי של S, ו-S תקרא מונואיד.

4) יהי $(S,*)$ מונואיד, ויהי $a\in S$. אם קיים $b\in S$ כך ש-$a*b=e$. אזי a הפיך מימין. באותו אופן יוגדר הפיך משמאל. אם a הפיך מימין ומשמאל נאמר שהוא הפיך.

5) יהי $(S,*)$ מונואיד בו כל איבר הפיך. אז $(S,*)$ חבורה. כלומר בחבורה צריכים להתקיים סגירות, אסוציאטיביות, איבר ניטרלי, הפיכים.

דוגמאות

1) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ חבורות
2) $(\mathbb{Z}_n,+)$ חבורה.
3) $(M_n(\mathbb{F}),+)$ חבורה, $(M_n(\mathbb{F}),\cdot)$ מונואיד.
4) $(\mathbb{R}^*,\cdot)$, $(\mathbb{C}^*,\cdot)$, $(\mathbb{Q}^*,\cdot)$ חבורות.
5) אם M מונואיד, ונסמן $U(M)$ כל האיברים ההפיכים ב-M אז $U(M)$ חבורה.

$U(M_n(\mathbb{F}))=GL_n(\mathbb{F})$ $\quad U(\mathbb{Z})=\{1,-1\}$ $\quad U(\mathbb{Q})=\mathbb{Q}\setminus\{0\}$

תרגיל

מצא חבורה למחצה בה יש איבר יחידה משמאל אך לא מימין.

פתרון

$$S=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\right\}$$

האיבר $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$ הוא יחידה משמאל. אבל הוא לא יחידה מימין. נראה שבS לא קיים איבר יחידה מימין. נניח ש- $\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$ יחידה מימין, אזי

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} ax & ay \\ 0 & 0 \end{pmatrix}\neq\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$$

תרגיל

מצא מונואיד M ואיבר $a\in M$ כך ש-a הפיך מימין אך לא משמאל.

פתרון

נסתכל על שדה $\mathbb{F}$ ונ"ו $V=\mathbb{F}^{\infty}$ מעל $\mathbb{F}$, ונסמן

$$Hom(V)=\{T: V\to V \mid T \text{ ה"ל}\}$$

$M=Hom(V)$ עם פעולת ההרכבה הוא מונואיד. נסתכל על העתקה

$$U(x_1,x_2,\dots)=(0,x_1,x_2,\dots)$$

$$D(x_1,x_2,\dots)=(x_2,x_3,\dots)$$

$$DU(x_1,x_2,\dots)=D(0,x_1,\dots)=(x_1,x_2,\dots)\Rightarrow DU=I$$

אבל

$$UD(x_1,x_2,\dots)=U(x_2,x_3,\dots)=(0,x_2,x_3,\dots)$$

ואם $x_1\neq 0$ נקבל שאין הפיכות

דוגמה

$S=\{a,b\}$

$\cdot$	a	b
a	b	b
b	b	a

אין אסוציאטיביות כי $(a\cdot b)b = a\neq b = a(b\cdot b)$

ולכן זו לא אפילו חבורה למחצה

שאלה

יהי $(X,\cdot)$ מונואיד ותהי $P_*(X)$ אוסף כל תתי הקבוצות הלא ריקות של X.

א. הראו כי $(P_*(X),\cdot)$ עם הפעולה $A\cdot B=\{a\cdot b \mid a\in A, b\in B\}$ הוא מונואיד

ובכן, סגירות:

יהיו $A,B\in P_*(X)$, $a\in A, b\in B$ ← $a\cdot b\in X$ כי X מונואיד ולכן $a\cdot b\in A\cdot B$.

מכאן שיש סגירות.

אסוציאטיביות:

הכל באותו אופן.

איבר ניטרלי: $\{e\}$.

ב. בדיוק האיברים ההפיכים מהצורה $\{a\}$ כאשר $a\in U(X)$.

היכרות [illegible] למונואידים ולחבורות

(1) X קבוצה כלשהי; כאשר $(P(X),\cap)$ הוא מונואיד, X הוא איבר יחידה. $(P(X),\cup)$ גם מונואיד, ϕ הוא איבר היחידה.

(2) נסתכל על $\mathbb{Z}_n$ ביחס לכפל ונסמן חבורה זו ב־U_n.

ובכן, אם p ראשוני אז $U_p=\mathbb{Z}_p\setminus\{0\}$

אם n לא ראשוני נצטרך להוציא את האיברים. לדוגמה נמצא את U_6.

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	[illegible]	1

⟵ רק ל־1 ול־5 יש הפיכים!!

$U_6=\{1,5\}$

משפט (לחישוב U_n)

$$U_n=\{0\le a\le n-1 \mid \gcd(a,n)=1\}$$

דוגמאות

(1)

$U_6=\{1,5\}$

0 לא זר לשום מספר

2 לא זר ל-6 (גורם 2)

3 לא זר ל-6 (גורם 3)

4 לא זר ל-6 (גורם 2)

(2)

$U_8=\{1,3,5,7\}$

הערה

אם $a\equiv b \pmod{n}$ אז $a^m\equiv b^m \bmod n$ לכל m

תרגיל

פתרו את המשוואה $7x\equiv12$ ב-$\mathbb{Z}_{34}$.

עכשיו, $1\equiv35\equiv5\cdot7$

ולכן $12\equiv12\cdot5\cdot7$

ולכן $7x\equiv12\cdot5\cdot7$

$x\equiv12\cdot5\equiv60\equiv26$

תרגיל

חשבו את הספרה האחרונה של 333^{333}

פתרון

$333=3\cdot111$

$$333^{333}=3^{333}\cdot111^{333}\equiv3^{333} \pmod{10}$$

נשאר לחשב את $3^{333} \bmod 10$

$$3^{333}=3^{4\cdot83+1}=3^{4\cdot83}\cdot3\equiv3$$

$3^4\equiv1$

לכן הספרה האחרונה היא 3

הגדרה

חבורה G תקרא ציקלית אם קיים $a \in G$ כך ש-

$$G=\{a^n \mid n\in\mathbb{Z}\}$$

דוגמאות

1) $(\mathbb{Z}_n,+)$ היוצר 1

2) $(\mathbb{Z},+)$ היוצרים $-1,1$

3) $(U_6=\{1,5\},\cdot)$ היוצר 5 $(5^2=1)$

4) $(U_8=\{1,3,5,7\},\cdot)$ אינה ציקלית

הגדרה

חבורה G היא ציקלית אם"ם קיים בה איבר מסדר $|G|$.

(סדר של איבר: $O(a)=\min\{n\in\mathbb{N} \mid a^n=e\}$)

לדוגמה: ב-U_6 אכן קיים איבר מסדר 2 $(5^2=1)$.

תרגיל

תהי G חבורה ויהיו $a,b\in G$. אם a,b מסדר סופי, האם ab מסדר סופי?

פתרון

אם G לא אבלית אז לאו דווקא נכון.

$$G=GL_2(\mathbb{R})$$

$$a=\begin{pmatrix}0&-1\\1&0\end{pmatrix} \qquad b=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$$

$$a^4=I \qquad b^3=I$$

$$ab=\begin{pmatrix}1&1\\0&1\end{pmatrix}$$

אבל ab היא מסדר אינסופי כי

$$(ab)^k=\begin{pmatrix}1&k\\0&1\end{pmatrix}$$

תורת החבורות

הוכחה עבור G אבלית:

יהיו a מסדר n, ו-b מסדר m

$$(ab)^{mn} = a^{mn} b^{mn} = e$$

כלומר הסדר קטן שווה מ- mn כפי שצ"ל.

תרגיל

תהי G חבורה. הוכיחו כי לכל $a \in G$: $o(a)=o(a^{-1})$

והכן, נסמן $o(a)=n$. אז $a^n=e$

$$(a^{-1})^n=e^{-1}=e$$

ולכן $n \ge o(a^{-1})$.

באותו אופן הולך כי $((a^{-1})^{-1}=a)$

תרגיל

תהי G חבורה כך ש- $a^2=e$ לכל $a \in G$. אז G אבלית.

פתרון

$$(ab)^2=e;\ a^2=e;\ b^2=e$$

$$\Downarrow$$

$$(ab)^2=abab=e=a^2b^2=a\cdot a\cdot b\cdot b$$

$$\Downarrow$$

$$a^{-1}/\ \ abab=aabb\ \ /b^{-1}$$

$\boxed{ba=ab}$ מ.ש.ל.

תורת החבורות

תרגיל

האם $\mathbb{Z}_n^2$ ציקלית?

פתרון

נסמן $G=\mathbb{Z}_n^2$, אז $|G|=n^2$ ועבור חיבור

היא ציקלית אמ"מ יש איבר מסדר n^2

אבל ב-G יש איברים רק עד סדר n

$(a,b)^n = n(a,b) = (na,nb) = (0,0)$

ולכן החבורה אינה ציקלית.

הערה

נשים לב ש-$(1\ 3)(1\ 2) \neq (1\ 2)(1\ 3)$ ולכן S_3 חבורה לא אבלית.

S_3 נוצרת ע"י שני איברים

$\sigma=(1\ 2\ 3)$ $\tau=(1\ 2)$

$S_3=\{id,\tau,\sigma,\sigma^2,\tau\sigma,\tau\sigma^2\}$

תת חבורות

הגדרה

תהי $(G,\cdot)$ חבורה, $\emptyset\neq H\subseteq G$ נקראת תת חבורה אם $(H,\cdot)$ חבורה

קריטריון מקוצר

$\emptyset\neq H\subseteq G$ היא תת חבורה אמ"מ יש:

סגירות וקיום הופכיים.

או שמספיק להראות ש-$h_1h_2^{-1}\in H$ $\forall h_1,h_2\in H$

דוגמאות 1) $(\mathbb{Q},+) ,(\mathbb{R},+) \le (\mathbb{C},+)$

2) לכל חבורה G: G, $\{e\}$ ת"ח של G

3) $(\mathbb{Q}^*,\cdot) ,(\mathbb{R}^*,\cdot) \le (\mathbb{C}^*,\cdot)$

4) האם $\mathbb{Z}_n$ ת"ח של $\mathbb{Z}$? לא! כי הפעולה שונה

5) האם $(\mathbb{R}^*,\cdot) \le (\mathbb{C},+)$? לא! כי לא אותה פעולה

תהי G חבורה, $a\in G$. נסתכל על $\langle a\rangle$. זו ת"ח של G והיא ציקלית.

7) $SL_n(\mathbb{R}) \le GL_n(\mathbb{R})$ עבור כל n

כל המט' ההפיכות ← כל המט' עם דטרמיננטה אחת

<u>הוכחה</u>

אזו תת קבוצה לא ריקה (ברור!)

כי אם $M,N \in SL_n(\mathbb{R})$ אז $\det(M)=1$ (ובפרט $\neq 0$)

<u>כעת</u> נשתמש בקריטריון המקוצר:

$$\det(MN^{-1}) = \det(M)\cdot\det(N^{-1}) = 1\cdot 1^{-1} = 1$$

8) Ω_n = חבורת כל שורשי היחידה מסדר n

למשל $\Omega_4=\{\pm1, \pm i\}$

תרגיל

יהי $a=\text{cis}\,30°=\frac{\sqrt{3}}{2}+\frac{1}{2}i$, ותהי $\langle a\rangle$ תת"ח של $\mathbb{C}^*$. חשבו את $|\langle a\rangle|$.

(סדר של איבר בחבורה = סדר של החבורה הציקלית שנוצרת ע"י איבר).

פתרון

$$a^n=\text{cis}(n\cdot 30°)$$

ברור ש- $|\langle a\rangle|\le 12$ כי $\text{cis}(12\cdot 30°)=1$

מצד שני אם $a^d=1$ עבור $d<1$ אז

$\sin(d\cdot 30°)=0$ ו- $\cos(d\cdot 30°)=1$

וזה מתקיים רק עבור $d=12$ בסתירה.

תרגיל

אם $n|m$ אז $\Omega_n \le \Omega_m$.

פתרון

ברור ש- $\Omega_n \subseteq \Omega_m$. נותר להראות שזו תת"ח (ידוע ש-Ω_m חבורה ולכן גם בה)

הגדרה

תהי G חבורה ציקלית. כל ת"ח של G היא ציקלית

דוגמה

מה הן תתי החבורות של $(\mathbb{Z},+)$?

$\mathbb{Z}$ ציקלית (למשל נוצרת ע"י 1) לכן כל ת"ח שלה ציקלית ולכן

כל ת"ח שלה מהצורה $\langle k\rangle = k\mathbb{Z}$

תרגיל

(די לבדוק סגירות:)

אם G חבורה סופית ו-$\emptyset \neq H \subseteq G$ [illegible] אז $H \leq G$.

פתרון

לפי הקריטריון המקוצר, נשאר להוכיח שלכל $a\in H \Rightarrow a^{-1}\in H$.

ובכן יהי $a\in H$, נסתכל על הקבוצה

$$A=\{a,a^2,a^3,\dots\}\subseteq G$$

סופית $\Rightarrow$ A סופית

לכן קיימים $m\neq n$ כך ש-$a^m=a^n$. אבל בחבורה אפשר לצמצם ונקבל $a^{m-n}=1$. כלומר $a\cdot a^{m-n-1}=1$ כנדרש.

תרגיל

תהי G חבורה, H_1,H_2 ת"ח שלה.

א. האם $H_1\cap H_2$ ת"ח של G.

ב. האם $H_1\cup H_2$ ת"ח של G.

פתרון

א. כן. נוכיח ע"פ הקריטריון המקוצר. יהיו $a,b\in H_1\cap H_2$. אזי

$$a,b\in H_1,\ a,b\in H_2 \Rightarrow a\cdot b\in H_1 \wedge a\cdot b\in H_2 \Rightarrow a\cdot b\in H_1\cap H_2$$

(חבורות)

$$\Downarrow$$

$$a^{-1}\in H_1,\ a^{-1}\in H_2 \Rightarrow a^{-1}\in H_1\cap H_2$$

ב. לא. למשל $G=\mathbb{Z}$, $H_2=3\mathbb{Z}$, $H_1=2\mathbb{Z}$

$2+3=5\notin H_1\cup H_2$ ($2\in H_1$, $3\in H_2$)

תרגיל

תהי G חבורה אבלית הראו שאוסף האיברים מסדר סופי מהווה ת"ח של G

פתרון

צריך להוכיח: קבוצה לא ריקה כי e נמצא בה

בקריטריון מקוצר

יהיו a,b מסדרים סופיים;

$a^n=e$, $b^m=e$ ולכן $(ab)^{nm}=e$ (מתקיים רק באבלית)

(a^{-1}) סגירות מתקיים

ההופכי באותו אופן.

משפט

תהי $G=\langle x\rangle$ חבורה ציקלית מסדר n. אז לכל a מתקיים

$$o(x^a)=\frac{n}{(n,a)}$$

דוגמה

$(\mathbb{Z}_{12},+)$ חבורה ציקלית $=\langle 1\rangle$

$|\mathbb{Z}_{12}|=12$

מה הסדר של 8

$$o(8)=o(8\cdot 1)=\frac{12}{(12,8)}=\frac{12}{4}=3$$

ואכן

$8+8=16=4$

$4+8=12=0$

הערה

בחבורה ציקלית יכול להיות יותר מיוצר אחד. למשל $\mathbb{Z}_7$ נוצר

ע"י 5 וגם ע"י 2

הגדרה

אם G ציקלית מסדר n אז יש בה $\varphi(n)$ יוצרים.

$$\left(\varphi(n)=\left|\{g\in\{1,\dots,n-1\}\mid (g,n)=1\}\right|\right)$$

נוסחה לחישוב

$$\varphi(n)=n\prod(1-\frac{1}{p_i})$$

כאשר $n=p_1^{a_1}\cdots p_k^{a_k}$, $p_1,\dots,p_k$ ראשוניים.

