אלגברה מופשטת 1

חוברת מערכי תרגול

עורך: סולי וישקאוצן

חוברת מערכי התרגול מבוססת על התרגולים של: מיקי פייר, מיכאל פרידמן וסולי וישקאוצן

תוכן העניינים

תרגול 1 אלגוריתם החלוקה של אוקלידס, חבורות ולא חבורות, טבלאות כפל, תרגילי הוכחה 2

תרגול 2 14

תרגול 3 21

תרגול 4 28

תרגול 5 36

תרגול 6 46

תרגול 7 55

תרגול 8 65

תרגול 9 71

תרגול 10 77

תרגול 11 85

תרגול 12 92

תרגול 13 100

תרגול 1: אלגוריתם החלוקה של אוקלידס, חבורות ולא חבורות, טבלאות כפל, תרגילי הוכחה

משפט אוקלידס - חלוקה עם שארית:

בהנתן שני מספרים $a,b\in\mathbb{Z}$ כך ש $b\neq 0$, ניתן לחלק את a ב b עם שארית: כלומר קיימים $r,q\in\mathbb{Z}$ כך ש $0\le r<|b|$ ומתקיים $a=qb+r$. המספר r נקרא **השארית** (remainder) של החלוקה, והמספר q הוא **המנה** (quotient) של החלוקה.

דוגמאות: $7=3\times 2+1$ (מנה 3, שארית 1). $7=(-3)\times(-2)+1$ (מנה -3 שארית 1).

תרגיל בית: הראו ש q,r נקבעים ביחידות.

הגדרה: יהיו $a,b\in\mathbb{Z}$. נאמר ש b **מחלק** את a אם קיים $c\in\mathbb{Z}$ כך ש $a=bc$. כלומר b מחלק את a ללא שארית.

הגדרה: בהנתן שני מספרים $0\neq a,b\in\mathbb{Z}$ נגדיר את **המחלק המשותף הגדול ביותר**(הממג"ב) שלהם להיות המספר השלם הגדול ביותר שמחלק את שניהם. נסמן ע"י $\gcd(a,b)$ או (a,b).
$\gcd=$ greatest common divisor .

הגדרה: בהנתן שני מספרים $a,b\in\mathbb{Z}$ שאינם שניהם 0, נגדיר את **הכפולה המשותפת הקטנה ביותר** (הכמקק"ב) שלהם להיות המספר **הטבעי** הקטן ביותר שמתחלק בשניהם.
נסמן ע"י $lcm(a,b)$. $lcm=$ least common multiple .

הערה: לשם הנוחיות נגדיר בצורה דומה **כפולה משותפת** ו**מחלק משותף** (כלומר לא בהכרח הגדולים ביותר או הקטנים ביותר).

דוגמא:

$$\gcd(6,4)=2,\ \gcd(6,12)=6,\ lcm(2,3)=6,\ lcm(2,4)=4$$

<u>הגדרה</u>: נאמר ש $a,b\in\mathbb{Z}$ הם **זרים** אם $\gcd(a,b)=1$.

<u>משפט (נקרא למשפט זה משפט ה- gcd):</u> בהנתן שני מספרים $0\neq a,b\in\mathbb{Z}$ קיימים מספרים $u,v\in\mathbb{Z}$ כך ש $au+bv=\gcd(a,b)$.

<u>הערה:</u> במערכי התרגול נסמן משפטים חשובים או כאלה שמשתמשים בהם בהמשך הקורס במסגרת אדומה.

<u>דוגמא:</u>

למשל, gcd(234,61)=1 (כי 61 הוא מספר ראשוני) וניתן לחשב ש-

61·(-23) + 6·234 = 1. נראה בהמשך איך מוצאים את המקדמים 23-, 6.

<u>הוכחת בניה של משפט ה gcd:</u>

נזכר באלגוריתם החלוקה של אויקלידס: בהנתן שני שלמים a,b , נבצע סדרה של חלוקות עם שארית:

$$
\begin{aligned}
a &= bq_1 + r_1\\
b &= r_1q_2 + r_2\\
r_1 &= r_2q_3 + r_3\\
&\vdots\\
r_{k-1} &= r_kq_{k+1} + r_{k+1}\\
r_k &= r_{k+1}q_{k+2}
\end{aligned}
$$

(תרגיל בית: הסבירו מדוע סדרת החלוקות חייבת להסתיים בכך שהשארית האחרונה r_{k+2} היא 0.)

כעת נראה ש $r_{k+1}=\gcd(a,b)$.

הוכיחו באינדוקציה את הטענה הבאה:

$$\gcd(a,b)=\gcd(b,r_1)=\gcd(r_1,r_2)=...=\gcd(r_k,r_{k+1})=r_{k+1}$$

(נראה את השלב הראשון: נסמן $d:=\gcd(a,b)$. אזי

$d\,|\,a,b\Rightarrow d\,|\,r_1\Rightarrow d\,|\,b,r_1\Rightarrow d\leq\gcd(b,r_1)$. הכיוון השני דומה).

כעת ניתן להוכיח באינדוקציה (הפוכה) שניתן להציג את r_{k+1} כצירוף לינארי של r_k, r_{k-1}, כולל כצירוף לינארי של a,b.

<u>דוגמא:</u> נפעיל את אלגוריתם הבניה עבור הדוגמא: gcd(234,61)=1.

$234 = 61\times 3 + 51$

$61 = 51\times 1 + 10$

$51 = 10\times 5 + 1$

$10 = 1\times 10$

ואז נקבל:

$\gcd(234,61) = \gcd(61,51) = \gcd(51,10) = \gcd(5,1) = 1$.

את הצירוף הלינארי המתאים נקבל כמו בהוכחה ע"י הצגת כל שארית כצירוף אלגברי מתאים של השאריות הקודמות:

$$1 = 51 - 10\times 5$$
$$10 = 61 - 51\times 1$$
$$51 = 234 - 61\times 3$$
$$\Rightarrow$$
$$1 = 51 - 10\times 5 = (234 - 61\times 3) - (61 - 51\times 1)\times 5 = (234 - 61\times 3) - (61 - (234 - 61\times 3)\times 1)\times 5 =$$
$$= 6\times 234 + (-23)\times 61$$

<u>הוכחת קיום של משפט ה gcd</u>: נסמן ב- S את קבוצת כל הצירופים הלינאריים החיוביים של a ו- b (שאלה: מדוע ה gcd תמיד חיובי?):

S = {au + bv | au + bv > 0, u,v ∈ Z}

נשים לב ש- S אינה ריקה (למה?), ומכיוון שזו קבוצה של מספרים אי–שליליים, קיים איבר קטן ביותר d>0. מהגדרת S קיימים y,x כך ש- d = ax + by. נראה ש- d = gcd(a,b), ז"א – d מחלק משותף מקסימלי של a ו- b.

ע"פ משפט החילוק ניתן למצוא מספרים שלמים q,r כך ש- a = qd+r, 0 ≤ r < d. למעשה:

r = a-qd = a-q(ax+by) = a(1-qx) + b(-qy)

נניח בשלילה ש- r שונה מ-0: נקבל ש- r היה איבר של S (כצירוף לינארי של a ו- b); בסתירה לכך ש- d הוא האיבר מינימלי ב- S (כי r < d). לכן r = 0 ולכן a = qd. כלומר d | a. באותו אופן מראים ש-

b | d, ולכן d מחלק משותף של a ו- b. נשאר להוכיח שהוא המחלק המשותף המקסימלי.

אם c מחלק משותף כלשהו של a ו- b , אז c | (ax+by) ולכן c | d. נובע מכך ש- c ≤ d ולכן d גדול מכל מחלק משותף חיובי של a ו- b. מהגדרת gcd מקבלים ש- d = (a,b) .

נשים לב שקיבלנו ש- d הוא האיבר המינימלי ב- S. □

<u>תרגיל בית: (טענות נוספות על gcd,lcm)</u>

1. אם c מחלק משותף של $a,b\in\mathbb{Z}$ אזי c מחלק את $\gcd(a,b)$ (נובע ישירות מלמת בזו).
2. אם c מתחלק ב $a,b\in\mathbb{Z}$ אזי c מתחלק ב $lcm(a,b)$.
3. אם $a=\prod_{i=1}^{m} p_i^{\alpha_i}, b=\prod_{i=1}^{m} p_i^{\beta_i}$ הם הפירוקים לגורמים ראשוניים, אזי $\gcd(a,b)=\prod_{i=1}^{m} p_i^{\min(\alpha_i,\beta_i)}, lcm(a,b)=\prod_{i=1}^{m} p_i^{\max(\alpha_i,\beta_i)}$.
4. $lcm(a,b)=\frac{ab}{\gcd(a,b)}$.
5. $\gcd(\frac{a}{\gcd(a,b)},\frac{b}{\gcd(a,b)})=1$.
6. אם $a\mid bc$ וגם $\gcd(a,b)=1$ אזי $a\mid c$.

<u>הגדרה:</u> חבורה היא קבוצה G עם פעולה בינארית $\otimes$: $G\otimes G\to G$

המקיימת את 4 האקסיומות הבאות:

1) **סגירות** (קשירות):

$$\forall a,b\in G \qquad a\otimes b\in G$$

כלומר אם לוקחים שני איברים ומפעילים עליהם את פעולת הכפל הנ"ל אז התוצאה היא איבר בקבוצה (למעשה זה נובע ישירות מ *).

2) **אסוציאטיביות** (קיבוציות):

$$\forall a,b,c\in G \qquad (a\otimes b)\otimes c=a\otimes(b\otimes c)$$

כלומר עם הכללה באינדוקציה אנו יכולים לומר שסדר השמת הסוגרים עבור מספר איברים סופי אינו משנה.

3) **קיום איבר יחידה** $e\in G$ כך ש: $\forall a\in G\ e\otimes a=a\otimes e=a$

4) **קיום הופכי**: $\forall a\in G\ \exists b\in G\ a\otimes b=b\otimes a=e$

אם בנוסף לארבעת האחרונים מתקיים:

5) **חילופיות**:

$$\forall a,b\in G \qquad a\otimes b=b\otimes a$$

אז החבורה נקראת חבורה **חילופית או אבלית** (או **קומוטטיבית**).

אם מתקיים רק 1-3 (כלומר לא מובטח קיום הפכי) אז נקרא לקבוצה **מונואיד**. אם מתקיים 1-2 (כלומר לא מובטח קיום איבר יחידה) אזי נקרא לקבוצה **אגודה** (semigroup).

<u>הערה:</u> לעתים רבות נשמיט את סימן פעולת החבורה, ונרשום ישירות ab במקום $a\otimes b$. לעיתים גם משתמשים בסימון $a\cdot b$ אם רוצים להפריד בין האותיות.

<u>הערה:</u> כאשר מתייחסים לחבורה, מקובל לכתוב $(G,\otimes,e)$ כדי לציין את הקבוצה, הפעולה, ואיבר היחידה.

<u>דוגמאות:</u> נבחן מספר דוגמאות של קבוצות ופעולות בינאריות עליהן, ונבחן האם מתקיימות האקסיומות 1-5 עבורן.

1) $S=(\mathbb{N},*)$ כאשר הפעולה * מוגדרת ע"י $a*b=b^a$.

סגירות: כיוון ש $a\in\mathbb{N}$ אזי $b^a=bb\cdots b\in\mathbb{N}$.

a פעמים

הפעולה אינה אסוציאטיבית: $2*(3*2)=(2^3)^2=64\neq 512=2^{(3^2)}=(2*3)*2$.

האם יש ב S איבר יחידה? נניח בשלילה ש $e\in S$ הוא איבר יחידה. אזי

$$1=1^e=e*1=1*e=e^1=e$$

אבל 1 אינה יחידה כיוון ש

$$1*2=2^1=2\neq 1=1^2=2*1$$

1 היא **יחידה שמאלית** (כלומר לכל איבר $a\in\mathbb{N}$ מתקיים $a*1=a$.

כיוון שאין איבר יחידה, אין מה לבדוק את האקסיומה של קיום איבר הפכי.

2) תהי X קבוצה. אזי $(P(X),\cup)$ היא מונואיד אבלי, כאשר $\varnothing$ היא היחידה, בקורס "מתמטיקה בדידה" ראינו סגירות, אסוציאטיביות וקומוטטיביות. P(X) אינה חבורה, כי אין איבר הפכי לאף איבר שונה מ $\varnothing$ (אם $A\cup B=\varnothing$ אזי $A=B=\varnothing$). $(P(X),\cap)$ גם היא מונואיד, כאשר X היא היחידה. לכל איבר $a\in P(X)$ בשני המונואידים מתקיים $a^2=aa=\begin{cases}a\cap a=a\\ a\cup a=a\end{cases}$. לאיברים במונואיד המקיימים $a^2=a$ קוראים **אידמפוטנטים**, ויש להם חשיבות רבה. בחבורה האידמפוטנט היחיד הוא איבר היחידה.

3) תהי X קבוצה לא ריקה. אזי $(P(X),\setminus)$ לא מקיימת אסוציאטיביות. כיוון ש $X\neq\varnothing$ נקח $a\in X$, ואת הקבוצה $\{a\}\in P(X)$, אזי $(\{a\}\setminus\varnothing)\setminus\{a\}=\{a\}\setminus\{a\}=\varnothing$ ולעומת זאת, $\{a\}\setminus(\varnothing\setminus\{a\})=\{a\}\setminus\varnothing=\{a\}\neq\varnothing$. האם קיים איבר יחידה? לא. אם קיים איבר יחידה $E\in P(X)$, אזי $\varnothing=\varnothing\setminus E=E\setminus\varnothing=E$, כלומר בהכרח $E=\varnothing$, אבל $\varnothing$ אינו איבר יחידה אם, כיוון ש $\varnothing\setminus X=\varnothing\neq X$. אבל $\varnothing$ יחידה ימנית.

4) נקח את קבוצת הנקודות $C=\{(x,y)\in\mathbb{R}^2 : x^2+y^2=1\}$ (זהו מעגל היחידה). נגדיר פעולה על הנקודות במעגל $(x,y)*(z,w)=(xz-yw,xw+yz)$. נבדוק שהפעולה הזאת אכן מגדירה חבורה, ובנוסף היא חבורה אבלית:

סגירות: צריך להראות שהנקודה $(xz-yw,xw+yz)$ אכן שייכת למעגל.

$$(xz-yw)^2+(xw+yz)^2 = x^2z^2-2xyzw+y^2w^2+x^2w^2+2xyzw+y^2z^2 =$$
$$= x^2z^2+y^2w^2+x^2w^2+y^2z^2 = (x^2+y^2)z^2+(x^2+y^2)w^2 = z^2+w^2 = 1$$

אסוציאטיביות: נקח 3 נקודות על המעגל, $(x,y),(z,w),(s,t)\in C$.

$$\left[(x,y)*(z,w)\right]*(s,t) = (xz-yw,xw+yz)*(s,t) =$$
$$= ((xz-yw)s-(xw+yz)t,(xz-yw)t+(xw+yz)s) =$$
$$= (sxz-syw-txw-tyz,txz-tyw+sxw+syz)$$
$$(x,y)*\left[(z,w)*(s,t)\right] = (x,y)*(sz-tw,tz+sw) =$$
$$= (x(sz-tw)-y(tz+sw),x(tz+sw)+y(sz-tw)) =$$
$$= (sxz-txw-tyz-syw,txz+sxw+syz-tyw)$$

איבר יחידה: $e=(1,0)$.

$$(1,0)*(x,y) = (1\cdot x-0\cdot y,1\cdot y+0\cdot x) = (x,y)$$
$$(x,y)*(1,0) = (x\cdot 1-y\cdot 0,x\cdot 0+y\cdot 1) = (x,y)$$

הפכי: $(x,y)^{-1}=(x,-y)$.

$$(x,y)*(x,-y) = (x^2+y^2,-xy+xy) = (1,0)$$
$$(x,-y)*(x,y) = (x^2+y^2,xy-xy) = (1,0)$$

מי זאת החבורה הזאת: ניתן לראות אותה באופן גיאומטרי כסכום הזויות של הוקטורים $(x,y),(z,w)\in C$, או לחלופין, לזהות את הנקודה (x,y) עם הנקודה $x+iy\in\mathbb{C}$ ואז הפעולה "המסובכת" הנ"ל היא פשוט כפל של מספרים מרוכבים.

<u>**הגדרה:**</u> **סדר** של חבורה הוא העוצמה של הקבוצה של החבורה.

<u>טבלאות כפל:</u>

כל חבורה סופית מוגדרת לחלוטין ע"י טבלת הכפל המתאימה לפעולה הבינארית של החבורה.

נראה כעת דוגמא: נשווה את טבלאות הכפל של החבורה $\mathbb{Z}_4$ (חיבור של המספרים {0,1,2,3} מודולו 4) והחבורה $\mathbb{Z}_2\times\mathbb{Z}_2$ (מכפלה קרטזית של שני עותקים של $\mathbb{Z}_2$) עם הפעולה

$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2)$ (למעשה זה מ"ו ממימד 2 מעל השדה $\mathbb{Z}_2$). חבורה זאת נקראת גם **חבורת קליין**. איבר היחידה הוא (0,0). טבלאות הכפל של שתי החבורות הן:

$\mathbb{Z}_2\times\mathbb{Z}_2$	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

$\mathbb{Z}_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

נשים לב ששתי הטבלאות סימטריות כי החבורות אבליות. שתי החבורות הן שונות! רואים זאת ע"י ההבדל בין האלכסונים. בחבורת קליין כל איבר הפכי לעצמו, וזה לא המצב בחבורה מודולו 4. בחבורות לא אבליות קוראים את הטבלה עמודה*שורה ($row*column$).

נשים לב שכל עמודה וכל שורה בטבלת הכפל היא **תמורה** של האיברים.

<u>תרגיל בית:</u> נסו לבנות טבלת כפל לחבורה כלשהיא מסדר 3, והראו שהיא חייבת להיות אבלית.

<u>טענה:</u> תהי G חבורה אז לכל $a\in G$ קיים איבר הפכי יחיד נסמן אותו ב: a^{-1}.

<u>טענה:</u> תהי G חבורה אז קיים איבר יחידה יחיד ב G נסמן אותו ב: e.

<u>הערה:</u> במונואיד M (ובפרט בחבורה) מתקיים שאם איבר $a\in M$ **הפיך מימין** (כלומר קיים $b\in M$ כך ש $ab=e$), וגם **הפיך משמאל** (כלומר קיים $c\in M$ כך ש $ca=e$) אזי בהכרח a הפיך ומתקיים $b=c=a^{-1}$. מוכיחים זאת ע"י $c=ce=c(ab)=(ca)b=eb=b$.

משתמשים כאן באסוציאטיביות

<u>תרגיל:</u> יהי M מונואיד. הראו שאם $a,b\in M$ הפיכים, אזי ab הפיך.

<u>פתרון:</u> $(ab)^{-1}=b^{-1}a^{-1}$, רואים זאת ע"י $(ab)(b^{-1}a^{-1})=a(bb^{-1})a^{-1}=aea^{-1}=aa^{-1}=e$, ואותו דבר בהכפלה מהכיוון השני. <u>שימו לב:</u> אנחנו השתמשנו כאן באסוציאטיביות של החבורה. ללא אסוציאטיביות, לא היינו יכולים להוכיח תרגיל זה.

<u>הגדרה:</u> יהי $x \in G$ איבר בחבורה, אזי נגדיר **חזקה** של איבר ע"י $x^n := x^{n-1} \otimes x = x \otimes ... \otimes x$.
כאשר $x^1 := x$ ו- $x^0 = e$.

<u>הערה:</u> יהי $a \in G$ איבר בחבורה, אזי $a^{m+n} = a^m a^n$ וגם $\left(a^m\right)^n = a^{mn}$. שימו לב שלא בהכרח מתקיים $\left(ab\right)^n = a^n b^n$, כיוון שלא בהכרח מתקיים $ab = ba$.

<u>כתיב חיבורי לעומת כתיב כפלי</u>

נשים לב שבחבורה בה הפעולה היא "חיבורית" (+) זה פחות נוח להשתמש בסימון כגון x^n , כיוון שלפי הגדרה $x^n = x + x + ... + x$ כאשר הסכום מתבצע n פעמים. הרבה יותר נוח להשתמש בסימון nx , ולכן נביא להלן מילון שבו נחליף את הסימונים המקובלים עבור חבורות בסימנים המקובלים עבור חבורות חיבוריות:

הפעולה	חבורה "כפלית"	חבורה "חיבורית"
כפל בחבורה	ab	$a+b$
איבר יחידה/ניטרלי/אדיש	1 או e	0
איבר הפכי	a^{-1}	$-a$
חזקה של איבר	a^n	na
כפל בהפכי	ab^{-1}	$a-b$

בהמשך הקורס נרחיב את הטבלה הזאת עם עוד מספר פעולות.

<u>הגדרה:</u> נאמר ששני איברים $a, b \in G$ בחבורה **מתחלפים** אם $ab = ba$.

<u>טענה:</u> חבורה G היא חבורה אבלית אם ורק אם כל שני איברים בה מתחלפים.

תרגיל: אם $(G,*)$ חבורה ולכל $x\in G$ מתקיים $x^2=e$ אז G חבורה אבלית.

הוכחה:

$$\forall x,y\in G$$
$$xx=e\to x=x^{-1}$$
$$(xy)^2=e$$
$$xyxy=e$$
$$xy=y^{-1}x^{-1}=yx$$

□

תרגיל: תהי $(G,*)$ חבורה. הוכח שלמשוואה:

$$xax=b$$

יש פתרון אם"ם ab הוא ריבוע (כלומר קיים $t\in G$ המקיים $t^2=ab$)

הוכחה:

כיוון א'(קל): נתון ל $xax=b$ יש פתרון צ"ל: קיים $t^2=ab$.

לפי הנתון מתקיים:

$$\exists c\in G\ \ cac=b$$

נכפיל את שני הצדדים ב a משמאל ונקבל:

$$acac=ab$$
$$(ac)^2=ab\to ac=t,t^2=ab$$

כיוון ב': נתון $\exists t\in G\ \ t^2=ab$ צ"ל: למשוואה $xax=b$ קיים פתרון ב G . נעזר בכיוון א': אנחנו כבר יודעים שאם קיים פתרון x אז בהכרח מתקיים t=ax. לכן "ננחש" שהפתרון הוא $x=a^{-1}t$:

$$xax=(a^{-1}t)a(a^{-1}t)=a^{-1}taa^{-1}t=$$
$$=a^{-1}t^2=a^{-1}ab=b$$

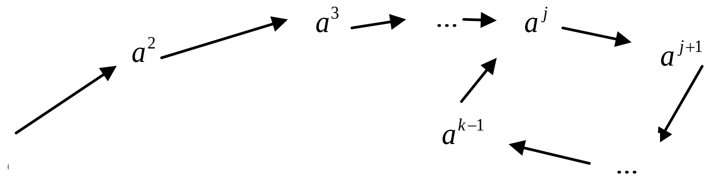
□ .

הגדרה: מונואיד M הוא בעל <u>צמצום משמאל</u> אם $\forall a,b,c\in M,\ ab=ac\Rightarrow b=c$. בצורה דומה מגדירים בעל צמצום מימין/בעל צמצום.

טענה: מונואיד סופי M בעל צמצום משמאל הוא חבורה.

הוכחה א: צ"ל שלכל איבר קים איבר הפכי. יהי $a\in M$ נגדיר פונקציה $M\to M$ ע"י $l_a(x)=ax$ פונקצית הכפלה משמאל ב a . הפונקציה היא חח"ע בגלל צמצום משמאל ($l_a(x)=l_a(y)\Rightarrow ax=ay\Rightarrow x=y$), וכיוון שהמונואיד סופי נקבל שהפונקציה היא על (לפי עקרון שובך היונים).

הוכחה ב: כנ"ל צ"ל שלכל איבר קים איבר הפכי. ניצור סדרה של חזקות $a,a^2,a^3,a^4,....$ עבור איבר $e\neq a\in M$. כיוון שהמונואיד סופי, קיימות שתי חזקות $j<k$ כך ש $a^j=a^k$. נמחיש זאת בעזרת הציור הבא (כל חץ מייצג הכפלה ב a):



כעת $a^j a^{k-j} = a^{j+(k-j)} = a^j = a^j e$. לפי תכונת הצמצום, נקבל $e = a^{k-j}$. כעת כיוון ש $k > j$ נקבל $k - j \geq 1$, כיוון ש $e \neq a$ בהכרח $k - j \geq 2$. לכן נקבל ש $e = a^{k-j-1}a = aa^{k-j-1}$. כלומר $a^{-1} = a^{j-k-1}$.

<u>תרגיל:</u>

1. אם A אגודה סופית, אזי קיים $a \in A$ כך ש $a^2 = a$.
2. הראו שזה לאו דוקא נכון אם A אגודה אינסופית.
3. אם A חבורה אזי $a^2 = a \Rightarrow a = e$.

<u>פתרון:</u>

1. בדומה להוכחה ב' בתרגיל הקודם, נבנה סדרה של חזקות עבור $a \in A$:
$a, a^2, a^3, a^4, ...$. כיוון שהאגודה סופית, נקבל שבהכרח קיימות שתי חזקות $j < k$ כך ש $a^j = a^k$. נטען שניתן להניח שמתקיים $k \geq 2j$, כיוון שלכל $t \geq 0$ מתקיים (באינדוקציה על t): $a^{k+t(k-j)} = a^k a^{t(k-j)} = a^k a^{k-j} a^{(t-1)(k-j)} = a^j a^{k-j} a^{(t-1)(k-j)} = a^k a^{(t-1)(k-j)} = ... = a^k$.
ולכן ניתן להגדיל את k כרצוננו. כעת נשים לב ש $a^{j+i} = a^j a^i = a^k a^i = a^{k+i}$. נמצא i מתאים כך שיתקיים: $2(j+i) = k + i$. מכאן ש $i = k - 2j$.
2. לדוגמא ב $(\mathbb{N}, +)$ הטענה לא מתקיימת. $2a = a \Rightarrow a = 0 \notin \mathbb{N}$.
3. מכפילים בהפכי של a בשני האגפים.

<u>תרגילי בית:</u>

1. במונואיד איבר שהוא הפיך מימין ומשמאל הוא הפיך.
2. מונואיד בו כל איבר הפיך מימין הוא חבורה.

תרגול 2

טענה: קבוצת האיברים ההפיכים U(M) במונואיד M היא חבורה.

הוכחה: סגירות: אם a,b הפיכים, אזי $(ab)^{-1}=b^{-1}a^{-1}$ כלומר ab הפיך. קיום הפכי: שימו לב שלדעת שאיבר הפיך זה לא מספיק, צריך גם להוכיח שההפכי שייך לקבוצה – כלומר במקרה זה יש להוכיח שההפכי הפיך. שאר התכונות – תרגיל בית.

דוגמא: קבוצת הפונקציות $F=\{f:X\to X\}$ היא מונואיד עם פעולת ההרכבה, ואיבר היחידה היא פונקצית הזהות. $U(F)$ היא קבוצת הפונקציות החח"ע ועל מ X ל X.

חבורת אוילר:

חשיבות מיוחדת יש לקבוצת האיברים ההפיכים ב $(\mathbb{Z}_n,*,1)$ אשר לפי הסימונים הנ"ל תסומן ב- $U(\mathbb{Z}_n,*)$.

הגדרה: נקרא לחבורות מהצורה $U((\mathbb{Z}_n,*,1))$ **חבורות אוילר**, ונסמן ב U_n או ב $Euler(n)$.

דוגמא: נחשב את החבורה U_6. נבנה תחילה את לוח הכפל של $\mathbb{Z}_6$:

*	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

(השמטנו את 0 מהטבלה כי הכפל בו תמיד 0). רואים ש $U_6=\{1,5\}$. ההפכי של 1 הוא 1, וההפכי של 5 הוא 5.

טענה: איבר $a\in(\mathbb{Z}_n,*,1)$ הפיך (כפלית) אם ורק אם $\gcd(a,n)=1$.

הוכחה:

$\gcd(a,n)=1$ אם ורק אם (לפי למת בזו) קיימים u,v שלמים כך ש $au+nv=1$ לכן כאשר נעבור ל mod n, נקבל $au\equiv1\ (\text{mod}\,n)$, כלומר a הפיך.