תרגיל

כמה יוצרים יש ב- $G=U_{10}$

ובכן, $U_{10}=\{[1],[3],[7],[9]\}$

נ"א בדקנו כי 3 יוצר אותה.

$\varphi(4)=2$

ולכן יש סה"כ שני יוצרים.

תרגיל

לחבורה ציקלית אינסופית יש בדיוק שני יוצרים

פתרון

אם a יוצר גם a^{-1} יוצר. לכן יש לפחות שני יוצרים.

נניח שיש יוצר נוסף, נסמנו b.

$b=a^n$, $a=b^m$

$a=(a^n)^m=a^{nm}$

$a^{nm-1}=e$

סתירה לאינסופיות של החבורה

תרגיל

נסתכל על U_{40} (נוצר ע"י $\omega=cis(9°)$, $|U_{40}|=40$).

כמה יוצרים יש בה?

פתרון

$40=2^3\cdot 5$

$\varphi(40)=40\cdot(1-\frac{1}{2})(1-\frac{1}{5})=16$

ב) מה הסדר של ω^{14} כאשר ω יוצר של U_{40}.

$\frac{40}{(40,14)}=20$

הגדרה

1) תהי G חבורה, A ת"ק של G.
התת"ח הנוצרת ע"י A מסומנת ע"י $\langle A\rangle$ ומוגדרת להיות התת"ח הקטנה ביותר המכילה את A.

2) אם קיימת A סופית כך ש- $G=\langle A\rangle$ נאמר ש-G נוצרת סופית.

דוגמאות

1) עבור $\mathbb{Z}$: $A=\{1\}$; $G=\langle A\rangle=\mathbb{Z}$.

2) ב-$\mathbb{Z}$: $A=\{2\}$ $\langle A\rangle=2\mathbb{Z}$.

3) ב-$\mathbb{Z}$: $A=\{2,3\}$ $\langle A\rangle=\mathbb{Z}$ (כי $1=3-2$ והתת"ח סגור)

4) U_8 נוצרת ע"י $\{3,5\}$

תרגיל הבית

אם a,b מתחלפים אז $\langle\{a,b\}\rangle$ תת"ח אבלית של G.

הערה

$\langle\{a,b\}\rangle=(a,b)\mathbb{Z}$ עבור $a,b\in\mathbb{Z}$

כדי להוכיח זאת יש צורך בטענה $a|b$ אמ"מ $b\mathbb{Z}\subseteq a\mathbb{Z}$

דוגמאות נוספות

5) S_3 נוצרת ע"י σ,τ שניתנו בהתחלה
$S_3=\langle\{\sigma,\tau\}\rangle$

הערות

1) אם G אבלית, אז התת"ח הנוצרת ע"י a,b היא $\{a^nb^m \mid n,m\in\mathbb{Z}\}$

2) אם G לא אבלית, ניתן לחשוב על התת"ח הנוצרת ע"י a,b כעל אוסף המילים הסופיות באותיות $\{a,b,a^{-1},b^{-1}\}$.
ובאופן כללי $\langle A\rangle$ הוא אוסף המילים עם אותיות מ- $A\cup A^{-1}$

תרגיל
הוכח כי $\mathbb{Z}\times\mathbb{Z}$ נוצרת סופית

פתרון
נבחר $A=\{(1,0),(0,1)\}$ ואז $\mathbb{Z}\times\mathbb{Z}=\langle A\rangle$

הערות
1) כל חבורה סופית נוצרת סופית.
2) כל חבורה ציקלית נוצרת סופית ע"י איבר אחד.
3) $\mathbb{Z}\times\mathbb{Z}$, S_n נוצרות סופית.
S_n נוצרת ע"י σ,τ כאשר σ מחזור מאורך n ו-τ חילוף (i,j)
או נוצרת ע"י כל החילופים (כי אפשר לכתוב כל מחזור באורך n כהרכבה $(n-1,n),\dots,(2,3),(1,2)$)
או ע"י כל החילופים מהצורה $(1\ n),(2\ n),\dots$

תרגיל
האם $(\mathbb{R},+)$ נוצרת סופית?

פתרון
לא. משיקולי עוצמה: $\mathbb{R}$ לא בת מנייה בעוד שאוסף כל המילים הסופיות מעל אוסף אותיות סופי הוא בן מנייה.

תרגיל
האם $(\mathbb{Q}^+,\cdot)$ נוצרת סופית?

פתרון
לא. נניח בשלילה שנוצרת סופית, כלומר $\mathbb{Q}^+=\langle a_1,\dots,a_n\rangle$
ונציג כל a_i כשבר מצומצם $a_i=\frac{m_i}{k_i}$.
נפרק כל מכנה למכפלה של גורמים ראשוניים
$$k_i=p_{i_1}^{a_{i_1}}\cdots p_{i_r}^{a_{i_r}}$$
מכיוון שיש אינסוף מספרים ראשוניים קיים p ראשוני הגדול מכל המס' הראשוניים המופיעים בפירוקים אלו, כלומר $(p,k_i)=1$ לכל i,
אז לא נוכל להציג את $\frac{1}{p}$, סתירה.

תרגילי בית

1) הראו כי $(\mathbb{Q},+)$ לא נוצרת סופית

2) הראו מפורשות כי $\mathbb{Z}_n \times \mathbb{Z}_m$ נוצרת סופית

תרגיל

מצאו את כל תתי החבורות של S_3

פתרון

$A_3 := \langle \sigma \rangle = \{id, (2\ 3), (1\ 3\ 2)\}$

ושתי החבורות הטריוויאליות

$\langle \tau \rangle = \{id, (1\ 2)\}$

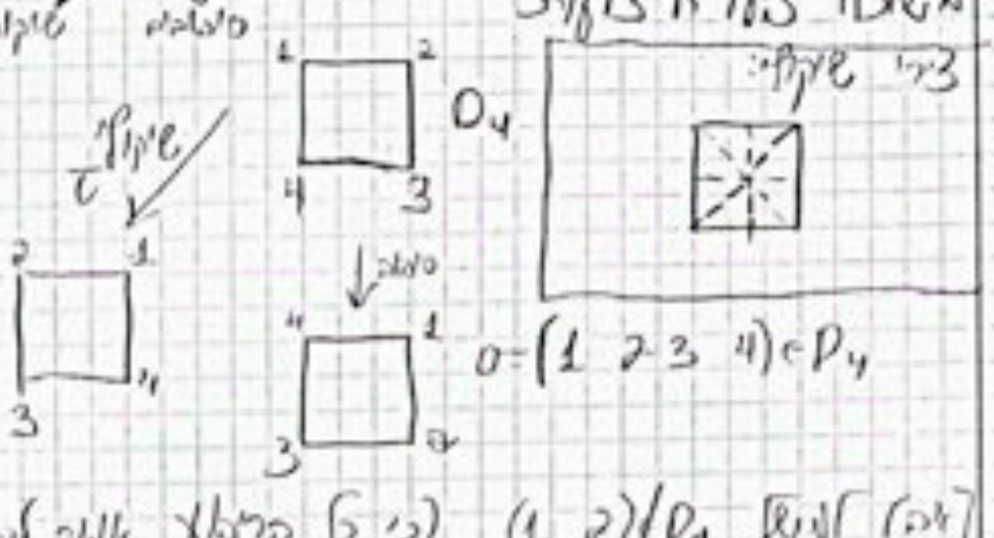
$\langle (1\ 3) \rangle = \{id, (1\ 3)\}$

$\langle (2\ 3) \rangle = \{id, (2\ 3)\}$

חבורות

הגדרה
חבורה דיהדרלית D_n היא חבורת הסימטריות של מצולע משוכלל בעל n צלעות.

סיבובים, שיקופים



שיקוף סימטרי על ציר אנך/אלכסוני

$\sigma=(1\ 2\ 3\ 4)\in D_4$

[זהו לא נכון $D_n/(1\ 2)$ כי לא הריבוע אותו לוסמנים.]

⇓

σ,τ הם יוצרים של החבורה

$D_4=\{id,\sigma,\sigma^2,\sigma^3,\tau,\tau\sigma,\tau\sigma^2,\tau\sigma^3\}$

(סיבוב $0°$, $90°$, $180°$, $270°$; שיקוף אנכי, שיקוף אופקי, שיקופים אלכסוניים)

$|D_4|=8$
$|D_n|=2n$

ולכן מתקיים באופן כללי
כי יש n סיבובים ו-n שיקופים

$O(\sigma)=4$ (סיבוב $360°$)
$O(\tau)=2$ (שיקוף + שיקוף מחזיר למצב המקורי)

הגדרה אלגברית
D_n היא חבורה בת $2n$ איברים ונוצרת ע"י σ,τ המקיימים
$O(\sigma)=n \quad O(\tau)=2$
$\tau\sigma\tau=\sigma^{-1}$

דוגמה

$D_3 = \{id, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$

כאשר σ סיבוב ב- 120°

ב- D_3:

$\sigma\tau = \tau\sigma^{-2}$

כי $\tau\sigma\tau = \sigma^{-1} = \sigma^2$ / $\tau^{-1} = \tau$.

$\sigma\tau = \tau\sigma^{2}$

ובדוגמה זו D_3 לא אבלית

תרגיל

תהי G חבורה סופית, $a,b \in G$. האם ייתכן ש $o(a)o(b) < o(ab)$

פתרון

ב- D_3:

$a = \tau \quad o(a) = 2$

$b = \tau\sigma \quad o(b) = 2$

$4 = o(a)o(b) > o(ab) = o(\tau^2\sigma) = o(\sigma) = 3$

קוסטים/מחלקות של תת חבורה

הגדרה

תהי G חבורה, $H \leq G$ ויהי $g \in G$

$gH = \{gh \mid h \in H\}$ קוסט שמאלי

$Hg = \{hg \mid h \in H\}$ קוסט ימני

דוגמה

$G = (\mathbb{Z}, +)$ $H = (5\mathbb{Z}, +)$. הקוסטים הם:

$0 + 5\mathbb{Z} = 5\mathbb{Z}$

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

$2 + 5\mathbb{Z}$

$3 + 5\mathbb{Z}$

$4 + 5\mathbb{Z}$

וכל השאר שווים להם.

כאן $\mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}_5$

$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$

הערה

1) אם G אבלית המחלקות השמאליות שוות למחלקות הימניות

אם G לא אבלית אז לאו דווקא:

נקח $H = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$ $G = GL_2(\mathbb{Q})$

$g = \begin{pmatrix} 5 & 0 \\ 1 & 0 \end{pmatrix}$

ואז $gH \neq Hg$:

$gH = \left\{ \begin{pmatrix} 5 & 5n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$

$Hg = \left\{ \begin{pmatrix} 5 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$

2) H תמיד מחלקה (כי $eH = He = H$)

3) המחלקות בסד"כ אינן ת"ח מלבד H עצמה

4) קיימת התאמה חח"ע ועל בין המחלקות הימניות והשמאליות של H ב-G

$gH \to (gH)^{-1} = Hg^{-1}$

ותרגיל הרצאה

קוסטים/מחלקות של תת חבורה

הגדרה

תהי G חבורה, $H\le G$ ויהי $g\in G$

$gH=\{gh|h\in H\}$ קוסט שמאלי

$Hg=\{hg|h\in H\}$ קוסט ימני

דוגמה

$G=(\mathbb{Z},+)$, $H=(5\mathbb{Z},+)$. הקוסטים הם:

$0+5\mathbb{Z}=5\mathbb{Z}$

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

$2+5\mathbb{Z}$

$3+5\mathbb{Z}$

$4+5\mathbb{Z}$

וכל השאר שווים להם.

כאן $\mathbb{Z}/5\mathbb{Z}\simeq\mathbb{Z}_5$

$\mathbb{Z}/n\mathbb{Z}\simeq\mathbb{Z}_n$

הערה

1) אם G אבלית המחלקות השמאליות שוות למחלקות הימניות
אם G לא אבלית אז לא בהכרח:

ניקח $H=\left\{\begin{pmatrix}1&n\\0&1\end{pmatrix}\middle| n\in\mathbb{Z}\right\}$ $G=GL_2(\mathbb{R})$

$g=\begin{pmatrix}5&0\\1&0\end{pmatrix}$

ואכן $gH\neq Hg$:

$gH=\left\{\begin{pmatrix}5&5n\\0&1\end{pmatrix}\middle| n\in\mathbb{Z}\right\}$

$Hg=\left\{\begin{pmatrix}5&n\\0&1\end{pmatrix}\middle| n\in\mathbb{Z}\right\}$

2) H תמיד מחלקה (כי $eH=He=H$)

3) המחלקות בדר"כ אינן תת"ח מלבד H עצמה

4) קיימת התאמה חח"ע ועל בין המחלקות הימניות והשמאליות של H ב-G

$gH\to(gH)^{-1}=Hg^{-1}$

לכן נגדיר את האינדקס של H ב-G כמספר המחלקות השמאליות של H ב-G ונסמן $[G:H]$

משפט

תה"נ G, $H \le G$. אזי:

א. לכל $a,b \in G$ מתקיים $aH=bH$ או $aH \cap bH = \emptyset$.

ב. $|aH|=|bH|$ $\forall a,b \in G$

ג. $G = \dot{\bigcup}_{g\in G} gH$

ד. $aH=bH$ אמ"מ $b^{-1}a \in H$.

בפרט $aH=H$ אמ"מ $a \in H$.

משפט לגרנג'

א. $|G|=|H|[G:H]$

ב. הסדר של תת"ח מחלק את סדר החבורה. (אם G חבורה סופית)

דוגמאות

1. $G=\mathbb{Z}_8$ $H=\langle 2\rangle=\{0,2,4,6\}$

המחלקות השמאליות הן:

H

$1+H=\{1,3,5,7\} \Rightarrow \mathbb{Z}_8 = H \dot{\cup} (1+H)$

2. $G=D_3$ $H=\langle\tau\rangle=\{id,\tau\}$

$[G:H]=\frac{|G|}{|H|}=\frac{6}{2}=3$

לכן יש 3 קוסטים:

H

$H\sigma=\{\sigma,\tau\sigma\}$

$H\sigma^2=\{\sigma^2,\tau\sigma^2\}$

$\dot{\bigcup}_{i=0}^{2} H\sigma^i = H$

תרגיל

ניתן חבורה G ותת חבורה H כך ש- $[G:H]$ אינסופי

הסבר

$G=\mathbb{Q}$ $H=\mathbb{Z}$

אם $0\leq a<b<1$ אז

$a+H\neq b+H$

לכן לכל $a\in[0,1)$ יש קוסט שונה, הפרט יש $\aleph_0$ קוסטים שונים.

פתרון נוסף:

$G=GL_2(\mathbb{Q})$ $H=\left\{\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix} \middle| a\in\mathbb{Q}\right\}$

נקח $\alpha\in\mathbb{Q}$ $g_\alpha=\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}$

$g_\alpha H=\left\{\begin{pmatrix}\alpha & \alpha a\\ 0 & 1\end{pmatrix} \middle| a\in\mathbb{Q}\right\}$

ונקבל אינסוף מחלקות כנדרש

מסקנות ממשפט לגרנז'

① תהיינה $G\geq H\geq K$, אזי:

$[G:K]=[G:H][H:K]$

② תהי G חבורה, $a\in G$, אזי $O(a)\,\|\,|G|$.

③ $a^{|G|}=e$

משפט אוילר $a^{\varphi(n)}\equiv 1 \mod n$

תרגיל מהמבחן

מצא את שתי הספרות האחרונות של 1959^{1999}

פתרון

$[a\equiv b \pmod n \Rightarrow a^n\equiv b^n \pmod n]$

לכן $1959^{1999}\equiv 59^{1999}$

נשתמש במשפט אוילר: $\varphi(100)=40 \Rightarrow 59^{40}\equiv 1$

כעת $59^{1999}=59^{49\cdot 40+39}\equiv 59^{39}\equiv 59^{-1}$

נחשב את 59^{-1} ב- $\mathbb{Z}_{100}$

שאלה:

$59x \equiv 1 \pmod{100}$

$\Updownarrow$

$59x + 100y = 1 \quad x,y \in \mathbb{Z}$

$(100,59)=1$ ולכן נשתמש באלגוריתם אוקלידס

$(100,59) = (59,41) = (41,18) = (18,5) = (5,3) = (3,2) = (2,1) = 1$

$100 = 1 \cdot 59 + 41$ $59 = 1 \cdot 41 + 18$ $41 = 2 \cdot 18 + 5$ $18 = 3 \cdot 5 + 3$ $5 = 3 + 2$ $3 = 2 + 1$

ובצע הצבה לאחוריות ונקבל 59^{-1}

ולכן שתי הספרות האחרונות הן 39.

(הצבה לאחורית)

$1 = 3 - 2 = 3 - (5 - 3) = 18 - 5 \cdot 3 - (5 - 18 + 5 \cdot 3) =$

$= 2 \cdot 18 - 7 \cdot 5 = 2 \cdot 18 - 7(41 - 18 \cdot 2) =$

$= -7 \cdot 41 + 16 \cdot 18 = -7 \cdot 41 + 16(59 - 41) =$

$= 16 \cdot 59 - 23 \cdot 41 = 16 \cdot 59 - 23 \cdot (100 - 59) =$

$= -23 \cdot 100 + \underline{\underline{39}} \cdot 59$

כנדרש

תרגיל מובחן

ויצאו את שתי הספרות האחרונות של $807376^{\ldots}$

$\begin{array}{ccc} ||| & & \\ 67^{1} & + & 11 \\ ||| & & ||| \\ 3 & & 11 \end{array}$

ולכן 2 הספרות האחרונות הן 14.

תרגיל

תהי G חבורה סופית ויהי $N \trianglelefteq G$ כך ש- $|b|\,\|\,k$. האם בהכרח ש[illegible]

ב-G איבר מסדר זה?

פתרון

לא. דוגמה נגדית: $G=\mathbb{Z}_2^4$ $\quad |G|=16$

אבל הסדר של G איבר בה, בפרט אין איבר מסדר 16

תרגיל

תהי G חבורה לא אבלית מסדר 8. הראו שיש לה תת חבורה ציקלית מסדר 4.

פתרון

סדרים אפשריים של איברים:

8: אין איברים (אחרת היא הייתה ציקלית → אבלית סתירה)

4: קיים אחד לפחות ש[illegible]

2: אם כל האיברים מסדר 2 אחרת G הייתה אבלית

לכן יש איבר מסדר 4 כנדרש

הגדרה

תהי G חבורה. $H \leq G$ תקרא תת חבורה נורמלית של G, $H \trianglelefteq G$

אם לכל $g\in G$ $h\in H$ מתקיים $ghg^{-1}\in H$ -

תנאים שקולים לנורמליות

1) $H \trianglelefteq G$

2) $gHg^{-1}\subseteq H$ לכל $g\in G$, [illegible]

3) $gHg^{-1}=H$ לכל $g\in G$

4) $gH=Hg$ לכל $g\in G$

5) אוסף כל המחלקות השמאליות = אוסף כל המחלקות הימניות

הגדרה

a,b צמודים אם יש c כך ש- $a=cbc^{-1}$

כלומר H נורמלית אם"ם H סגורה להצמדה.

הגדרה

יהא G חבורה ו-H תת חבורה של G נורמלית

היא תקרא נורמלית אם לכל $g\in G$, $h\in H$ מתקיים $ghg^{-1}=h'\in H$

דוגמאות

1) $G=S_3$, $H=\langle(1\ 2)\rangle$ לא נורמלית כי:

$(1\ 2\ 3)(1\ 2)(1\ 2\ 3)^{-1}\notin H$

2) $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$

הוכחה:

יהי $H\in SL_n(\mathbb{R})$, $G\in GL_n(\mathbb{R})$

$|GHG^{-1}|=|H|$

ולכן $GHG^{-1}\in SL_n(\mathbb{R})$

תרגיל

תהי $H\le G$ מאינדקס 2 אז H נורמלית.

הוכחה

נסתכל על קוסטים שמאליים: $G=H\uplus aH$

ימניים: $G=H\uplus Ha$

$\Downarrow$

$aH=Ha$

כנדרש

ה

חבורות נורמליות

תרגיל

יהיו G חבורה, $H \leq G$, $N \trianglelefteq G$.

הוכח כי $H \cap N \trianglelefteq H$

פתרון

ראינו שחיתוך של תת חבורות הוא ת"ח. נראה נורמליות:

יהיו $a \in H \cap N$, $h \in H$. צ"ל ש- $hah^{-1} \in H \cap N$

והכן $a \in N$ ולכן $hah^{-1} \in N$ כי N נורמלית ב-G.

$h, a \in H$ ולכן מסגירות $hah^{-1} \in H$.

ולכן $hah^{-1} \in H \cap N$ כנדרש.

הגדרה

אם H, G תתי חבורות, נגדיר את המכפלה שלהן

$$GH = \{g \cdot h \mid g \in G, h \in H\}$$

אם אחת מהן נורמלית המכפלה היא ת"ח

אם שתיהן נורמליות המכפלה ת"ח נורמלית.

תרגיל

תן דוגמא לחבורה G ולתתי חבורות H_1, H_2 כך ש-H_1H_2 לא ת"ח של G.

פתרון

ניקח $G = D_3$, $H_1 = \langle \tau \rangle = \{id, \tau\}$ (שיקוף), $H_2 = \langle \tau\sigma \rangle = \{id, \tau\sigma\}$ (שיקוף)

$$H_1H_2 = \{id, \tau\sigma, \tau, \tau\tau\sigma\}, \quad \tau\tau\sigma = \sigma$$

ולכן זו אינה ת"ח כי אין סגירות או כי $|G| \nmid |H_1H_2|$ בסתירה למשפט לגרנג'.

הגדרה

הומומורפיזם בין חבורות G_1 ל-G_2 זו פונק' φ המוגדרת על החבורה

φ שומר: $\varphi(a\cdot b)=\varphi(a)*\varphi(b)$

מונומורפיזם - הומו' חח"ע

אפימורפיזם - הומו' על

} איזומורפיזם - הומו' חח"ע ועל

אם קיים איזומורפיזם מ-G_1 ל-G_2 נסמן $G_1\cong G_2$.

דוגמאות

1. $\varphi:\mathbb{Z}_2\to\mathbb{Z}_2$ ע"י $\varphi(0)=0$, $\varphi(1)=1$

זהו איזומורפיזם

2. $\varphi:\mathbb{Z}\to\mathbb{Z}_n$ ע"י $\varphi(a)=[a]_n$

זהו אפימורפיזם אך לא איזומורפיזם.

3. האם $\mathbb{Z}_2^2\cong\mathbb{Z}_4$?

מכאן נניח שקיים איזו' $\varphi:\mathbb{Z}_2^2\to\mathbb{Z}_4$

נניח לכן $2\cdot\varphi((0,1))=\varphi(0,0)=0$

לכן $\varphi(0,1)=[0]$ זה סותר חח"ע או $\varphi(0,1)=[2]$

ואז באותו אופן נקבל $\varphi(1,0)=2$ בסתירה לחח"ע

4) בין כל שתי חבורות G_1,G_2 קיים הומומורפיזם טריוויאלי

$\forall g\in G_1;\ \varphi(g)=e_{G_2}$

5) בהינתן שתי חבורות $H\leq G$ עם אותה פעולה,

נגדיר מונומורפיזם $\varphi:H\to G$ ע"י $\forall h\in H;\ \varphi(h)=h$

זה שיכון, וגם הוא חח"ע.

6) תהי G חבורה אבלית ויהי $n\in\mathbb{N}$. אזי $\varphi_n:G\to G$ המוגדרת ע"י $\varphi_n(g)=g^n$ הינו הומומורפיזם.

לדוגמה: $G=(\mathbb{Z},+)$, $n=5$, אזי $\varphi_5(z)=5z$ הומומורפיזם

ד) R לא איזומורפית ל-Q כי אחד מהם אינו עצמי.

ה) למשל $2\mathbb{Z} \subseteq \mathbb{Z}$, אז $\mathbb{Z} \cong 2\mathbb{Z}$, צריך כי יש רק חבורה ציקלית אחת עד כדי איזומורפיזם

תכונות של הומומורפיזם מ-G_1 ל-G_2

1. $\varphi(e_{G_1}) = e_{G_2}$

כי $\varphi(e_1)=\varphi(e_{G_1}^2)=\varphi(e_{G_1})^2 \Rightarrow e_{G_2}=\varphi(e_{G_1})$

a. $\varphi(x^{-1})=\varphi(x)^{-1}$

b. $\varphi(x^n)=\varphi(x)^n$ לכל $n\in\mathbb{Z}$

תרגיל

יהי $\varphi: G\to H$ איזומורפיזם. הוכח:

G אבלית אמ"מ H אבלית

פתרון

נניח G אבלית

$$\varphi(a)*\varphi(b)=\varphi(a\cdot b)=\varphi(b\cdot a)=\varphi(b)*\varphi(a)$$

G אבלית

ולכן אבלית מכיוון ש...
ובאותה דרך לכיוון השני.

תרגיל האם $D_3\cong\mathbb{Z}_6$

פתרון לא כי $\mathbb{Z}_6$ אבלית ו-D_3 לא.

תרגיל יהי $\varphi:G\to H$ הומומורפיזם. הוכח שלכל $g\in G$ $o(\varphi(g))\mid o(g)$

פתרון

$$\varphi(g)^{o(g)}=\varphi(g^{o(g)})=\varphi(e)=e$$

ולכן $o(\varphi(g))\mid o(g)$

מסקנה

אם $G\cong H$ אז לכל $g\in G$ $o(g)=o(\varphi(g))$.

כלומר לחבורות איזומורפיות יש אותם סדרים.

הערה $G\cong H$ אז G ציקלית אמ"מ H ציקלית.

הערה

איזומורפיזם שומר תכונות יחודיות לקבוצות ונגזרות.

תרגיל

הוכח או הפרך

יש איזומורפיזם $F:(\mathbb{Q}^+,\cdot)\to(\mathbb{Q},+)$

פתרון: לא. נניח בשלילה שיש איזומורפיזם כזה $\varphi:(\mathbb{Q}^+,\cdot)\to(\mathbb{Q},+)$

יהי $3\in\mathbb{Q}^+$, נסמן $\varphi(3)=c$ מעל. $\frac{c}{2}+\frac{c}{2}=c$. $\varphi(x)=\frac{c}{2}$

כלומר $\varphi(x^2)=c\Rightarrow x^2=3$

אבל $\sqrt{3}\notin\mathbb{Q}^+$.

תרגיל

הוכח או הפרך:

קיים איזו' $\varphi:H\to\mathbb{Z}_3^2$ כאשר $H=\langle 5\rangle\le(\mathbb{R}^*,\cdot)$

פתרון

לא קיים איזו' כזה כי H ציקלית והחבורה $\mathbb{Z}_3^2$ אינה ציקלית.

תרגיל

הוכח או הפרך

קיים מונו' $\varphi:(GL_2(\mathbb{Q}),\cdot)\to(\mathbb{Q}^{10},+)$

פתרון

לא. אם היה קיים φ כזו אז $G\cong\operatorname{Im}\varphi$ - תת חבורה של אבלית של $\mathbb{Q}^{10}$ אז $\mathbb{Q}^{10}$ אבלית ולכן G תהיה שהיא אבלית בסתירה.

הגדרות

יהי $\varphi:G\to H$ הומומורפיזם.

הגרעין של φ הוא $\ker\varphi:=\{g\in G\mid\varphi(g)=e\}$

התמונה של φ היא $\operatorname{Im}\varphi:=\{\varphi(g)\mid g\in G\}$

תרגיל

יהי $\varphi:G\to H$ הומומורפיזם. φ חח"ע אם"ם $\ker\varphi=\{e_G\}$

פתרון

(⇐) בהרצ: אם φ חח"ע, נניח ש-$\varphi(a)=e$. משום ש-$\varphi(e)=e$ נקבל $a=e$.

(⇒) נניח $\ker\varphi=\{e\}$. נניח $\varphi(g_1)=h=\varphi(g_2)$

$$\varphi(g_1)\varphi(g_2)^{-1}=e$$

$$\varphi(g_1g_2^{-1})=e$$

ו-$\ker\varphi=\{e\}$ ⇐ $g_1g_2^{-1}=e$ ⇐ $g_1=g_2$

דוגמאות לגרעין ותמונה

1. $\varphi:(\mathbb{C}^*,\cdot)$ המוגדרת ע"י $\varphi(x)=x^4$

$\ker\varphi=\{1,-1,i,-i\}=\Omega_4$

$Im\,\varphi=\mathbb{C}^*$

2. $\varphi:(\mathbb{Q}^*,\cdot)$ המוגדרת ע"י $\varphi(x)=x^4$

$\ker\varphi=\{1,-1\}$ $\quad Im\,\varphi\subset\mathbb{Q}^*$

3. $\det:GL_n(\mathbb{R})\to(\mathbb{R}^*,\cdot)$

$\ker(\det)=\{M\mid\det(M)=1\}=SL_n(\mathbb{R})$

$Im(\det)=\mathbb{R}^*$

משפט

יהי $\varphi:G\to H$. אזי:

1. $Im\,\varphi\leq H$
2. $\ker\varphi\trianglelefteq G$

הוכחת 2

ראשית נראה ת"ח:

יהיו $a,b\in\ker\varphi$, צ"ל $ab^{-1}\in\ker\varphi$

$$\varphi(ab^{-1})=\varphi(a)\varphi(b)^{-1}=e\cdot e^{-1}=e$$

נורמליות:

יהיו $k\in\ker\varphi$ ויהי $g\in G$:

$$\varphi(gkg^{-1})=\varphi(g)\varphi(k)\varphi(g^{-1})=\varphi(g)e\varphi(g)^{-1}=e$$

ולכן $gkg^{-1}\in\ker\varphi$

חבורות מנה

יהי G חבורה ו-$N \trianglelefteq G$. נסתכל על אוסף המחלקות השמאליות של N ב-G. נסמן אוסף זה כ- G/N

כלומר
$$G/N=\{gN \mid g\in G\}$$

על G/N ניתן להגדיר פעולת חבורה, נקראת חבורת המנה: אם aN,bN מחלקות, אז
$$aN \oplus bN=(ab)N$$

דוגמאות

1) $G=\mathbb{Z}$, $G \trianglerighteq H=n\mathbb{Z}$

$$G/H=\{n\mathbb{Z}, n\mathbb{Z}+1,\dots, n\mathbb{Z}+n-1\}$$

סה"כ n מחלקות.