תרגיל בית:

ניתן להוכיח את הכיוון $\Rightarrow$ גם בצורה "אלגברית יותר": הראו שהקבוצה $\{a\in\mathbb{Z}_n \mid \gcd(a,n)=1\}$ הוא מונואיד (כפלי) בעל צמצום, ולכן ע"פ טענה מהתרגול הקודם, נקבל שהקבוצה הנ"ל היא חבורה, ובפרט כל האיברים המקיימים $\gcd(a,n)=1$ הם הפיכים.

<u>מסקנה:</u> $U_n=\{a\in\mathbb{Z}_n \mid 1\le a\le n-1,\ \gcd(a,n)=1\}$.

<u>דוגמאות:</u> $U_{14}=\{1,3,5,9,11,13\},\ U_{12}=\{1,5,7,11\}$.

אם p ראשוני, אזי $U_p=\mathbb{Z}_p^{\,*}$, זאת כיוון שכל $1\le a<p$ הוא זר ל p.

<u>תרגיל:</u> האם ל 5 קיים הפיך כפלי ב $\mathbb{Z}_{10}$?

<u>פתרון:</u> לא. כיוון ש 5 אינו זר ל 10.

<u>הגדרה:</u> **פונקצית אוילר** $\varphi(n)$, היא מספר מספר האיברים בחבורה U_n (כלומר מספר הטבעיים הקטנים ל n וזרים לו). לדוגמא, $\varphi(p)=p-1$ עבור p ראשוני, $\varphi(14)=6,\varphi(12)=4$.

<u>תרגיל בית:</u> חשבו את $\varphi(pq)$ כאשר p,q ראשוניים (טפלו גם במקרה $p=q$).

<u>חבורות מטריצות:</u>

<u>סימון:</u>

$M_n(F)$ קבוצת המטריצות עם ערכים מהשדה F.

$GL_n(F):=U(M_n(F))$ קבוצת כל המטריצות ההפיכות מגודל nXn עם ערכים מהשדה F.

$SL_n(F)$ קבוצת כל המטריצות ההפיכות עם דטרמיננטה 1 מגודל nXn עם ערכים מהשדה F.

<u>טענה:</u>

$M_n(F)$ היא מונואיד (לא לכל מטריצה יש הפכית).

$GL_n(F)$, $SL_n(F)$ חבורות, כאשר הכפל הוא כפל מטריצות.

<u>הוכחה (חלקית):</u>

נראה ש- $SL_n(F)$ חבורה.

איך מוכיחים?

מראים $SL_n(F)$ מקיימת את כל התנאים של חבורה:

1) סגירות:

$\det(A*B)=\det A*\det b=1*1=1$ $\forall A,B\in SL_n(F)$ כלומר $A*B\in SL_n$

2) אסוציאטיביות:

מתקיימת כי הכפל הוא כפל מטריצות.

3) קיום יחידה:

$$I=\begin{pmatrix}1&\dots&0\\ \vdots&\ddots&\vdots\\ 0&\cdots&1\end{pmatrix}$$

איבר יחידה המקיים $\det I=1 \wedge (A*I=I*A)$(ראה אלגברה ליניארית 1)

4) הופכי: לפי הגדרת החבורה לכל $A\in SL_n$ $\quad \exists A^{-1},\quad \det(A^{-1})=\det(A)^{-1}=1$

לכן $A^{-1}\in SL_n$

<u>תרגיל בית:</u> הוכיחו ש $SL_n(F)$ אינה חבורה אבלית.

<u>דוגמא:</u>

האם $A=\left\{\begin{bmatrix}a&b\\0&0\end{bmatrix} \mid a,b\in\mathbb{Q}\right\}$ עם כפל מטריצות רגיל היא חבורה? האם היא אגודה/מונואיד?

יש סגירות לכפל: $\begin{bmatrix}a&b\\0&0\end{bmatrix}\begin{bmatrix}c&d\\0&0\end{bmatrix}=\begin{bmatrix}ac&ad\\0&0\end{bmatrix}$

אנחנו יודעים ש A אסוציאטיבית, כי כפל ב- $M_2(\mathbb{Q})$ הוא אסוציאטיבי.

האם ל A יש יחידה? אם $\begin{bmatrix}a&b\\0&0\end{bmatrix}$ היא יחידה שמאלית, אזי

$\begin{bmatrix}ac&ad\\0&0\end{bmatrix}=\begin{bmatrix}a&b\\0&0\end{bmatrix}\begin{bmatrix}c&d\\0&0\end{bmatrix}=\begin{bmatrix}c&d\\0&0\end{bmatrix}$ ונקבל ש $a=1$. כלומר כל איבר מהצורה $\begin{bmatrix}1&b\\0&0\end{bmatrix}$ הוא יחידה שמאלית. למעשה זה כבר אומר שהקבוצה A אינה חבורה, כי יש אינסוף יחידות שמאליות, ובחבורה/מונואיד יכולה להיות רק אחת. לכן A היא אגודה בלבד.

<u>תמורות:</u>

! <u>הגדרה:</u> חבורת הסימטריה S_n הינה חבורת כל התמורות על $\{1,\dots,n\}$. נזכיר שתמורה היא פונקציה חח"ע ועל $\pi:\{1,\dots,n\}\to\{1,\dots,n\}$. ישנן $n!$ תמורות.

<u>דוגמא:</u> $x=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ $x\in S_3$ כלומר x היא התמורה שמעבירה את 1 ל3 את 2 ל2 ואת 3 ל1. כל תמורה לוקחת את n האיברים ומסדרת אותם בסדר כלשהו.

! <u>משפט:</u> S_n עם פעולת ההרכבה של תמורות הינה חבורה**.** איבר היחידה הוא פונקצית הזהות $id(i)=i$ לכל $i\in\{1,\dots,n\}$.

מה זה הרכבת תמורות? מתייחסים לתמורות כפונקציות, ומבצעים הרכבה.

נסביר ע"י דוגמא ב S_4:

$$x=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\quad y=\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}$$

$$xy=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix},\quad yx=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$$

איך מחשבים? כמו בהרכבת פונקציות שמים את התמורות אחת ליד השניה:

$$x=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix},\quad y=\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}$$

$$xy=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}$$

ואז מתחילים לחשב מימין לשמאל ובודקים מה הטווח של כל מספר מ1 עד 4:

1 הולך ל4 ו 4 הולך ל4 לכן סך הכול 1 הולך ל 4.

2 הולך ל2 ואז 2 הולך ל1 אז סך הכול 2 הולך ל 1.

3 הולך ל3 שהולך 3 סך הכל 3 הולך ל 3.

4 הולך ל1 ו1 הולך 2 אז סך הכל 4 הולך ל 2.

עבור $n\neq 2$ חבורת התמורות אינה חבורה אבלית.

<u>איך מוצאים תמורה הפכית?</u>

בהנתן $x=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$ צריך להחליף בין השורות, ואז לסדר מחדש:

$$x^{-1}=\begin{pmatrix}2&1&3&4\\1&2&3&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}$$

<u>פירוק תמורה למחזורים זרים:</u>

מחזור הוא תמורה הנכתבת בצורה (1,2,3) כלומר 1 עובר ל 2, 2 עובר ל 3 וגם 3 עובר ל 1. כל תמורה ניתנת לפירוק למחזורים זרים, לדוגמא:

$x = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (1,2)(3)(4)$. מקובל להסיר מחזורים מאורך 1, ולכתוב בכתיב חסר: (1,2).

איבר היחידה הוא מחזור ריק: $(1)(2)(3)(4)$, ובקיצור רושמים (1).

בהמשך הקורס נראה שניתן לכתוב כל תמורה ככפל מחזורים זרים בצורה יחידה.

נשים לב שמחזורים זרים מתחלפים: $(1,2,3)(4,5) = (4,5)(1,2,3)$.

<u>תתי חבורות:</u>

<u>תת חבורה:</u> תהי $(G,*,e)$ חבורה אז תת קבוצה $H \subseteq G$ תקרא תת חבורה של G אם H חבורה ביחס לפעולה *.

<u>סימון:</u> $H \le G$

<u>טרמינולוגיה:</u> קוראים לחבורה $\{e\}$ **<u>החבורה הטריוויאלית</u>**. כאשר אומרים **<u>תתי-החבורות הטריוויאליות</u>** של חבורה G, מתכוונים ל- $\{e\}, G$.

<u>דוגמאות לת"ח</u>

1. $(\mathbb{Z},+,0) \le (\mathbb{Q},+,0)$

2. $SL_n(\mathbb{F}) \le GL_n(\mathbb{F})$

3. $n\mathbb{Z} \le \mathbb{Z}$. האם יש ל $\mathbb{Z}$ ת"ח מצורה שונה? תהי $\{0\} \ne H \le \mathbb{Z}$, וניקח את $0 < n \in H$ המינימלי, ונטען ש $H = n\mathbb{Z}$. יהי $k \in H$ ונחלק את n ב k חלוקה עם שארית: $k = nq + r, 0 \le r < n$ ואז נקבל $k - nq = r \in H$ וזה יכול להיות רק אם $r = 0$ (אחרת סתירה למינימליות n). בצורה דומה ניתן להראות שכל ת"ח של $n\mathbb{Z}$ הם מהצורה $m\mathbb{Z}$ כאשר $n | m$.

4. $m\mathbb{Z}_n \le \mathbb{Z}_n$ כאשר $m | n$. נראה בתרגול הבא שכל ת"ח של $\mathbb{Z}_n$ היא מהצורה הזאת.

5. האם: $\mathbb{Z}_3 \le \mathbb{Z}_6$? תשובה: לא!! כי הפעולות שונות בשתי הקבוצות שונה. למה אנחנו מתכוונים בפעולות שונות? שימו לב ש 2 הוא ההפכי של 1 ב- $\mathbb{Z}_3$, אבל ב $\mathbb{Z}_6$ זה לא נכון. בצורה דומה $\mathbb{Z}_n \not\le \mathbb{Z}$.

6. קבוצת כל החזקות של איבר מסוים בחבורה היא ת"ח. כלומר אם G חבורה, ו- $x \in G$ אזי $\{x^n \mid n \in \mathbb{Z}\} \le G$. קבוצת כל החזקות החיוביות היא אגודה, קבוצת כל החזקות הלא-שליליות היא מונואיד.

7. יהי Ω_n אוסף הפתרונות של המשוואה $z^n = 1$ ב $\mathbb{C}$. אזי $\Omega_n \le \mathbb{C}^*$. נראה זאת: נניח ש $a,b \in \Omega_n$, ז"א $a^n = b^n = 1$. אזי $(ab)^n = a^n b^n = 1$ (בגלל האבליות ב $\mathbb{C}$). עבור $a \in \Omega_n$ ניקח את $a^{-1} \in \mathbb{C}$. אזי $\left(a^{-1}\right)^n = \left(a^n\right)^{-1} = 1$ ולכן $a^{-1} \in \Omega_n$. נשים לב ש $\Omega_n = \{cis(\frac{2\pi k}{n}) \mid 0 \le k \le n-1\}$, כאשר $cis(\alpha)$ הוא סימון מקוצר ל $cis(\alpha) = \cos(\alpha) + i\sin(\alpha)$ (לדוגמא: $cis(30) = \cos(30) + i\sin(30) = \frac{\sqrt{3}}{2} + \frac{1}{2}i$).

זאת כיוון ש $cis(\alpha)cis(\beta) = cis(\alpha+\beta)$, ולכן $\left(cis(\frac{2\pi k}{n})\right)^n = cis(2\pi k) = 1$.

ל Ω_n קוראים **חבורת שורשי-** n **של היחידה**.

<u>קריטריונים לבדיקה האם תת-קבוצה היא ת"ח:</u>

<u>משפט קיצור הדרך 1:</u>

תהי H תת קבוצה לא ריקה של G . אז $H \le G$ אם ורק אם:

1) $\forall a,b \in H,\ ab \in H$

2) $\forall a \in H,\ a^{-1} \in H$

<u>משפט קיצור הדרך 2:</u>

תהי H תת קבוצה לא ריקה של G . אז $H \le G$ אם ורק אם:

$$\forall a,b \in H,\ \ ab^{-1} \in H$$

<u>הערה:</u> אם $A,B \le G$ וגם $A \subseteq B$ אזי בוודאי שגם $A \le B$ (אין צורך להוכיח זאת, זה נובע ישירות מהגדרה, הרבה סטודנטים מנסים להוכיח זאת בעזרת משפטי קיצור הדרך).

טענה: אם G חבורה סופית ו- H תת-קבוצה של G אזי $H \le G$ אם ורק אם $H \neq \emptyset$ וגם $x, y \in H \Rightarrow xy \in H$.

הוכחה: כיוון <= ברור. בכיוון השני, מספיק לפי משפט קיצור הדרך להראות $\forall a \in H,\ a^{-1} \in H$.
יהי $e \neq a \in H$ (אם $H = \{e\}$ אזי סיימנו). לפי התנאי, מתקיים $a \in H \Rightarrow a^2 = aa \in H$,
ובאינדוקציה רואים שכל החזקות החיוביות של של a הן ב H. אבל החבורה היא סופית, ולכן
בסדרה $a, a^2, a^3, ..., a^n, ...$ קיימים $i < j$ כך ש $a^i = a^j$ ונקבל $a^{j-i} = e$, ומכאן נקבל ש-
$a^{-1} = a^{j-i-1} \Leftarrow aa^{j-i-1} = a^{j-i-1}a = e$.

<u>תרגול 3</u>

<u>משפט:</u> יהי G חבורה ו $H,K \le G$ אז $H \cap K \le G$.

<u>משפט :</u> יהי $\{H_i\}_{i\in I}$ סדרה לא בהכרח סופית של תתי חבורת אז חיתוכן הוא תת חבורה.

<u>דוגמא:</u>

יהיו $a\mathbb{Z}, b\mathbb{Z}$ ת"ח של $\mathbb{Z}$. אזי $a\mathbb{Z} \cap b\mathbb{Z} = lcm(a,b)\mathbb{Z}$ (לדוגמא: $2\mathbb{Z} \cap 3\mathbb{Z} = lcm(2,3)\mathbb{Z} = 6\mathbb{Z}$).

מדוע? אם $m \in a\mathbb{Z} \cap b\mathbb{Z}$ אזי $a \mid m$ וגם $b \mid m$ ולכן לפי תכונות של הכפולה המשותפת המינימלית, $lcm(a,b) \mid m$, ולכן $m \in lcm(a,b)\mathbb{Z}$. אם $m \in lcm(a,b)\mathbb{Z}$ אזי $lcm(a,b) \mid m$ ואז לפי טרנזטיביות חילוק נקבל $a \mid lcm(a,b) \Rightarrow a \mid m$ ואותו דבר גם עבור b . לכן $m \in a\mathbb{Z} \cap b\mathbb{Z}$.

אם נסמן $a\mathbb{Z} + b\mathbb{Z} = \{an + bm \mid n, m \in \mathbb{Z}\}$ אזי $a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}$ (הוכחה: תרגיל בית).

<u>דוגמא:</u> אם G חבורה ו $H,K \le G$ אז $H \bigcup K$ לא בהכרח תת חבורה של G :

נסתכל על $\mathbb{Z}_{10}$, ועל הת"ח $2\mathbb{Z}_{10} = \{0,2,4,6,8\}$ ו $5\mathbb{Z}_{10} = \{0,5\}$. אזי $2\mathbb{Z}_{10} \cup 5\mathbb{Z}_{10} = \{0,2,4,5,6,8\}$. אבל לא מתקיימת סגירות ב $2\mathbb{Z}_{10} \cup 5\mathbb{Z}_{10}$, כיוון ש $2+5=7 \notin 2\mathbb{Z}_{10} \cup 5\mathbb{Z}_{10}$. נשים לב שבמקרה זה $2\mathbb{Z}_{10} \cap 5\mathbb{Z}_{10} = \{0\}$, וזו אכן ת"ח.

<u>מכפלה ישרה של חבורות:</u>

תהיינה A,B חבורות. **המכפלה הישרה** של A,B היא הקבוצה $A \times B = \{(a,b) \mid a \in A, b \in B\}$ עם פעולה בינארית המוגדרת ע"י:

$$(a_1,b_1)(a_2,b_2) = (a_1 *_A a_2, b_1 *_B b_2) .$$

<u>במילים אחרות:</u> המכפלה הנ"ל היא מכפלה קרטזית (כמו שלמדתם בבדידה או בתורת הקבוצות) כאשר פעולה בקבוצה מוגדרת כמכפלה רכיב רכיב.

<u>משפט:</u> מכפלה ישרה $A \times B$ היא חבורה.

<u>הוכחה:</u>

- קיים איבר יחידה $e_{A\times B} = (e_A, e_B)$
- אסוציאטיביות נובעת מאסוציאטיביות ב A ו B .

- סגירות: $\forall x,y\in A\times B, x=(a_1,b_1), y=(a_2,b_2),$ $i=1,2, a_i\in A, b_i\in B, xy=(a_1a_2,b_1b_2)\in A\times B$

- הופכי: $x\in A\times B, \exists a\in A, b\in B, x=(a,b),$ $x^{-1}=(a^{-1},b^{-1}), a^{-1}\in A, b^{-1}\in B$ $x*x^{-1}=(e_A,e_B)=e_{A\times B}$

וסיימנו להוכיח ש $A\times B$ חבורה תחת הפעולה הנ"ל.

<u>דוגמאות:</u>

1. ראינו בתרגול הראשון את חבורת קליין $\mathbb{Z}_2\times\mathbb{Z}_2$. החיבור בחבורה מתבצע רכיב רכיב: $(1,1)+(1,0)=(0,1)$. כיוון ששתי החבורות הן חיבוריות, נרשום את הפעולה של המכפלה הישרה בצורה חיבורית. נשים לב שכיוון שכל רכיב הוא אבלי, אזי גם המכפלה הישרה היא אבלית.

2. $S_3\times\mathbb{Z}_2$. נראה שחבורה זאת אינה אבלית.

$$((1,2,3),1)*((1,2),0)=((1,2,3)(1,2),1+0)=((1,3),1)$$
$$((1,2),0)*((1,2,3),1)=((1,2)(1,2,3),0+1)=((2,3),1)$$

<u>ת"ח ציקליות:</u>

הראינו בתרגול הקודם שעבור חבורה G ואיבר $a\in G$, קבוצת כל החזקות של a היא ת"ח ($\{a^n \mid n\in\mathbb{Z}\}\le G$).

<u>הגדרה:</u> ! נקרא ל $\{a^n \mid n\in\mathbb{Z}\}\le G$ ת"ח **הציקלית** של G **הנוצרת** ע"י a ונסמן ב $<a>$.

חבורה הנוצרת ע"י איבר אחד נקראת **חבורה ציקלית** ($<a>=G$).

המשמעות של הגדרה זו שאם G חבורה ציקלית אז קיים איבר $a\in G$ כך שכל איבר $g\in G$ מקיים $g=a^n$. כלומר כל איבר ב G הוא חזקה של a .

<u>דוגמאות:</u>

1. בחבורה $\mathbb{Z}$ נקבל $<1>=\{1,1+1=2,1+1+1=3,...\}=\mathbb{Z}$. $<2>=\{2,4,6,8,...\}=2\mathbb{Z}$.

2. בחבורה $\mathbb{Z}_6$ נקבל $<2>=\{2,2+2=4,2+2+2=6=0\}=\{0,2,4\}=2\mathbb{Z}_6$. בחבורה $\mathbb{Z}_5$ נקבל $<2>=\{2,4,6=1,3,0\}=\mathbb{Z}_5$.

3. $(\mathbb{Z}_n,+,0)$ היא חבורה ציקלית לכל n , כיוון ש $<1>=\mathbb{Z}_n$.

4. בחבורה S_3 של תמורות על {1,2,3} נקבל עבור $\pi=(1,2,3)$ שמתקיים:
$<\pi>=\{\pi,\pi^2=(1,3,2),\pi^3=id\}$.

<u>משפט:</u>

1. $<a>$ היא ת"ח המינימלית (ביחס להכלה) של G המכילה את a.
2. $<a>$ היא החיתוך של כל הת"ח של G שמכילות את a ($<a>=\bigcap_{a\in H\le G} H$).

<u>משפט:</u> כל חבורה ציקלית היא אבלית.

<u>הגדרה:</u> סדר של חבורה הוא מספר האיברים בחבורה, ויסומן ע"י $|G|$.

<u>דוגמאות:</u>

1. $(\mathbb{Z},+,0)$ חבורה מסדר ∞.
2. $\mathbb{Z}_n$ היא חבורה מסדר n.
3. $|S_n|=n!$.
4. הסדר של החבורה $\text{Euler}(\text{n})=U_n=U(\mathbb{Z}_n{}^*,*)$ (חבורת האיברים ההפיכים כפלית ב $\mathbb{Z}_n$) הוא מספר המספרים הקטנים מ n וזרים לו. נסמן מספר זה ב $\varphi(n)$. הפונקציה φ נקראת <u>פונקצית אוילר</u>. לדוגמא $\varphi(5)=4,\varphi(6)=2$.
5. $|A\times B|=|A||B|$ לפי תכונות של מכפלה קרטזית.

<u>הגדרה:</u> סדר של איבר מוגדר כסדר התת חבורה הציקלית הנוצרת על ידו, והסימון הוא $o(g):=|<g>|$, נסמן פעמים רבות גם $|g|$.

<u>משפט</u>: $o(g)=\min(n>0|g^n=e)$ אם קיים n כזה או $o(g)=\infty$ אם לא קיים n המקיים את הנ"ל.

<u>דוגמאות:</u>

1. לכל חבורה G, $|e|=1$.
2. לכל $x\in\mathbb{Z}$ מתקיים $o(x)=\infty$.

3. ראינו ש $U_6=\{1,5\}$ (האיברים ההפיכים כפלית ב $\mathbb{Z}_6$). הסדר של 5 הוא 2, כיוון ש $5^1=5\neq 1$, וגם $5^2=25=1\ (\text{mod}\,6)$. לכן $|5|=2$. נשים לב שקיבלנו $<5>=\{1,5\}=U_6$ כלומר U_6 היא חבורה ציקלית מסדר 2.

$U_8=\{1,3,5,7\}$ אזי $|U_8|=4$, נחשב את סדרי האיברים:

$3^2=9=1\ (\text{mod}\,8),\ 7^2=49=1\ (\text{mod}\,8),\ 5^2=25=1\ (\text{mod}\,8)$. אם כך $|3|=|7|=|5|=2$. שימו לב ש U_8 היא דוגמא לחבורה אבלית **שאינה** ציקלית.

4. ב S_5 האיבר $\pi=(1,2,3)(4,5)$ הוא מסדר 6, נראה זאת:

$$\begin{aligned}
&\pi=(1,2,3)(4,5)\neq id\\
&\pi^2=(1,2,3)(4,5)(1,2,3)(4,5)=(1,2,3)(1,2,3)=(1,3,2)\neq id\\
&\pi^3=(1,3,2)(1,2,3)(4,5)=(4,5)\\
&\pi^4=(4,5)(1,2,3)(4,5)=(1,2,3)\\
&\pi^5=(1,2,3)(1,2,3)(4,5)=(1,3,2)(4,5)\\
&\pi^6=(1,3,2)(4,5)(1,2,3)(4,5)=(1)=id
\end{aligned}$$

5. בחבורה $GL_2(\mathbb{R})$ - המטריצות ההפיכות מגודל 2x2 עם ערכים ב $\mathbb{R}$. איבר היחידה הוא מטריצת הזהות $I=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. נבדוק את הסדר של האיבר $B=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$ ($\det(B)=1$ ולכן $B\in GL_2(\mathbb{R})$):

$$\begin{aligned}
&B^2=\begin{pmatrix}0&1\\-1&-1\end{pmatrix}\begin{pmatrix}0&1\\-1&-1\end{pmatrix}=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}\\
&B^3=B^2B=\begin{pmatrix}-1&-1\\1&0\end{pmatrix}\begin{pmatrix}0&1\\-1&-1\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}=I\\
&\Rightarrow\ o(B)=3
\end{aligned}$$

6. יהי $x\in\mathbb{Z}_n$, כך ש $x\,|\,n$, אזי $o(x)=\frac{n}{x}$. אם $d=\gcd(x,n)$ אזי $o(x)=\frac{n}{d}$ כיוון ש: $x\cdot\frac{n}{d}\equiv\frac{x}{d}\cdot n\equiv 0\ (\text{mod}\,n)$, כלומר $o(x)\leq\frac{n}{d}$. אם $o(x)=m$ אזי $mx\equiv 0\ (\text{mod}\,n)$ כלומר $n\,|\,mx$ ולכן $\frac{n}{d}\,|\,m\frac{x}{d}$, וכיוון ש $\gcd(\frac{n}{d},\frac{x}{d})=1$ נקבל ש $\frac{n}{d}\,|\,m$ ולכן $\frac{n}{d}\leq m$.

7. הסדר של החבורה $\mathbb{Z}_n\times\mathbb{Z}_n$ הוא $|\mathbb{Z}_n\times\mathbb{Z}_n|=n^2$. לכל $(a,b)\in\mathbb{Z}_n\times\mathbb{Z}_n$ מתקיים $n(a,b)=(na,nb)=(0,0)\ (\mathrm{mod}\, n)$ (אנחנו מתייחסים כאן ל $\mathbb{Z}_n\times\mathbb{Z}_n$ כחבורה חיבורית, והסימונים בהתאם). לכן $|(a,b)|\le n$. נקבל שאין אף איבר מסדר n^2 ולכן $\mathbb{Z}_n\times\mathbb{Z}_n$ אינה חבורה ציקלית.

<u>תרגיל:</u> אם $g^n=e$ אזי $o(g)\,|\,n$.

<u>הוכחה:</u> ברור ש $o(g)\le n$. נבצע חלוקה עם שארית $n=o(g)q+r$ כאשר $0\le r<o(g)$, ונקבל $e=g^n=g^{o(g)q+r}=(g^{o(g)})^q g^r=g^r$. הדרך היחידה שזה יכול לקרות היא אם $r=0$.

<u>המשפט היסודי של חבורות ציקליות:</u>

1. כל ת"ח של חבורה ציקלית היא ציקלית.
2. הסדר של כל ת"ח של חבורה ציקלית מסדר n הוא מחלק של n (למעשה בהמשך נוכיח שזה נכון לכל חבורה).
3. אם G חבורה ציקלית מסדר n אזי לכל מחלק k של n **<u>קיימת</u>** ת"ח **<u>יחידה</u>** מסדר k.

<u>הוכחה:</u>

1. ההוכחה דומה מאד להוכחה שהראינו בתרגול הקודם לכך שכל התת-חבורות של $\mathbb{Z}$ הן מהצורה $n\mathbb{Z}$: תהי $G=<a>$ חבורה ציקלית, ותהי $H\le G$, אם $H=\{e\}$ אז סיימנו, אחרת קיים $t>0$ מינימלי כך ש- $a^t\in H$. כעת הראו באותה דרך כמו בתרגול הקודם ש $H=<a^t>$.

2. ראינו בדוגמא 6 לעיל את הטענה עבור $\mathbb{Z}_n$, וההוכחה לכל חבורה ציקלית כמעט זהה.

3. יהי k|n, ויהי a יוצר של G. אזי $o(a^{\frac{n}{k}})=k$ (מדוע?). תהי H ת"ח כלשהיא מסדר k, אזי לפי 1 ו 2, נקבל $H=<a^m>$ כאשר $m\,|\,n$. אבל אז $k=o(a^m)=\frac{n}{m}$ כלומר $m=\frac{n}{k}$ כנדרש.

<u>תרגיל בית:</u> הראו שהסדר של כל איבר $a^t\in G$ השייך לחבורה ציקלית מסדר n, הוא $\frac{n}{\gcd(n,t)}$.

דוגמא:

נשים לב שלחבורה ציקלית יש יותר מיוצר אחד (זה נובע גם לדוגמא גם מתרגיל הבית הנ"ל).

אם ניקח מספר t<n כך ש gcd(t,n)=1 אזי סדר האיבר a^t (כאשר a הוא יוצר של החבורה הציקלית) יהיה n. לדוגמא, ניקח ב $\mathbb{Z}_7$ את 5, אזי $o(5)=7$:

$$5+5=10\equiv 3(\bmod 7)$$
$$5+5+5=15\equiv 1(\bmod 7)$$
$$5+5+5+5=20\equiv 6(\bmod 7)$$
$$5+5+5+5+5\equiv 4(\bmod 7)$$
$$5+5+5+5+5+5\equiv 2(\bmod 7)$$
$$5+5+5+5+5+5+5\equiv 0(\bmod 7)$$

שאלה: אז כמה יוצרים יש בחבורה ציקלית?

תשובה: בהנתן חבורה ציקלית מסדר n, מספר היוצרים הוא כמספר המספרים הקטנים מ n וזרים לו, כלומר בדיוק $\varphi(n)$ (פונקצית אוילר).

בהנתן חבורה ציקלית אינסופית, כמה יוצרים יש? בדיוק 2.

תרגיל: הוכיחו או הפריכו: אם $a,b\in G$ מסדר סופי בחבורה, אזי ab הוא מסדר סופי.

פתרון: הטענה נכונה בחבורה אבליות, אבל לא בכל חבורה. אם $|a|=n,|b|=m$, אזי בחבורה אבלית מתקיים $(ab)^{mn}=a^{mn}b^{mn}=\left(a^n\right)^m\left(b^m\right)^n=ee=e$, ולכן $|ab|\le mn<\infty$. נראה חבורה בה הטענה לא מתקיימת: ניקח את $GL_2(\mathbb{R})$, ואת האיברים $A=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}, B=\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}$. ראינו ש $|B|=3$, ובדקו שמתקיים $|A|=4$, כלומר שניהם איברים מסדר סופי. כעת $AB=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$ ומתקיים:

$$\left(AB\right)^2=\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix},\left(AB\right)^3=\begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix},\ldots,\left(AB\right)^n=\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}$$

לכן לא קיים $n\in\mathbb{N}$ כך ש $\left(AB\right)^n=I$, כלומר $|AB|=\infty$.

תרגיל: תהי G חבורה מסדר זוגי. הוכיחו שקיים איבר מסדר 2 ב G .

הוכחה: נבחר צמדים ב G כל צמד יהיה מורכב מאיבר והופכי שלו (לכל איבר ב G קיים הופכי והוא יחידי) מכיוון שסדר החבורה זוגי ול e אין הופכי אז ישאר איבר בודד (לפחות 1) שלו לא

יהיה זוג ($a \in G$) כלומר אין לו הופכי בכל שאר אברי החבורה, אבל מכיוון שהוא בחבורה קיים לא הופכי ונשאר שהוא הופכי לעצמו כלומר $a^2 = e$ ולכן $O(a) = 2$ □

תרגיל: תהי G חבורה כלשהי, ויהיו $g,h \in G$ איברים מתחלפים ($gh = hg$) כך ש- $|g| = n, |h| = k$ כך ש $\gcd(k,n) = 1$. הראו ש- $|gh| = |g| \cdot |h|$.

פתרון: נסמן $m := |gh|$. אזי:

$(gh)^{nk} = g^{nk}h^{nk} = \left(g^n\right)^k \left(h^k\right)^n = e$ (השיויון השמאלי נכון בגלל ש $gh = hg$). לכן $m \mid nk$.

$g^{mk} = g^{mk}e = g^{mk}\left(h^k\right)^m = (gh)^{mk} = e$ ולכן $n \mid mk$. כיוון ש $\gcd(n,k) = 1$ אזי $n \mid m$. בצורה דומה נקבל ש $k \mid m$, ולכן $lcm(n,k) \mid m$ אבל $lcm(n,k) = \frac{nk}{\gcd(n,k)} = nk$, ולכן $nk \mid m$.

קיבלנו $m \mid nk$ וגם $nk \mid m$ ולכן $m = nk$.

תרגול 4

ת"ח הנוצרת ע"י קבוצת איברים:

הגדרה : תהי G חבורה ותהי $A\subseteq G$ תת קבוצה של איברים ב-G (כך ש $A\neq\emptyset$)

A אינה בהכרח תת חבורה של G. נגדיר **תת חבורה הנוצרת** ע"י להיות התת-חבורה המינימלית המכילה את A ונסמנה $<A>$.

אם $G=<A>$ אזי נאמר ש G **נוצרת ע"י** A.

עבור קבוצה סופית של איברים, נכתוב בקיצור $<x_1,...,x_k>$ במקום $<\{x_1,...,x_k\}>$.

משפט:

א. $<A>=\bigcap\limits_{\substack{H_i\leq G\\ A\subseteq H_i}} H_i$

ב. $<A>=\{x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k}\mid x_1,...,x_k\in A, n_1,...n_k\in\mathbb{Z}, k\in\mathbb{Z}\}$

הערה: אם החבורה חיבורית, סעיף ב. במשפט מקבל את הצורה:

$<A>=\{n_1x_1+n_2x_2\cdots+n_kx_k\mid x_1,...,x_k\in A, n_1,...n_k\in\mathbb{Z}, k\in\mathbb{Z}\}$

דוגמאות:

א. אם ניקח $\{2,3\}\subseteq\mathbb{Z}$ אזי $H:=<2,3>=\mathbb{Z}$ (כיוון ש $2\in H\Rightarrow -2\in H\Rightarrow(-2)+3=1\in H$. כעת נקבל ש $1\in H\Rightarrow\mathbb{Z}=<1>\subseteq H$).

ב. אם ניקח $\{4,6\}\subseteq\mathbb{Z}$ אזי לפי המשפט (סעיף ב.) נקבל $<\{4,6\}>=\{4n+6m\mid m,n\in\mathbb{Z}\}$. נטען ש $<\{4,6\}>=\gcd(4,6)\mathbb{Z}=2\mathbb{Z}$, מדוע? ברור ש $2\mid 4m+6n$ ולכן $<\{4,6\}>\subseteq 2\mathbb{Z}$. יהי $2k\in 2\mathbb{Z}$ אזי $2k=4(-k)+6k\in<\{4,6\}>$, ולכן $<\{4,6\}>\supseteq 2\mathbb{Z}$. באופן דומה מראים עבור $a,b\in\mathbb{Z}$ ש $<a,b>=\gcd(a,b)\mathbb{Z}$.

ג. בדקו שמתקיים $S_3=<(1,2),(1,2,3)>=<(1,2),(2,3)>$.

ד. במקרה שהחבורה אבלית, קל יותר לתאר את הת"ח הנוצרת: לדוגמא אם ניקח שני יוצרים $a,b\in G$ נקבל: $<a,b>=\{a^ib^j\mid i,j\in\mathbb{Z}\}$, כלומר ניתן לסדר את כל ה- a-ים יחד, ואת כל ה b-ים יחד.לדוגמא $abaaab^{-1}bbba^{-1}=a^3b^3$. שימו לב שהשיווין הנ"ל לאו דוקא נכון בחבורה לא אבלית. באופן כללי יותר: בחבורה אבלית מתקיים

$< a_1,...,a_n >=\{a_1^{k_1}\cdots a_n^{k_n} \mid \forall 1\le i\le n, k_i\in\mathbb{Z}\}$ (השוו עם ההגדרה הכללית בסעיף ב. של המשפט).

ה. נוח לעתים לחשוב על $< A >\le G$ בתור קבוצת "המילים" שניתן לכתוב באמצעות "האותיות" בקבוצה A . נסביר: נגדיר את הא"ב שלנו להיות $A\cup A^{-1}$ כאשר $A^{-1}=\{a^{-1}\mid a\in A\}$. כעת מילה היא סדרה סופית של אותיות מהא"ב. המילה הריקה מייצגת כאן את איבר היחידה בחבורה G. קל לראות שההגדרה השקולה בסעיף ב. במשפט היא בדיוק רשימת כל המילים שניתן ליצור מאברי A.

<u>תרגיל בית:</u>

תהי G חבורה. הראו שאם $a,b\in G$ מתחלפים (כלומר $ab=ba$) אזי $< a,b >$ היא ת"ח אבלית של G.

<u>הגדרה:</u> חבורה G **נוצרת סופית** היא חבורה שיש לה קבוצת יוצרים סופית. כלומר קיימים $a_1,...,a_n\in G$ כך ש $< a_1,...,a_n >= G$.

<u>דוגמאות:</u>

א. מההגדרה אפשר להסיק <u>שכל</u> חבורה סופית היא נוצרת סופית.

ב. <u>כל</u> חבורה ציקלית היא נוצרת סופית (ע"י איבר אחד).

ג. $\mathbb{Z}\times\mathbb{Z}$ נוצרת סופית, כיוון שלכל $g\in\mathbb{Z}\times\mathbb{Z}$ קיימים $m,n\in\mathbb{Z}$ כך ש $g=(m,n)$ ואז: $(m,n)=m(1,0)+n(0,1)\in< (0,1),(1,0) >$. לכן $\mathbb{Z}\times\mathbb{Z}=< (0,1),(1,0) >$.

ד. נראה בהמשך הקורס ש S_n היא נוצרת סופית, $S_n=< (1,2),(1,2,...,n) >$, בוודאי שאינה נוצרת ע"י איבר אחד עבור n>2 (כיוון שאינה ציקלית – כל ציקלית היא אבלית, וקל להראות ש S_n עבור n>2 אינה אבלית).

ה. $(\mathbb{R},+,0)$ אינה נוצרת סופית. ניתן להראות זאת לפי שיקולי עצמה. אם $\mathbb{R}=< a_1,...,a_n >=\{a_1^{k_1}\cdots a_n^{k_n} \mid \forall 1\le i\le n, k_i\in\mathbb{Z}\}$ אזי כל איבר ב $(\mathbb{R},+,0)$ מתואר ע"י סדרה סופית באורך n של מספרים שלמים, ואוסף סדרות זה הוא בן-מניה, כאשר $(\mathbb{R},+,0)$ אינה בת-מניה, סתירה.

ו. $(\mathbb{Q}^*,\cdot,1)$ גם אינה נוצרת סופית, כיוון שאם

$\mathbb{Q}^*=<\frac{a_1}{b_1},...,\frac{a_n}{b_n}>=\{(\frac{a_1}{b_1})^{k_1}\cdots(\frac{a_n}{b_n})^{k_n} \mid \forall 1\le i\le n, k_i\in\mathbb{Z}\}$ (שימו לב שניתן לסדר

מכפלת חזקות של $\frac{a_1}{b_1},...,\frac{a_n}{b_n}$ לפי סדר האינדקסים, כלומר בצורה $(\frac{a_1}{b_1})^{k_1}\cdots(\frac{a_n}{b_n})^{k_n}$ רק

בגלל שהחבורה $\mathbb{Q}^*$ היא אבלית). אזי קל לראות שהגורמים הראשוניים במכנים של

האיברים הנוצרים מוגבלים לקבוצת הגורמים הראשוניים של $b_1,...,b_n$, אבל זאת קבוצה

סופית, ולכן לא ניתן לקבל את כל השברים ב $(\mathbb{Q}^*,\cdot,1)$, סתירה.

ז. בתרגול השני הצגנו את החבורה של **שורשי-** n **של היחידה**:

$\Omega_n=\{cis(\frac{2\pi k}{n}) \mid 0\le k\le n-1\}$, כל הפתרונות של $z^n=1$ בחבורה הכפלית $\mathbb{C}^*$. כעת

נגדיר $\Omega_\infty:=\bigcup_{n=1}^{\infty}\Omega_n$ חבורת כל שרשי היחידה. זהי חבורה, כיוון ש

$cis(\frac{2\pi k}{n})cis(\frac{2\pi j}{m})=cis(\frac{2\pi(mk+nj)}{mn})$ ולכן מכפלת שרשי יחידה היא שורש יחידה

(הקיום של הפכי לכל איבר ברור מהגדרת החבורה). Ω_∞ אינה נוצרת סופית, שכן יש

בה אינסוף איברים, אבל כל קבוצת סופית של איברים יוצרת מספר סופי של איברים.

נראה זאת: יהיו $a_1,...,a_k$ שורשי יחידה מסדרים $n_1,...,n_k$, אזי

$<a_1,...,a_k>=\{a_1^{i_1}\dots a_k^{i_k} \mid 0\le i_j\le n_j, 1\le j\le k\}$ (כיוון ש $\mathbb{C}^*$ חבורה אבלית, ניתן לסדר

כל מכפלת חזקות של האיברים $a_1,...,a_k$ לפי סדר האינדקסים ולקבל איברים מהצורה

הנ"ל). לכן יש מספר סופי של איברים ב- $<a_1,...,a_k>$.

<u>תרגילי בית:</u>

1. הראו ש $(\mathbb{Q},+,0)$ אינה נוצרת סופית.

2. הראו ש $\mathbb{Z}_n\times\mathbb{Z}_m$ נוצרת סופית.

<u>עובדה:</u> ניתן לתאר חבורות ע"י קבוצת יוצרים וקבוצת יחסים (=כללי צמצום) $G=<S \mid R>$. לא נוכיח זאת כאן, אבל נתאר באופן כללי את הבניה. הרעיון דומה לבניית מילים שראינו בסעיף ד. בתחילת התרגול:

קבוצת **היוצרים** S היא קבוצת אותיות (הפעם לא מתוך חבורה, אלא סתם קבוצת אותיות). הא"ב שלנו הוא $\sum = S\cup S^{-1}$. שימו לב שהפעם $S^{-1}=\{s^{-1}\mid s\in S\}$ אינה קבוצת ההפכיים של S אלא סתם אותיות. כעת נגדיר את $\sum^*$ להיות קבוצת המילים שנוצרות מהאותיות ב $\sum$, כלומר סדרות סופיות של אותיות, כאשר נסמן ב ε (או ב $\varnothing$) את המילה הריקה. ניתן לתת ל $\sum^*$ מבנה של מונואיד, כאשר פעולת הכפל היא שרשור מילים, המילה הריקה היא איבר היחידה של המונואיד. לדוגמא אם $S=\{a,b\}$ אזי $\sum=\{a,b,a^{-1},b^{-1}\}$ ו- $\sum^*=\{\varepsilon,a,ab,aba,ba^{-1},aaaa^{-1}bb,...\}$. שימו לב שבמונואיד $\sum^*$ לא מתקיים $aa^{-1}=\varepsilon$. כעת תהי $R\subseteq\sum^*$ קבוצה כלשהי של מילים. ונגדיר יחס שקילות $\sim$ על $\sum^*$ באופן הבא: $w_1\sim w_2$ אם ניתן "להגיע" מ w_1 אל w_2 ע"י הוספה והורדה של מספר סופי של מילים מהצורה $rr^{-1},r^{-1}r$ כאשר $r\in R\cup S$. כעת ניתן להוכיח ש $<S\mid R>:=\sum^*/\sim$ היא חבורה. לדוגמא: אם $S=\{a,b\}$ אזי בחבורה $<S\mid>$ (חבורה נוצרת מ S ללא יחסים) מתקיים $abb^{-1}a^{-1}\sim aa^{-1}\sim\varepsilon$.

הרעיון הוא ש R היא קבוצת מילים שניתן למחוק אותן, או שהן שוות למילה הריקה.

__דוגמאות:__

א. לחבורה $<S\mid>$ (חבורה נוצרת מ S ללא יחסים) קוראים **החבורה החפשית** על S. אם S סופית עם n איברים, אזי מסמנים לעתים את החבורה החפשית "מדרגה n" ע"י F_n . החבורות החפשיות הן חבורות גדולות מאד.

ב. החבורה החפשית מדרגה 1 היא: $F_1=<x\mid>=\{x^i\mid i\in\mathbb{Z}\}\cong\mathbb{Z}$.

ג. בדקו שמתקיים: $<x\mid x^n>=\{e,x,x^2,...,x^{n-1}\}\cong\mathbb{Z}_n$.

ד. בדקו שמתקיים: $<a,b\mid aba^{-1}b^{-1}>\cong\mathbb{Z}\times\mathbb{Z}$. שימו לב שהמילה $aba^{-1}b^{-1}$ היא יחס הדורש ש a,b יתחלפו. כלומר בחבורה מתקיים $aba^{-1}b^{-1}=e\Rightarrow ab=ba$.

__תרגיל:__ תנו דוגמא לחבורה נוצרת סופית בה היוצרים הם כולם מסדר סופי, אך החבורה מסדר אינסופי.

__פתרון:__ $G=<a,b\mid a^2,b^2>$. בחבורה זו המילה ab היא מסדר אינסופי (הוכיחו), ולכן G אינסופית.

__תרגיל בית:__ הסבירו מדוע זה לא יכול להתקיים בחבורה אבלית.

<u>תרגילי בית:</u>

חשבו מהן החבורות הבאות:

א. $G=<a\,|\,a^3,a^{13}>$

ב. $G=<a,b\,|\,a^7,ab^{-1}>$

ג. $G=<a,b\,|\,a^2,b^2,aba^{-1}b^{-1}>$

<u>הומומורפיזם ואיזומורפיזם</u>

<u>! הגדרה:</u> תהיינה $(G,*,e_1)$ ו $(H,\oplus,e_2)$ חבורות.

העתקה (פונקציה): $\varphi:G\to H$ תקרא **הומומורפיזם**. אם היא **כפלית**, כלומר אם מתקיים:

$$\varphi(a*b)=\varphi(a)\oplus\varphi(b) \qquad \forall a,b\in G$$

שימו לב לכך ש * הופך ל $\oplus$ מכיוון שב H הפעולה * לא מוגדרת.

<u>הגדרות נוספות:</u>

<u>מונומורפיזם:</u> פונקציה $\varphi:G\to H$ תקרא מונומורפיזם אם היא הומומורפיזם חד חד ערכי.

<u>אפימורפיזם:</u> פונקציה $\varphi:G\to H$ תקרא אפימורפיזם אם היא הומומורפיזם על

<u>! איזומורפיזם:</u> פונקציה $\varphi:G\to H$ תקרא איזומורפיזם אם היא הומומורפיזם חד חד ערכי ועל.

<u>הערה:</u> שימו לב שחד-חד ערכיות ועל בהגדרת איזומורפיזם מבטיח קיום פונקציה הפכית, אבל לא מבטיח שהפונקציה ההפכית היא הומומורפיזם (כלומר לא מובטחת תכונת הכפליות). למעשה זה תמיד מובטח במקרה של איזומורפיזם חבורות, אבל צריך להוכיח זאת.

<u>סימון:</u> $G\cong H$ משמעותו G איזומורפי ל H כלומר קיימת פונקציה איזומורפית $\varphi:G\to H$. המשמעות המעשית היא שהקבוצות G ו H הם למעשה זהות והפונקציה φ היא מילון שמתאים לכל איבר ב G איבר ב H .

<u>אוטומורפיזם:</u> אוטומורפיזם הוא איזומורפיזם $\varphi:G\to G$ כלומר מחבורה לעצמה.

<u>אנדומורפיזם:</u> אנדומורפיזם הוא הומומורפיזם $\varphi:G\to G$ כלומר מחבורה לעצמה.

<u>תכונות של הומומורפיזמים:</u>

1. $\varphi(e_G)=e_H$ יחידה עוברת ליחידה

2. $\varphi(x^{-1})=\varphi(x)^{-1}$ הפכי עובר להפכי

3. $\varphi(x^{n})=\varphi(x)^{n}$ חזקה עוברת לחזקה (הוכחה באינדוקציה)

4. $\varphi(x^{-n})=\varphi(x)^{-n}$

<u>משפט:</u> אם $O(g)=\infty$ אזי $<g>\cong\mathbb{Z}$ ואם $O(g)=n$ אזי $<g>\cong\mathbb{Z}_n$. כלומר כל חבורה ציקלית איזומורפית ל $\mathbb{Z}$ אם היא אינסופית, וכל חבורה ציקלית סופית מסדר n איזומורפית ל $\mathbb{Z}_n$.

<u>דוגמאות:</u>

א. $\varphi:\mathbb{Z}_2\to\mathbb{Z}_2$ המוגדרת $\varphi(0)=0,\ \varphi(1)=1$ היא אוטומורפיזם מכיוון ש: φ חח"ע ועל ובנוסף גם כפלית $1=\varphi(0+1)=\varphi(0)+\varphi(1)=0+1=1$.

ב. $f:\mathbb{Z}\to\mathbb{Z}_n$ המוגדרת $\forall a\in\mathbb{Z}\ f(a)\equiv a\,(\mathrm{mod}\,n)$

$$f(a+b)=(a+b)\bmod n=$$
$$(a\bmod n+b\bmod n)\bmod n=\ f(a)+f(b)$$

ובנוסף ברור ש f על לכן f הנ"ל היא אפימורפיזם. האם f חח"ע?

ג. האם $\mathbb{Z}_2\times\mathbb{Z}_2\cong\mathbb{Z}_4$? אם קיים איזומורפיזם $\varphi:\mathbb{Z}_2\times\mathbb{Z}_2\to\mathbb{Z}_4$ אזי

$$\varphi((0,1))\varphi((0,1))=\varphi((0,1)+(0,1))=\varphi((0,0))=0$$

כלומר $\varphi((0,1))$ הפכי לעצמו ולכן הוא בהכרח 0 או 2, אבל אם הוא 0 אז הפונקציה לא חח"ע. אם הוא 2, אזי בצורה דומה מראים שגם $\varphi((1,0))=2$ ולכן שוב לא חח"ע. לכן החבורות **לא** איזומורפיות.

ד. נגדיר $G=(\mathbb{R},+,0)$ ו- $H=(\mathbb{R}\setminus\{0\},*,1)$ ואת ההעתקה $\varphi:G\to H$ המוגדרת ע"י $\varphi(x)=e^{x}$. זהו הומומורפיזם $\varphi(x+y)=e^{x+y}=e^{x}e^{y}=\varphi(x)\varphi(y)$. קל לבדוק שזה מונומורפיזם (כלומר חח"ע), אבל לא אפימורפיזם (לא על), כי $\varphi(x)>0$ לכל $x\in\mathbb{R}$.

ה. בין כל שתי חבורות קיים תמיד לפחות הומומורפיזם אחד: $\varphi(G)=e_H$.

ו. בהנתן שתי חבורות $H\subseteq G$ (בעלות אותה פעולה) נגדיר מונומורפיזם "שיכון טבעי" $i:H\to G$ ע"י $i(h)=h$.

ז. תהי G חבורה אבלית. יהי $n\in\mathbb{Z}$ אזי $\varphi(x):=x^{n}$ הוא הומומורפיזם:

$\varphi(xy)=(xy)^n=x^ny^n=\varphi(x)\varphi(y)$.

ח. $\mathbb{R}$ אינו איזומורפי ל $\mathbb{Q}$, כיוון שהקבוצות אינן שוות עצמה, ולכן לא קיימת פונקציה חח"ע ועל ביניהן.

ט. שימו לב שלמרות ש $2\mathbb{Z}<\mathbb{Z}$ מתקיים $\mathbb{Z}\cong 2\mathbb{Z}$, ע"י $f(x)=2x$. (למעשה כבר הערנו שכל החבורות הציקליות האינסופיות הן איזומורפיות ומתקיים $<2>=2\mathbb{Z}$).

<u>תרגילי בית:</u>

1. הוכיחו או הפריכו: א. $l_a(x):=ax$ הוא הומומורפיזם. ב. $c_a(g):=aga^{-1}$ הוא איזומורפיזם.

2. הוכיחו או הפריכו: $f:\mathbb{Z}\to\mathbb{Z}$, המוגדרת ע"י $f(n)=-n$ היא איזומורפיזם.

<u>טענה:</u> $f:G\to H$ היא אפימורפיזם, אזי G אבלית אם ורק אם H אבלית.

<u>הוכחה:</u> יהיו $a,b\in G$ ונסמן $c=f(a),d=f(b)$ אזי

$ab=ba\Leftrightarrow f(ab)=f(ba)\Leftrightarrow f(a)f(b)=f(b)f(a)\Leftrightarrow cd=dc$. בוודאי שזה מתקיים גם לכל $c,d\in H$ כיוון ש f היא על.

<u>תרגיל בית:</u> הראו שאם $f:G\to H$ היא איזומורפיזם אזי G ציקלית אם ורק אם H ציקלית.

<u>טענה:</u> $f:G\to H$ היא הומומורפיזם, אזי $o(f(a))\mid o(a)$ (הסדר של התמונה מחלק את סדר המקור).

<u>הוכחה:</u> $f(a)^{o(a)}=f(a^{o(a)})=f(e)=e$. לפי התרגיל השני בתרגול זה נקבל את הדרוש.

<u>תרגיל בית:</u> הראו שאם $f:G\to H$ היא איזומורפיזם, אזי $o(f(a))=o(a)$.

<u>תרגילי בית:</u>

א. הראו שאם $f:G\to H$ הומ' אזי $\mathrm{Im}(f)=f(G)\le H$.

ב. הראו שאם $f:G\to H$ הוא מונומורפיזם אזי $f(G)\cong G$.

דוגמאות:

א. $\mathbb{Z}$ אינה איזומורפית ל $\mathbb{Q}$, כיוון ש $\mathbb{Z}$ היא חבורה ציקלית, ו $\mathbb{Q}$ היא לא.

ב. הראו שלא קיים שיכון $\mathbb{Q}\times\mathbb{Q}\times\mathbb{Q}...\times\mathbb{Q} = f: GL_3(\mathbb{Q}) \to \mathbb{Q}^{20}$: בוודאי ש $GL_3(\mathbb{Q})$ אינה אבלית, אך אם קיים שיכון (מונומורפיזם), אזי $\text{Im}(f) \le \mathbb{Q}^{20}$ אבל כל תת-חבורה של חבורה אבלית היא אבלית, ולכן $GL_3(\mathbb{Q}) \cong \text{Im}(f)$ היא אבלית, סתירה.

תרגילי בית:

א. $\mathbb{Q}^*$ אינה איזומורפית ל $\mathbb{Q}$ (הבדילו בין החבורות לפי סדרי האיברים בחבורות, כלומר השתמשו בתרגיל הבית הקודם ע"מ להפריך).

ב. השתמשו באותה שיטה כמו בא. כדי להוכיח בדרך אחרת ש- $\mathbb{Z}_2\times\mathbb{Z}_2 \ncong \mathbb{Z}_4$.

<u>תרגול 5</u>

<u>כפל (פנימי) :</u>

<u>הגדרה</u>: בהנתן $H,K \subseteq G$ (שתי תת קבוצות, לאו דווקא ת"ח) נגדיר **מכפלה של תת-קבוצות** $HK := \{hk \mid h \in H, k \in K\}$. שימו לב שאם $H,K \leq G$ אזי $HK \subseteq G$ אך המכפלה אינה בהכרח תת-חבורה.

<u>הערה:</u> במקרה ו- G חבורה חיבורית, נהוג לרשום $H+K=\{h+k \mid h \in H, k \in K\}$ במקום HK .

<u>דוגמא:</u>
$G=S_3$. ניקח $H=<(1,2)>$, $K=<(2,3)>$. אזי $HK=\{id,(1,2),(2,3),(1,2,3)\}$. זאת לא חבורה כיוון שלאיבר (1,2,3) אין הפכי בקבוצה (למעשה גם אין סגירות לכפל, כפי שהראינו בתרגול).

<u>משפט:</u> בהנתן $H,K \leq G$, $HK \leq G \Leftrightarrow HK=KH$.

<u>מסקנה:</u> אם $HK=G$ אזי $HK=KH$.

<u>משפט:</u> בהנתן $H,K \leq G$, $|HK|=\frac{|H||K|}{|H \cap K|}$.

<u>סימון:</u> במכפלה של תתי-קבוצות, אם אחת הקבוצות היא איבר בודד אז נהוג להשמיט את הסוגריים: $aH:=\{a\}H, Ha:=H\{a\}$. אם החבורה היא חיבורית, רושמים $a+H$.

<u>תרגיל:</u> תהי H חבורה הוכח: $HH=H$

<u>הוכחה:</u> נוכיח ע"י הכלה דו כיוונית:

1. ($\subseteq$) יהי $x \in HH$ אז $s,t \in H$ $x=st$ ומכיוון ש H חבורה היא סגורה לכפל לכן $x \in H$ ובפרט $HH \subseteq H$.
2. ($\supseteq$) יהי $y \in H$ אז $e \in H, y \in H \Rightarrow y=ey \in HH$ ולכן $H \subseteq HH$.