עבור $n=5$:
$$G/H=\{5\mathbb{Z},5\mathbb{Z}+1,\dots,5\mathbb{Z}+4\}=\{[0],\dots,[4]\} \cong \mathbb{Z}_5$$

ובאופן כללי
$$\mathbb{Z}/n\mathbb{Z}=\mathbb{Z}_n$$

2) $G=(\mathbb{R}^2,+) \trianglerighteq H=\{(a,0) \mid a\in\mathbb{R}\}$

נורמלית כי אבלית

דוגמה לקוסט: $(5,2)+H=\{(a,2) \mid a\in\mathbb{R}\}$

$$\mathbb{R}^2/H \cong \mathbb{R}$$

כי אם נקח נציגים מכל ישר שיהיו נקודה על הציר נקבל את הקו הזה.

הערה

עבור G סופית
$$|G/H|=[G:H]=\frac{|G|}{|H|}$$

תרגיל: תהא G חבורה סופית, $H \leq G$ כך ש- $[G:H]=n$.
אז לכל $a \in G$ מתקיים $a^n \in H$

פתרון

G/H היא חבורה מסדר n, ולכן לכל $\bar{a} \in G/H$ מתקיים
$\bar{a}^n = e_{G/H} = H$. (קוסט היחידה)

$\bar{a}$ היא מחלקה שמאלית לכן יש $a \in G$ כך ש- $\bar{a} = aH$:

$(aH)^n = H$

$a^n H = H$

ומהמשפט $aH = bH$ אמ"מ $b^{-1}a \in H$ נקבל $a^n \in H$ כנדרש.

תרגיל

תהי $H \leq G$ מאינדקס 2. הוכיחו כי G/H חבורה אבלית.

פתרון

G/H חבורה כי ראינו שכל ת"ח מאינדקס 2 היא נורמלית.
$|G/H| = \frac{|G|}{|H|} = [G:H] = 2$

כלומר זו חבורה עם שני איברים ולכן אבלית

תת חבורה מאינדקס 2

תהי $H \leq G$, הוכח $H \trianglelefteq G$.

פתרון

H מאינדקס 2 ולכן $G = H \uplus_{a \notin H} aH = H \uplus_{a \notin H} Ha$

ולכן $aH = Ha$ לכן $H \trianglelefteq G$ כנדרש.

אוטומורפיזמים

הגדרה: G חבורה. $Aut(G)=\{f:G\to G \text{ איזומורפיזם}\}$

דוגמא

1) $id:G\to G$ אוטומורפיזם זהותי (טריוויאלי).

2) עבור G חבורה אבלית, $g\mapsto g^{-1}$ אוטומורפיזם.

3) הצמדה: לכל $a\in G$ נגדיר $\varphi_a\in Aut(G)$ ע"י $g\mapsto aga^{-1}$.

תרגיל

חשב את $Aut(\mathbb{Z})$

פתרון

$\mathbb{Z}$ ציקלית לכן יוצר עובר ליוצר תחת איזומורפיזם.
אם נגדיר φ אוטומורפיזם על היוצר של $\mathbb{Z}$, אז נקבל אוטו' של $\mathbb{Z}\to\mathbb{Z}$.
יש שתי אפשרויות ל-$\varphi(1)$:

$\varphi(1)=1 \Rightarrow id$

$\varphi(1)=-1 \Rightarrow n\mapsto -n$

$\Rightarrow |Aut(\mathbb{Z})|=2$

$Aut(\mathbb{Z})\cong\mathbb{Z}_2$

דוגמא

חשב את $Aut(\mathbb{Z}_n)$

פתרון

כמו בדוגמה הקודמת היוצר חייב לעבור ליוצר של $\mathbb{Z}_n$.
היוצרים של $\mathbb{Z}_n$ הם בדיוק האיברים הזרים ל-n מ-1 עד n. נראה $Aut(\mathbb{Z}_n)\cong U_n$. כאשר מספיק לקבוע את $f(1)$. $Aut(\mathbb{Z}_n)=\{f:\mathbb{Z}_n\to\mathbb{Z}_n \mid f(1)\in U_n\}$
נסתכל על הפונקציה $\varphi:U_n\to Aut(\mathbb{Z}_n)$ המוגדרת ע"י $a\mapsto f_a$
כאשר $f_a:\mathbb{Z}_n\to\mathbb{Z}_n$ מוגדרת ע"י $f_a(1)=a$.
הומומורפיזם: $\varphi(ab)=f_{ab}=f_a\circ f_b=\varphi(a)\cdot\varphi(b)$
על מניה והקבוצות סופיות גם חח"ע.
מכאן קיבלנו $U_n\cong Aut(\mathbb{Z}_n)$ כנדרש.

תרגיל

חשב את $Aut(\mathbb{Z}_2^2)$

פתרון

(האיזומורפיזמים)

$Aut(\mathbb{Z}_2\times\mathbb{Z}_2)$ הוא כל ההעתקות ההפיכות מ-$\mathbb{Z}_2^2$ לעצמו,

כלומר זה כל ה״ה הליניאריות מ-$\mathbb{Z}_2^2$ ל-$\mathbb{Z}_2^2$.

מאלגברה ליניארית זה איזומורפי ל-$GL_2(\mathbb{Z}_2)$.

$$= \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}\right\}$$

זו חבורה מסדר 6 ולא אבלית $\cong S_3$

8.1

הגדרה: תהי G חבורה, $a \in G$. ההעתקה I_a המוגדרת ע"י $g \mapsto aga^{-1}$ נקראת <u>הצמדה</u> או <u>אוטו' פנימי</u>.

נסמן את אוסף האוטומורפיזמים הפנימיים ב- $Inn(G)$, כלומר $Inn(G)=\{I_a \mid a \in G\}$

<u>משפט</u>: $Inn(G) \trianglelefteq Aut(G)$

<u>הוכחה</u>: (1) $Inn(G)$ לא ריקה כי e מוגדרת, ולכן $\forall g \in G$ ... $I_e \in Inn(G)$

(2) יהיו $I_a, I_b \in Inn(G)$ צ"ל $I_a I_b^{-1} \in Inn(G)$

$(I_a \circ I_b^{-1})(x) = I_a(I_b^{-1}(x)) = I_a(b^{-1}xb) = ab^{-1}xba^{-1} = (ab^{-1})(x)(ab^{-1})^{-1} = I_{ab^{-1}}$

(3) תהי $f \in Aut(G)$ ו- $I_a \in Inn(G)$

צ"ל ש- $f I_a f^{-1} \in Inn(G)$

$(f I_a f^{-1})(x) = f(I_a(f^{-1}(x))) = f(af^{-1}(x)a^{-1}) = f(a)f(f^{-1}(x))f(a^{-1}) =$

$= f(a)\, x\, f(a^{-1}) = I_{f(a)} \in Inn(G)$

<u>משפטי האיזומורפיזם הבסיסיים:</u>

<u>משפט</u>: יהיו G,H חבורות, $\varphi: G \to H$ הומו' אזי $Im\,\varphi \cong G/ker\,\varphi$

<u>מסקנה</u>: אם f הומו' אפימורפיזם אזי $H \cong G/ker\,\varphi$.

<u>דוגמה</u>: (1) $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. נגדיר $f: \mathbb{Z} \to \mathbb{Z}_n$ המוגדרת ע"י $a \mapsto [a]_n$

הוא אפימורפיזם, והגרעין הוא $ker\,\varphi = \{a \in \mathbb{Z} \mid \varphi(a) \equiv 0 (mod\, n)\} = n\mathbb{Z}$.

ולכן ... .

(2) הראו כי $GL_n(F)/SL_n(F) \cong F^*$ [תרגיל]

פתרון: נגדיר $det: GL_n(F) \to F^*$. הוא הומו', ...

... $\begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \mapsto a$:

... $ker(det) = \{A \in GL_n(F) \mid det(A)=1\} = SL_n(F)$

<u>תרגיל</u>: יהי $f: \mathbb{Z}_{14} \to D_{10}$ הומו'. מה האפשרויות ל- $ker f$!

<u>פתרון</u>: ... $ker\,f \leq \mathbb{Z}_{14}$ לכן $|ker\,f| \mid 14$

$|ker\,f| \in \{1,2,7,14\}$

(1) אם $|ker\,f|=1$, אזי ... : $\mathbb{Z}_{14} \cong \mathbb{Z}_{14}/\{0\} \cong Im\,f$

אבל $Im\,f \leq D_{10}$

$|D_{10}|=20$ ולא $14 \mid 20$ ...

(2) $|ker\,f|=2$ $Im\,f \cong |\mathbb{Z}_{14}/ker\,f| = \frac{|\mathbb{Z}_{14}|}{|ker\,f|}$.

... $=7$

(ב) ההגדרות שהוגדרו אלו הם להומומ'. כעת נראה f ... לא

ראשית נסמן 7. $f: \mathbb{Z}_{14} \to D_{14}$

נסמן את $H = \langle \tau \rangle = \{id, \tau\} : D_{14}$ ונגדיר הומומורפיזם:

$f: \mathbb{Z}_{14} \to H$ $f([\text{זוגי}]) = id$

$f([\text{אי-זוגי}]) = \tau$

⇓

$\frac{|\mathbb{Z}|}{|\ker f|} = 2$ $\mathbb{Z}_{14}/\ker f \cong |H|$

לפי משפט האיזומורפיזם, לפי משפט 1: $\mathbb{Z}_{14}/\ker f \cong H$

$\left|\mathbb{Z}_{14}/\ker f\right| = |H| = 2$

$\frac{|\mathbb{Z}_{14}|}{|\ker f|} = 2 \to \frac{14}{|\ker f|} = 2 \to |\ker f| = 7$

(ג) $|\ker f| = 14$. נניח [illegible] ניקח את ההומו' הטריוויאלי

$f: \mathbb{Z}_{14} \to D_{14}$ $z \to id$

וכו', לפי משפט 1 $\to |\ker f| = 14$

מסקנה חשובה: אם $f: G \to H$ הומו' אז $|\mathrm{Im}\, f| \,/\, |G|$ לפי משפט 1.

הגדרה: תהי G חבורה. המרכז של G הוא קב' כל האיברים של G המתחלפים עם כל איברי G כלומר: $Z(G) = \{g \in G \mid ga = ag \ \forall a \in G\}$

תרגיל ♥: G אבלית ⟸ $G = Z(G)$

תרגיל ♥: $Z(G)$ תת-חבורה נורמלית של G.

תרגיל ♥: תהי G חבורה. נגדיר הומו': $G \to \mathrm{Inn}(G)$ ע"י $a \mapsto I_a$

מה הגרעין של הומו' זה? המרכז $Z(G)$, לכן לפי משפט 1: $G/Z(G) \cong \mathrm{Inn}(G)$

תרגיל: אם G לא אבלית (במקרה: $|G/Z(G)| > 1$) אז $G/Z(G)$ לא ציקלית.

פתרון: נסמן $H = Z(G)$ ולכן $G = \bigcup gH$.

נניח בשלילה ש- $G/Z(G)$ ציקלית. לכן קיים a כך ש: $G/Z(G) = \langle aH \rangle$

לכן $G = \bigcup_{n \in \mathbb{N}} a^n H$

יהי $x \in G$ לכן מההגדרה קיים $k \in \mathbb{N}$ כך ש: $x \in a^k H$.

ובנוסף $H = Z(G)$, לכן קיים z כך ש: $z \in Z(G)$, $k \in \mathbb{N}$. $x = a^k z$. יהיו $x_1, x_2 \in G$, קיימים $k_1, k_2 \in \mathbb{N}$ ו- $z_1, z_2 \in Z(G)$

כך ש: $x_1 = a^{k_1} z_1$ ו- $x_2 = a^{k_2} z_2$

$x_1x_2 = a^{k_1}z_1 a^{k_2}z_2 \underset{z_1\in Z(G)}{=} a^{k_1}a^{k_2}z_1z_2 = a^{k_1+k_2}z_2z_1 = a^{k_2}a^{k_1}z_2z_1 =$

$= a^{k_2}z_2a^{k_1}z_1 = x_2x_1$

מש"ל, G אבלית – סתירה למה.

<u>תרגיל:</u> תהי $G=\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix} \middle| a,b,c\in \mathbb{Z}_3\right\}$

מה הסדר של $Inn(G)$?

<u>פתרון:</u> $|G|=27$ לכן, לפי לגרנז' $|Z(G)| \mid 27$.

$|Z(G)|\in\{1,3,9,27\}$

1 לא יכול כי יש לפחות 2 איברים במרכז, היחידה ו- $\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix}$

אם $|Z(G)|=27$ אז $G=Z(G)$ ולכן G אבלית, סתירה כי G לא אבלית.

אם $|Z(G)|=9$ אז $|G/Z(G)| = \frac{|G|}{|Z(G)|}=\frac{27}{9}=3$

ולכן $G/Z(G)\cong \mathbb{Z}_3$ ולכן ציקלית ← G אבלית – סתירה.

האפשרות היחידה שנשארה היא $|Z(G)|=3$ ולכן $Inn(G)=\frac{27}{3}=9$

<u>חבורת הפרמוטציות</u> – S_n

~~[illegible]~~

• S_n – קבוצת התמורות על $\{1,2,\ldots,n\}$ (עם הרכבה (הכפלה)).

סימון – ניתן לסמן: $\begin{pmatrix}1,2,\cdots & n\\ \sigma(1),\cdots & \sigma(n)\end{pmatrix}$

מחזור, כל תמורה אפשר לכתוב כמכפלה של מחזורים זרים.

הערה על כתיבה: כותבים את ההרכבה מימין לשמאל (כמו פונקציות).

ובמחזורים, הכתיבה היא לפי סדר של המחזור: $(4,3,2,1) \leftarrow (1\,2\,3\,4)$

<u>הגדרה:</u> המחזורים $(i_1\ldots i_n)$ ו- $(j_1\ldots j_k)$ נקראים זרים אם $\{i_1\ldots i_n\}\cap\{j_1\ldots j_k\}=\phi$.

<u>הערה חשובה:</u> מחזורים זרים מתחלפים זה עם זה.

<u>סדרים של איברים ב- S_n:</u>

(1) אם σ מחזור באורך k אז $o(\sigma)=k$

(2) טענה: אם G חבורה, $a,b\in G$ כך ש: $ab=ba$ ו- $\langle a\rangle\cap\langle b\rangle=\{e_G\}$

אז $o(ab)=lcm(o(a),o(b))$

ולכן ב- S_n אם σ_1,σ_2 מחזורים זרים $o(\sigma_1\sigma_2)=lcm(o(\sigma_1),o(\sigma_2))$

תרגיל: מצאו תת"ח מסדר 45 ב-S_{15}

פתרון: נשתמש בכך שאיבר מסדר 45. מספיק לקחת מכפלה של מחזורים זרים מאורכים 9, 5 כי $(9,5)=1$, וגם $lcm(9,5)=45$

אז ניקח למשל: $\sigma = (1,2,\dots,9)(10,\dots,14)$

ואז $\langle\sigma\rangle$ היא התת"ח המבוקשת.

תרגיל: כמה מחזורים מאורך r יש ב-S_n?

פתרון: בוחרים r איברים מתוך n: $\binom{n}{r}$.