לפי 1 ו2 נקבל $HH = H$ □

<u>תרגיל בית:</u> הראו שכפל של תת-קבוצות הוא אסוציאטיבי.

<u>הערה:</u> מהתרגילים הנ"ל נקבל ש- P(G) (קבוצת החזקה של G) היא מונואיד. שימו לב שקבוצת תת-החבורות של G לאו דווקא מונואיד (לפי הדוגמא לעיל). אך יש מקרים פרטיים בהם זה כן מתקיים.

<u>תרגיל בית:</u> הראו שאם G חבורה אבלית, אזי קבוצת התת-חבורות של G הוא מונואיד. האם הוא חבורה?

<u>מחלקות בחבורה:</u>

<u>מחלקות ימניות ושמאליות:</u>

<u>הגדרה:</u> תהי G חבורה $H \leq G$ **ויהי** $a \in G$

מחלקה שמאלית מוגדרת ע" $aH := \{ah \mid h \in H\}$.

מחלקה ימנית מוגדרת ע"י $Ha := \{ha \mid h \in H\}$.

<u>דוגמא:</u> $a = 2$ $H = 6\mathbb{Z}$ $G = \mathbb{Z}$ ונקבל ש

$$2 + 6\mathbb{Z} = 6\mathbb{Z} + 2 = \{\ldots, -10, -4, 2, 8, 14, \ldots\}$$

<u>משפט:</u> אם $H \leq G$ $a, b \in G,$ אז מתקיים:

א. $aH = bH$ או $aH \bigcap bH = \varnothing$ כלומר כל 2 מחלקות שמאליות (ימניות) זהות או זרות.

ב. $aH = H$ אם ורק אם $a \in H$.

<u>תרגיל:</u> הראו שמחלקה gH היא חבורה אם ורק אם $g \in H$.

<u>פתרון:</u> אם $g \in H$ אזי $gH = H$ כי הכפלה באיבר משמאל היא חח"ע ועל (כפי שראינו בתרגול הראשון). אם gH היא חבורה, אז $e \in gH$ ולכן קיים $h \in H$ כך ש $gh = e$, ולכן $g = h^{-1} \in H$.

כלומר $g \in gH \cap H$ ולכן לפי המשפט הנ"ל, נקבל $gH = H$.

משפט: $H \le G$ $a,b \in G$ אז $aH = bH \Leftrightarrow b^{-1}a \in H$. עבור מחלקות ימניות: $Ha = Hb \Leftrightarrow ab^{-1} \in H$. היחס $a \sim b \Leftrightarrow b^{-1}a \in H$ הוא יחס שקילות. מחלקות השקילות הן בדיוק המחלקות השמאליות.

מסקנה: $G = \coprod xH$ $H \le G$ (כאשר $\coprod$ הוא איחוד זר שעובר על נציגי כל המחלקות השמאליות).

תרגיל בית: תהי $H \le G$ הוכיחו: $g_2 \in Hg_1 \Leftrightarrow Hg_2 = Hg_1$

הגדרה: תהי G חבורה, ותהי X תת-קבוצה של G, אזי $X^{-1} := \{x^{-1} \mid x \in X\}$.

תרגיל בית: הוכיחו או הפריכו: במונואיד הכפלי של תת-קבוצות של G, X^{-1} הוא ההפכי של X. רמז: מהו H^{-1} עבור $H \le G$.

תרגיל: $(Hg)^{-1} = ?$

פתרון:
$$(Hg)^{-1} = \{(hg)^{-1} \mid h \in H\} = \{g^{-1}h^{-1} \mid h \in H\} = \{g^{-1}h \mid h \in H\} = g^{-1}H$$

משפט: קיימת התאמה חח"ע (פונקציה חח"ע ועל):

{מחלקות שמאליות}$\leftrightarrow${מחלקות ימניות}

המוגדרת ע"י $gH \mapsto Hg^{-1}$.

תרגיל בית: האם $gH \mapsto Hg$ היא התאמה חח"ע כנ"ל?

משפט: אם $H \le G$ ת"ח **סופית** אז לכל מחלקה xH מתקיים $|xH| = |H|$.

הגדרה: $[G:H]$ הוא מס' המח' הימניות (השמאליות) של H ב G נקרא האינדקס של H ב G.

! משפט לגראנז' (נוסח א') : תהי G **סופית** ו- $H \le G$ אז $|G| = [G:H]|H|$

! משפט לגראנז' (נוסח ב'): תהי G **סופית** ו- $H \le G$ אז $|H|\,|\,|G|$ כלומר סדר התת-חבורה מחלק את סדר החבורה.

מסקנה חשובה ממשפט לגרנג':

יהיו $K \le H \le G$ ת"ח. אזי $[G:K] = [G:H][H:K]$.

תרגיל: $|G| = 20$. לפי משפט לגראנז' איזה סדר אפשרי לתתי החבורות של G ?

פתרון: סדר התת-חבורה מחלק את סדר החבורה לכן סדר התתי חבורות של G חייב לחלק את 20 ולכן הסדרים האפשריים הם: 1,2,4,5,10,20. אלה גם הסדרים היחידים האפשריים עבור איברים ב G, כפי שנראה במשפט הבא.

תרגיל בית: אותה שאלה עם שינוי קטן. תהי $H \le G$ כאשר ידוע שב- H יש איבר מסדר 2, מהם הסדרים האפשריים של H? (פתרו שאלה זו אחרי התרגילים בעמוד הבא).

משפט: תהי G סופית ו- $g \in G$ אז $o(g)\,|\,|G|$ כלומר סדר איבר בחבורה סופית מחלק את סדר החבורה. (ההוכחה מיידית לפי משפט לגרנג' והגדרת סדר של איבר).

מסקנה: לכל איבר $g \in G$ מתקיים $g^{|G|} = e$.

הוכחה: לפי המשפט $o(g)\,|\,|G|$ ולכן $\frac{|G|}{o(g)}$ הוא מספר שלם. אם כך מתקיים

$(g^{o(g)})^{\frac{|G|}{o(g)}} = e^{\frac{|G|}{o(g)}} = e$.

המשפט הקטן של פרמה:

יהי $p > 0$ מס' ראשוני לכל מס' שלם a מתקיים $a^p \equiv a \bmod p$

הוכחה: הסדר של חבורת אוילר הוא $p-1 = |Euler(p)| = \varphi(p)$ (מדוע?).

לכן לפי המסקנה לעיל, נקבל שעבור $a\neq 0$ מתקיים $a^{\varphi(p)}=a^{p-1}=e$. נכפיל את שני האגפים ב- a , ונקבל $a^p=a$. כעת נשאר להוכיח עבור המקרה של $a=0$, אבל זה ברור.

<u>דוגמא:</u> $3^7\equiv 3 \bmod 7$.

<u>תרגיל בית:</u> כל חבורה מסדר p ראשוני היא ציקלית (ובפרט אבלית).

<u>תרגיל:</u> הראו שחבורה היא מסדר זוגי אם ורק אם קיים בה איבר מסדר 2.

<u>הוכחה:</u> <= אם אין איברים מסדר 2, אז ניתן להצמיד כל איבר להפכי שלו (שהוא איבר שונה ממנו). ביחד עם איבר היחידה, נקבל מספר אי-זוגי.

=> אם קיים איבר מסדר 2 אז לפי לגרנג' (או המשפט בתחילת העמוד) הסדר שלו (2) מחלק את סדר החבורה, ולכן סדר החבורה הוא זוגי.

<u>תרגיל:</u> תהי G חבורה מסדר $2p$ (p ראשוני) אז יש ל G איבר מסדר p (בפרט תת חבורה מסדר p).

<u>הוכחה:</u>

נפטר קודם מהמקרה p=2. אם p=2 אזי G חבורה מסדר 4, ולכן היא בהכרח איזומורפית ל $\mathbb{Z}_2\times\mathbb{Z}_2$ או ל $\mathbb{Z}_4$ (ראינו שאלה טבלאות הכפל היחידות האפשריות לחבורה מסדר 4). בשני המקרים קיימים איברים מסדר 2 (בדקו).

כעת נניח ש p ראשוני אי-זוגי.

לפי משפט לגראנז' הסדרים האפשריים של איברים הם: $1,2,p,2p$.

אם יש איבר מסדר p אז סיימנו ואם יש איבר a מסדר $2p$ אז גם כן סיימנו כי $(a^2)^p=a^{2p}=e\Rightarrow o(a^2)\leq p$. נשתמש כעת בתרגיל מתרגול קודם, האומר שאם $a^n=e$ אזי $n\,|\,o(a)$: לכן לפי הנ"ל נקבל ש $o(a^2)\,|\,p$, אבל לא ייתכן ש $o(a^2)=1$ כי אז $o(a)\leq 2$ ונקבל סתירה להנחה ש $o(a)=2p>2$. לכן בהכרח $o(a)=p$.

כעת נניח בשלילה שכל האיברים בחבורה הם מסדר 2 (פרט לאיבר היחידה מסדר 1).

כבר ראינו בתרגול הראשון שחבורה כזאת בהכרח אבלית.

לכן החבורה G אבלית וכיוון שיש לפחות שני איברים שונים מסדר > 1, קיימת ל G תת חבורה $\{1,a,b,ab\}$ האיזומורפית לחבורת קליין ($\mathbb{Z}_2\times\mathbb{Z}_2$) **[הוכיחו את זה]** ולכן נקבל לפי לגראנז' ש $4\,|\,2p$ סתירה לכן קיים איבר מסדר p או $2p$ □

תת חבורות נורמליות:

הגדרה: תהי G חבורה ו $H \le G$ אם לכל $g \in G$ מתקיים $gH = Hg$ אז H נקראת תת חבורה נורמלית של G והיא תסומן ע"י $H \lhd G$.

משפט: התנאים הבאים שקולים:

1. $H \lhd G$
2. $\forall g \in G\ gHg^{-1} = H$
3. $\forall h \in H, \forall g \in G, g^{-1}hg \in H$ או במילים אחרות מספיק להוכיח ש: $\forall g \in G, gHg^{-1} \subseteq H$.

דוגמא:

לא כל ת"ח היא נורמלית. לדוגמא: $G = S_3$, $H = \{Id, (1\quad 2)\}$

טענה: H לא תת חבורה נורמלית של G .

הוכחה: $(1\quad 2\quad 3) \in G, (1\quad 2\quad 3)^{-1} = (1\quad 3\quad 2)$

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

ולכן H לא תת חבורה נורמלית של G .

דוגמא: אם G חבורה אבלית אז כל תת חבורה שלה היא נורמלית כי $ghg^{-1} = h$ $\Leftarrow$ $gHg^{-1} = H$.

תרגיל בית: הראו (ללא שימוש במשפטים בהמשך התרגול) שאם $H \lhd G$ אזי לכל $g \in G$ מתקיים $< g > H \le G$.

הגדרה: תהי G חבורה כלשהי אז **המרכז של** G מוגדר כ:

$$Z(G) = \{g \in G \mid \forall x \in G \qquad gx = xg\}$$

כלומר המרכז היא קבוצת כל האיברים G שמתחלפים עם כל אברי G .

דוגמא: אם G אבלית אז $Z(G)=G$

משפט: $Z(G)\le G$. (תרגיל בית)

משפט: $Z(G)\triangleleft G$ (קל להוכיח לפי הגדרה)

תרגיל: יהי $A,B\triangleleft G$ הוכח: $A\bigcap B\triangleleft G$ (כלומר חיתוך של תתי חבורות נורמליות הוא תת חבורה נורמלית).

הוכחה: לפי משפט $A\bigcap B\le G$ נותר להוכיח ש $gA\bigcap Bg^{-1}=A\bigcap B$ נוכיח זאת לפי ההגדרות

$$g(A\bigcap B)g^{-1}=\{gxg^{-1}\mid x\in A\bigcap B\}=\{gxg^{-1}\mid x\in A\wedge x\in B\}$$
$$=\{gxg^{-1}\mid x\in A\}\bigcap\{gxg^{-1}\mid x\in B\}=A\bigcap B\square$$

תרגיל: תהי $H\le G$ $[G:H]=2$ הוכח: $H\triangleleft G$

הוכחה: מכיוון ש $[G:H]=2$ אז קיימות רק 2 מחלקות שמאליות אחת מהן שווה ל $eH=H$ והאחרת שווה ל aH (לכל $a\in G\setminus H$) ומתקיים $G=H\dot{\bigcup}aH$ (איחוד זר) באופן דומה עבור המחלקות ימניות מתקיים $G=H\dot{\bigcup}Ha$ ולכן נקבל $aH=Ha$. $\square$

הגדרה: **גרעין** של הומ' φ מוגדר כ:

$$\ker(\varphi)=\{g\in G\mid\varphi(g)=e_H\}$$

הגדרה: **תמונה** של העתקה מוגדרת כ:

$$\mathrm{Im}(\varphi)=\{h\in H\mid\exists g\in G,\varphi(g)=h\}$$

משפט: $K\mathrm{er}\,\varphi\le G$ ו $\mathrm{Im}\,\varphi\le H$.

משפט: $\ker\varphi\triangleleft G$

הערה: המשפט הנ"ל מספק תנאי מספיק נוסף לכך שת"ח היא נורמלית. אם $H \le G$ ונצליח למצוא חבורה K כך שקיים הומ' $\varphi: G \to K$ כך שהגרעין הוא בדיוק H, אזי H היא תח"נ של G.

נראה דוגמא לכך בתרגיל הבא:

תרגיל:

נגדיר $\bar{A} := \{(a, e_B) \mid a \in A\}$, $\bar{B} := \{(e_A, b) \mid b \in B\}$

אזי הוכיחו שמתקיים $\bar{A}, \bar{B} \lhd A \times B$.

הוכחה:

$$\pi_A : A \times B \to A, \pi_A((a,b)) = a$$
$$\pi_B : A \times B \to B, \pi_B((a,b)) = b$$

מהו הגרעין של האיזומורפיזם π_A ? תשובה: $\ker \pi_A = \bar{B}$ לכן $\bar{B} \lhd A \times B$ באותו אופן מוכיחים $\bar{A} \lhd A \times B$.

תרגיל בית: הוכיחו או הפריכו: $\operatorname{Im} \varphi \lhd H$.

משפט: φ חח"ע ערכית $\Leftrightarrow$ $\ker \varphi = \{e_G\}$

הוכחה: נשתמש במשפט שהומומורפיזם מעביר יחידה ליחידה כלומר:

$$\varphi(e_G) = e_H$$

$(\Leftarrow)$ נניח φ חח"ע נניח בשלילה ש $\ker \varphi \ne \{e_G\}$ לכן קיים $e_G \ne x \in G, \varphi(x) = e_H$ אבל $\varphi(x) = \varphi(e_G)$ לכן לפי ש φ חח"ע נקבל $x = e_G$ סתירה! לכן $\ker \varphi = \{e_G\}$

$(\Rightarrow)$ אם $\ker \varphi = \{e_G\}$ אז מתקיים

$$a, b \in G \qquad \varphi(a) = \varphi(b) \Rightarrow \varphi(a)\varphi(b)^{-1}$$
$$= \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) = e_H$$

לכן $a = b \Leftrightarrow ab^{-1} = e_G \Leftrightarrow ab^{-1} \in \ker \varphi$ לכן לפי הגדרה φ חח"ע □

הגדרה: יהיו $a, g \in G$ איברים בחבורה, אזי נקרא לאיבר gag^{-1} **הצמוד** של a ע"י g.

הערה: ע"פ אחד מהתנאים השקולים לנורמליות (נקרא לו מעתה קריטריון הנורמליות) שראינו בתרגול הקודם, אם ת"ח H **סגורה להצמדה** ב G, אזי היא נורמלית. מה הכוונה בסגורה להצמדה:

$$\forall g\in G,\forall h\in H, ghg^{-1}\in H$$

אומרים גם ש H אינוריאנטית (נשמרת) תחת פעולת ההצמדה.

<u>תרגיל:</u> יהיו $N,H\le G$ תתי חבורות. הוכיחו שאם $N\lhd G$ אז $NH\le G$. (שימו לב שלא בהכרח $NH\lhd G$).

<u>פתרון:</u> מספיק להוכיח ש- $NH=HN$ לפי משפט מתחילת התרגול הקודם. יהי $x\in NH$, ואז $x=ab$ כך ש $a\in N,b\in H$. לפי נורמליות N, מתקיים $Nb=bN$ ולכן קיים $a'\in N$ כך ש $ab=ba'\in HN$. לכן $NH\subseteq HN$. בצורה דומה מראים הכלה בכיוון השני.

<u>תרגיל:</u>

יהיו $N,H\le G$ תתי חבורות. הוכיחו שאם $N\lhd G,H\lhd G$ אז $NH\lhd G$.

<u>הוכחה:</u> $NH\le G$, לפי התרגיל הקודם. נותר לכן להוכיח את הנורמליות

$$\forall g\in G, g^{-1}(nh)g=g^{-1}ngg^{-1}hg=$$
$$(g^{-1}ng)(g^{-1}hg)\underset{N,H\lhd G}{=}\bar{n}\bar{h}\in NH$$

לכן לפי קריטריון הנורמליות מהתרגול הקודם נקבל ש $NH\lhd G$.

<u>תרגיל:</u>

תהי G חבורה כלשהי, ותהי $H\le G$ התת חבורה הנוצרת על ידי כל הריבועים של איברי G.

הוכח: $H\lhd G$.

<u>הוכחה:</u> כשאנו אומרים חבורה נוצרת ע"י איברים ת $g_1,g_2,...,g_n,...$ אז כל איבר בחבורה הוא מכפלה סופית של איברים אלו ושל הפכיהם במקרה שלנו

מתקיים $h\in H, g_i\in G, h=g_1^2*g_2^2*...*g_n^2$

אז לכל
$$a\in G, aha^{-1}=a^{-1}g_1^2g_2^2...g_n^2a=(a^{-1}g_1^2a)(a^{-1}g_2^2a)...*(a^{-1}g_n^2a)=$$
$$(a^{-1}g_1a)^2(a^{-1}g_2a)^2...*(a^{-1}g_na)^2\in H$$
ולכן לפי קריטריון הנורמליות קיבלנו $H\lhd G$ $gHg^{-1}\subseteq H\Rightarrow$ כנדרש.

נספח: תרגילים נוספים על תח"נ:

תרגיל:

$N \lhd G$ ויהי $g \in G$. הראה כי לכל $n \in N$ קיים $\bar{n} \in N$ כך ש $gn = \bar{n}g$.

פתרון: לפי הגדרה $N \lhd G$ לכן $\forall g \in G, gN = Ng$ כלומר לכל $\forall n \in N$ מתקיים

$$gn \in gN \underset{gN=Ng}{\Rightarrow} gn \in Ng \Rightarrow \exists \bar{n}, gn = \bar{n}g \quad \square$$

תרגיל:

תהי G חבורה ויהי $N \lhd G, H \leq G$ הוכח כי $N \bigcap H \lhd H$

פתרון: הוכחנו כי חיתוך של שני תתי חבורות היא תת חבורה, ולכן $N \bigcap H \leq H$. נשאר להוכיח רק שהיא תת חבורה נורמלית $h \in H \bigcap N \Leftrightarrow h \in H \wedge h \in N$ מכיוון ש N תת חבורה נורמלית אז $\forall g \in G \supseteq H, gNg^{-1} = N$ וכמו כן H תת חבורה לכן היא סגורה לכפל ולהופכי לכן $\forall g \in H, ghg^{-1} \in H$ וקיבלנו ש $\forall h \in H \bigcap N, \forall g \in H, g(H \bigcap N)g^{-1} \subseteq H \bigcap N$. מצד שני

$$\forall g \in H, h \in H \bigcap N, h \in N = gNg^{-1} \Rightarrow \exists n \in N, h = gng^{-1}$$
$$n = g^{-1}hg \in H \Rightarrow n \in H \bigcap N \Rightarrow h \in g(H \bigcap N)g^{-1}$$

ולכן $g(H \bigcap N)g^{-1} \supseteq H \bigcap N$ $\forall g \in H$ לכן $\forall g \in H, g(H \bigcap N)g^{-1} = H \bigcap N$ ולכן $H \bigcap N \lhd H \square$

תרגיל:

תהיינה $M, N \lhd G$ שמקיימות $N \bigcap M = \{e\}$. הוכח: כי לכל $n \in N, m \in M$ מתקיים $nm = mn$

פתרון: נגדיר איבר ונוכיח שהוא בחיתוך $a = n^{-1}m^{-1}nm = n^{-1}(m^{-1}nm) = (n^{-1}m^{-1}n)m$

מה קיבלנו? $N \lhd G$ לכן $x = m^{-1}nm \in N$ ולכן בגלל ש N תת חבורה ולכן סגורה לכפל נקבל $a = n^{-1}x \in N$.

כמו כן $M \lhd G$ לכן $y = n^{-1}m^{-1}n \in M$ ולכן בגלל ש M תת חבורה וסוגרה לכפל נקבל $a = ym$

. ואיזה יופי הוכחנו ש $a \in N \bigcap M = \{e\} \Rightarrow a = e$

ולכן $n^{-1}m^{-1}nm = e \underset{mn}{\Rightarrow} nm = mn \square$

תרגול 6

חוסר טרנזיטיביות של נורמליות:

כאשר אנו מדברים על תת-חבורות, טבעי לרשום שרשרת של הכלות של תתי-חבורות בצורה $H \le K \le J \le ... \le G$. אין בעיה בצורת רישום זאת, כיוון שיחס $\le$ ("תת-חבורה של") הוא יחס טרנזיטיבי. כלומר למעלה $H \le K$ וגם $K \le J$ ולכן $H \le J$.

כשאנחנו משתמשים ברישום דומה עבור תח"נ ($H \lhd K \lhd J \lhd ... \lhd G$) צריך מאד להזהר, כיוון שיחס $\lhd$ אינו טרנזיטיבי.

דוגמא: (נראה דוגמא בה אין טרנזיטיביות של $\lhd$)

נציג חבורה בעזרת יוצרים ויחסים (ראו תרגול 4).

$$G = \langle a, x \mid a^4 = x^2 = e, xax = a^{-1} \rangle$$

$$= \{e, a, a^2, a^3, x, ax, a^2x, a^3x\}$$

תרגיל בית: הראו שאין עוד איברים ב G, וכל הנ"ל איברים שונים זה מזה (רמז: כל איבר ב G הוא מהצורה $a^k x^t$ או $x^t a^k$).

$$H_1 = \langle x \rangle, \qquad H_2 = \langle a^2 x \rangle, \qquad K = \langle x, a^2 \rangle$$

תרגיל בית: חשבו את החבורות H_1, H_2, K .

כעת $K \lhd G$ כיוון ש $[G:K] = 2$ (לפי תרגיל בתרגול הקודם, כל ת"ח מאינדקס 2 היא נורמלית). בנוסף גם $H_1 \lhd K$ מאותה סיבה. אך $H_1 \ntriangleleft G$ כיוון ש $axa^{-1} = axa^3 = a^2x \notin H_1$ (לכן H_1 אינה סגורה להצמדה, ולכן לפי קריטריוני הנורמליות שהצגנו בתרגול הקודם, היא אינה נורמלית ב G).

תרגיל בית: הראו ש $H_2 \ntriangleleft G$.

לסיכום: מותר לכתוב שרשראות כגון $K \lhd H \lhd G$ אבל חשוב להבין שאין בהכרח טרנזיטיביות.

<u>חבורת המנה</u>

<u>! משפט:</u> יהי $H \lhd G$ קבוצת המחלקות $\{aH \mid a \in G\}$ עם כפל תתי קבוצות של G ($aHbH = abH$) מהווה חבורה.
כלומר לקחנו תת-חבורה נורמלית ויצרנו בעזרתה ובעזרת החבורה המקורית חבורה חדשה חבורה זו נקראת **חבורת המנה**.

<u>הערה:</u>
שימו לב שהגדרת הכפל הזאת הגיונית רק במקרה ש H נורמלית ב G, אחרת כלל לא ודאי שמתקיים $aHbH = abH$.

תרגיל בית: מצאו חבורה G ותת חבורה H כך שכפל של שתי מחלקות שמאליות אינו מחלקה שמאלית.
יש להראות שהכפל מוגדר היטב. מה הכוונה? שפעולת הכפל היא חד ערכית, כלומר אם $aH = cH, bH = dH$ אזי $aHbH = cHdH$.

תרגיל בית: הראו שהכפל מוגדר היטב ע"פ תכונות של מחלקות שמאליות.

<u>סימון:</u> יהי $H \lhd G$ אז **חבורת המנה** תסומן ע"י:

$$G/H = \{aH \mid a \in G\}$$

<u>משפט:</u> $|G/H| = [G:H] = \frac{|G|}{|H|}$

<u>הוכחה:</u> לפי משפט לגרנז'

<u>משפט:</u> אם $K \lhd H \lhd G$ וגם $K \lhd G$ אזי $|G/K| = |G/H||H/K|$.

<u>הוכחה</u>: לפי מסקנה ממשפט לגרנג'

דוגמאות:

1. $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$.

איך ניתן להראות זאת (נראה דרך קלה יותר בהמשך בעזרת משפטי האיזומורפיזם)? מספיק להראות ש $\mathbb{Z}/n\mathbb{Z}$ היא ציקלית מסדר n, וכידוע כל חבורה ציקלית מסדר n היא איזומורפית ל $\mathbb{Z}_n$.

בדקו כעת ש $1+n\mathbb{Z}$ יוצר את $\mathbb{Z}/n\mathbb{Z}$ והוא מסדר n.

2. $\mathbb{Z}_n/m\mathbb{Z}_n\cong\mathbb{Z}_m$, כאשר m|n.

בודקים בצורה דומה ש $1+m\mathbb{Z}_n$ יוצר את החבורה. כאן קל להוכיח שהסדר של $\mathbb{Z}_n/m\mathbb{Z}_n$ הוא m: משתמשים במשפט $|\mathbb{Z}_n/m\mathbb{Z}_n|=[\mathbb{Z}_n:m\mathbb{Z}_n]=\frac{|\mathbb{Z}_n|}{|m\mathbb{Z}_n|}=\frac{n}{n/m}=m$.

תרגיל:

הראו ש $\mathbb{R}^*/\mathbb{R}^{*2}$ היא חבורה סופית.

הוכחה:

נרצה לבדוק "מהי" חבורת המנה $\mathbb{R}^*/\mathbb{R}^{*2}$ (כלומר אם אנחנו יכולים לזהות אותה – עד כדי איזומורפיזם – עם חבורה אחרת שאנו מכירים). נזכור ששני איברים a,b הם שקולים במנה אם ורק אם $b^{-1}a=\frac{a}{b}\in\mathbb{R}^{*2}$. נשים לב ש $\mathbb{R}^{*2}=\mathbb{R}^{*>0}$ (המספרים הממשיים החיוביים), ולכן נסיק ששני איברים הם שקולים אם הם בעלי אותו סימן, לכן יש רק שתי מחלקות שקילות, האיברים החיוביים והאיברים השליליים. כבר ראינו שהחבורה היחידה עם שני איברים היא $\mathbb{Z}_2$ ולכן $\mathbb{R}^*/\mathbb{R}^{*2}\cong\mathbb{Z}_2$.

תרגיל:

הראו ש $\mathbb{Q}^*/\mathbb{Q}^{*2}$ היא חבורה אינסופית.

הוכחה:

אם ניקח $\mathbb{Q}$ במקום $\mathbb{R}$ נקבל חבורה אחרת לגמרי. בחבורה $\mathbb{Q}^*/\mathbb{Q}^{*2}$ נקבל ששני איברים a,b הם שקולים במנה אם ורק אם $b^{-1}a=\frac{a}{b}\in\mathbb{Q}^{*2}$. אבל $\frac{a}{b}\in\mathbb{Q}^{*2}\Leftrightarrow(\frac{a}{b})b^2=ab\in\mathbb{Q}^{*2}$. אם ניקח

a,b מספרים ראשוניים שניים, נקבל שהם שקולים אם ורק אם $ab \in \mathbb{Z}^{*2}$, אבל זה בלתי אפשרי כי מכפלת ראשוניים שונים היא לעולם לא ריבוע.