מסדרים אותם. יש r! דרכים לסדר אותם, אך כל r מהם זהים (הזזה מעגלית), ולכן בסך הכל נקבל: $\frac{1}{r}\cdot r!\cdot\binom{n}{r}$

תרגיל: מצא את הסדרים האפשריים ב-S_4 (א), S_6 (ב)

פתרון: (א) $id, (12), (123), (1234), (12)(34) \Rightarrow 1,2,3,4$

(ב) $id, (12), (123), (1234), (12345), (123)(45) \Rightarrow 1,2,3,4,5,6$

תרגיל: הוכח/הפרך: $S_4 \cong D_{12}$

פתרון: לא נכון, כי ב-D_{12} יש איבר מסדר 12 (סיבוב)

סימן של תמורה, ו-A_n:

סימן של מחזור באורך k = $(-1)^{k-1}$

$|A_n| = \frac{n!}{2}$, $[S_n:A_n]=2 \Rightarrow A_n \trianglelefteq S_n$

תרגיל: (א) מה הם הסדרים האפשריים ב-A_4

(ב) האם A_4 איזו' ל-D_6.

פתרון: (א) $id, (123), (12)(34) \Rightarrow 1,3,2$

(ב) לא, כי ב-D_6 יש איבר מסדר 6.

תרגיל: כמה איברים מסדר 2 יש ב-A_n עבור $n\ge 8$?

פתרון: מכפלה של מס' זוגי של חילופים: A_3: אין איברים מסדר 2

$A_4 \dots A_7$: שתי חילופים זרות $(__)(__)$: $\frac{1}{2}\cdot\binom{n}{2}\cdot\binom{n-2}{2}$

A_8: ארבע חילופים זרות $(__)(__)$ או $(__)(__)(__)(__)$

סה"כ: $\frac{1}{2}\cdot\binom{8}{2}\cdot\binom{6}{2} + \frac{1}{4!}\cdot\binom{8}{2}\cdot\binom{6}{2}\cdot\binom{4}{2}\cdot\binom{2}{2}$

פעולת הצמדה: יהי $(i_1,\dots,i_k)$ מחזור ב-S_n

ויהי $\mu\in S_n$ אז $\mu(i_1\dots i_k)\mu^{-1}=(\mu(i_1)\dots\mu(i_k))$

מסקנה חשובה מאוד: שתי תמורות ב-S_n הן צמודות אם״ם יש להן אותו מבנה מחזורים.

דוגמה: יהיו $\alpha,\beta,\gamma\in S_5$ המוגדרות ע״י $\alpha=(1\,4\,5)$, $\beta=(1\,3\,2)$, $\gamma=(1\,5)$

אזי:
$$\alpha\gamma\alpha^{-1}=(2\;3)$$
$$\alpha\beta\alpha^{-1}=(1\;3\;2)$$

משפט: חבורת הסימטריה S_n נוצרת ע״י 2 איברים: $\tau=(1\,2)$, $\sigma=(1,2,\ldots,n)$

הוכחה: (1) כל תמורה ב-S_n ניתנת לכתיבה כמכפלה של חילופים (טרנספוזיציות), לכן מספיק להראות שכל חילוף נוצר ע״י σ,τ.

(1) נראה שכל מחזור נוצר ע״י חילופים.
$$(a_1,a_2,\ldots,a_k)=(a_1,a_2)\cdots(a_{k-1},a_k)$$

(2) נראה שכל חילוף נוצר ע״י σ,τ, נראה כי כל חילוף נוצר ע״י חילופים מהצורה $(i,i+1)$, $1\le i\le n-1$.

יהי (a,b) חילוף כלשהו $b>a$. אם $b=a+1$ אז סיימנו. אחרת, נניח באינדוקציה על $b-a$ כך ש-$b-a>1$
$$(a\;b)=(a\;a+1)(a+1\;b)(a\;a+1)$$

סימון ♥: עד כה הוכחנו כי $S_n=\langle\{(i,i+1),1\le i\le n-1\}\rangle$

כלומר ל-S_n יש קבוצת יוצרים בגודל $n-1$.

(3) נראה שכל חילוף מהצורה $(i,i+1)$ ניתן לכתיבה ע״י σ,τ
$$\sigma(1\,2)\sigma^{-1}=(2,3)$$
$$\sigma^k(1\,2)\sigma^{-k}=(1+k,2+k)\longrightarrow \text{וכו׳}$$

כלומר, $S_n=\langle\sigma,\tau\rangle$
$$\mathrm{rank}(S_n)=2$$

משפט חשוב מאוד: המרכז של S_n ($n\ge3$) הוא $Z(S_n)=\{id\}$

הוכחה: נניח שקיים $id\ne a\in Z(S_n)$. יהי b ב-S_n שונה מ-a בעל אותו מבנה מחזורים, אז הן צמודות, כלומר קיים $w\in S_n$ כך ש- $waw^{-1}=b$

אבל $a\in Z(S_n)$ ולכן $b=waw^{-1}=ww^{-1}a=a$

כלומר $a=b$ סתירה.

הערה חשובה: כדי לבדוק האם תת-חבורה של S_n היא נורמלית, מספיק לבדוק עבור כל תמורה σ בתת-החבורה, האם היא מכילה את כל התמורות בעלות אותו מבנה מחזורי.

דוג': (ii) S_n , $n\geq 3$

$\{id,(12)\}=\langle(12)\rangle$ אינה נורמלית ב-S_n כי לפי: הצמדה [illegible]. ואז לא נשמר

את (13) לא נורמלית.

$\{id,(12)(34),(13)(24),(14)(23)\}=V\trianglelefteq S_4$ נורמלית ב-S_4. למה? כי הצמדה את כל התמורות משמרת מבנה המחזורים.

<u>תרגיל:</u> הפרך את המשפט ההפוך של לגראנז': כלומר, נכון תמיד ש-G חבורה ו-$n\,|\,|G|$ אז קיים ל-G תת חבורה מסדר n.

<u>פתרון:</u> נסתכל ב-$G=A_4$, $|G|=\frac{4!}{2}=12$ נוכיח כי אין ל-G תת חבורה מסדר 6. נניח בשלילה שקיימת תת חבורה $H\leq G$ מסדר 6. אז היא מאינדקס $\frac{12}{6}=2$, לכן היא נורמלית ב-G. ואם לפי תרגיל קודם [illegible] לכל $\sigma\in A_4$ ו- $\sigma^2\in H$. אז: $\sigma\in G$ מחזור באורך 3. אז $\sigma^2\in H$ ולכן $\sigma=\sigma^4=(\sigma^2)^2\in H$ כלומר כל מחזור באורך 3 נמצא ב-H. אבל $\binom{4}{3}\cdot(3-1)!=8$ מחזורים באורך 3, $8>6$ סתירה.

<u>תרגיל:</u> הראה שנורמליות אינה (תכונה) טרנזיטיבית. כלומר, מצא $K\trianglelefteq N\trianglelefteq G$ כך ש-K אינה נורמלית ב-G.

<u>פתרון:</u> ניקח $G=S_4$, $N=V$, $K=\langle(12)(34)\rangle$

$N\trianglelefteq G$

$K\trianglelefteq N$ כי היא מאינדקס 2.

אבל K לא נורמלית ב-G: כי ניתן את התמורה $(12)(34)$ להצמיד ל- $(13)(24)$ [illegible] מחזורים באותו מבנה, ולכן לא נורמלית.

מרכז:

הגדרה: G אבלית אמ"מ $G=Z(G)$

• $Z(G)$ תמיד לא ריקה כי $e\in Z(G)$

• <u>טענה:</u> $Z(G)\trianglelefteq G$

<u>הוכחה:</u> [illegible], לא ריקה.

תהיינה $a,b\in Z(G)$ נראה $ab^{-1}\in Z(G)$

כלומר יהי $c\in G$ נראה $ab^{-1}c=cab^{-1}$

$acb = cab$ ✓

הוכחה: אם $a \in Z(G)$ אז $a^{-1} \in Z(G)$. אכן, יהי $c \in G$

$a^{-1}c = ca^{-1}$ אזי $ac^{-1} = c^{-1}a$ ⟸ $(ac^{-1})^{-1} = (c^{-1}a)^{-1}$

⟸ $ca^{-1} = a^{-1}c$

נורמליות: $Z \trianglelefteq G$, $g \in G$, צ"ל $gZg^{-1} \subseteq Z(G)$

אכן, $gzg^{-1} = gg^{-1}z = z \in Z(G)$

דוגמה: $Z(S_n)$ של S_n ($n>2$) הוא טריוויאלי.

(ב) המרכז של $GL_n(K)$ הוא: המטריצות הסקלריות.

דוגמה: שורשי היחידה $(\mathbb{C}^*, \cdot)$ ונסמן אותם ב- Ω_∞ והוא

$$\Omega_\infty = \bigcup_{n\in\mathbb{N}} \Omega_n = \bigcup_{n\in\mathbb{N}} \left\{cis\frac{2\pi k}{n} \mid 0\le k\le n-1\right\}$$

נראה זו תת חבורה. לפי הקריטריון המקוצר, יהיו $a,b \in \Omega_\infty$

אז: $a = cis\frac{2\pi k_1}{n_1},\ b = cis\frac{2\pi k_2}{n_2}$

$$ab^{-1} = cis\left(\frac{2\pi k_1}{n_1}\right) \cdot cis\left(\frac{2\pi k_2}{n_2}\right)^{-1} = cis\frac{2\pi(k_1n_2 - k_2n_1)}{n_1 n_2} \in \Omega_{n_1n_2} \subseteq \Omega_\infty$$

(ג) נראה שלכל איבר ב-Ω_∞ יש סדר סופי: $\forall x\in\Omega_\infty\ \exists n\in\mathbb{N}: x\in\Omega_n$

ד) Ω_∞ לא ציקלית: נניח בשלילה $\Omega_\infty = \langle a \rangle$ אזי: $o(a)=\infty$

ה) $\Omega_\infty \trianglelefteq \mathbb{C}^*$ אבל $\mathbb{C}^*$ אבלית ולכן Ω_∞ נורמלית, ולכן נוכל להסתכל על $\mathbb{C}^*/\Omega_\infty$

טענה: אם $e \ne a \in \mathbb{C}^*/\Omega_\infty$ אז הסדר שלו הוא ∞

הוכחה: יהי $e \ne a \in \mathbb{C}^*/\Omega_\infty$, אז יש $z\in\mathbb{C}^*$ כך ש: $a = z\Omega_\infty$, $a\ne e$

ולכן $z \notin \Omega_\infty$.

נניח בשלילה ש- $o(a)=n\in\mathbb{N}$ אז $a^n = e_{\mathbb{C}^*/\Omega_\infty}$ אבל אז,

$a^n = (z\Omega_\infty)^n = z^n\Omega_\infty$ כלומר $z^n \in \Omega_\infty$ כלומר יש $m\in\mathbb{N}$

כך ש- $(z^n)^m = 1$ ⟸ $z^{nm} = 1$ ⟸ $z\in\Omega_\infty$ סתירה.

הערה: Ω_∞ לא נוצרת סופית

הסבר: נראה כי G קבוצה סופית של איברים ב-Ω_∞ לא יכולה לייצר את כל האיברים. (ל-Ω_∞ יש ∞ איברים). אם $a_1,\dots,a_n$ שורשי יחידה מסדר

$n_1,\dots,n_n$ המתאימים אז

$$\langle a_1,\dots,a_n\rangle = \{a_1^{i_1}\cdots a_n^{i_n} \mid 1\le i_r\le n_r\}$$

וזו קבוצה סופית

חבורות

מיון חבורות אבליות סופיות

1. אם G חבורה אבלית מסדר $p_1 \cdot p_2 \cdots p_n$ כאשר p_i ראשוניים שונים
אזי
$$G \cong \mathbb{Z}_{p_1} \times \dots \times \mathbb{Z}_{p_n}$$

2. אם G חבורה אבלית מסדר p^n (p ראשוני) אז קיימים m_i
כך ש- $n = m_1 + m_2 + \dots + m_r$ טבעיים
$$G \cong \mathbb{Z}_{p^{m_1}} \times \mathbb{Z}_{p^{m_2}} \times \dots \times \mathbb{Z}_{p^{m_r}}$$

למשל אם נתונה G אבלית מסדר 27 אז היא איזומורפית
לאחת מהבאות: $\mathbb{Z}_{3}, \mathbb{Z}_9 \times \mathbb{Z}_3, \mathbb{Z}_3^3$
(וכל אחת מהחבורות הללו לא איזומורפיות אחת לשניה)

הגדרה

עבור $n \in \mathbb{N}$ נסמן ב-$p(n)$ את מס' הסדרות הסופיות
של מס' טבעיים $\{s_i\}_{i=1}^{r}$ כך ש- $\sum_{i=1}^{r} s_i = n$
$$s_1 \geq s_2 \geq \dots \geq s_r$$

למשל
$$p(4) = 5$$
(כי $4 = 4, 3+1, 2+2, 2+1+1, 1+1+1$)

מסקנה

כל חבורה אבלית מסדר $p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ (p_i ראשוניים שונים)
איזומורפית ל- $H_{p_1} \times \dots \times H_{p_n}$
כאשר H_{p_i} חבורה אבלית (איזומורפית לחבורה אבלית)
מסדר $p_i^{\alpha_i}$.

דוגמא

כל G חבורה אבלית מסדר 45 ($3^2 \cdot 5$), אז G איזומורפית לאחת
מן הבאות:
$$G \cong H_3 \times H_5$$
כאשר
$$H_5 \cong \mathbb{Z}_5 \qquad H_3 \cong \mathbb{Z}_9$$
או
$$H_3 \cong \mathbb{Z}_3^2$$

מסקנה

מס' החבורות האבליות (עד כדי איזומורפיזם) מסדר $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ הוא $p(\alpha_1)p(\alpha_2)\cdots p(\alpha_k)$

משפט

$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$ (חבורות ציקליות) אם"ם $(m,n)=1$

מחלקות צמידות

הגדרה

תהי G חבורה, $x\in G$. אזי מחלקת הצמידות של x, היא

$$[x]=conj(x):=\{gxg^{-1} \mid g\in G\}$$

תכונות

1) $x\in[x]$

2) G אבלית $\iff$ לכל $x\in G$: $[x]=\{x\}$

3) $x\in Z(G) \iff [x]=\{x\}$

4) מחלקות הצמידות הן זרות או שוות (כלומר אם $y\in[x]$ אז $[x]=[y]$),

5) $|conj(x)| \,\big|\, |G|$: $\forall x\in G$

דוגמה

מחלקת צמידות ב-S_n מכילה את כל התמורות בעלות אותו מבנה מחזורים. למשל עבור $\sigma=(1\,2\,3)\in S_4$

אז $[\sigma]=\{(1,2,3),(1,2,4),\ldots\}$

$|conj(\sigma)|=8=\binom{4}{3}(3-1)!$

תרגיל

כמה מחלקות צמידות יש ב-

א) S_4

ב) A_4

[illegible]

א. מבני המחזורים האפשריים הם

$(_\ _\ _\ _)$

$(_\ _\ _)$

$(_\ _)$

$(_\ _)(_\ _)$

id

לכן יש 5 מחלקות צמידות (כי ה-[illegible] שתי תמורות צמודות אמ"מ יש להן אותו מבנה מחזורים)

ב. מבני המחזורים האפשריים הם

$(_\ _\ _)$

$(_\ _)(_\ _)$

id

אבל כאן זה לא אומר שיש שלוש מחלקות צמידות!!!

(כי המשפט לעיל לא עובד ב-A_n)

$conj(id)=\{id\}$

כעת עבור $a=(1\ 2)(3\ 4)$

יש לו ב-S_4 שני צמודים נוספים (1 4)(2 3), (1 3)(2 4)

האם הם צמודים גם ב-A_4?

$b=(1\ 2\ 3)\in A_4 \quad c=(1\ 3\ 2)\in A_4$

$bab^{-1}=(1\ 4)(2\ 3)$

$cac^{-1}=(1\ 3)(2\ 4)$

$|conj(a)|=3$

לכן

עבור ציקלים מצורה $(_\ _\ _)$: בהתחשב בכך שלא

מחלקת צמידות ב-A_4 5 $|A_4|=12$ אבל יש 8 איברים

כאלו

ולכן עבור $u=(1\ 3\ 2)$: $conj(u)=\{(1\ 3\ 2),(2\ 4\ 1),(2\ 3\ 4),(1\ 4\ 3)\}$

ועבור $v=(1\ 2\ 3)$: $conj(v)=\{(1\ 2\ 3),(1\ 3\ 4),(1\ 4\ 2),(2\ 4\ 3)\}$

כי $|[v]|=|[u]|=4$ ולכן יש 4 מחלקות שקילות

תרגיל

תהי G חבורה מסדר p (ראשוני). כמה מחלקות צמידות יש ב-G?

פתרון

חבורה מסדר ראשוני היא ציקלית, ולכן אבלית ולכן $\{a\}=[a]$ $\forall a\in G$

לכן יש p מחלקות צמידות.

תרגיל

תהי G חבורה, $N\trianglelefteq G$ ו-C מח"צ ב-G. הוכח

$N\cap C=\phi$ **או** $C\subseteq N$

פתרון

אם $N\cap C=\emptyset$ הקבוצה ריקה אז סיימנו.

אחרת יהי $x\in N\cap C \Leftarrow x\in C \wedge x\in N$.

יהי $y\in C$ צ"ל ש-$y\in N$.

אבל x,y באותה מח"צ, לכן קיים $g\in G$ כך ש-
$y=g^{-1}xg$

אך $x\in N$ ולכן גם $y\in N$ כנדרש.

מסקנה

כל ת"ח נורמלית היא איחוד זר של מח"צ של איבריה

הגדרה

נאמר ש-G פשוטה אם אין לה ת"ח נורמליות לא טריוויאליות

משפט

A_n פשוטה לכל $n\geq 5$.

עבור קטנים: A_4 לא פשוטה כי $\{id,(1,2)(3,4),(1,4)(2,3),(1,3)(2,4)\}\trianglelefteq A_4$

$A_3\cong\mathbb{Z}_3$ ולכן פשוטה.

$A_2\cong\mathbb{Z}_2$ לכן פשוטה

$A_1=\{id\}$ ״

תרגיל
$|A_5|=60$ פשוטה. האם כל חבורה מסדר 60 פשוטה?
פתרון
לא! $\mathbb{Z}_{60}$, שכן $\mathbb{Z}_n$ פשוטה אם"ם n ראשוני.

<u>פעולה של חבורה על קבוצה</u>

הגדרה
תהיינה G חבורה, X קבוצה. פעולה של G על X היא פונקציה
בינארית $G\times X\to X$ שמסומנת ע"י $(g,x)\mapsto g*x$
כך שמתקיים:
1) $(gh)*x=g*(h*x)$ $\quad\forall g,h\in G,\ x\in X$
2) $e_G*x=x$ $\quad\forall x\in X$
(צר שקול להומומורפיזם מ-G ל-S_X, הפעולה לא יתכן כי עבור $x_1\neq x_2$ יתקיים $g*x_1=g*x_2$)

דוגמאות
1) G פועלת על עצמה ע"י כפל משמאל: (וכאן $G=X$)
כלומר $g*x=gx$
2) G פועלת על עצמה ע"י הצמדה:
$g*x=gxg^{-1}$
3) $G=S_n$, $X=\{1,\dots,n\}$, אז (צריך $\sigma*i=\sigma(i)$),
4) $G=S_n$, $X=F[x_1,\dots,x_n]$, $\sigma*f(x_1,\dots,x_n)=f(x_{\sigma(1)},\dots,x_{\sigma(n)})$

הגדרה
מסלול של $x\in X$ הוא $\{g*x\mid g\in G\}$ ומסומן $G*x$ או $[x]$ או $Orb(x)$
סימון: כש-G פועלת על עצמה ע"י הצמדה אז מסלול של $x\in G$
הוא $conj(x)$.

הגדרה
אם קיים $x\in X$ כך ש-$X=G*x$ אז נאמר שהפעולה טרנזיטיבית

הגדרה

המייצב של איבר x הוא $stb(x)$ מוגדר ע"י

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

כמו כן $stb(x)\le G$, $G*x\subseteq X$

תרגיל $stb(x)\le G$ לכל $x\in X$.

פתרון

הופכי: יהי $g\in stb(x)$, כלומר $g*x=x$, אז

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

כפל: יהיו $a,b\in stb(x)$, אזי $(ab)*x=a*(b*x)=a*x=x$

לכן $ab\in stb(x)$

כמו כן $stb(x)\neq\emptyset$ כי $e\in stb(x)$

דוגמה

תהי $G=S_3$, $X=F[x_1,x_2,x_3]$ עם הפעולה שראינו קודם.

מצא את המסלול של $f(x)=x_1(x_2+x_3)$.

פתרון

$$Orb(f(x))=\{x_1(x_2+x_3),\ x_2(x_1+x_3),\ x_3(x_1+x_2)\}$$

הערה

פעולה של G על X מגדירה יחס על X ע"י $x\sim y$ אם"ם $\exists g\in G: g*x=y$. מחלקות השקילות הם המסלולים, אך

לכל $x,y\in X$ $G*x=G*y$ או $G*x\cap G*y=\emptyset$. כלומר אם $y\in G*x$ אז $G*x=G*y$

ב- $X=\bigcup_x G*x$ ואפשר לקבל איחוד זר אם נקח נציג אחד מכל מסלול.

משפט

לכל $x\in X$ מתקיים $|G*x|=[G:stb(x)]$. אם G סופית אז

$$|G*x|=\frac{|G|}{|stb(x)|}$$

בפרט הגודל של כל מסלול מחלק את הסדר של G.

לגבי הדוגמה הקודמת ראינו ש- $|G*f(x)|=3$

$$\Rightarrow |stb(f(x))|=\frac{6}{3}=2$$

תרגיל

עבור פעולת ההצמדה של G על עצמה, נראה שסדר של מח"צ מחלק את סדר החבורה. חשבו את מס' התמורות המתחלפות עם $\beta=(1\ 2)(3\ 4)$ ב-S_n

פתרון

$$\{\alpha\in S_n \mid \alpha\beta=\beta\alpha\} = \{\alpha\in S_n \mid \alpha\beta\alpha^{-1}=\beta\} =$$

$$= \{\alpha\in S_n \mid \alpha*\beta=\beta\} = stab(\beta)$$

לכן $$|stab(\beta)| = \frac{|G|}{|G*\beta|} = \frac{n!}{|G*\beta|}$$

נשאר לחשב את המסלול של β ב-S_n. אך מסלול תחת ההצמדה הוא מח"צ ואת המח"צ נמצא לפי מבני מחזורים.

$$|[\beta]| = \frac{1}{2}\binom{n}{2}\binom{n-2}{2}$$

ולכן מס' התמורות המתחלפות עם β הן

$$\frac{n!}{0.5\binom{n}{2}\binom{n-2}{2}} = 8(n-4)!$$

<u>הערה</u>

מהפעולה של G על עצמה ע"י הצמדה ניתן לקבל פעולה של G על תתי החבורות שלה (ע"י הצמדה). כלומר

$$X=\{H \mid H\le G\}$$

$$g*H = gHg^{-1}$$

תת"ח שהן שקולות ביחס לפעולה זו (כלומר נמצאות באותו מסלול) נקראות תת"ח צמודות.

המייצב של תת"ח H הוא בדיוק תת"ח הקרויה המנרמל של G. כלומר $N(H)=\{g\in G \mid gHg^{-1}=H\}$

כאשר G סופית מספר תת"ח הצמודות ל-H הוא לפי משפט המסלול שהוא: $$|G*H| = \frac{|G|}{|N(H)|}$$

כיוון ש-$H\le N(H)$ אז אם G סופית, $|H| \mid |N(H)|$

ולכן $[G:N(H)]$ מחלק את הסדר של $[G:H]$ כי

$[G:N(H)] = \frac{|G|}{|N(H)|}$ וגם $[G:H] = \frac{|G|}{|H|}$

מסקנה

$N(H)$ היא התת חבורה הגדולה ביותר של G אשר בה H נורמלית

תרגיל

תהי G חבורה $|G|=p^{n}$, כך ש... הראו כי G לא פשוטה.

פתרון

G פועלת על עצמה ע"י הצמדה, $Z=\{g\in G \mid \dots\}$

לכן $G \trianglerighteq Stab(g)$.

הגדרה

נקודת שבת היא איבר $x\in X$ כך שלכל $g\in G$ מתקיים $g\cdot x = x$.

הגדרה

יהי $g\in G$. נסמן $X^{g}=\{x\in X \mid g\cdot x = x\}$ כקב' נקודות השבת של g.

(!!!) הלמה של ברנסייד

תהי G חבורה הפועלת על X. נסמן ב-κ את מס' המסלולים של הפעולה. אזי

$$\kappa=\frac{1}{|G|}\sum_{g\in G}|X^{g}|$$

כלומר מס' המסלולים היא ממוצע נקודות השבת.

תרגיל

אני מעוניין לצבוע כרטיס של 6 משבצות ב-4 צבעים.

נסמן ב-$M_i(x)$ את צבע המשבצת ה-i של הכרטיס x.

אם נהוי שני כרטיסים x ו-y מתקיים

$M_1(x)=M_5(y)$, $M_2(x)=M_4(y)$, $M_3(x)=M_6(y)$

נאמר שהכרטיסים שקולים ולא נחשיב כאותו צביעה נפרדת

ר"ל שנספור את מס' הצביעות השונות

מצוי בכמה דרכים אפשר לצבוע כרטיס

תרגיל

עבור פעולת ההצמדה של G על עצמה, נראה שסדר של מח"צ מחלק את סדר החבורה. חשבו את מס' התמורות המתחלפות עם $\beta=(1\ 2)(3\ 4)$ ב-S_n.

פתרון

$$\{\sigma\in S_n \mid \sigma\beta=\beta\sigma\}=\{\sigma\in S_n \mid \sigma\beta\sigma^{-1}=\beta\}=$$
$$=\{\sigma\in S_n \mid \sigma*\beta=\beta\}=stab(\beta)$$

לכן
$$|stab(\beta)|=\frac{|G|}{|G*\beta|}=\frac{n!}{|G*\beta|}$$

נשאר לחשב את המסלול של β ב-S_n. אך מסלול תחת ההצמדה היא מח"צ ואת המח"צ נמצא לפי מבנה מחזורים.

$$|[\beta]|=\frac{1}{2}\binom{n}{2}\binom{n-2}{2}$$

ולכן מס' התמורות המתחלפות עם β הוא

$$\frac{n!}{0.5\binom{n}{2}\binom{n-2}{2}}=8(n-4)!$$

הערה

מהפעולה של G על עצמה ע"י הצמדה ניתן לקבל פעולה של G על תת-החבורות שלה ע"י הצמדה. כלומר

$$X=\{H \mid H\leq G\}$$
$$g*H=gHg^{-1}$$

ת"ח שונות שקולות ביחס לפעולה זו (כלומר נמצאות באותו מסלול) נקראות ת"ח צמודות.

המייצב של ת"ח $H\leq G$ הוא בדיוק ת"ח הנקראת המנרמל של G. כלומר
$$N(H)=\{g\in G \mid gHg^{-1}=H\}.$$

כאשר G סופית מספר ת"ח הצמודות ל-H הוא אינדקס המנרמל שכן:
$$|G*H|=\frac{|G|}{|N(H)|}$$

כיוון ש-$H\leq N(H)$ אז אם G סופית, $|H| \mid |N(H)|$

ולכן $[G:N(H)]$ מחלק את הסדר של $[G:H]$ כי $[G:N(H)]=\frac{|G|}{|N(H)|}$ וגם $[G:H]=\frac{|G|}{|H|}$

פתרון

סימונים: צביעה { ☐☐☐☐☐☐ ; שקולות { ☐☐☐☐☐☐

ומכן הקבוצה היא $X=(\mathbb{Z}_4)^6$, שכן כל האפשרויות לצביעות הן $|X|=4^6$

נתבונן ב $\mathbb{Z}_2=S_6$ (ו) ת"מ לס' האפשר

$\sigma=(1\ 5)(2\ 4)(3\ 6)$

ו) הפעולה של $\mathbb{Z}_2$ על X (כלומר החזרה קנונית).

מס' הצביעות הן מס' המסלולים של הפעולה על X.

לכן נחשב את $n=\frac{1}{2}\left(|X_{id}|+|X_{\sigma}|\right)$

$|X_{id}|=|X|=4^6$

$|X_{\sigma}|=4^3$ כי אפשר לבחור רק 3 משבצות

לכן מספר הצביעות הוא $\frac{4^6+4^3}{2}=2080$

תרגיל

נמצא את מס' הצביעות האפשריות של משולש שווה צלעות אם מותר לצבוע כל קודקוד ב-3 צבעים.

פתרון

$G=D_3=\{id, r, r^2, c, cr, cr^2\}$, $X=$ כל הצביעות האפשריות $=\mathbb{Z}_3^3$.

$|X|=3^3=27$

לפי הרנסייד:

$n=\frac{1}{6}\left(|X_{id}|+|X_r|+|X_{r^2}|+|X_c|+|X_{cr}|+|X_{cr^2}|\right)$

$|X_{id}|=|X|=27$

$|X_r|=3$

$|X_{r^2}|=3$ כל הקודקודים באותו צבע

$|X_c|=3\cdot 3=9$ באותו אופן

$cr^2=r$ ... (בשוליים)

אפשרויות לקודקוד של הסימטריה ← אפשרויות לשני הקודקודים האחרים

9 (בשוליים)

$n=\frac{1}{6}(27+6+27)=10$

לכן

תרגיל

נתון משושה משוכלל שרוצים לצבוע את צלעותיו ב-5 צבעים שונים
אם מותר לסובב את המשושה ב-180° (כלומר סיבוב כפי הוא)
לאורך צלעותיו, כמה צביעות שונות יש

פתרון

נסתכל על $G=\langle\sigma^3\rangle=\{id,\sigma^3\}$

לפי ברנסייד

$$N=\frac{1}{2}(|X^{id}|+|X^{\sigma}|+|X^{\sigma^2}|)=$$

$$=\frac{1}{2}(5^6+5^2+5^2)=5225$$

תרגיל

נתונה פעולה $G\times X\to X$ כאשר $|X|=23$, $|G|=49$.
הוכיחו כי קיימת לפעולה כזו לפחות נקודת שבת אחת.

פתרון

x נקודת שבת $\iff G=Stab(x) \iff |G*x|=1$

נתבונן בכל המסלולים של הפעולה וניקח נציג אחד מכל מסלול.
נסמן את קב' הנציגים ב-$\{x_1,\dots,x_k\}$. אז מתקיים

$X=\bigcup G*x_i$ זרים

$$23=\sum_{i=1}^{k}|G*x_i|$$

כמו כן $|G*x_i|\,\big|\,|G|$

23 הוא סכום של מס' המחלקים את 49,
בפרט יהיה מס' ששווה לאחד כנדרש.

~~תרגיל~~ (בית)

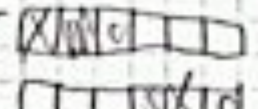
יהי G חבורה, X קבוצה $|G|=|X|=13$, G פועלת על X. הראו כי
יש לפעולה נקודת שבת

הגדרה

יהי G חבורה, מס' יוצרים מינימלי של G הוא מינימום.
לדוגמא: ומכאן של ציקלית הוא 1, ואחוס של ... הוא 2

כלומר יש ל-G יותר מ-1 יוצרים.