לכן יש אינסוף מחלקות שקילות, כלומר $\left|\mathbb{Q}^* / \mathbb{Q}^{*2}\right| = \infty$. קל לראות שכל האיברים בחבורה הם מסדר 2 (כי מספר בריבוע הוא ריבוע). ניתן להוכיח ש $\mathbb{Q}^* / \mathbb{Q}^{*2} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times ...$.

<u>תרגיל:</u>

<u>תרגיל ממבחן תשס"ז, מועד ב':</u>

א. הוכיחו שלחבורת המנה $\mathbb{Q}/\mathbb{Z}$ אין תת-חבורה איזומורפית ל- $\mathbb{Z}$.

ב. הוכיחו שהחבורה $\mathbb{Q}/\mathbb{Z}$ אינה נוצרת סופית.

<u>פתרון:</u>

א. כל איבר ב $\mathbb{Q}/\mathbb{Z}$ הוא מהצורה $\frac{m}{n}+\mathbb{Z}$. האיבר $\frac{m}{n}+\mathbb{Z}$ הוא מסדר שמחלק את n, כיוון ש $n(\frac{m}{n}+\mathbb{Z}) = \frac{nm}{n}+\mathbb{Z} = m+\mathbb{Z} = \mathbb{Z}$. לכן כל האיברים ב- $\mathbb{Q}/\mathbb{Z}$ הם מסדר סופי, ואם היתה ת"ח איזומורפית ל $\mathbb{Z}$ אזי היה איבר מסדר אינסופי היוצר אותה.

ב. כיוון שכל איבר בחבורה הוא מסדר סופי, והחבורה היא אבלית, נקבל שהת"ח הנוצרת מקבוצה סופית של איברים היא סופית, וב- $\mathbb{Q}/\mathbb{Z}$ יש אינסוף איברים (לדוגמא $\{\frac{1}{2^n}+\mathbb{Z} \mid n \in \mathbb{N}\}$, **הראו שכל האיברים בקבוצה שונים זה מזה**).

<u>משפטי איזומורפיזם</u>

<u>! משפט איזומורפיזם 1:</u> תהיינה G,H חבורות ותהי $\varphi : G \to H$ אפימורפיזם אז $G/\ker\varphi \cong H$.

אם φ היא הומומורפיזם (לא בהכרח אפימורפיזם) אז $G/\ker\varphi \cong \operatorname{Im}\varphi$.

<u>משפט:</u> כל ת"ח נורמלית היא גרעין של הומומורפיזם.

<u>הוכחה:</u> ההומ' הוא $\pi : G \to G/N$ המוגדר ע"י $\pi(g) = gN$.

הומומורפיזם זה נקרא **ההומומורפיזם הטבעי**. בדקו: π הוא אפימורפיזם, והגרעין הוא N.

<u>דוגמאות:</u>

1. $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$. ניתן לראות זאת ממשפט האיזו' הראשון:
   נגדיר $\varphi:\mathbb{Z}\to\mathbb{Z}_n$ ע"י $\varphi(x)=x \pmod n$. בדקו ש $\varphi:\mathbb{Z}\to\mathbb{Z}_n$ אפימורפיזם, והגרעין הוא בדיוק $n\mathbb{Z}$.

2. $\mathbb{Z}_n/m\mathbb{Z}_n\cong\mathbb{Z}_m$. תרגיל בית: הגדירו אפימורפיזם מתאים, במקרה זה יש לבדוק שהוא מוגדר היטב, והוכיחו שהגרעין שלו הוא בדיוק $m\mathbb{Z}_n$, נראה בהמשך שניתן להוכיח את הטענה הזו גם בעזרת משפט איזו' 3.

<u>תרגיל:</u> הוכח כי $(\mathbb{R}^*)^+\cong\mathbb{C}^*/S^1$ כאשר $S^1:=\{z\in\mathbb{C}^* \mid |z|=1\}$

<u>הוכחה:</u> הרעיון של ההוכחה:מגדירים העתקה בין $(\mathbb{R}^*)^+$ ל $\mathbb{C}^*$ כך ש S^1 הגרעין וכך בעזרת משפט האיזו' 1נ מוכחים את הטענה.

גדיר העתקה מ $\varphi:\mathbb{C}^*\to(\mathbb{R}^*)^+$ ע"י: $\varphi(z)=|z|$

$$\ker\varphi=\{z\in\mathbb{C}^* \mid \varphi(z)=|z|=1\}=S^1$$

כעת כדי להוכיח את הטענה נשאר רק להוכיח ש φ אפימורפיזם.

1. נוכיח ש φ הומומורפיזם:
   $\varphi(z_1z_2)=|z_1z_2|=|z_1||z_2|=\varphi(z_1)\varphi(z_2) \quad \forall z_1,z_2\in\mathbb{C}^*$
2. φ היא על כי
   $\varphi(r)=r \quad \forall r\in(R^*)^+$ לכן φ היא על

והוחנו ש φ היא אפימורפיזם ולכן לפי משפט האיזומורפיזם 1 נקבל

$$(\mathbb{R}^*)^+\cong\mathbb{C}^*/S^1 \quad \square$$

<u>תרגיל:</u>

$N\lhd G$ ויהי $a\in G$ איבר מסדר סופי. הוכח כי הסדר של $aN\in G/N$ מחלק את הסדר של a .

<u>הוכחה:</u> ניתן לבדוק זאת ישירות, או: מיידי מההומ' הטבעי: $\pi(a)=aN$ וידוע שסדר התמונה מחלק את סדר המקור (ראינו בתרגול קודם).

<u>משפט איזמורפיזם 2:</u> תהי G חבורה $N \lhd G, H \le G$ אז:

1. $H \bigcap N \lhd H$
2. $H / H \bigcap N \cong HN / N$

<u>תרגיל:</u> תהי G חבורה סופית ויהיו $N, M \lhd G$, $H \le G$ נניח כי $H \bigcap M = H \bigcap N = \{e\}$.

הוכח כי: $HM / M \cong HN / N$

<u>הוכחה:</u> $M, N \lhd G$ לכן $HM, HN \le G$ (הוכחה תרגיל בית)לפי משפט האיזומורפיזם 2 נקבל:

$HM / M \cong H / H \bigcap M = H / \{e\} = H$ ומסיבות סימטריה נקבל: $HN / N \cong H$ ולכן מטרנזיטיביות

האיזומורפיזם נקבל $HM / M \cong HN / N$□

<u>משפט איזומורפיזם 3 (משפט הצמצום):</u>

תהיינה G חבורה $N \lhd K \lhd G$ וגם $N \lhd G$, אזי $K/N \lhd G/N$ ומתקיים $\dfrac{G/N}{K/N} \cong G/K$.

<u>דוגמא:</u>

נראה (שוב, אך הפעם בעזרת איזו' 3) ש $\mathbb{Z}_6 / 3\mathbb{Z}_6 \cong \mathbb{Z}_3$:

נסתכל על השרשרת של תח"נ: $6\mathbb{Z} \lhd 3\mathbb{Z} \lhd \mathbb{Z}$. לפי משפט איזו 3 נקבל:

$$\mathbb{Z}_3 \cong \mathbb{Z} / 3\mathbb{Z} \cong (\mathbb{Z} / 6\mathbb{Z}) / (3\mathbb{Z} / 6\mathbb{Z}) \cong \mathbb{Z}_6 / 3\mathbb{Z}_6$$

(למעשה האיזומורפיזם הזה ברור כי יש רק חבורה אחת מסדר 3).

האיזומורפיזם הכי ימני נובע מכך ש: $\mathbb{Z} / 6\mathbb{Z} \cong \mathbb{Z}_6$ לפי איזו' 1, וגם לפי איזו 1 ניתן להראות את $3\mathbb{Z} / 6\mathbb{Z} \cong 3\mathbb{Z}_6$ (בדקו זאת!). **שימו לב:** צריך להזהר כאן, כיוון שזה לא תמיד נכון שמתקיים $G / H \cong K / L$ כאשר $G \cong K \wedge H \cong L$ (מצאו דוגמא נגדית). מותר לעשות זאת כאן כיוון שאנחנו משתמשים באותה העתקה $\pi : \mathbb{Z} \to \mathbb{Z}_6$ המוגדרת ע"י $\pi(x) = x (\bmod 6)$.

<u>נספח א': תרגילים נוספים על חבורות מנה</u>

<u>תרגיל:</u> תהי G חבורה. $H \le G$ מאינדקס 5 ו- $a \in Z(G)$ איבר מסדר 3. הראו ש $a \in H$.

פתרון: $Z(G)H \le G$ בגלל ש $Z(G) \lhd G$. נקבל $H \le Z(G)H \le G$ ואז לפי מסקנה ממשפט לגרנג' נקבל $5=[G:H]=[G:Z(G)H][Z(G)H:H]$.

לכן יש שתי אפשריות:

א. $[Z(G)H:H]=1$ ואז בהכרח נקבל $Z(G)H=H$ ולכן $aH \subseteq H$ כלומר $a \in H$.

ב. $[Z(G)H:H]=5$ ואז $G=Z(G)H$. מכאן נקבל ש $H \lhd G$ כיוון ש $gHg^{-1}=(zh)H(zh)^{-1}=zhHh^{-1}z^{-1}=zHz^{-1}=zz^{-1}H=H$.

כעת $aH \in G/H$ והסדר של איבר זה מחלק גם את 5 וגם את 3. לכן בהכרח $o(aH)=1$, כלומר $aH=H$ ולכן $a \in H$.

תרגיל:

תהי $G=GL_n(\mathbb{C})$ החבורה של המטריצות ההפיכות מסדר $n \times n$ מעל שדה המורכבים. נגדיר: $A=\{M \in G \mid |\det M|=1\}$. הוכיחו ש- $A \lhd G$ ו- G/A אבלית.

פתרון:

הראו ש- $A \le G$. נוכיח עכשיו שהיא נורמלית. לפי הקריטריון לנורמליות מספיק להוכיח $\forall S \in G, \forall M \in A, SMS^{-1} \in A$.

$$|\det(SMS^{-1})|=|\det S*\det M*\det S^{-1}|=$$
$$|\det M|*|\det S|*|\det S^{-1}|=|\det M|*|\det(S*S^{-1})|=1*1=1$$

כלומר $\forall S \in G, \forall M \in A, SMS^{-1} \in A$ לכן $\forall S \in G, SAS^{-1} \subseteq A \Rightarrow G \rhd A$.

נוכיח ש G/A אבלית:

$$\forall SA, TA \in G/A, SA*TA=STA=TSA$$
$$\Leftrightarrow (ST)^{-1}TS=T^{-1}S^{-1}TS \in A$$
$$\det(T^{-1}S^{-1}TS)=\det T^{-1}\det S^{-1}\det T\det S=$$
$$\det(T*T^{-1})\det(S*S^{-1})=1$$
$$(ST)^{-1}TS \in A \Rightarrow SATA=TASA$$

כלומר A אבלית!

תרגיל בית: תהי $N=\{M \in G \mid \det M=1\}$, הוכיחו ש- $N \lhd G$ ו- G/N אבלית.

תרגיל: תהי G חבורה ונניח ש $H \le Z(G)$ וגם G/H ציקלית. הוכיחו ש G אבלית.

פתרון: כיוון ש G/H ציקלית קיים $g \in G$ כך ש $G/H = \langle gH \rangle$. אזי מתקיים $G = \bigcup_{n\in\mathbb{Z}} g^n H$

(איחוד זר). נניח ש $x, y \in G$ אזי $x = g^{n_1}h_1, y = g^{n_2}h_2$. אזי

$xy = g^{n_1}h_1 g^{n_2}h_2 = ... = g^{n_2}h_2 g^{n_1}h_1 = yx$.

נספח ב': תרגילים נוספים על משפטי האיזומורפיזם:

תרגיל: תהי G חבורה מסדר סופי. ותהי $N \lhd G$ כך ש $[G:N] = m$ וגם $|N| = n$. אם

$\gcd(m,n) = 1$ אזי N היא הת"ח היחידה ב G מסדר n.

הוכחה: תהי H ת"ח של G מסדר n.

לפי איזו 2 נקבל $H/_{H \cap N} \cong HN/_N$. נסמן $k = \left| H/_{H \cap N} \right| = \left| HN/_N \right|$.

אזי לפי המסקנות ממשפט לגרנג', נקבל: $k = \left| H/_{H \cap N} \right| = \frac{n}{|H \cap N|} \Rightarrow k \mid n$.

מצד שני, $HN/_N \le G/N$, ולכן לפי לגרנג' נקבל: $k = |HN/N| \mid |G/N| = m$.

כלומר $k \mid m, n \Rightarrow k \mid \gcd(m,n) = 1 \Rightarrow k = 1$.

לכן $|H \cap N| = n$ ומכאן בהכרח $H = N$.

נספח ג': משפט ההתאמה

משפט ההתאמה:

יהי $\varphi : G \to H$ אפימורפיזם. נסמן $K := Ker\varphi$.

קיימת התאמה חח"ע (פונקציה חח"ע ועל) בין התת-חבורות של H לבין התת-חבורות של G המכילות את הגרעין. התאמה זאת שומרת על יחס סדר הכלה ממש, כלומר $K \le H_1 < H_2 \le G$ אם ורק אם $\varphi(H_1) < \varphi(H_2) \le H$.

קיימת התאמה חח"ע בין התח"נ של H לבין התח"נ של G, וגם כאן נשמר יחס סדר ההכלה.

דוגמא:

נראה שוב שכל הת"ח של $\mathbb{Z}_n$ הן מהצורה $m\mathbb{Z}_n$ כאשר m|n. $\mathbb{Z}_n$ היא תמונה אפימורפית של $\mathbb{Z}$ ע"י ההומ' $\varphi(x)=x(\mathrm{mod}\, n)$. הגרעין הוא $n\mathbb{Z}$.

לכן לפי משפט ההתאמה, יש התאמה חח"ע בין הת"ח של $\mathbb{Z}$ המכילות את $n\mathbb{Z}$ לבין הת"ח של $\mathbb{Z}_n$. אנחנו כבר מכירים את כל הת"ח של $\mathbb{Z}$, ואם ת"ח כזאת מכילה את $n\mathbb{Z}$ אזי בהכרח היא מהצורה $m\mathbb{Z}$ כאשר m|n, ויש בדיוק אחת כזאת לכל מחלק.

<u>תרגיל:</u> יהיו $M \lhd N \lhd G$ כך ש $M \lhd G$, G/N ציקלית וגם $[N:M]=2$. הראו ש G/M אבלית.

<u>פתרון</u>: נפעיל את משפט ההתאמה על ההעתקה הטבעית $\pi: G \to G/M$. נקבל התאמה של תת-חבורות נורמליות:

$$\{M \lhd H_1 \lhd G\} \leftrightarrow \{H_2 \lhd G/M\}$$

בפרט $N \lhd G$ ולכן $\varphi(N)=N/M \lhd G/M$.

<u>תרגיל עזר (הופיע בבוחן 2010):</u> הראו שאם $K \lhd L$ כך ש $|K|=2$ אזי $K \le Z(L)$.

<u>פתרון תרגיל עזר:</u> $K=\{e,a\}$, ונתון שלכל $b \in L$ מתקיים $bK=Kb$ כלומר $ba \in Kb=\{b,ab\}$. אם $ba=b$ אזי $a=e$ סתירה. לכן בהכרח $ba=ab$ ולכן $a \in Z(L)$ וידוע ש $e \in Z(L)$ ולכן $K \le Z(L)$.

כעת ידוע ש $|N/M|=[N:M]=2$ ולכן לפי תרגיל העזר, נקבל ש $N/M \le Z(G/M)$.

לפי משפט איזו' 3, נקבל $(G/M)/(N/M) \cong G/N$ שלפי הנחה היא ציקלית.

נסכם: $N/M \le Z(G/M)$ וגם $(G/M)/(N/M) \cong G/N$ היא ציקלית, לכן לפי משפט מהתרגול הקודם, נקבל ש G היא אבלית.

תרגול 7

מחלקות צמידות:

הגדרה: תהי G חבורה, $g_1, g_2 \in G$. g_1 **צמוד** ל g_2 אם קיים $x \in G$ כך ש: $xg_1x^{-1} = g_2$.

הערה: למעשה ראינו כבר את החשיבות של פעולת ההצמדה כשדיברנו על תח"נ. ראינו שתח"נ היא ת"ח שאינווריאנטית (נשמרת) תחת פעולת ההצמדה.

משפט: יחס הצמידות היינו יחס שקילות.

הוכחה: יחס שקילות היינו יחס המקיים את הדברים הבאים:

1) רפלקסיביות: g צמוד לעצמו, $ege^{-1} = g$

2) סימטריות: g_1 צמוד ל g_2 אז g_2 צמוד ל g_1 ,

$$xg_1x^{-1} = g_2, x^{-1}g_2(x^{-1})^{-1} = g_1$$

3) טרנזטיביות: g_1 צמוד ל g_2 ו g_2 צמוד ל g_3 אז g_1 צמוד ל g_3

$$xg_1x^{-1} = g_2, yg_2y^{-1} = g_3 \Rightarrow yxg_1x^{-1}y^{-1} = yxg_1(yx)^{-1} = g_3$$

הגדרה: בהנתן איבר ניתן להסתכל על מחלקת השקילות שלו תחת היחס הזה. מחלקת השקילות היא קבוצת כל האיברים שצמודים לאיבר זה. כל מחלקת שקילות כזאת נקראת **מחלקת צמידות**. שני איברים הם **צמודים** אם הם נמצאים באותה מחלקת צמידות.

שאלה: יהי $A \in SL_n$ מיהן כל המטריצות הצמודות ל A ?

תשובה: כל המטריצות B כך שקיים $C \in SL_{n,} CAC^{-1} = B$ או כמו שלמדנו באלגברה ליניארית כל המטריצות הדומות ל A שמייצגות אותה העתקה ליניארית (רק בבסיס אחר).

סימון: $x \in G$, $conj(x)$ הינו מחלקת הצמידות המכילה את x. כלומר:

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

משפט: החבורה G היא איחוד זר של כל מחלקות הצמידות שלה (זה נובע ישירות מהתכונות של יחס שקילות).

דוגמאות:

1. אם G חבורה אבלית אז מה הם מחלקות הצמידות של כל איבר?

תשובה: לכל האיבר האיבר היחידי שצמוד לו זה הוא עצמו כי מתקיים:

$$\forall g,x\in G, xgx^{-1}=g$$
$$conj(g)=\{xgx^{-1}\mid x\in G\}=\{g\}$$

לכן בחבורה אבלית כל איבר צמוד לעצמו ומספר מחלקות הצמידות הוא $|G|$.

2. תהי G חבורה ויהי $x\in Z(G)$ (כלומר x הוא איבר במרכז) אז מה $conj(x)$?

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

כי אם x במרכז אז הוא מתחלף עם כל איברי החבורה כלומר $\forall g\in G, gx=xg$.

תרגיל בית:

הראו שאם $H\lhd G$ וגם $a\in H$ אזי $conj(a)\subseteq H$.

חבורות סימטריה

נרצה להראות בצורה מלאה מהן כל מחלקות הצמידות של S_n עבור n נתון. לכן נבצע חזרה קלה על התכונות של S_n ונוכיח תכונות חדשות.

תזכורת:

<u>חוקי כתיבה:</u> כל תמורה כזאת אפשר לכתוב כפירוק למחזורים זרים. נסביר איך עושים זאת בעזרת דוגמאות:

1. $\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}=\begin{pmatrix}1&2&3&4\end{pmatrix}$

הסבר: מתחילים לקרוא את המחזור משמאל לימין:1 הולך ל2, 2 הולך ל3 , 3 הולך ל4 ו4 הולך ל1(באופן מחזורי).

2. $\begin{pmatrix}1&2&3&4&5&6\\1&3&2&6&4&5\end{pmatrix}=\begin{pmatrix}2&3\end{pmatrix}\begin{pmatrix}4&6&5\end{pmatrix}$

הסבר: מתחילים משמאל לימין: 2 הולך ל3 ו3 ל2 לכן הם במחזור אחד, 4 הולך ל6 ו6 הולך 5 ו5 הולך 4. את 1 אנו לא מוסיפים כי 1 הולך לעצמו.

<u>הערה:</u> שימו לב שניתן "לסובב" מחזור: כלומר $(312)=(231)=(123)$.

תרגיל בית: כמה דרכים שונות יש לכתוב אותו מחזור?

משפט: כל תמורה ב S_n אפשר לפרק למכפלת מחזורים זרים. פירוק זה יחיד עד כדי סדר המחזורים, ו"סיבוב" האיברים בכל מחזור.

הערה: איך מוצאים את ההפכי של מחזור? פשוט "הופכים" את המחזור:
$(1\ \ 2\ \ 3)^{-1} = (3\ \ 2\ \ 1)$.

תרגיל (בקומבינטוריקה): כמה מחזורים שונים באורך k יש ב S_n?

תשובה: כמספר הדרכים לבחור k מתוך n אנשים ולהושיבם במעגל. סה"כ: $\binom{n}{k}(k-1)!$.

טענה: הסדר של מחזור (כאיבר בחבורה) הוא אורכו, כלומר מס' האיברים שבמחזור.
במילים אחרות: מחזור באורך k הוא מסדר k. לדוגמא (3 4) מחזור מסדר 2 המכונה **חילוף**.
מדוע הטענה הנ"ל נכונה? נראה בעזרת דוגמא שקל להכלילה: $[(12...k)^k](i) = (i+k) \pmod k$
, כלומר

$$(12...k)(1) = 2$$
$$(12...k)(2) = 3 \Rightarrow (12...k)^2(1) = 3$$
$$...$$
$$(12...k)(k-1) = k \Rightarrow (12...k)^{k-1}(1) = k$$
$$(12...k)(k) = 1 = (k+1) \pmod k \Rightarrow (12...k)^k(1) = 1$$

טענה: איך מוצאים את הסדר של תמורה? תחילה מפרקים למחזורים **זרים**: $\pi = \sigma_1 \cdots \sigma_k$ אזי
$o(\pi) = lcm(o(\sigma_1), ..., o(\sigma_k))$.

הוכחה: נשאיר זאת כתרגיל עם הדרכה:

1. הראו שאם $a,b \in G$ בחבורה כלשהיא מתחלפים ($ab = ba$) אזי $o(ab) \mid lcm(o(a), o(b))$.

2. מצאו מצב כנ"ל בו $o(ab) < lcm(o(a), o(b))$.

3. הראו שאם $a,b \in G$ מתחלפים וגם $<a> \cap <b> = \{e\}$ אזי $o(ab) = lcm(o(a), o(b))$.

4. כעת הסיקו את הטענה מהנ"ל.

<u>**דוגמא:**</u> $o((123)(45))=lcm(o((123)),o((45)))=lcm(3,2)=6$. **שימו לב:** אם המחזורים אינם זרים הטענה **אינה נכונה**. $o((123)(34))=o((1234))=4$. אם נתונה לכם מכפלה של מחזורים שאינם זרים, פשוט פרקו אותה למכפלת מחזורים זרים וחשבו את הסדר.

<u>**הערה:**</u> ניתן גם לכתוב תמורה בכתיב פונקציות:

$$\pi=\begin{pmatrix}1&2&3&4&5&6\\1&3&2&6&4&5\end{pmatrix}$$

$$\pi(1)=1 \quad \pi(2)=3 \quad \pi(4)=6$$

<u>**משפט:**</u> כל תמורה ב- S_n אפשר להציג כמכפלה של חילופים למשל:

$$(a_1\,a_2\quad a_3\quad\dots\quad a_k)=(a_1\quad a_k)(a_1\quad a_{k-1})\cdots(a_1\quad a_2)$$

(בתמורה כללית פשוט מפרקים למחזורים זרים, ואז מפרקים כל מחזור זר לחילופים.)

<u>**דוגמא:**</u> $(1\quad 5\quad 4\quad 3\quad 2)=(1\quad 2)(1\quad 3)(1\quad 4)(1\quad 5)$

<u>**מסקנה:**</u> קבוצת החילופים ב S_n יוצרת את S_n.

<u>**הגדרה:**</u> **היפוך** (או **הפרת סדר**) בתמורה הוא זוג $i<j$ כך ש $\pi(j)<\pi(i)$

<u>**דוגמא:**</u> $S=\begin{pmatrix}1&2&3&4&5&6\\1&3&2&6&4&5\end{pmatrix}$ כמה היפוכים יש בתמורה S ?

<u>**תשובה:**</u>

<u>היפוך 1:</u> 2 ו 3 <u>היפוך 2:</u> 4 ו 5 <u>היפוך 3:</u> 4 ו 6 לכן סך הכל יש ב S 3 היפוכים.

איך מחשבים את מספר ההיפוכים בקלות?

נמחק את השורה הראשונה של התמורה, ונישאר עם השורה השנייה בלבד: 132645.

נתחיל משמאל, ונבדוק האם מימינו של 1 יש מספרים הקטנים ממנו: כמובן שאין.

אח"כ נבדוק האם מימינו של 3 יש מספרים הקטנים ממנו: יש אחד כזה והוא 2, לכן נוסיף 1 למספר היפוכי הסדר.

אח"כ נבדוק האם מימינו של 2 יש מספרים הקטנים ממנו: אין.

אח"כ 6: 4,5 קטנים ממנו, ולכן מוסיפים 2 למספר ההיפוכים.

אח"כ 4: אין. אח"כ 5: אין. סה"כ קיבלנו 3 היפוכי סדר.

<u>**תרגיל בית:**</u>

1. מצאו את מספר ההיפוכים בתמורה: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 1 & 4 & 2 & 5 \end{pmatrix}$.

2. הסבירו מדוע האלגוריתם שהצגנו בדוגמא לחישוב מספר ההיפוכים באמת עובד.

<u>סימון:</u> מס' ההיפוכים בתמורה S יסומן ע"י $Inv(S)$

<u>! הגדרה:</u> סימן של תמורה יוגדר ע"י $sign(S)=(-1)^{Inv(S)}$

אם $sign(S)=1$ התמורה תקרא תמורה זוגית ואם $sign(S)=-1$ התמורה תקרא תמורה אי זוגית.

<u>תרגיל בית:</u> הראו ש $sign(\pi)=\prod_{i<j}\frac{\pi(j)-\pi(i)}{j-i}$.

<u>! משפט:</u> $sign:S_n\to\{-1,1\}$ הוא הומומורפיזם של חבורות.

<u>! מסקנה:</u>

תמורה זוגית*תמורה זוגית= תמורה זוגית

תמורה אי-זוגית*תמורה זוגית= תמורה אי-זוגית

תמורה אי-זוגית*תמורה אי-זוגית= תמורה זוגית

(מציבים במקום זוגי 1 ובמקום אי זוגי 1- ומשווים את התוצאה)

בגלל שהומ' מעביר יחידה ליחידה, נקבל שתמורת הזהות היא תמיד זוגית (ניתן לראות זאת גם לפי מספר ההיפוכים).

<u>סימון</u>: את קבוצת התמורות הזוגיות אנו מסמנים ב A_n.

<u>משפט:</u> $A_n \triangleleft S_n$

<u>"הוכחה":</u> הגרעין של העתקת הסימן $sign:S_n\to\{-1,1\}$ היא בדיוק קבוצת התמורות הזוגיות.

<u>משפט:</u> S_n חצי מהתמורות זוגיות וחצי אי זוגיות.

<u>הוכחה:</u> כאמור, $sign:S_n\to\{-1,1\}$ אפימורפיזם.

לפי איזו 1, $S_n/A_n\cong\mathbb{Z}_2$.

נקבל כעת לפי לגרנג' נקבל $|S_n/A_n|=2\Rightarrow|A_n|=\frac{|S_n|}{2}=\frac{n!}{2}$.

<u>תרגיל בית:</u> הראו שאם $\pi\in S_n$ היא תמורה אי-זוגית, אזי πA_n היא קבוצת כל התמורות האי-זוגיות. האם קבוצת התמורות האי-זוגיות היא ת"ח?

<u>משפט:</u> A_n נוצרת ע"י מחזורים באורך 3.

<u>הגדרה:</u> מבנה מחזורים של תמורה הוא קבוצת אורכי המחזורים של תמורה מסודרים מהגדול לקטן.

<u>דוגמא:</u> מבנה המחזורים של $(8\ 7\ 6)(5\ \ 6\ \ 4)(3\ \ 2)$ הוא 3,3,2.