פתרון
שימו לב:



והבין הקבוצה היא $X=(\mathbb{Z}_4)^{16}$, שכן כל האפשרויות לצביעות הן 4^{16}

נתבונן ב $G=\mathbb{Z}_6$ (σ) תמורה כך שמתקיים

$\sigma=(1\ 5)(2\ 4)(3\ 6)$

(ד) הסתכל של (σ) ב X (כלומר התמורה קואורדינטות).

מס' הצביעות הינו מס' המסלולים של הפעולה של G על X.

לכן נחשב את $n=\frac{1}{2}(|X_{id}|+|X_\sigma|)$

$|X_{id}|=|X|=4^{6}$

כי אפשר לבחור רק 3 משבצות $|X_\sigma|=4^3$

לכן מספר הצביעות הוא $\frac{4^6+4^3}{2}=2080$

תרגיל

נמצא את מס' הצביעות האפשריות של משולש שווה צלעות אם מותר לצבוע כל קודקוד ב-3 צבעים.

פתרון

$G=D_3=\{id,\tau,\tau^2,\sigma,\sigma\tau,\sigma\tau^2\}$, $X=$ קבוצת הצביעות האפשריות $=\mathbb{Z}_3^3$.

$|X|=3^3=27$

לפי הרנס"ב:

$n=\frac{1}{6}(|X_{id}|+|X_\tau|+|X_{\tau^2}|+|X_\sigma|+|X_{\sigma\tau}|+|X_{\sigma\tau^2}|)$

$|X_{id}|=|X|=27$

כל הקודקודים באותו צבע $|X_\tau|=3$

באותו אופן $|X_{\tau^2}|=3$

$\sigma\tau=t$ $|X_t|=3\cdot3=9$

אפשרויות לקודקוד שעובר 3 אפשרויות ← אפשרויות לבחור צבעים לשני הקודקודים

$n=\frac{1}{6}(27+6+27)=10$

לכן

צמודות

תרגיל

עבור $H \leq G$ נגדיר

$$C(H)=\{g\in G \mid \forall h\in H: ghg^{-1}=h\}$$

הוכח:

1. $C(H)\leq G$
2. $C(H)\trianglelefteq N(H)$

פתרון

1.

$$C_x=Stab(x)=\{g\in G \mid gxg^{-1}=x\}$$

$$C(H)=\bigcap_{x\in H} C_x$$

ולכן $C(H)$ ת"ח כחיתוך של ת"ח.

2. ראשית נוכיח ת"ח (הוכח כי היא חבורה במוכלת ב-$N(H)$).

נותר להראות נורמליות:

יהי $g\in N(H)$, $a\in C(H)$ צ"ל $gag^{-1}\in C(H)$

מתקיים לכל $h\in H$ אמור להתקיים:

$$(gag^{-1})h(gag^{-1})^{-1}=h$$

$$gag^{-1}hga^{-1}g^{-1}=gah_1a^{-1}g^{-1}=gh_1g^{-1}=h$$

(שייך ל-$N(H)$, נסמן h_1) ($C(H)$) (כי נבחר כך $h_1=g^{-1}hg$)

תזכורת הגדרה

חבורת-p היא חבורה G מסדר p^n (כלשהו).

תרגיל

תהא G חבורת p, ו- $H\trianglelefteq G$, $p=|H|$. הוכח כי $H\subseteq Z(G)$.

פתרון

$p=|H|$, ולכן ציקלית: $H=\langle a\rangle$.

כמו כן $H\trianglelefteq G$ ולכן $gHg^{-1}=H$, כלומר לכל $g\in G$: $gag^{-1}=a^i$

לכל $a\in H$ אזי כל הצמודים של a נמצאים ב-H אז

כלומר יש ל-a לכל היותר $p-1$ צמודים.

כלומר $|conj(a)| \le p-1$
וגם הוא אמור לחלק את סדר החבורה, ולכן $|conj(a)|=1$
וזה מתקיים אמ"ם $a \in Z(G)$.
$a \in Z(G)$ ולכן מקבלים חבורה ציקלית $H \le Z(G)$.

<u>המרכז של חבורת p</u>

G פועלת על עצמה ע"י הצמדה:

$$G = \dot{\bigcup_{i=1}^{n}} conj(x_i)$$

כאשר $x_1, \dots, x_n$ נציגים של מחלקות הצמידות.

$$|G| = \sum_{i=1}^{n} |conj(x_i)| = |Z(G)| + \sum_{i=m} |conj(x_i)|$$

[illegible]

נקבל משוואת המחלקות:

$$|G| = |Z(G)| + \sum_{i=1}^{m} |conj(x_i)|$$

ובכן תהי G חבורת p, נראה $|Z(G)| \neq 1$
והרי $e \in Z(G)$, לכן $|Z(G)| \ge 1$. נניח בשלילה $|Z(G)| = 1$

$$p^n - 1 = \sum |conj(x_i)|$$

סכום של מספרים שמתחלקים ב-p, לא מתחלק ב-p

סתירה, לכן $|Z(G)| > 1$ כלומר המרכז אינו טריוויאלי!!

תרגיל

כל חבורה מסדר p^2 אבלית

פתרון

$|Z(G)| \mid |G|$, וכמו כן זו חבורת p ולכן $|Z(G)| \in \{p, p^2\}$
אם המרכז מסדר p^2 סיימנו.
נניח שהמרכז מסדר p, אזי נקבל ש- $|G/Z(G)| = p$
ונקבל שזו ציקלית, בסתירה לכך שהוכחנו שתמיד $G/Z(G)$:
אינה ציקלית (בסתירה למקרה היחיד שבו $G/Z(G)$
ציקלית זה אם מסדרה 1).

משפט: תהי G חבורה לא אבלית אזי $G/Z(G)$ אינה ציקלית.

דוגמה

מיין את החבורות מסדר 9.

ובכן, $9=3^2$ ולכן החבורה חייבת להיות אבלית

נמיין יסודית אבליות: $\mathbb{Z}_9, \mathbb{Z}_3^2$.

הגדרה

המרכז הוא $C_a=\{g\in G \mid gag^{-1}=a\}\le G$

תרגיל

תהי G חבורה לא אבלית מסדר p^3. נניח ש-$a\notin Z(G)$.

הוכח $p=|Z(G)|$, $|C_a|=p^2$, $|conj(a)|=p$.

פתרון

$|Z(G)|\in\{1,p,p^2,p^3\}$ ולכן $|Z(G)|=p$.

כעת $a\in C_a$ ולכן C_a בפרט ריקה.

$|C_a|\in\{1,p,p^2,p^3\}$ ולכן $|C_a|=p^2$.

(כי יש שני איברים: $Z(G)\cup\{a\}\subseteq C_a$)

כעת $p=\frac{|G|}{|C_a|}=[G:Stab(a)]=|conj(a)|$ כנדרש!!

דוגמה

$$\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix} \;\middle|\; a,b,c\in\mathbb{Z}_5\right\}\to G,\quad |G|=5^3$$ ולכן $|Z(G)|=5$.

משפט קושי

תהי G חבורה סופית ויהי p ראשוני כך ש-$p\mid |G|$. אזי יש ב-G איבר מסדר p.

הערה

קיימות 5 חבורות מסדר 2^3, באבליות: $\mathbb{Z}_8, \mathbb{Z}_2^3, \mathbb{Z}_4\times\mathbb{Z}_2$

הלא אבליות ...

משפטי סילו

הגדרה
תהא G חבורה, $|G|=p^m m$ כאשר $p \nmid m$.
ת"ח $H \le G$ תקרא ת"ח p סילו של G אם
סדר אותו הוא $p^m=|H|$.

דוגמה
נתבונן ב- S_3, $|S_3|=2\cdot 3$.
יש ת"ח 2-סילו: $\langle(1\ 2)\rangle, \langle(1\ 3)\rangle, \langle(2\ 3)\rangle$
יש ת"ח 3-סילו: $\langle(1\ 2\ 3)\rangle$

משפט סילו 1
תהא G חבורה סופית כך ש- $p \mid |G|$. אזי יש ל-G ת"ח p-סילו.

מסקנה (קושי)
לכל חבורה סופית, אם $p \mid |G|$ אזי יש ת"ח מסדר p.

הערה
כל חבורת p מוכלת בחבורת p סילו כלשהי

דוגמה $|D_4|=2^3 \Rightarrow$ יש ל-D_4 ת"ח 2-סילו מסדר 8, והיא D_4 בעצמה.
לפי קושי יש ת"ח מסדר 2, ולפי הכלל א' יש ת"ח מסדר 4.

משפט סילו 2
כל חבורות p-סילו צמודות זו לזו.
כלומר אם H_1, H_2 חבורות סילו $\Rightarrow$ $gH_1g^{-1}=H_2$

מסקנה
תת חבורה p-סילו היא נורמלית $\iff$ היא ת"ח p-סילו יחידה.

משפט סילו 3
יהי r_p מספר תתי החבורות p סילו של G סופית, $|G|=p^m m$. אזי
1) $r_p \mid m$
2) $r_p \equiv 1 \pmod p$

מסקנה
חבורת p סילו נורמלית $\Leftrightarrow$ $r_p=1$.

דוגמה

הראה שחבורה מסדר 45 אינה פשוטה.

פתרון

$$45 = 3^2 \cdot 5$$

נסמן n_5 חבורות 5-סילו:

n_5 אמור לקיים $n_5 = 1 \pmod 5 \wedge n_5 | 9$

לכן נקבל $n_5 = 1$ ולכן חבורת ה-5 סילו יחידה

לכן יש ת"ח נורמלית לא טריוויאלית ולכן החבורה אינה פשוטה.

הערה

חבורות p-סילו מסדרים שונים נחתכות באופן טריוויאלי, כלומר החיתוך הוא $\{e\}$.

תרגיל

תהי G חבורה לא אבלית מסדר 21. כמה ת"ח 7 סילו יש? וכמה ת"ח 3-סילו יש?

פתרון

n_7: $n_7 = 1 \pmod 7 \wedge n_7 | 3 \Rightarrow n_7 = 1$

n_3: $n_3 \equiv 1 \pmod 3 \wedge n_3 | 7$ לכן $n_3 \in \{1, 7\}$

נבדוק ספירת איברים:

סדר	כמה כאלה יש בחבורה
1	1 היחידה
3	14
7	6 מאחר וה-7 סילו יחידה, G 7-סילו ציקלית,
21	0 כי אינה ציקלית

אם $n_3 = 1$ היינו מקבלים סה"כ רק שני איברים מסדר 3 בספירה, לכן $n_3 = 7$.

[illegible]

הערה

ניתן לראות שגם תחת נתוני $|G|=pq$, $p>q$ ראשוניים, $p\not\equiv 1 \pmod q$ היא ציקלית.

הוכחה

$$r_p \equiv 1 \pmod p \;\wedge\; r_p \mid q$$
$$\Downarrow$$
$$r_p=1$$

ולכן יש חבורה p סילו יחידה.

באותו אופן $r_q=1 \Rightarrow$ יש תת"ח q סילו יחידה.

נספור איברים:

סדר	כמות
1	1
p	$p-1$
q	$q-1$
pq	

שאר האיברים: לא ייתכן שזה אפס, כי אחרת $pq=1+(p-1)+(q-1)$ בסתירה לכך ש[illegible] רק [illegible].

לכן יש איבר מסדר pq והיא ציקלית.

תרגיל

הראה שלא קיימת חבורה פשוטה מסדר $132=2^2\cdot3\cdot11$.

פתרון

צריך ש: $r_2\neq1$ וגם $r_3\neq1$ וגם $r_{11}\neq1$

r_{11}: $r_{11}\equiv1 \pmod{11}$ $\wedge$ $r_{11}\mid 12$. $r_{11}\in\{1,12\}$.

אם $r_{11}=1$ סיימנו. אחרת נניח $r_{11}=12$ ונספור איברים.

נגלה כמה איברים יש לנו עד כה?

$1+12\cdot10=121$

כעת נעבור ל-r_3: $r_3\equiv1 \pmod 3$ $\wedge$ $r_3\mid44$

$r_3\in\{1,4,22\}$

אם $r_3=1$ סיימנו. נניח $r_3=4$ ונקבל שכבר יש 129 איברים בחבורה.

עבור r_3: $r_2 \equiv 1 \pmod 2 \wedge r_2 | 33 \Rightarrow r_2 \in \{1,3,11,33\}$

אם $r_3=1$ סיימנו.

אחרת $r_3=3$. חבורת 2-סילו היא מסדר 4. אבל (נתון) עו
רק שלושה איברים לחלק לכן ניתן למנות 3 חבורות שונות
מסדר 11 משלושה איברים שונים. סתירה.

לכן $r_{11}=1$ כנדרש!!

משפט

תהא G חבורה מסדר q^2p, עבור q,p ראשוניים. חבורה כזו
אינה פשוטה.

הוכחה

נרצה להראות $r_q=1$ או $r_p=1$

עבור r_p: $r_p | q \Rightarrow r_p \in \{1,q\}$

עבור r_q: $r_q | p^2 \Rightarrow r_q \in \{1,p,p^2\}$

נניח בשלילה ש- $r_p=q$ ו- $r_q \in \{p,p^2\}$

כמה איברים מסדר q יש? $r_q(q-1)$

נניח ראשית ש- $r_q=p^2$ אזי יש $p^2(q-1)=p^2q-p^2$ איברים
מסדר q. כלומר נותרו לנו מספיק איברים ליצור רק חבורת
p סילו אחת, בסתירה להנחה ש $r_p \neq 1$.

לכן צריך ש- $r_q=p$, אבל יש בעיה כאן כי $r_q=p \wedge r_p=q$
כי אומר שמתקיים ש- $q \equiv 1 \pmod p$
$p \equiv 1 \pmod q$
בסתירה לראשוניות של q,p.

לכן $r_p=1$ או $r_q=1$ ובכל מקרה החבורה אינה
פשוטה.

תרגיל

תהא G חבורה סופית ותהא $K \trianglelefteq G$ תת"ח.
תהא H תת"ח p סילו של K. הוכח שקיימת תת"ח p סילו $\underline{P}$ של G כך ש- $K \cap P = H$.

הוכחה

$|K| = p^t m$, ולכן $|H| = p^t$ (כי H p סילו של K).
H היא חבורת p של G.
לכן קיימת תת"ח p-סילו $\underline{P}$ של G כך ש- $\underline{P} \ge H$.
קיבלנו ש- $H \le \underline{P}$, ונרצה להראות $K \cap P = H$.
$\underline{P} \ge K \cap \underline{P}$. נסמן $|\underline{P}| = p^s$, אזי $|K \cap \underline{P}| \,\big|\, p^s$
ולכן $|K \cap \underline{P}| = p^a$, $a \le s$. צ"ל ש- $t = a$,
כי אזי $K \cap \underline{P} = H$.
$H \le K \cap \underline{P}$ ולכן $t \le a$. נותר להראות ש- $a \le t$.

$K \cap \underline{P} \le K$

$|K \cap \underline{P}| \,\big|\, |K|$

$p^a \,|\, p^t m$

$\Rightarrow a \le t$

לכן $t = a$ כנדרש.