<u>תרגיל:</u> לתמורה ולהפכית שלה יש אותו מבנה מחזורים.

<u>פתרון:</u> כבר ראינו שהתמורה ההפכית היא פשוט המחזורים כתובים הפוך...

<u>הצמדה של תמורות:</u>

בהנתן שתי תמורות $\sigma, \pi \in S_n$ ברצוננו לחשב את ההצמדה $\pi\sigma\pi^{-1}$.

נשים לב שאפשר להניח ש σ היא מחזור בודד, כיוון ש:

$\pi\sigma\pi^{-1} = \pi(...)(...)...(...)\pi^{-1} = \pi(...)\pi^{-1}\pi(...)\pi^{-1}\pi...\pi^{-1}\pi(...)\pi^{-1}$ (כלומר מצמידים תמורה מחזור אחר מחזור).

<u>דוגמא:</u> נראה הצמדה של המחזור (3 2 1) ע"י המחזור (2 1):

$(1\ 2)(1\ 2\ 3)(1\ 2) = (1\ 3\ 2) = (213)$.

מה קיבלנו? שימו לב שלקחנו את המחזור (3 2 1) ופשוט הפעלנו על איבריו את התמורה $\pi = (1\ 2)$. כלומר $(1\ 2)(1\ 2\ 3)(1\ 2) = (\pi(1)\ \pi(2)\ \pi(3)) = (2\ 1\ 3) = (123)$.

<u>טענה:</u> נראה שזה המקרה הכללי, כלומר אם $\sigma = (i_1\ i_2\ \dots\ i_k)$ אזי:

$$(*) \qquad \pi\sigma\pi^{-1} = \pi(i_1\ i_2\ \dots\ i_k)\pi^{-1} = (\pi(i_1)\ \pi(i_2)\ \dots\ \pi(i_k))$$

<u>הוכחה:</u> בכתיב הפונקציונלי של תמורות שהצגנו קודם, קל לראות ש $\sigma(i_j) = i_{j+1\,(\mathrm{mod}\,k)}$ (כלומר התמונה של i_j היא האיבר שיושב מימינו במחזור). במילים אחרות, האיבר שיושב לימינו של i במחזור הוא $\sigma(i)$.

טריק: נבדוק מי יושב לימינו של $\pi(j)$ במחזורים של $\pi\sigma\pi^{-1}$. נבדוק זאת פשוט ע"י הפעלת התמורה: $\pi\sigma\pi^{-1}(\pi(j)) = \pi(\sigma(j))$. כלומר מי שיושב לימינו של $\pi(j)$ הוא $\pi(\sigma(j)) = \pi(j+1)$.

התבוננות זהירה תראה לנו שזה בדיוק מה שרצינו להוכיח, כלומר קיבלנו את (*).

<u>טענה:</u> גם הכיוון ההפוך נכון, כלומר בהנתן שתי תמורות בעלות אותו מבנה מחזורים, קיימת תמורה המצמידה אותן.

<u>הוכחה:</u>

נראה שוב את המקרה של מחזורים. בהנתן שני מחזורים באותו אורך:

$$\sigma = (i_1\ i_2\ \dots\ i_k)$$
$$\tau = (j_1\ j_2\ \dots\ j_k)$$

פשוט נצמיד ע"י התמורה הבאה:

$$\pi = \begin{pmatrix} i_1\ i_2\ \dots\ i_k \\ j_1\ j_2\ \dots\ j_k \end{pmatrix}$$

משפט: S_n שתי תמורות צמודות אם"ם יש להם אותו מבנה מחזורים.

מסקנה: כל תמורה צמודה להפכית שלה.

הערה: בהנתן שתי תמורות צמודות, לא בהכרח יש יחידות של האיבר המצמיד אחת לשנייה. לדוגמא ידוע ש- $\tau = (1\ 2\ 3)$ צמודה להפכית שלה $\tau^{-1} = (2\ 1\ 3)$. ניתן להגיע מאחת לשנייה ע"י כל אחת מהתמורות הבאות: $(1\ 2), (2\ 3), (1\ 2)$.

דוגמא: בהנתן שתי תמורות $b = (1579)$ $a = (135)(12)$, מצאו את: $a^{-1}ba$.

פתרון: נשים לב שאנחנו לא מצמידים ב a אלא ב a^{-1}. לכן לפי הטענה הנ"ל, כדי לחשב את $a^{-1}ba$ צריך פשוט להפעיל את $a^{-1} = (1\ 2)(1\ 5\ 3)$ על אברי b: כלומר

$$a^{-1}ba = (a^{-1}(1)\ a^{-1}(5)\ a^{-1}(7)\ a^{-1}(9)) = (5\ 3\ 7\ 9)\ .$$

שאלה: כמה מחלקות צמידות יש ב S_3?

תשובה: מבנים אפשרים:

3,21,111 כלומר ב S_3 יש שלוש מחלקות צמידות.

תרגיל: מיהן כל הת"ח הנורמליות ב S_3?

פתרון: נראה שידיעת מחלקות הצמידות מקלה על מציאת תח"נ:

לפי לגרנג', פרט לתח"נ הטריוויאליות $\{e\}, S_3$, תח"נ בהכרח מסדר 2,3.

בהנתן איבר $\pi \in N \lhd S_3$ אנחנו יודעים שגם כל הצמודים שלו נמצאים ב- N.

אם N מסדר 3, היא ציקלית ולכן מכילה מחזור מסדר 3, ואז כל המחזורים מסדר 3 הם ב N. אזי N היא בהכרח $\{e, (123), (213)\}$. ואכן N נורמלית כי היא סגורה תחת הצמדה.

(ניתן לראות שהיא נורמלית גם מכך שהאינדקס שלה הוא 2).

אם N מסדר 2, אזי היא מכילה חילוף, אבל אם היא מכילה חילוף, היא מכילה את כל החילופים, וכיוון שהחילופים יוצרים את S_3 נקבל ש $S_3 = N$.

שאלה: כמה מחלקות צמידות יש ב S_4?

תשובה: מבנים אפשרים:

4

31

22

2111

1111

כלומר ב S_4 יש 5 מחלקות צמידות.

<u>תרגיל:</u> מיהן כל הת"ח הנורמליות ב S_4?

<u>תשובה:</u>

אם $\pi \in N \triangleleft S_4$, אנחנו יודעים שגם כל הצמודים שלו נמצאים ב- N.

אם N אינה תח"נ טריוויאלית, אזי לפי לגרנג' סידרה הוא בהכרח 2,3,4,6,8 או 12.

אם N מכילה איבר מהצורה (4 3)(2 1) אזי היא מכילה את הת"ח (בדקו שזאת אכן ת"ח)

$K = \{e, (12)(34), (13)(24), (14)(23)\}$. ת"ח זאת איזומורפית לחבורת קליין (הוכיחו).

K נורמלית, כיוון שהיא סגורה תחת הצמדה.

אם N מכילה חילוף, אזי היא מכילה את כל החילופים, ואלה יוצרים את כל S_4 ואז $S_4 = N$.

אם N מכילה מחזור מסדר 3, אזי הוא מכיל את כל המחזורים מאורך 3, ואלה יוצרים את A_4,

ולכן $A_4 \le N \triangleleft S_4$, זה אפשרי רק אם $S_4 = N$ או $A_4 = N$ כי אין מחלקים נוספים של 24

הגדולים מ 12.

אם N מכילה מחזור מאורך 4, אזי היא מכילה את כולם. נשים לב ש

(3 4 1)=(4 3 1 2)(4 3 2 1), ולכן N מכילה גם את (3 4 1), ולכן N מכילה את A_4 ממש ולכן

בהכרח $S_4 = N$.

<u>הגדרה:</u> חבורה נקראת פשוטה אם אין לה תח"נ לא טריוויאליות.

<u>משפט:</u> לכל $n \ge 5$ $A_n \triangleleft S_n$ היא התח"נ היחידה של S_n.

<u>משפט גלואה:</u> A_n פשוטה לכל $n \ge 5$.

<u>הערה:</u> משפט גלואה לא נובע מהמשפט הקודם לו, בגלל חוסר טרנזיטיביות של נורמליות.

כלומר אם $H \triangleleft A_n \triangleleft S_n$ זה לא אומר ש $H \triangleleft S_n$.

<u>תרגיל ממבחן תשס"ח:</u>

נניח שקיים אפימורפיזם מ- A_6 לחבורה G . מצא את G

(מיין את האפשרויות עד כדי איזומורפיזם) .

פתרון: לפי משפט איזו' 1, $G\cong A_6/Ker\varphi$. אבל $Ker\varphi \lhd A_6$, וכיוון ש A_6 פשוטה (לפי משפט גלואה), נקבל ש $Ker\varphi=\{e\}$ או $Ker\varphi=A_6$, ולכן $G\cong A_6,\{e\}$

תרגיל: הראו שב A_4 אין ת"ח מסדר 6.

הוכחה: אפשר כמובן למצוא את כל הת"ח ב A_4 או להשתמש בשיקולי סדר ומשפט לגרנג', אך יותר קל להשתמש בתכונות של מחלקות הצמידות. נשים לב שאם H ת"ח מסדר 6 אז $[A_4:H]=2$ ולכן H ת"ח נורמלית של A_4. ראינו בתרגול קודם שבכל חבורה מסדר זוגי יש איבר מסדר 2, ולכן קיים ב H איבר מסדר 2, והוא בהכרח מהצורה (ij)(kl) (הסבירו מדוע!). לכן כל האיברים מהצורה הנ"ל נמצאים ב H כיוון שכל מחלקת הצמידות של (ij)(kl) מוכלת ב H. לכן $K=\{(1),(12)(34),(13)(24),(14)(23)\}\subset H$. קל לבדוק ש $K\le H$ שאיזומורפית לחבורת קליין ($\mathbb{Z}_2\times\mathbb{Z}_2$). אבל זאת ת"ח מסדר 4 בתוך חבורה מסדר 6, ונקבל סתירה למשפט לגרנג' (הסבירו מדוע!).

תת-קבוצות יוצרות של S_n:

ראינו קודם שקבוצת החילופים ב- S_n היא קבוצה שיוצרת את כל החבורה. כלומר כל תמורה ניתנת להצגה כמכפלה של חילופים.

נראה כעת מספר קבוצות יוצרים נוספות:

א. נראה שקבוצת החילופים $(1,2),(1,3),...,(1,n)$ יוצרת את S_n. מספיק להראות שניתן בעזרת החילופים הנ"ל ליצור את כל החילופים. נרצה לבנות תמורה α מהחילופים הנ"ל שעבור יתקיים $\alpha(1,j)\alpha^{-1}=(\alpha(1),\alpha(j))=(i,j)$. נשים לב ש $(1,i)(1,j)(1,i)=(i,j)$.

ב. חילופים סמוכים: $(1,2),(2,3),...,(i,i+1),...,(n-1,n)$. נרצה לבנות את כל החילופים מסעיף א. $(1,j)=(1,2)(2,3)...(j-2,j-1)(j-1,j)...(2,3)(1,2)$.

ג. התמורות: $(1,2),(1,2,...,n)$. נראה שניתן ליצור את כל החילופים הסמוכים מסעיף ב. נשים לב שמ- $(1,2,...,n)$ ניתן ליצור את $(1,2,...,n)^{-1}=(1,2,...,n)^{n-1}$. כעת נסמן $\alpha=(1,2,...,n)$. אזי $\alpha(1,2)\alpha^{-1}=(2,3),\quad \alpha(2,3)\alpha^{-1}=(3,4),...$.

תרגול 8

שיכון חבורות:

! הגדרה: תהיינה G,H חבורות $\varphi : H \to G$ הומומורפיזם חח"ע (מונומורפיזם) . φ הנ"ל נקרא שיכון.

משפט קיילי: כל חבורה **סופית** G ניתנת לשיכון בחבורת סימטריה מתאימה ($S(G) \cong S_{|G|}$).

"הוכחה": השיכון מוגדר ע"י כך שכל איבר $g \in G$ עובר לתמורה $l_g : G \to G$ המוגדרת ע"י $l_g(x) := gx$. ראינו כבר שפונקציה זאת היא חח"ע ועל, ולכן היא תמורה על אברי G.

רואים גם ש $l_g \neq l_h$ כאשר $g \neq h$.

הערה: למה "טובים" השיכונים האלה? אנחנו רוצים להעתיק חבורה שעליה לא ידוע הרבה, לחבורה אחרת, שעליה ידוע יותר. בעזרת מידע מוקדם על S_n נוכל להוכיח דברים על חבורות אחרות. לעתים אפילו רק בזכות העובדה שידוע לנו $|S_n| = n!$, כיוון שמשפט לגרנג' מגביל אותנו בסדרי התת-חבורות של S_n.

דוגמאות:

1. נראה שחבורת קליין $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ אכן משוכנת ב S_4.

   נסמן את אברי החבורה כך: $V = \{1, a, b, ab\}$ אזי:

$$l_1 = id \Rightarrow (1) \in S_V$$

$$l_a(1) = a, l_a(a) = 1, l_a(b) = ab, l_a(ab) = b \Rightarrow l_a = \begin{pmatrix} 1 & a & b & ab \\ a & 1 & ab & b \end{pmatrix} = (1,a)(b,ab) \in S_V$$

$$l_b(1) = b, l_b(a) = ba = ab, l_b(b) = 1, l_b(ab) = bab = abb = a \Rightarrow l_b = \begin{pmatrix} 1 & a & b & ab \\ b & ab & 1 & a \end{pmatrix} = (1,b)(a,ab) \in S_V$$

$$l_{ab}(1) = ab, l_{ab}(a) = b, l_{ab}(b) = a, l_{ab}(ab) = 1 \Rightarrow l_{ab} = \begin{pmatrix} 1 & a & b & ab \\ ab & b & a & 1 \end{pmatrix} = (1,ab)(a,b) \in S_V$$

2. קיימות חבורות מסדר n אותן ניתן לשכן ב S_m כאשר $m < n$. לדוגמא ניקח את H= <(1 2),(3 4),(5 6)> , ב S_6. הסדר של H ב S_6 הוא 8=1+3+3+1 (האיברים שנוצרים ע"י 0 יוצרים, 1, 2 או 3). רואים ש 8>6 ושיכון קיילי הוא בזבזני במקרה הזה.

שיכון של חבורות ב GL_n(R): (המטריצות ההפיכות מעל הממשיים).

נראה שניתן לשכן כל חבורה מסדר n בחבורת המטריצות GL_n(R).

איך נעשה זאת? תחילה נשכן את החבורה בתוך S_n (בעזרת קיילי) ואז נשכן את S_n בתוך GL_n(R).

אנחנו רוצים מטריצה A_π המתאימה לתמורה $\pi \in S_n$ שתקיים:

$$A_\pi \begin{bmatrix} 1 \\ \vdots \\ n \end{bmatrix} = \begin{bmatrix} \pi(1) \\ \vdots \\ \pi(n) \end{bmatrix}.$$

מטריצות כאלה נקראות **מטריצות תמורה**.

נשים לב ל"תופעה" הבאה:

$$E_{ij} \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} = \left[\delta_{ij}\right] \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow j = \begin{bmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{bmatrix} \leftarrow i$$

המטריצה האלמנטרית E_{ij} (1 במקום ה ij, 0 בכל מקום אחר), מעבירה 1 במקום ה j ל 1 במקום ה i. לדוגמא:

$$E_{32} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \qquad E_{13} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

בדקו בתור <u>**תרגיל בית**</u> ש $E_{ij} = \left[\delta_{ij}\right] \begin{bmatrix} 1 \\ \vdots \\ \vdots \\ \vdots \\ n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ j \\ \vdots \\ 0 \end{bmatrix} \leftarrow i$ (כלומר המטריצה E_{ij} מאפסת את הוקטור $\begin{bmatrix} 1 \\ \vdots \\ \vdots \\ \vdots \\ n \end{bmatrix}$ ומעבירה את j למקום ה i).

כעת נראה שניתן לסכום מטריצות אלמנטריות מתאימות כדי לבנות את התמורה:

$$A_\pi = \sum_{1\le i\le n} E_{i,\pi(i)}$$

כעת:
$$A_\pi\begin{bmatrix}1\\ \vdots\\ n\end{bmatrix} = \left(\sum_{1\le i\le n} E_{i,\pi(i)}\right)\begin{bmatrix}1\\ \vdots\\ n\end{bmatrix} = \sum_{1\le i\le n}\left(E_{i,\pi(i)}\begin{bmatrix}1\\ \vdots\\ n\end{bmatrix}\right) = \sum_{1\le i\le n}\left(\begin{bmatrix}0\\ \vdots\\ \pi(i)\\ \vdots\\ 0\end{bmatrix}\leftarrow i\right) = \begin{bmatrix}\pi(1)\\ \vdots\\ \pi(i)\\ \vdots\\ \pi(n)\end{bmatrix}$$

לדוגמא:

$\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}\begin{bmatrix}1\\2\\3\end{bmatrix}=\begin{bmatrix}3\\1\\2\end{bmatrix}$ שמתאימה לתמורה $(1,3,2)=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\pi$.

בגלל שמטריצת התמורה מייצגת במדויק את התמורה שלנו, קל לראות ש**הבנייה הזאת אכן חח"ע**. נבדוק בהמשך האם בנייה זאת היא הומומורפיזם, אך תחילה נראה דרך פשוטה יותר לבנית מטריצת התמורה.

__**דרך אחרת להסתכל על מטריצות תמורה:**__

נסתכל בדוגמא האחרונה. נשים לב שכדי לקבל את מטריצת התמורה של $(1,3,2)=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\pi$, למעשה ביצענו תמורה של **העמודות** של מטריצת היחידה, לפי "הוראות" התמורה π:

$$\begin{bmatrix}1&0&0\\0&1&0\\0&0&1\end{bmatrix}\xrightarrow{\pi}\begin{bmatrix}0&0&1\\1&0&0\\0&1&0\end{bmatrix}$$

עמודה 1 עוברת לעמודה 3, עמודה 3 עוברת לעמודה 2, ועמודה 2 עוברת לעמודה 1.

דרך זו מאפשרת לחשב בקלות רבה את מטריצת התמורה.

כעת נרצה לראות מה קורה כשאנחנו מרכיבים תמורות (כלומר האם הגדרנו לעיל הומומורפיזם).

אבל יש בעיה!

נראה שאם מכפילים את התמורות כרגיל, נקבל שהמטריצות צריכות להיות מוכפלות הפוך.

לדוגמא אם ניקח את $(1,3,2)=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\pi$ ואת $\sigma=(1,2)$ נקבל את המטריצות המתאימות:

$$A_\pi = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \quad A_\sigma = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

מסתבר שאם נכפיל $A_\sigma A_\pi = A_{\pi\circ\sigma}$ נקבל את הכפל ההפוך לזה הרצוי.

נראה זאת בדוגמא הנ"ל:

$$A_\sigma A_\pi \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} = \begin{bmatrix} 1 \\ 3 \\ 2 \end{bmatrix}$$

והכפל מתאים לתמורה $(2,3)$ אבל $\sigma\pi = (1,3)$!

נשים לב ש $\pi\sigma = (2,3)$.

לסיכום דבר, מה שנקבל הוא שכדי שההתאמה שלנו תהיה הומומורפיזם, צריך להכפיל מטריצות הפוך מהרגיל, כלומר להגדיר כפל מטריצות ב GL_n(R) להיות $A * B = BA$ ואז הכל יסתדר (בתקווה).

אם אנחנו רוצים כפל מטריצות רגיל, אפשר להגדיר את מטריצות התמורות קצת אחרת, אבל אז היא תפעל על הוקטורים בצורה קצת שונה – היא תעביר את 1 למקום $\pi(1)$ במקום להיפך, ואז יהיה קצת קשה יותר לקרוא את התמורות (בדרך הבניה השנייה נראה שהתמורה בעצם מתמירה את השורות במקום העמודות).

<u>תרגילי בית:</u>

1. הראו ש $\left(A_\pi\right)^{-1} = A_{\pi^{-1}} = A_\pi^T$ (כלומר המטריצה ההפכית היא פשוט המטריצה המשוחלפת). כלומר לכל $\pi \in S_n$ מתקיים A_π היא מטריצה אורתוגונלית.

2. הראו ש $[1,\cdots,n]A_\pi = [\pi^{-1}(1),...,\pi^{-1}(n)]$.

<u>הערה:</u> ניתן להחליף את $\mathbb{R}$ בשדה סופי גדול מספיק, וכך לקבל שיכון לתוך חבורת מטריצות סופית.

<u>נספח: הכללה של משפט קיילי</u>

תהי G חבורה סופית, ותהי $H \le G$. אזי קיים הומ' (לא טריוויאלי) $\varphi : G \to S_{[G:H]}$.

נראה שכל איבר $g \in G$ פועל כתמורה על המחלקות השמאליות של G על H. נגדיר את ההעתקה $l_g(tH) := g(tH)$, וזאת פונקציה חח"ע כיוון ש $g(tH) = g(sH) \Rightarrow tH = sH$. כיוון שהקבוצה סופית, נקבל שהפונקציה היא תמורה. כלומר מגדירים $\varphi(g) := l_g$.

נראה את התכונות הבאות לגבי ההומ' φ:

1. $Ker\varphi \subseteq H$.

נובע בגלל שאם $g \in Ker\varphi$ אזי $gH = \varphi(g)(H) = H$.

2. $g \in Ker\varphi$ אם ורק אם כל הצמודים של g הם ב H.

$g \in Ker\varphi$ אם ורק אם $gtH = tH$ לכל $t \in G$ אם ורק אם $t^{-1}gt \in H$ לכל $t \in G$.

__תרגיל:__

אם G פשוטה ו $H < G$ אזי ההומ' $\varphi: G \to S_{[G:H]}$ מהכללת קיילי הוא שיכון.

__פתרון:__

ברור כי $Ker\varphi \subseteq H < G$ וגם $Ker\varphi \lhd G$ וזה יכול להיות רק אם $Ker\varphi = \{e\}$.

__תרגיל:__

תהי G חבורה פשוטה ונניח כי קיימת $H < G$ כך ש $[G:H] = p$ עבור p ראשוני.

הוכיחו ש p הוא הראשוני המקסימלי כך ש $p \mid |G|$ וגם $p^2 \nmid |G|$.

__פתרון:__

נשתמש ב $\varphi: G \to S_{[G:H]}$ שהגדרנו בהכללת משפט קיילי. ראינו בתכונות של ההומ' הנ"ל, ש $Ker\varphi \leq H$. ידוע ש $Ker\varphi \lhd G$ וגם G פשוטה, לכן כיוון ש $H < G$ נקבל בהכרח $Ker\varphi = \{e\}$.

לכן $\varphi: G \to S_{[G:H]}$ היא שיכון. לכן נקבל $G \cong \varphi(G) \leq S_p$, ולפי לגרנג' $|G| \mid |S_p| = p!$. אם $q \mid |G|$ ראשוני, אזי $q \mid p!$ ולכן בהכרח $q \leq p$ (כי ב !p יש רק גורמים ראשוניים קטנים שווים ל p).

בנוסף לפי לגרנג' גם $p \mid |G|$ וברור ש $p^2 \nmid |G|$ כי $p^2 \nmid p!$.

__תרגיל:__

תהי $H<G$ כאשר $|G|=n,[G:H]=k$, ויהי $d=\gcd(k!,n)$. אזי H מכילה תת-חבורה נורמלית $N\lhd G$ עם $[G:N]|d$. בפרט N לא תח"נ טריוויאלית אם $n\nmid k!$.

<u>הוכחה:</u>

נשתמש שוב בהומ' $\varphi:G\to S_{[G:H]}$ מהכללת משפט קיילי. נקח $N=Ker\varphi\le H$, אזי $[G:N]=|\varphi(G)|\,|\,|S_k|=k!$ (לפי איזו' 1). אבל $[G:N]|n$ ולכן $[G:N]|d=\gcd(n,k!)$.

אם $N=\{e\}$, אזי אזי $[G:N]=n$ ואז נקבל $n|k!\Leftarrow n|d|k!$, ולכן אם $n\nmid k!$ נקבל סתירה.

<u>תרגיל:</u>

יהי p הראשוני הקטן ביותר שמחלק את $|G|$. אם $H\le G$ כך ש $[G:H]=p$ אזי $H\lhd G$.

<u>הערה:</u> זאת הכללה של התרגיל הקלאסי שלנו שאם $[G:H]=2$ אזי $H\lhd G$.

<u>הוכחה:</u>

נשים לב ש $\gcd(p!,|G|)=p$ (כי ל $p!$ כל הגורמים הראשוניים קטנים שווים ל p, ולפי הנחה ל- $|G|$ בדיוק ההפך). בנוסף גם ברור ש $|G|\nmid p!$ ולכן לפי התרגיל הקודם נקבל תח"נ $\{e\}<N\lhd G$ עם אינדקס שמחלק את p. לפי לגרנג' נקבל:

$$[G:N]=[G:H][H:N]=p[H:N]$$

אבל המספר משמאל מחלק את p והמספר מימין גדול שווה ל p, ולכן $[H:N]=1$, כלומר $H=N$.

תרגול 9

פעולות של חבורות על קבוצות

תהי G חבורה ו X-קבוצה אז הומומורפיזם $\varphi: G \to S(X)$ נקרא **פעולה של החבורה G על הקבוצה X.**

במילים אחרות: אם אנו אומרים ש G **פועלת** על X ע"י φ אז הכוונה היא שהעתקה φ מתאימה לכל איבר בחבורה G פונקציה חח"ע ועל מ X ל X.

מנהג נפוץ הוא להתייחס לאיברים ב G כפונקציות על X, ולרשום g(x) במקום $\varphi(g)(x)$.

הנקודה החשובה בהגדרה הנ"ל היא שהפעולה היא הומ', ולכן:

$$\varphi(gh)(x) = [\varphi(g)\varphi(h)](x) = \varphi(g)[\varphi(h)(x)]$$

כלומר ניתן להכפיל את האיברים ב G ואז לחשב את הפעולה, או שניתן לחשב את הפעולה של h ואח"כ של g. בכתיב המקוצר נקבל:

$$(gh)(x) = g(h(x))$$

שמזכיר קצת את כלל האסוציאטיביות.

הערה: במקרה שהחבורה G פועלת על עצמה, כלומר X=G, אזי זה יכול להיות מבלבל להשתמש בכתיב המקוצר, ועדיף להשתמש בכתיב המסורבל יותר כדי למנוע בלבולים.

דרך נוספת להגדרת פעולה של חבורה:

בהנתן חבורה G וקבוצה X, פעולה של G על X היא פונקציה בינארית $G \times X \to X$ שנסמנה ע"י $(g,x) \mapsto g * x$, כך שמתקיים:

1. $(gh)*x = g*(h*x)$
2. $e*x = x$

תרגילי בית:

א. הראו שבהגדרה החדשה, כשקובעים את $g \in G$ מקבלים ש $g*: X \to X$ היא פונקציה חח"ע ועל. רמז: שימו לב ששתי התכונות (1,2) דרושות כדי להוכיח תרגיל זה.

ב. הראו שההגדרה הנ"ל שקולה להגדרת פעולה על קבוצה שראינו בעמוד הקודם.

דוגמאות:

1. $G = S_n$ $X = \{1, 2, ..., n\}$ מהו $S(X)$ במקרה זה?

תשובה: $S(X)=S_n, |X|<\infty$ נגדיר $\varphi=Id$ כלומר הפעולה על החבורה זו מתאימה כל תמורה לעצמה (תזכרו שתמורה היא פונקציה) (תרגיל: הוכיחו שזהו אכן הומומורפיזם).

2. **פעולת כפל משמאל:** G חבורה ו $X=G$ כלומר החבורה G פועלת על עצמה ע"י $\varphi: G\to S(G), \forall g\in G, \varphi(g)(x)=gx$.

כלומר φ מתאימה לכל איבר ב G פונקציה $\Pi\in S(G), \Pi: G\to G, \Pi(x)=gx$ כאשר $\Pi=\varphi(g)$.

נוכיח שאכן φ פעולה:

1) נוכיח ש $\forall g\in G, \varphi(g)=\Pi\in S(G)$ (כלומר Π הנ"ל היא חח"ע ועל) אם

$$\Pi(x_1)=\varphi(g)(x_1)=\varphi(g)(x_2)=\Pi(x_2)$$
$$\Leftrightarrow gx_1=gx_2\Leftrightarrow x_1=x_2$$

ואכן Π חח"ע.

על: יהי $x\in G$ אזי מתקיים $g^{-1}x\in G$ כי G חבורה ולכן סגורה לכפל.

$\Pi(g^{-1}x)=gg^{-1}x=x$ ולכן Π על.

ובסך הכל קיבלנו ש $\Pi=\varphi(g)\in S(G)$.

2) נוכיח שאכן φ הנ"ל היא הומומורפיזם:

<u>שימו לב</u>: **שפעולת הכפל בחבורה $S(G)$ היא הרכבה:**

$$\varphi(g_1)\varphi(g_2)(x)=\varphi(g_1)(g_2x)=g_1(g_2x)=(g_1g_2)x=$$
$$\varphi(g_1g_2)(x)$$

והראינו שאכן φ הנ"ל הינה פעולה (השתמשנו בשיויון השלישי באסוציאטיביות של החבורה G).

<u>שימו לב:</u> כפל מימין אינה בהכרח פעולה: אם נגדיר $\psi(g)(x)=xg$ אזי $\psi(gh)(x)=x(gh)=\psi(h)\psi(g)(x)$ ולכן ψ אינה הומ' (אלא אם כן החבורה היא אבלית).

<u>הגדרה:</u> **<u>מסלול</u>** (Orbit) של איבר $x\in X$ מסומן כ

$$\theta(x)=\{y\in X \mid \exists g\in G, \varphi(g)(x)=y\}=$$
$$\{\varphi(g)(x)\mid g\in G\}\subseteq X$$

<u>הסבר:</u> יש לנו חבורה G שפעולת על קבוצה X אז מסלול של איבר $x\in X$ הוא כל האיברים ש"ניתן להגיע" אליהם ע"י הפעולה φ.

<u>דוגמאות:</u>

1. **<u>פעולת ההצמדה:</u>** נגדיר עוד פעולה של חבורה G על עצמה:

$g \in G, \varphi(g) \in S(G), \varphi(g)(a) = gag^{-1}$.

$\theta(a) = \{gag^{-1} \mid g \in G\} = conj(a)$.

<u>שימו לב:</u> ההצמדה ההפוכה $\psi(g)(a) = g^{-1}ag$ אינה פעולה, כיוון שלא יתקיים התנאי שדורש ש ψ היא הומ' (בדקו זאת).

2. $H \leq G$. נגדיר פעולה של H על G ע"י כפל משמאל כלומר

$g \in G, h \in H, \varphi(h)(g) = hg$ מהו המסלול של $g \in G$?

$\theta(g) = \{\varphi(h)(g) \mid h \in H\} = \{hg \mid h \in H\} = Hg$.

<u>הגדרה:</u> **<u>נקודת שבת</u>** היא נקודה $x \in X$ כך ש $\theta(x) = \{x\}$.

<u>משפט:</u> היחס *"x במסלול של y"* הוא יחס שקילות. מסקנה: היחס הנ"ל מחלק את הקבוצה X למסלולים זרים.

<u>מסקנות:</u>

א. $X = \coprod \theta(x)$ האיחוד הוא זר כאשר בוחרים נציג אחד מכל מסלול.

ב. אם נסמן ב $Fixed$ את קבוצת נקודות השבת אזי $|X| = |Fixed| + \sum_{|\theta(x)| \geq 2} |\theta(x)|$.

<u>הגדרה:</u> ה**מייצב** (stabilizer) של איבר $x \in X$ מוגדר כ (ישנם כמה סימונים מקובלים):

$$St(x) = C_x = \{g \in G \mid \varphi(g)(x) = x\}$$

<u>משפט:</u> $C_x \leq G$, כלומר המייצב הוא תת חבורה של G .

<u>תרגיל בית:</u> אם $x \in X$ היא נקודת שבת, אזי $C_x = ?$.

<u>דוגמאות (בהתאם לדוגמאות הקודמות):</u>

1. φ פעולת ההצמדה ויהי $a \in X = G$ מהו C_a?

$$C_a = \{g \in G \mid \varphi(g)(a) = a\} = \{g \in G \mid gag^{-1} = a\} = \{g \in G \mid ga = ag\} = Z_a$$

<u>כלומר:</u> הוכחנו כעת שהמייצב של איבר תחת פעולת ההצמדה הוא המרכז של האיבר בחבורה.

2. $H \leq G$ פועלת על G ע"י כפל משמאל כלומר $\varphi(h)(g) = hg$ מהו C_g עבור $g \in G$?

$$C_g = \{h \in H \mid \varphi(h)(g) = g\} =$$
$$\{h \in H \mid hg = g\} = \{h \in H \mid h = e_H\} = \{e_H\}$$

שאלה: מהו הקשר בין מסלול למייצב? תשובה:

משפט: $|\theta(a)| = [G : C_a]$.

משפט(מסקנה מהמשפט הקודם): $|\theta(a)|\,|\,|G|$ סדר המסלול מחלק את סדר החבורה.

תרגיל בית: בדוגמאות הקודמות אכן נקבל ש- $\theta(a)$ מחלק את סדר החבורה (הראו זאת).

תרגיל: הראו שבפעולה של חבורה G מסדר 27 על קבוצה X עם 223 איברים בהכרח יש נקודות שבת.

הוכחה: לפי משפט קודם ראינו ש $|X| = |Fixed| + \sum_{|\theta(x)|\ge 2} |\theta(x)|$. נניח ש $|Fixed| = 0$. אזי $|X|$ היא סכום של מחלקי 27 הגדולים מ 1 (לפי המשפט האחרון). כלומר בהכרח $|\theta(x)| = 3, 9, 27$ לכל $x \in X$. לכן 223=3k+9j+27l . נעבור למודולו 3, ונקבל $1 \equiv 0 (\bmod 3)$, סתירה. כלומר בהכרח $|Fixed| \neq 0$.

תרגיל ממבחן תשס"ז, מועד ב':

החבורה **S4** פועלת על פולינומים ב-4 משתנים באופן הבא:

$\pi(f(x_1, \ldots, x_4)) = f(x_{\pi(1)}, \ldots, x_{\pi(4)})$.

מצא את סדר המסלול ואת סדר המייצב של x1x2 .

פתרון:

נראה קודם דוגמא של פעולת החבורה: נפעיל את התמורה $\pi = (1,3)(2,4)$ על הפולינום $x_1 + x_2^3 x_3$:

$\pi(x_1 + x_2^3 x_3) = x_3 + x_4^3 x_1$.

מספיק למעשה למצוא את סדר המסלול, ואת סדר המייצב נחשב לפי המשפט הנ"ל.

$$\theta(x_1x_2) = \{x_1x_2, x_1x_3, x_1x_4, x_2x_3, x_2x_4, x_3x_4\}$$

ולכן, $|\theta(x_1x_2)| = 6$.

אם כך $[S_4 : C_{x_1x_2}] = 6 \Rightarrow |C_{x_1x_2}| = \frac{4!}{6} = 4$.

משוואת מחלקות הצמידות

תהי G חבורה ו $x \in G$:

1. מחלקת הצמידות של x היא $conj(x) := \{gxg^{-1} \mid g \in G\}$
2. מרכז של x הוא $Z_x := \{g \in G \mid gx = xg\} = \{g \in G \mid x = gxg^{-1}\}$.
3. **משפט:** $|conj(x)| = [G : Z_x]$ (נובע ישירות מהמשפטים של פעולות על חבורות שראינו קודם).
4. מה קורה אם $x \in Z(G)$ (x מתחלף עם כל איברי G)?

   תשובה: במקרה זה x היא נקודת שבת של הפעולה:

   $Z_x = G, conj(x) = \{x\}, |conj(x)| = 1$.

משפט: $G = \coprod conj(x)$ כלומר G הוא איחוד זר של מחלקות הצמידות שלה (כאשר לוקחים נציג אחד מכל מחלקת צמידות)

מסקנה: (**משוואת המחלקות**) $|G| = |Z(G)| + \sum_{|conj(x_i)| \ge 2} [G : Z_{x_i}]$

כאשר הסכום עובר על איברים שמחלקת הצמידות שלהם גדולה או שווה ל 2.

משפט: תהי G חבורה. אם $G/Z(G)$ ציקלית אז G אבלית (ואז מלכתחילה $Z(G) = G$).

הוכחה: יהיו $x, y \in G$. מכיוון ש $G/Z(G)$ ציקלית קיים $a \in G$ כך ש

$G/Z(G) = \langle aZ(G) \rangle = \{(aZ(G))^i \mid i \in \mathbb{Z}\} = \{a^i Z(G) \mid i \in \mathbb{Z}\}$.

כעת $xZ(G) \in G/Z(G)$ ולכן $xZ(G) = a^i Z(G)$ עבור i מסוים, ולכן $x = a^i z_1$ עבור $z_1 \in Z(G)$.

בצורה דומה $y = a^j z_2$ עבור $z_2 \in Z(G)$.

כעת $xy = a^i z_1 a^j z_2 = a^j z_2 a^i z_1 = yx$ (הסבירו את השיויונות הנ"ל).

מסקנה: הראו שבחבורה G מסדר pq כאשר p,q ראשוניים (לאו דווקא זרים) מתקיים Z(G)=G (כלומר החבורה אבלית) או Z(G)={e}.

הוכחה: תרגיל בית.

תרגיל: הראו שמספר המחלקות בחבורה מסדר 15 הוא 15 או 5. למעשה מספר המחלקות חייב להיות 15 (ואז החבורה היא ___?) אבל לא נוכיח כעת.

הוכחה:

לפי המסקנה הנ"ל, ידוע ש $|Z(G)|=15 \vee |Z(G)|=1$ (מדוע?). אם $|Z(G)|=15$ אזי מספר המחלקות הוא 15, אחרת (המרכז טריויאלי) נקבל לפי משוואת המחלקות:

$$15=1+3k+5l$$

(זאת כיוון שהסדר של מחלקת צמידות חייב לחלק את סדר החבורה, ולכן מחלקות הצמידות הגדולות מ 1 חייבות להיות בגודל 3 או 5, מדוע?).

לפי שיקולי גודל, נקבל ש $l\le 2$, אבל $l\neq 0$ כי $3\nmid 14$ וגם $l\neq 2$ כי $3\nmid 4$. לכן בהכרח $l=1$ ומכאן נקבל $k=3$, ובסה"כ נקבל 5 מחלקות.

תרגיל בית: אם נקבל באמת מחלקה אחת מגודל 5 בתרגיל הנ"ל, מהו סדר האיברים במחלקה? מכאן ניתן לקבל סתירה לכך שקיימת מחלקה מגודל 5 ולהסיק שחבורה מסדר 15 היא בהכרח אבלית.

שאלה ממבחן תשס"ט, מועד א':

מצאו את כל החבורות הסופיות להן שתי מחלקות צמידות.

תשובה:

נשים לב שאיבר היחידה תמיד נמצא במרכז, וכל איבר במרכז הוא במחלקת צמידות משל עצמו. אם יש עוד איבר במרכז, אזי כבר יש לנו 2 מחלקות צמידות, ולכן יש רק 2 איברים בחבורה, כלומר החבורה היא $\mathbb{Z}_2$. אחרת רק היחידה במרכז, ונקבל לפי משוואת המחלקות $|G|=1+[G:Z_x]$, כאשר x איבר כלשהו השונה מהיחידה, וגם $[G:Z_x]\ge 2$. אבל ידוע ש $[G:Z_x]\,|\,|G|$, אבל $|G|=[G:Z_x]+1$ וזה ייתכן רק אם $[G:Z_x]=1$, סתירה לכך ש $[G:Z_x]\ge 2$.

תרגיל: כל חבורה מסדר p^2 היא אבלית.

פתרון: כאמור Z(G)=G או Z(G)={e}. אם Z(G)=G אז סיימנו. אחרת, Z(G)={e}. אבל אז נקבל $p^2=|G|=1+tp$ (כל מחלקת צמידות חייבת לחלק בגודלה את p^2, אבל המקרה היחיד האפשרי כאן הוא p). נעבור ל (mod p), ונקבל $0\equiv 1 (\bmod p)$, סתירה.

תרגול 10

עוד על פעולות:

הגדרה: נאמר ששתי תת-קבוצות (בפרט ת"ח) $S,T \subseteq G$ הן **צמודות** אם קיים $g \in G$ כך ש $gSg^{-1} = T$.

תרגילי בית:

1. בדקו שצמידות תת-חבורות הוא יחס שקילות על קבוצת הת"ח של G.
2. הראו ששתי ת"ח צמודות הן איזומורפיות.
3. הוכיחו או הפריכו: ת"ח איזומורפיות הן צמודות (רמז: חבורה אבלית).

דוגמא: נגדיר פעולה של חבורה G על X , קבוצת תת החבורות של G, ע"י הצמדה:

$$\varphi(g)(H) = gHg^{-1}$$

תרגיל בית: הראו שהפעולה הנ"ל היא אכן פעולה.

נשים לב שהמייצב של ת"ח תחת הפעולה הנ"ל הוא בדיוק המנרמל (נורמליזטור Normalizer) של הת"ח:

$$St(H) = N_G(H) = \{g \in G \mid gHg^{-1} = H\} \leq G$$

המסלול של ת"ח H היא קבוצת כל הת"ח של G שצמודות ל H.

ניתן לחשב את מספר הת"ח שצמודות ל H ע"י: $|O(H)| = [G : N_G(H)]$.

תרגילי בית:

1. הראו ש $H \lhd N_G(H)$.
2. הראו שאם $H \lhd K \leq G$ אזי $K \leq N_G(H)$ (כלומר המנרמל של H היא הת"ח המקסימלית כך ש H היא תח"נ שלה).
3. אם G חבורה אבלית אזי $N_G(H) = G$.
4. הוכיחו או הפריכו: אם $H \leq G$ כך ש H אבלית, אזי $N_G(H) = G$.

תרגיל: מיהן נקודות השבת תחת הפעולה הנ"ל?

פתרון: H נקודת שבת אם ורק אם $N_G(H)=G$. זה קורה אם ורק אם $gHg^{-1}=H$ לכל $g\in G$ וזה קורה אם ורק אם H היא ת"ח נורמלית של G.

הגדרה: בהנתן פעולה של חבורה G על קבוצה X, נגדיר את **מרחב המסלולים** להיות קבוצת המסלולים של הפעולה. כלומר:

$$X/G:=\{O(x)\mid x\in G\}$$

שימו לב: קבוצה זאת היא קבוצה של קבוצות. היא גם קבוצת המנה של יחס השקילות על X שמוגדר ע"י "x נמצא במסלול של y". כל הקבוצות ב X/G הן זרות ואיחודן הוא כל X.
כנהוג בקבוצות מנה, ניתן לקחת נציג ממחלקת שקילות, ולתת לו לייצג איבר ב X/G.

תרגיל: תנו דוגמא לחבורה G וקבוצה אינסופית X, כך ש G פועלת עליה, ומרחב המסלולים הוא מסדר 3.

פתרון: (בוודאי ש G חייבת להיות גם אינסופית, אחרת מספר המסלולים היה אינסופי. מדוע?).
ניקח $X=\mathbb{Z}$ (חבורה חיבורית) וגם $G=3\mathbb{Z}$ (כת"ח של $\mathbb{Z}$). לת"ח יש פעולה טבעית על חבורה ע"י כפל משמאל, במקרה זה כיוון ש $3\mathbb{Z}\le\mathbb{Z}$ הן חבורות חיבוריות, הפעולה היא חיבור משמאל.
כלומר $3k*z=3k+z$ כאשר $3k\in G=3\mathbb{Z}, z\in X=\mathbb{Z}$.

המסלול של איבר $z\in X=\mathbb{Z}$ הוא כל המספרים עם אותו שארית מודולו 3 (הראו זאת ישירות).
למעשה זה נובע מכך שהראינו בתרגול הקודם שאם $H\le G$ ו H פועלת על G ע"י כפל משמאל, אזי $O(g)=Hg$, כלומר המסלול של איבר ב G הוא המחלקה הימנית שלו.

לכן $X/G:=\{O(0),O(1),O(2)\}$.

שימו לב שמקרה זה שני הסימונים של חבורת מנה ומרחב המסלולים תואמים:
$\mathbb{Z}/3\mathbb{Z}=\{3\mathbb{Z},3\mathbb{Z}+1,3\mathbb{Z}+2\}$.

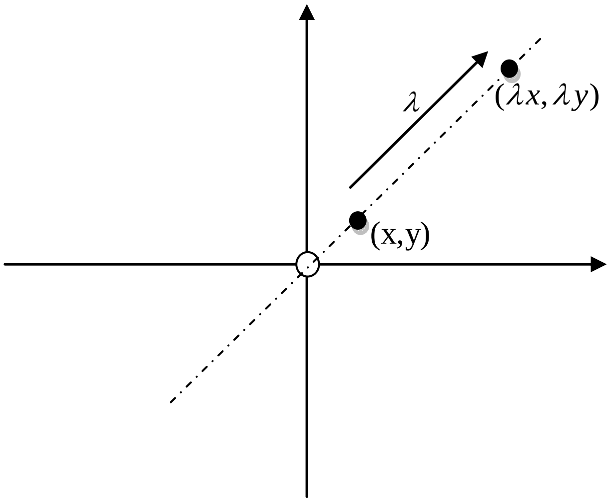
דוגמא: המרחב הפרויקטיבי.

בהנתן שדה $\mathbb{F}$ ראינו ש $\mathbb{F}^*$ היא חבורה כפלית. נגדיר פעולה של $\mathbb{F}^*$ על המרחב $\mathbb{F}^{n*}=\mathbb{F}^n\setminus\bar{0}$ כלומר מרחב n-מימדי ללא ראשית הצירים:

$$\lambda*(x_1,\dots,x_n)=(\lambda x_1,\dots,\lambda x_n)$$

כאשר $\lambda\in\mathbb{F}^*,(x_1,\dots,x_n)\in\mathbb{F}^{n*}$.

איך נראית הפעולה מנקודת מבט גיאומטרית? לדוגמא בשני מימדים:



כלומר הפעולה מזיזה את הנקודה על הישר המחבר בינה לבין ראשית הצירים.

אם כך, מסלול של נקודה הוא הישר המחבר בינה לבין ראשית הצירים, ללא ראשית הצירים.

לכן מרחב המסלולים הוא בהתאמה חח"ע עם קבוצת כל הישרים העוברים דרך הראשית.

מרחב המסלולים הזה נקרא **המרחב הפרויקטיבי**, ויש לו שימוש נרחב בגיאומטריה, והסימון שלו הוא:

$$\mathbb{FP}^{n-1} = \mathbb{F}^{n*}/\mathbb{F}^{*}$$

מדוע n-1? לא נסביר זאת כאן במדויק, אבל זה די אינטואיטיבי שאם אוסף הנקודות הוא n-מימדי, אזי אוסף הישרים דרך הראשית הוא n-1 מימדי. אנחנו גם מבצעים מנה ב"מרחב חד-מימדי" ($\mathbb{F}^{*}$), וגם זה מרמז על ירידה במימד אחד.

כעת נראה עבור הדוגמא $\mathbb{CP}^1 = \mathbb{C}^{2*}/\mathbb{C}^{*}$ בחירה של נציג אחד מכל מסלול, וניתן פרשנות גאומטרית לבחירה זו. נסמן $(x_1, y_1) \sim (x_2, y_2)$ אם שתי הנקודות נמצאות באותו מסלול. נחלק לשני מקרים:

<u>מקרה א'</u>: $x_1 \neq 0$. אזי $(x_1, y_1) \sim (1, \frac{y_1}{x_1}) \sim (1, y)$, כאשר $y = \frac{y_1}{x_1} \in \mathbb{C}$. לכן קיבלנו שעבור כל נקודה $(x_1, y_1) \in \left(\mathbb{C}^2\right)^*$ כך ש $x_1 \neq 0$ מתאימה בדיוק נקודה מרוכבת אחת.

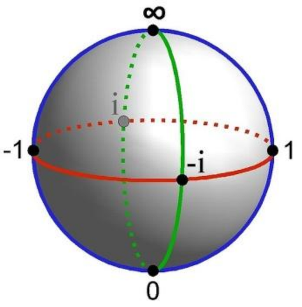
<u>מקרה ב'</u>: $x_1 = 0$. אזי בהכרח $y_1 \neq 0$ (מדוע?). לכן $(x_1, y_1) \sim (0, y_1) \sim (0,1)$. לכן יש רק מסלול אחד כזה, והוא מתאים לנקודה (שונה מכל נקודה במקרה הקודם.

סה"כ קיבלנו את המישור המרוכב + נקודה אחת נוספת (שלא על המישור).

במרחב הפרויקטיבי נותנים לנקודה הנוספת הזאת את הפירוש שהיא **הנקודה באינסוף**.

מה האינטואיציה? אם $y_1 \to \infty$ אזי בפרט $y_1 \neq 0$, ולכן $(x_1, y_1) \sim (\frac{x_1}{y_1}, 1) \to (0,1)$.

שימו לב שהמרחב הפרויקטיבי הוא מישור ממשי דו-מימדי, כאשר מוסיפים את הנקודה באינסוף, ניתן לדמיין את המישור מתקפל אל הנקודה האינסופית, וביחד הם יוצרים ספירה (שנקראת **הספירה של רימן**).



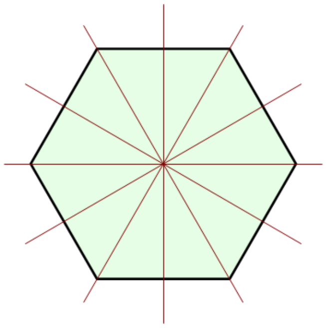
כלומר, $\mathbb{CP}^1 = \mathbb{C} \cup \{\infty\}$

למידע נוסף: http://he.wikipedia.org/wiki/מרחב_פרויקטיבי.

<u>תרגיל בית</u>: נסו להבין איך נראים המרחבים $\mathbb{CP}^2, \mathbb{RP}^1, \mathbb{RP}^2$.

<u>חבורות דיהדרליות:</u>

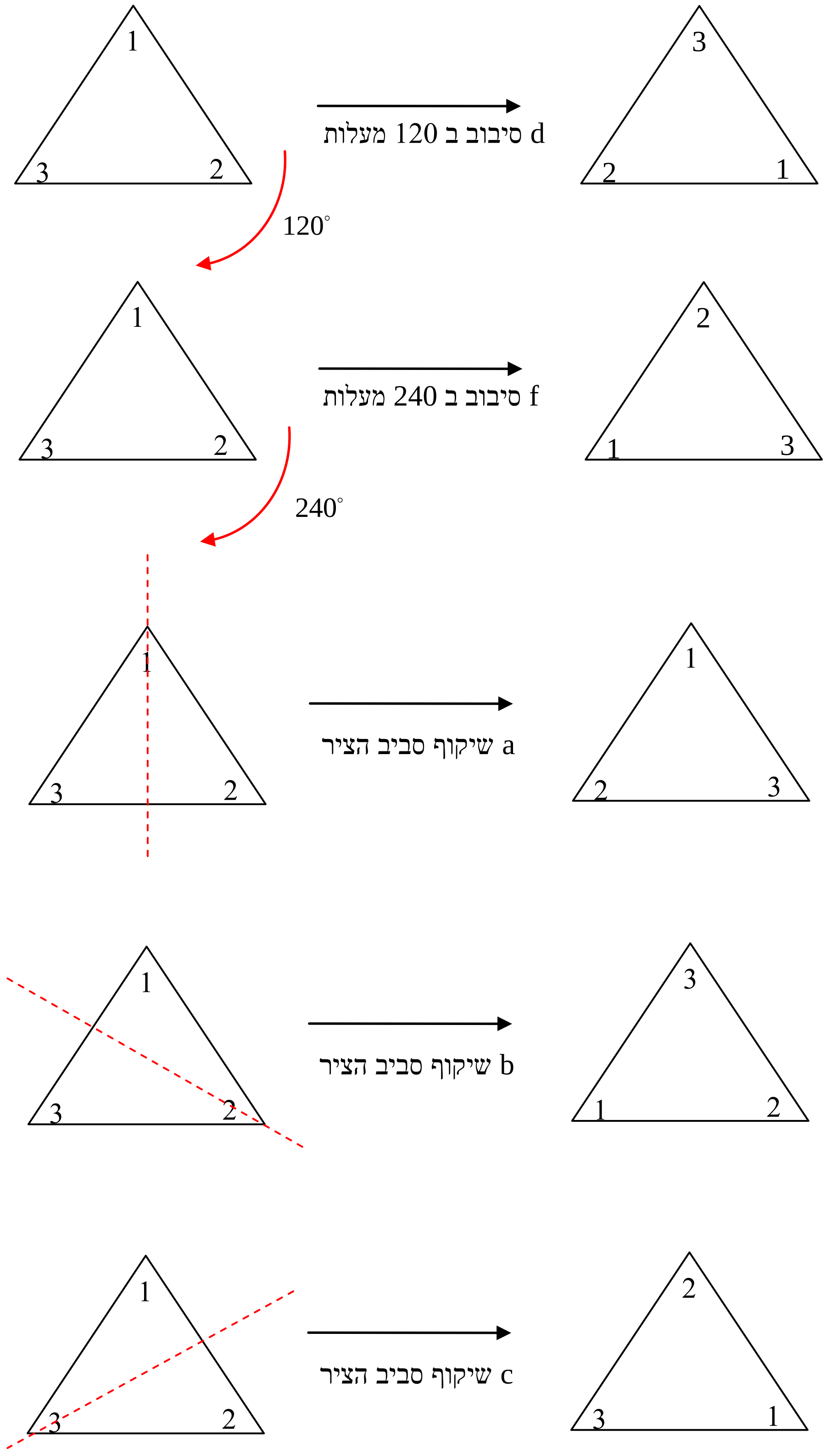
יהי $n \geq 3$. החבורות הדיהדרליות D_n הן חבורות לא קומוטטיביות מסדר 2n של סימטריות של מצולעים משוכללים (עם n צלעות), הכוללות סיבובים ושיקופים של המצולע. לדוגמא אלה כל השיקופים של משושה משוכלל:



לכל מצולע משוכלל עם n צלעות יש n שיקופים ו n סיבובים (איבר היחידה נחשב כסיבוב ב 360 מעלות, או סיבוב טריויאלי).

פעולת החבורה היא הרכבה של ההעתקות הנ"ל (כלומר קוראים מימין לשמאל). נראה בפירוט את הדוגמא של D_3 , חבורת הסימטריה של המשולש:

d,f הם סיבובים ב 120 ו 240 מעלות בהתאמה. a,b,c הם שלושת השיקופים.


d סיבוב ב 120 מעלות
120°
f סיבוב ב 240 מעלות
240°
a שיקוף סביב הציר
b שיקוף סביב הציר
c שיקוף סביב הציר

בדקו שמתקיים

$$d^2 = f = d^{-1}, f^2 = d = f^{-1},$$
$$a^2 = b^2 = c^2 = e,$$
$$da = c,$$
$$ada = f = d^{-1}$$

וכו'. טבלת הכפל של D_3 :

*	e	a	b	c	d	f
e	*e*	a	b	c	d	f
a	a	*e*	d	f	b	c
b	b	f	*e*	d	c	a
c	c	d	f	*e*	a	b
d	d	c	a	b	f	*e*
f	f	b	c	a	*e*	d

כל סימטריה של מצולע משוכלל היא תמורה על הקדקדים (ההיפך לא תמיד נכון, **נסו** למצוא תמורה ב D_4 שאינה מתאימה לאף שיקוף/סיבוב). כלומר ניתן לשכן את החבורה D_n בחבורה S_n. במקרה של D_3 יש 6 תמורות של הקדקדים, אבל ב S_3 יש 6 איברים, ולכן S_3 ו- D_3 הן חבורות איזומורפיות.

ניתן להציג סיבובים ושיקופים של D_n כהעתקות לינאריות במישור הממשי - כלומר ניתן להציג את כל החבורות D_n כתת-חבורות (נגדיר תת-חבורות בהמשך התרגול) של $GL_2(\mathbb{R})$.