משפט

תהא G חבורה מסדר $2p$, p ראשוני. אזי
$G \cong D_p$ או $G \cong \mathbb{Z}_{2p}$

הוכחה

$|G| = 2p \Rightarrow r_2 \equiv 1 \pmod 2 \wedge r_2 \,|\, p$

$r_p \,|\, 2 \wedge r_p \equiv 1 \pmod p \Rightarrow \boxed{r_p = 1}$

נסמן $K = \langle a \rangle = \{1, a, \dots, a^{p-1}\}$

$r_2 = 1$! יש תת"ח נורמלית מסדר 2 ונסמן $H = \{1, b\}$

ומתקיים $o(ab) = 2p$

לכן G ציקלית $G \cong \mathbb{Z}_{2p}$.

אם $r_2=p$ יש לנו p חבורות 2-סילו נורמליות מסדר 2.

נניח אחת מהן ב-H

$o(ab)\in\{1,2,p,2p\}$

$ab=e$ — סתירה

$2p \to G\cong \mathbb{Z}_{2p}$

כעת אם $p=o(ab)$ בסתירה שיש תת נורמלית יחידה מסדר

כעת אם נקבל $2=o(ab)$:

$abab=e$

$$\begin{cases} bab=a^{-1} \\ a^p=b^2=e \end{cases}$$ ולכן זו החבורה הדיהדרלית

תרגיל

תהא H תת חבורה של G. הוכיחו שזו היא תת החבורה ... יחידה של $N(H)$.

תרגיל

תהא G חבורה מסדר 30. הוכיחו שאינה פשוטה.

פתרון $30=2\cdot3\cdot5$

נבחר r_2: $r_2\equiv1 \pmod 2$ ו-$r_2|15$

$r_2\in\{1,3,5,15\}$

r_5: $r_5\equiv1 \pmod 5$ ו-$r_5|6$

$r_5\in\{1,6\}$

r_3: $r_3\in\{1,10\}$

ראשית אם $r_3=1$ סיימנו.

אחרת $r_3=10$: משפט איברים יש לנו כעת 21 איברים. כעת אם $r_5=1$ סיימנו, אחרת $r_5=6$, G חבורה מעל 4 איברים, בסה"כ [illegible] איברים.

סדרות נורמליות וסדרות הרכב

הגדרה

תהי G חבורה. סדרה של ת"ח

$$G=G_0 \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq \{e_G\}$$

תקרא סדרה נורמלית של G.

עידון של סדרה $G \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq \{e_G\}$ היא

$$G \trianglerighteq G_1 \trianglerighteq \ldots \trianglerighteq G_i \trianglerighteq \ldots \trianglerighteq G_{i+1} \trianglerighteq \ldots \trianglerighteq \{e_G\}$$

הגורמים של הסדרה הם החבורות המנה G_i/G_{i+1}.

עידון ממש הוא עידון שבו כל הגורמים נבחרים לא טריוויאליים כלומר $\{e\} \neq G_i/G_{i+1}$.

דוגמה

1) לכל חבורה G יש סדרה נורמלית $G \trianglerighteq \{e_G\}$

2) נתבונן על הסדרה הנורמלית הבאה של S_3

$$S_3 \trianglerighteq A_3 \trianglerighteq \{e\}$$

זה עידון של הסדרה מ-1.

הגורמים של הסדרה: $A_3/\{e\} \cong \mathbb{Z}_3$ $\quad S_3/A_3 \cong \mathbb{Z}_2$

הגדרה

סדרת הרכב היא סדרה נורמלית שאין לה עידונים ממש

משפט

סדרה נורמלית היא סדרת הרכב אמ"מ כל הגורמים שלה פשוטים

מסקנה

מכיוון שאנו יודעים שחבורה אבלית כלשהי G היא פשוטה אמ"מ סדרה ראשוני, אם מופיע גורם אבלי מסדר לא ראשוני אזי בהכרח זו לא סדרת הרכב.

דוגמאות

1) $G=\mathbb{Z}_2\times\mathbb{Z}_4$

$G \trianglerighteq \mathbb{Z}_2\times\{0,2\} \trianglerighteq \mathbb{Z}_2\times\{0\} \trianglerighteq \{0\}\times\{0\} = e_G$

$\mathbb{Z}_2$ גורמי $\mathbb{Z}_2$ גורמי $\mathbb{Z}_2$ גורמי

לכן זו סדרת הרכב

2) עבור $n\geq 5$: $S_n \trianglerighteq A_n \trianglerighteq \{id\}$ סדרת הרכב

כי $A_n/\{id\} \cong A_n$ פשוטה עבור $n\geq5$, $S_n/A_n \cong \mathbb{Z}_2$ (פשוטה)

3) $S_4 \trianglerighteq A_4 \trianglerighteq K_4 \trianglerighteq \{1, (12)(34)\} \trianglerighteq \{id\}$

גורמים: $\mathbb{Z}_2$ $\mathbb{Z}_3$ $\mathbb{Z}_2$ $\mathbb{Z}_2$

4) דוגמה של סדרות נורמליות של D_4

$D_4 \trianglerighteq \langle\sigma^2\rangle \trianglerighteq \{id\}$

[illegible]

גורמים: $\mathbb{Z}_2^2$ $\mathbb{Z}_2$

לכן לפי הגדרה זו לא סדרת הרכב. כי היא אינה עדינה מקסימלית.

$D_4 \trianglerighteq \langle\sigma\rangle \trianglerighteq \langle\sigma^2\rangle \trianglerighteq \{id\}$

לעומת זאת זו סדרת הרכב

סדרת הרכב נוספת היא

$D_4 \trianglerighteq \langle\tau,\sigma^2\rangle \trianglerighteq \langle\tau\rangle \trianglerighteq \{id\}$

עם כאלה הגורמים פשוטים.

5) $D_{15} \trianglerighteq \langle\sigma\rangle \trianglerighteq \langle\sigma^3\rangle \trianglerighteq \{id\}$

$\mathbb{Z}_2$ $\mathbb{Z}_3$ $\mathbb{Z}_3$

גורמים

שתי סדרות הרכב

$D_{15} \trianglerighteq \langle\sigma\rangle \trianglerighteq \langle\sigma^5\rangle \trianglerighteq \{id\}$

$\mathbb{Z}_2$ $\mathbb{Z}_3$ $\mathbb{Z}_5$

הערה

סדרת הרכב היא לא בהכרח יחידה אבל לכל שתי סדרות הרכב של G, יש אותם גורמים.

ט) נמצא סדרת הרכב ל-$\mathbb{Z}/p^k\mathbb{Z}$ (p ראשוני) כך שכל הגורמים איזומורפיים ל-$\mathbb{Z}_p$.

ראשית נשים לב ש $p^m\mathbb{Z}/p^{m+1}\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$ לכל m.

כמו כן $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z}$.

לפי החבורה שלנו הג"ח הן גם המנה $\mathbb{Z}/p^k\mathbb{Z}$.

לכן נקח את סדרת ההרכב

$$\{0\} \trianglelefteq p^{k-1}\mathbb{Z}/p^k\mathbb{Z} \trianglelefteq \dots \trianglelefteq p^2\mathbb{Z}/p^k\mathbb{Z} \trianglelefteq p\mathbb{Z}/p^k\mathbb{Z} \trianglelefteq \mathbb{Z}/p^k\mathbb{Z}$$

הגורמים פשוטים לפי משפט (?) המתאימים בסדרה

הגדרה: תהי G חבורה נאמר כי G פתירה אם יש ל-G סדרה נורמלית שכל גורמיה אבליים.

דוגמאות,

1) כל חבורה אבלית G היא פתירה: $\{e\} \trianglelefteq G$

$G/\{e\} \cong G$ אבלי

2) D_n הן פתירות:

$D_n \trianglerighteq C_n \trianglerighteq \{id\}$

$D_n/C_n \cong \mathbb{Z}_2$ אבלי

$C_n/\{e\} \cong C_n \cong \mathbb{Z}_n$ אבלי

3) עבור $n \geq 5$, A_n, S_n לא פתירות

A_n לא פתירה כי היא פשוטה.

S_n כי אי אפשר לקחת את $\{id\} \trianglelefteq A_n \trianglelefteq S_n$ ולהגיע כאלו

$A_n/\{id\} \cong A_n$ אינה אבלית.

תרגיל

הראו שהחבורה $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \middle| a,b,c \in \mathbb{Z}_p \right\}$ פתירה

פתרון

G לא אבלית ולכן $\{e\} \trianglelefteq G$ לא מתאימה.

נשים לב $\{e\} \trianglelefteq Z(G) \trianglelefteq G$ היא סדרה מתאימה, שכן

$|G| = p^3$, $|Z(G)| = p \Rightarrow |G/Z(G)| = p^2$ וכל חבורה מסדר p^2 אבלית

כמו כן $Z(G)/\{e\} \cong Z(G)$ שהיא בוודאי אבלית.

משפט
כל חבורת-p היא פתירה.

תרגיל
תהי G חבורה מסדר pq עבור p,q ראשוניים. הראו שG פתירה.

פתרון
אם $q=p$ אז $|G|=p^2$ ולכן G אבלית ולכן פתירה.
אחרת $q\neq p$ אז $r_p\equiv 1 \pmod{p}$, $r_p | q$
$r_q\equiv 1 \pmod{q}$, $r_q | p$
אם $q<p$ אז $r_p=1$ כלומר $\exists!$ p-סילו של G
היא נורמלית $\{e\} \trianglelefteq P \trianglelefteq G$ ולכן פתירה.
$\downarrow \quad \downarrow$
$\mathbb{Z}_q \quad \mathbb{Z}_p$
עבור $p>q$ באותו אופן

תרגיל
תנו דוגמה ל:

	פתרון
א. חבורה פשוטה פתירה	$\mathbb{Z}_p$, p ראשוני
ב. חבורה פשוטה לא פתירה	A_n עבור $n\geq 5$
ג. חבורה לא פשוטה פתירה	D_n (או כל חבורה מסדר pq)
ד. חבורה לא פשוטה לא פתירה	S_n עבור $n\geq 5$

תרגיל
(p,q ראשוניים)
תהי G חבורה מסדר p^2q. הראו שG פתירה.

פתרון
בתרגול שעבר ראינו שבG יש p-סילו נורמלית או יש q-סילו נורמלית. אם $r_q=1$ נבחר הסדרה:
$\{e\} \trianglelefteq Q \trianglelefteq G$
$|Q/\{e\}|=q$ ← ציקלית ← אבלית
$|G/Q|=p^2$ ← אבלית

עבור $r_p=1$ באותו אופן.

תרגיל

תהי G חבורה מסדר 34. הראו כי היא פתירה.

פתרון

$|G|=2\cdot 17$, וראינו שכל חבורה מסדר $2p$ איזומורפית ל- $\mathbb{Z}_{2p}$ או ל- D_p ושתיהן פתירות.

תרגיל

הוכח כי כל חבורה G מסדר 1089 היא פתירה

פתרון

$|G|=3^2\cdot 11^2$, כמו כן $r_3 | 11^2$, $r_3 \equiv 1 \pmod 3$,

$r_{11} | 3^2$, $r_{11} \equiv 1 \pmod{11} \Rightarrow r_{11}=1$

לכן ת"ח 11 סילו היא נורמלית, נסמנה ב-N. אזי:

$$G \trianglerighteq N \trianglerighteq \{e\}$$

$|G/N|=3^2$ ולכן אבלי

$|N/\{e\}|=11^2$ לכן אבלי

הגדרה

תהי G חבורה, ויהיו $a,b\in G$. הקומוטטור של a,b, מסומן ב- $[a,b]$ ומוגדר כ- $[a,b]=a^{-1}b^{-1}ab$.

תת חבורת הקומוטטור היא $G'=\langle [a,b] \mid a,b\in G\rangle$

משפט

G אבלית אמ"ם $G'=\{e\}$

הערה

$[a,b]^{-1}=[b,a]$

תרגיל

תהי G חבורה פשוטה שאינה אבלית. הראה כי $G'=G$.

פתרון

$G' \trianglelefteq G$ לפי משפט קודם, G לא אבלית לכן $G'\neq\{e\}$ ובגלל G פשוטה לכן $G'=G$

בנוסף

נראה ש- D_3 פתירה מאוצעות המושג:

$D_3' = \langle \sigma \rangle \underset{\text{אבלי}}{\cong} \mathbb{Z}_3 \Rightarrow \langle \sigma \rangle' = \{id\}$

כנדרש

תרגיל

הוכח או הפרך: כל חבורה מסדר 60 היא פתירה.

פתרון

A_5 אינה פתירה! לכל $n \geq 5$ $A_n = A_n'$ ולכן לא פתירה.

תרגיל

תהי G חבורה [illegible] מסדר 28. הוכח:

א) קיימת ת"ח 7 סילו נורמלית.

ב) אם G לא אבלית אז $7 = |G'|$.

ג) אם G לא אבלית ויש לה ת"ח נורמלית מסדר 2 אז $G/Z(G) \cong D_7$.

פתרון

א) $|G| = 2^2 \cdot 7$. לפי סילו 3

$r_7 = 1 \pmod 7$ וגם $r_7 \mid 4$, $r_7 \equiv 1$ ולכן $r_7 = 1$

לכן התת"ח הנ"ל נורמלית. נסמנה ב- Q.

ב) $Q \trianglelefteq G$, $|G/Q| = 4 = 2^2$ ולכן G/Q לא אבלית ולכן

$G' \neq \{e\}$. נסמן מכיוון ש- Q מסדר ראשוני (קבוצה)

$G' = Q$ ולכן $|G'| = 7$

$|Z(G)| \in \{1, 2, 4, 7, 14\}$ (לא אבלית)

$|G/Z(G)| = 4$ לכן אבלית לכן $G' \leq Z(G)$ אבל $|G'| = 7$ לכן $G' = Z(G)$

אם יש תת"ח נורמלית מסדר 2 [illegible]

2 נורמליות ומצבי 2 לכן $1 \neq Z(G)$

כי אז היינו מקבלים

ש- $|G/Z(G)|$ ראשוני בסתירה. אבל לכן נשלם.

לכן צריך בסתירה

כמו כן אם $|Z(G)| = 2$ [illegible]

לכן $Z(G)$ בסתירה כי יתקיים

לא מתקיים

ג) $|Z(G)| = 2$ ולכן $|G/Z(G)| = 14$, $G/Z(G)$ לא ציקלית ולכן

$G/Z(G) \cong D_7$ כנדרש

תרגיל

עבור $\mathbb{F}$ שדה הראו כי

$$G=\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}\;\middle|\; a,b,c\in\mathbb{F}\right\}$$ פתירה.

פתרון

כל שדה סופי הוא מסדר p^n (ח ראשוני) לכן

$$|G|=(p^n)^3=p^{3n}$$

כלומר G חבורת p ולכן פתירה.

אם $\mathbb{F}$ אינסופי, נסמן $(a,b,c)=\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}$

ונסמן כפל מטריצות ב-$*$, אזי:

$$(a,b,c)*(d,e,f)=(a+d,\ e+b+af,\ c+f)$$

והיחידה הוא $(0,0,0)$, ו- $(a,b,c)^{-1}=(-a,ac-b,-c)$

$$[(a,b,c),(d,e,f)]=(a,b,c)*(d,e,f)*(-a,ac-b,-c)*(-d,df-e,-f)=$$
$$=(0,\ ,0)$$

ולכן $A=\left\{\begin{pmatrix}1&0&b\\0&1&0\\0&0&1\end{pmatrix}\;\middle|\; b\in\mathbb{F}\right\}\geq G'$. A אבלית, ולכן G' אבלית,

ולכן $\{id\}=G''$, לכן $A'=G'$.

כאמור $G''=\{id\}$ ולכן G פתירה.