עבור D_4 נראה הצגה כנ"ל:

$$R_0=\begin{pmatrix}1&0\\0&1\end{pmatrix},\quad R_1=\begin{pmatrix}0&-1\\1&0\end{pmatrix},\quad R_2=\begin{pmatrix}-1&0\\0&-1\end{pmatrix},\quad R_3=\begin{pmatrix}0&1\\-1&0\end{pmatrix},$$

$$S_0=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad S_1=\begin{pmatrix}0&1\\1&0\end{pmatrix},\quad S_2=\begin{pmatrix}-1&0\\0&1\end{pmatrix},\quad S_3=\begin{pmatrix}0&-1\\-1&0\end{pmatrix}.$$

R הן מטריצות הסיבוב, ו S הן מטריצות השיקוף.

<u>תרגיל בית:</u> הראו ש D_4 המוצגת ע"י מטריצות היא חבורה, ונסו להתאים כל מטריצה לסימטריה המתאימה.

בצורה כללית: בחבורה D_n הסיבובים והשיקופים הם:

$$R_k=\begin{pmatrix}\cos 2\pi k/n & -\sin 2\pi k/n\\ \sin 2\pi k/n & \cos 2\pi k/n\end{pmatrix}$$

$$S_k=\begin{pmatrix}\cos 2\pi k/n & \sin 2\pi k/n\\ \sin 2\pi k/n & -\cos 2\pi k/n\end{pmatrix}.$$

כאשר R_k הם הסיבובים ו S_k הם השיקופים. שימו לב שהמטריצות של השיקוף בעלות דטרמיננטה 1-, והסיבובים עם דטרמיננטה 1.

<u>טענות:</u>

1. קבוצת הסיבובים בחבורה D_n היא תת-חבורה ציקלית מסדר n, ונוצרת ע"י סיבוב ב $\frac{2\pi}{n}$ שנסמנו σ. יתר על כן $<\sigma>\triangleleft D_n$ (**מדוע?**).

2. $\tau\sigma\tau=\sigma^{n-1}=\sigma^{-1}$. בנוסף מתקיים $\tau\sigma=\sigma^{n-1}=\sigma^{-1}\tau^{-1}=\sigma^{-1}\tau$.

3. יהיה τ שיקוף כלשהו (כל שיקוף יוצר ת"ח ציקלית מסדר 2), אזי $D_n=<\sigma,\tau>$. בפרט, כל איבר ב D_n ניתן להצגה כ $\sigma^i\tau^j$ כאשר $0\le i<n, 0\le j\le 1$.

4. קיים שיכון $D_n\to S_n$ ע"י (שימו לב שמספיק להגדיר לאן היוצרים עוברים):
$\sigma\mapsto(1,2,...,n)$. $\tau\mapsto(2,n)(3,n-1)\ldots(\left\lceil\frac{n}{2}\right\rceil+1,\left\lfloor\frac{n}{2}\right\rfloor+1)$.

<u>תרגיל:</u> הראו ש $\tau\sigma^i\tau=\sigma^{-i}$ לכל $0\le i\le n-1$.

<u>פתרון:</u> $\tau\sigma^i\tau=(\tau\sigma\tau)(\tau\sigma\tau)(\tau\sigma\tau)\cdots(\tau\sigma\tau)=\sigma^{-1}\sigma^{-1}\sigma^{-1}\cdots\sigma^{-1}=\sigma^{-i}$ (כאשר השיוויון האמצעי נובע מטענה 2 לעיל).

מכפלה i פעמים

הערה: בעזרת התרגיל האחרון ניתן להוכיח את טענה 3 לעיל. כל איבר שהוא מכפלה מהצורה $\tau^{j_1}\sigma^{i_1}\tau^{j_2}\sigma^{i_2}\tau^{j_3}\cdots\in<\sigma,\tau>$ ניתן להביא לצורה $\sigma^i\tau^j$ ע"י שימוש חוזר בתרגיל האחרון.

תרגיל:

1. האם $D_4\cong S_4$? לא. שתי החבורות מסדר שונה (אחת מסדר 24 והשניה מסדר 8).
2. האם $D_{12}\cong S_4$? לא. בחבורה S_4 יש איברים רק מסדרים 1,2,3,4. ב D_{12} יש איבר מסדר 12 (הסיבוב ב 30 מעלות).

תרגיל: האם $D_n\cong\mathbb{Z}_n\times\mathbb{Z}_2$?

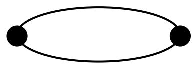
פתרון: למרות שהחבורות הן מאותו סדר, $D_n\ncong\mathbb{Z}_n\times\mathbb{Z}_2$ זאת כיוון שהחבורה מימין היא אבלית (**מדוע?**), והחבורה משמאל לא (במקרה ש $n\neq 2$), ניתן לראות את חוסר האבליות מטענה 2 לדוגמא.

תרגיל: H ת"ח ציקלית של D_n . האם בהכרח $H\lhd D_n$?

פתרון: לא. נסתכל על $<\tau>=\{1,\tau\}$. אזי $\sigma\tau\sigma^{-1}=\sigma\tau\sigma^{n-1}=\tau\sigma^{-1}\sigma^{n-1}=\tau\sigma^{n-2}\notin<\tau>$.

המקרה של n=2:

במקרה של n=2 אין מצולע משוכלל בן שתי צלעות, אך ניתן לראות את החבורה D_2 כחבורות הסימטריות של האובייקט הגיאומטרי הבא:



הוא בעל 2 "צלעות" ושני קדקדים. וקל לראות שיש לו שני סיבובים ושני שיקופים (הוכיחו זאת). לכן $D_2\cong\mathbb{Z}_2\times\mathbb{Z}_2$. רואים ש- D_2 יוצאת דופן, כי היא חבורה אבלית.

תרגול 11

תרגיל: תהי G חבורה, $a \in G$. הראו ש $Z(G) \leq Z_a$.

פתרון: (שימו לב שמספיק להראות הכלה $Z(G) \subseteq Z_a$, מדוע?) אם $g \in Z(G)$ אזי לפי הגדרה $gx = xg$ לכל $x \in G$. בפרט מתקיים עבור a, ולכן $ga = ag$ ולכן $g \in Z_a$.

תרגיל: תהי G חבורה לא אבלית מסדר p^3 עבור p ראשוני. יהי $a \notin Z(G)$. הוכיחו:

א. $|Z(G)| = p, |Z_a| = p^2, |conj(a)| = p$ (להוכיח משמאל לימין)

ב. מצאו את מספר מחלקות הצמידות ב G.

פתרון:

א. לפי משפט לגרנג', $|Z(G)|\,|\,|G|$, לכן $|Z(G)| = 1, p, p^2, p^3$. אבל:

I. $|Z(G)| \neq p^3$ כי הנחנו שהחבורה אינה אבלית.

II. $|Z(G)| \neq 1$ כי המרכז של חבורת p אינו טריויאלי (לפי נוסחת המחלקות).

III. $|Z(G)| \neq p^2$ כי אחרת לפי משפט לגרנג' נקבל $|G / Z(G)| = p$ ואז המנה היא ציקלית, ולפי משפט זה ייתכן רק אם החבורה אבלית, סתירה.

לכן קיבלנו ש $|Z(G)| = p$.

כעת נחשב את $|Z_a|$: כיוון ש Z_a ת"ח נקבל לפי לגרנג' ש $|Z_a| = 1, p, p^2, p^3$, אבל:

I. $|Z_a| \neq 1$ כי לפי התרגיל הקודם מתקיים $Z(G) \leq Z_a$ ולכן $|Z_a| \geq |Z(G)| = p$.

II. $|Z_a| \neq p^3$ כי אם $|Z_a| = p^3$ אזי $Z_a = G$ ואז $a \in Z(G)$, סתירה, כיוון שהנחנו ש $a \notin Z(G)$.

III. $|Z_a| \neq p$ כיוון שאז לפי התרגיל הקודם נקבל $Z(G) = Z_a$ אבל $a \in Z_a$ ונקבל סתירה להנחה ש $a \notin Z(G)$.

לכן קיבלנו ש $|Z_a| = p^2$. כעת לפי משפט $p = \frac{p^3}{p^2} = \frac{|G|}{|Z_a|} = [G:Z_a] = |conj(a)|$.

ב. לכל איבר $g \in Z(G)$ מתאימה מחלקת צמידות בגודל 1. לכן לפי סעיף א, יש p מחלקות צמידות בגודל 1. בנוסף כל מחלקת צמידות אחרת (שוב לפי סעיף א) היא בגודל p.
כיוון שכל שתי מחלקות צמידות שונות הן זרות, נקבל שיש $(p^3 - p)/p = p^2 - 1$ מחלקות צמידות בגודל p.

סה"כ קיבלנו $p^2 + p - 1$ מחלקות צמידות.

משפטי סילוא (Sylow)

הגדרה: תהי G חבורה סופית, כך שמתקיים $p^m \mid |G|, p^{m+1} \nmid |G|$, עבור p ראשוני. תת חבורה מסדר p^m של G נקראת תת חבורה **p-סילוא**.

דוגמא: נמצא חבורת 2-סילוא ב S_3: כיוון ש $|S_3| = 6$ בהכרח חבורת 2-סילוא היא מסדר 2. יש 3 ת"ח כאלה: $<(1,2)>,<(2,3)>,<(1,3)>$. נשים לב שהראינו כעת שתת-חבורת p-סילוא לא בהכרח יחידה! בנוסף גם הראינו שתת-חבורת p-סילוא לא בהכרח תת-חבורה נורמלי.
נמצא חבורת 3-סילוא ב S_3: כיוון ש $|S_3| = 6$ בהכרח חבורת 2-סילוא היא מסדר 3. יש רק ת"ח אחת כזאת: $<(1,2,3)>$.

משפט (הכללה של משפט קושי): לכל G סופית, p ראשוני, אם $p^m \mid |G|$ אז קיימת ת"ח של G מסדר p^m.

מסקנה: משפט סילוא 1: תהי G חבורה סופית. אז לכל ראשוני p המחלק את סדר G, G מכילה תת חבורה p סילוא.

דוגמא: D_4 היא חבורה בה תת-חבורת 2-סילוא היא D_4, כיוון שמתקיים $|D_4| = 2^3$. לכן לפי המשפט הלפני-אחרון יש ת"ח של D_4 מסדרים 2,4. ת"ח מסדר 4 נוצרת ע"י סיבוב ב 90 מעלות, ות"ח מסדר 2 נוצרת לדוגמא ע"י אחד השיקופים.

תזכורת:

הגדרה: נאמר ששתי תת-קבוצות (בפרט ת"ח) $S,T \subseteq G$ הן **צמודות** אם קיים $g \in G$ כך ש $gSg^{-1} = T$.

הערה: נשים לב שאם $H,K \le G$ ת"ח צמודות **שונות** של G אזי H,K אינן תח"נ של G. זאת כיוון שקיים $g \in G$ כך ש $gHg^{-1} = K \neq H$ ולכן H אינה אינוריאנטית להצמדה, ולכן אינה תח"נ (ואותו דבר עבור K).

משפט סילוא 2: כל תתי חבורות p -סילוא של חבורה סופית G צמודות זו לזו.

הערה: אם H ת"ח p-סילוא של G, אזי gHg^{-1} היא גם ת"ח p-סילוא של G, לכל $g \in G$. זאת כיוון ש $gHg^{-1} \cong H$ (הראו זאת).

מסקנה: יש רק ת"ח p-סילוא אחת אם ורק אם היא תח"נ.

הוכחה: אם קיימת ת"ח p-סילוא אחת H, אזי לפי הנחה $gHg^{-1} = H$ לכל $g \in G$, אחרת היו שתי תת-חבורות p-סילוא לפי ההערה. לכן H תח"נ. אם H ת"ח p-סילוא נורמלית, אזי $gHg^{-1} = H$ לכל $g \in G$, ואם היתה תת-חבורת p-סילוא שניה K אזי הן היו צמודות לפי משפט סילוא 2, כלומר קיים $g \in G$ כך ש $gHg^{-1} = K \neq H$, סתירה.

איך מחשבים את מספר תת-חבורות p-סילוא?

בתרגול הקודם ראינו את פעולת ההצמדה של חבורה G על קבוצת הת"ח של G:

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

תהי H ת"ח p-סילוא. אזי:

. $St(H) = N_G(H) = \{g \in G \mid gHg^{-1} = H\}$

$O(H) = \{gHg^{-1} \mid g \in G\}$ אבל אלה בדיוק כל תת-חבורות p-סילוא לפי משפט סילוא 2 וההערה שאחריו. לכן מספר ת"ח p-סילוא הוא $[G : N(H)]$ $= |O(H)|$.

דוגמא:

נחזור לדוגמא של S_3. אזי קל לראות שהת"ח שצמודות ל $H =< (1,2) >$ הן בדיוק $< (1,2) >, < (1,3) >, < (2,3) >$, ולכן מספר תת-חבורות p-סילוא הוא 3.

נחשב מחדש בכל זאת בעזרת המנרמל:

$$N(H) = \{id, (1,2)\}$$

(בדקו שאכן כל תמורה אחרת אינה מצמידה את H לעצמה). לכן:

$$[S_3 : N(H)] = \frac{6}{2} = 3$$

וקיבלנו שאכן יש 3 תת-חבורות p-סילוא.

משפט סילוא 3: יהי r_p מספר תתי החבורות של p -סילוא של חבורה סופית G אז:

- $r_p \mid |G|$
- $r_p \equiv 1 \bmod p$

מסקנה: $\gcd(r_p, p) = 1$.

מסקנה: חבורת p-סילוא היא נורמלית אם ורק אם $r_p = 1$ (נובע ישירות מהמסקנה ממשפט סילוא 2).

תרגיל: אם G אינה חבורת p, ומתקיים $p \mid |G|$ וגם $r_p = 1$ (כלומר יש ת"ח p - סילוא יחידה) אז G אינה פשוטה. כלומר קיימת $H \triangleleft G$ כאשר $H \neq G, \{e\}$.

פתרון: תהי H ת"ח p-סילוא, אזי בגלל ש $r_p = 1$ מתקיים $gHg^{-1} = H$ לכל $g \in G$, כיוון שגם gHg^{-1} היא חבורת p-סילוא (אבל יש רק אחת כזאת). לכן H תח"נ של G, והיא אינה ת"ח טריויאלית בגלל ההנחות (מדוע?).

משפטון: r_p מחלק את $\frac{|G|}{p^m}$.

הוכחה:

$$H \leq G, |H| = p^m$$
$$|G| = |H|[G:H] = p^m * n, p \nmid n$$
$$r_p \mid |G|, r_p \bmod p = 1 \Rightarrow \gcd(r_p, p^m) = 1 \Rightarrow r_p \mid n = \frac{|G|}{p^m}$$

תרגיל: הראו שחבורה מסדר 40 אינה פשוטה

תשובה: $40 = 5 * 2^3$ לפי משפטי p סילוא יש תת חבורה 2 סילוא מסדר 8 ויש תת חבורה 5 סילוא מסדר 5. ובאופן טריוואלי יש תת חבורה מסדר $1, 40$ שאלה האם חבורה מסדר 40 פשוטה? לפי המשפט הקודם מספיק להוכיח $r_5 = 1 \vee r_2 = 1$.

לפי משפט סילוא 3 מתקיים $r_5 \mid 40, r_5 \equiv 1 \bmod 5$ לכן

$$r_5 \in A = \{1, 2, 4, 8, 5, 10, 20, 40\}$$

נקבל $r_5 \in B = \{1, 6, 11, 16, 21, 26, 31, 36, 41, ...\}$

$$A \cap B = \{1\} \Rightarrow r_5 = 1$$

לכן חבורה מסדר 40 אינה פשוטה.

<u>תרגיל:</u> האם חבורה מסדר 10 פשוטה?

<u>תשובה:</u> $10=5*2$ לפי משפט סילו קיימת תת חבורה 5 סילוא מסדר 5 נסמן אותה ב

$H\le G, |G|=10$ לפי לגראנז' $|G|=|H|[G:H]$ במקרה שלנו $10=5*[G:H]\Leftrightarrow[G:H]=2$

וכבר הוכחנו כל תת חבורה מאינדקס 2 נורמלית לכן חבורה מסדר 10 אינה פשוטה.

<u>מסקנה:</u> באופן כללי כל חבורה מסדר $2p^m$ עבור p ראשוני אינה פשוטה (אותה הוכחה (בערך)).

<u>תרגיל:</u> אם $|G|=pq$ כך ש $p\neq q$ ראשוניים ו $q\neq 1 \bmod p$ אז יש ל G ת"ח p סילוא נורמלית:

<u>הוכחה:</u>

$$r_p \mid pq \in\{1,p,q,pq\},$$
$$r_p = 1 \bmod p \in\{1\}$$
$$\Rightarrow r_p=1$$

ולכן לפי משפט G קיימת תת חבורה p סילוא שהיא נורמלית ולכן G אינה פשוטה.

<u>הערה:</u> אם מוסיפים את הדרישה $p<q$ בתרגיל, נקבל שגם $r_q=1$, זאת כיוון שאם $p<q$ אזי $p\not\equiv 1(\bmod q)$, **ואז:**

$$r_q \mid pq \in\{1,p,q,pq\},$$
$$r_q = 1 \bmod q \in\{1\}$$
$$\Rightarrow r_q=1$$

מכאן ניתן להסיק שהחבורה G היא ציקלית (נראה זאת בתרגול הבא), כלומר נקבל את המשפט:

<u>משפט:</u> יהיו p,q ראשונים $q\not\equiv 1 \bmod p, p<q$ כל חבורה מסדר pq היא ציקלית (כלומר איזומורפית ל Z_{pq})

<u>תרגיל:</u> הוכח כי חבורה מסדר 84 אינה פשוטה.

<u>פתרון:</u> לפי המשפטון נקבל:

$$r_7 \mid \frac{84}{7} = 12 \Rightarrow r_7 \in \{1,2,3,4,6,12\} \wedge$$
$$r_7 \bmod 7 = 1 \Rightarrow r_7 = 1$$

קיבלנו $r_7 = 1$ ולכן לפי משפט החבורה G אינה פשוטה.

<u>תרגיל עזר:</u> יהי p ראשוני, תהי G חבורה, ויהיו H,K שתי תת-חבורות שונות מסדר p. אזי $H \cap K = \{e\}$.

<u>הוכחה:</u> $H \cap K \le G$ ולכן $H \cap K \le H$, לכן לפי לגרנג' נקבל $|H \cap K| = 1, p$ אבל אם $|H \cap K| = p$ נקבל ש H=K, סתירה, לכן $|H \cap K| = 1$.

<u>מסקנה:</u> מספר האיברים מסדר p ראשוני בחבורה G מתחלק ב p-1.

<u>הוכחה:</u> כל איבר x מסדר p שייך לת"ח של G מסדר p (לדוגמא ל <x>), ובחבורה כזאת יש p-1 איברים מסדר p (מדוע?). יהי k מספר הת"ח מסדר p. לפי תרגיל העזר נקבל שיש k(p-1) איברים מסדר p.

<u>תרגיל:</u> אם $|G| = p^2 q$, p,q ראשונים זרים.אז או שיש ל G תת חבורה נורמלית p-סילוא (מסדר ?) **או** שיש ל-G תת חבורה נורמלית q-סילוא (מסדר ?). בכל מקרה G אינה פשוטה!

<u>הוכחה:</u> יש ל G תתי חבורות p-סילוא מסדר p^2 ו q-סילוא מסדר q. נניח בשלילה שאין ל G תח"נ לכן בהכרח $r_q, r_p > 1$. לפי משפטי סילוא נקבל ש:

$$1 < r_p, r_q \mid |G| = p^2 q \Rightarrow r_p, r_q \in \{p, q, p^2, p^2 q\}$$
$$r_p \bmod p = 1 \Rightarrow r_p = q \Rightarrow q > p$$
$$r_q \bmod q = 1 \Rightarrow r_q \in \{p, p^2\}$$

עכשיו כל איבר מסדר q יוצר תת חבורה q סילוא בעלת q איברים מסדר q. כל 2 תתי חבורות שונות מסדר q נחתכות רק ב $\{e\}$ ולכן ב G יש $r_q(q-1)$ איברים מסדר q. אם:

- $r_q = p^2$, אזי מספר האיברים שאינם מסדר q הם:

  $|G| - p^2(q-1) = p^2 q - p^2 q + p^2 = p^2$ נסמן ב P את תת חבורה p סילוא בתת חבורה זו יש p^2 שאינה מסדר q אבל יש בסך הכל p^2 איברים שאינם מסדר q ולכן כולם P ואין עוד תת חבורה P סילוא אחרת (כי כל האברים נמצאים ב-P) לכן $r_p = 1$, סתירה.

- $r_q = p$ לכן $p \bmod q = 1 \wedge q > p \Rightarrow p = 1$ וקיבלנו סתירה.

לכן קיבלנו סתירה להנחה, ומכאן שבהכרח $r_p = 1 \vee r_q = 1$. בכל מקרה החבורה אינה פשוטה!

תרגול 12

משפט (סילוא):

אם H תת-חבורת-p של G אזי קיימת תת-חבורת סילוא של G כך ש H מוכלת בה.

תרגיל:

הוכיחו או הפריכו: אם H תת-חבורת-p **אבלית** של G אזי H מוכלת בכל תת-חבורת p-סילוא של G.

פתרון:

נפריך: ניקח $G=S_3$, $H=<(1,2)>$. בוודאי ש H אבלית, והיא חבורת-2, אבל היא אינה מוכלת בכל תת-חבורת 2-סילוא של G, שהן כל החבורות מסדר 2.

תרגיל:

הוכיחו ללא שימוש במשפט הנ"ל: תהי H תת-חבורת-p המוכלת במרכז של G אזי H מוכלת בכל תת-חבורת p-סילוא של G.

פתרון:

תהי K תת-חבורת p-סילוא כלשהי של G (קיימת כזאת לפי משפט סילוא 1). אזי $K \lhd N(K)$ (זה נכון לכל תת-חבורה, **הראו זאת**). כיוון ש $H \le Z(G)$, גם $H \le N(K)$ (**הראו זאת**) ולכן $HK \le N(K)$. $|HK|=\frac{|H||K|}{|H\cap K|}$ ולכן HK היא גם תת-חבורת-p של G, והיא מכילה את K, ולכן היא שווה לה. לכן $H \le K$.

מיון חבורות אבליות

שאלה: מתי מכפלה (פנימית) של שתי תת-חבורות איזומורפית למכפלה (החיצונית) הישרה שלהן?

כלומר $H,K \le G$, מתי מתקיים $HK \cong H \times K$?

שימו לב:

א. זכרו שבהרבה מקרים HK היא בכלל לא ת"ח, ואז השאלה לא רלוונטית.

ב. $H \times K$ אינה ת"ח של G! (במקרה הטוב היא איזומורפית לתת-חבורה שלה).

ג. במיוחד מענין המקרה בו $HK = G \cong H \times K$ כי אז אנחנו מקבלים "פירוק" של החבורה.

<u>דוגמאות:</u>

1. נסתכל על $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ אזי אם ניקח $H =<(1,0)>, K =<(0,1)>$ אזי $HK = G \cong H \times K$. את השיווין השמאלי בדקו אתם, האיזומורפיזם מימין נובע כיוון ש H, K חבורות מסדר 2, ולכן איזומורפיות ל $\mathbb{Z}_2$. במקרה זה שמים לב ש H,K הן תח"נ (כי החבורה G היא אבלית).

2. נסתכל על $G = S_3$ אז ניקח $H =<(1,2)>, K =<(1,2,3)>$, ואז $HK = G$ כיוון ש $|HK| = \frac{|H||K|}{|H \cap K|} = \frac{2 \cdot 3}{1} = 6 = |G|$ ($|H \cap K| = 1$ בגלל ש $H \cap K \le H, H \cap K \le K$ ולפי לגרנג' נקבל $|H \cap K| \mid 3, |H \cap K| \mid 2 \Rightarrow |H \cap K| = 1$). ניתן היה גם לבדוק ש $HK \le G$ לפי זה ש K היא תח"נ של G, אבל זה מיותר. אבל $HK = G \ncong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ כי החבורה מימין היא אבלית. נשים לב שבדוגמא זאת K היא תח"נ, אבל H אינה תח"נ.

3. נסתכל על $G = \mathbb{Z}_6$ אז ניקח $H =<2>= 2\mathbb{Z}_6 \cong \mathbb{Z}_3, K =<3>= 3\mathbb{Z}_6 \cong \mathbb{Z}_2$, נשים לב שכיוון ש G היא חבורה חיבורית, נרשום $H + K$ במקום HK. אזי קל לבדוק ש $H + K = G$ (ידנית או בעזרת שיקולי הסדר מהדוגמא הקודמת). כעת $H + K = G \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ כיוון ש $\mathbb{Z}_2 \times \mathbb{Z}_3$ היא חבורה ציקלית מסדר 6, עם היוצר (1,1). שוב במקרה זה אנחנו רואים ש H,K תח"נ.

רואים בדוגמאות שיש קשר בין הנורמליות של שתי הת"ח H,K לבין האיזומורפיות של מכפלתן ל $H \times K$. לכן נגדיר:

<u>הגדרה:</u> ! תהא G חבורה ו $H_1, H_2 \lhd G$ כך ש:

1. $H_1 \bigcap H_2 = e$
2. $H_1 H_2 = G$

אז G נקראת **מכפלה פנימית ישרה** של H_1, H_2.

משפט ("מכפלה חיצונית מכפלה פנימית"): תהי G חבורה ויהיו $A,B \le G$. אם G מכפלה פנימית ישרה של A ו B אזי היא מכפלה חיצונית ישרה של A ו B, או יותר במדויק $G \cong A\times B$.

הערה: ההפך של המשפט אינו מדויק, לדוגמא אם ניקח $G=\mathbb{Z}_2\times\mathbb{Z}_2$ וניקח $A=B=<(1,0)>$ אזי $G\cong A\times B$ אבל $AB=A\neq G$. אבל ניתן לומר:

משפט: אם G היא מכפלה (חיצונית) ישרה של תת-חבורות H,K אזי קיימות $A,B\le G$ כך ש G היא מכפלה פנימית ישרה של A,B, כך ש $A\cong H, B\cong K$.

הערה: בזכות שני המשפטים האחרונים אנחנו רואים שאין הבדל עקרוני בין "מכפלה חיצונית ישרה" לבין "מכפלה פנימית ישרה" ולכן כאשר אומרים מכפלה ישרה ניתן להתייחס אליה גם כפנימית וגם כחיצונית.

! משפט: תהי G חבורה אבלית סופית מסדר $\prod_{i=1}^{k} p_i^{r_i}$ כאשר p_i ראשוניים שונים אז $G\cong H_{p_1}\times H_{p_2}\times\ldots\times H_{p_k}$ כאשר H_{p_i} תת חבורה p_i סילוא. בוודאי שפירוק זה הוא יחיד עד כדי סדר הגורמים, ואם דורשים בפירוק ש $p_1<p_2<\ldots<p_k$ אזי הוא יחיד.

שימו לב: החבורות H_{p_i} אינן בהכרח ציקליות. לדוגמא עבור $G=\mathbb{Z}_2\times\mathbb{Z}_2$ יש רק חבורת סילוא אחת בפירוק, והיא $H_2=\mathbb{Z}_2\times\mathbb{Z}_2$.

מסקנה: כל חבורה אבלית סופית איזומורפית למכפלה ישרה של חבורות p.

משפט: כל חבורת- p אבלית איזומורפית למכפלה ישרה של חבורות-p ציקליות. גם כאן הפירוק יחיד עד כדי סדר הגורמים.

! המשפט היסודי לחבורות אבליות סופיות: כל חבורה אבלית סופית איזומורפית למכפלה ישרה של חבורות-p ציקליות. הפירוק יחיד עד כדי סדר הגורמים.

הוכחה: המשפט נובע ישירות משני המשפטים הקודמים. "האלגוריתם" כזה: קודם "מפרקים" כל חבורה אבלית למכפלה של חבורות-p, ואז "מפרקים" כל חבורת-p בפירוק הנ"ל למכפלה של חבורות-p ציקליות.

הערה: שימו לב: אם לא דורשים שהפירוק הוא לחבורות-p ציקליות, אז הפירוק אינו יחיד (אפילו לא עד כדי סדר הגורמים)!!! לדוגמא $\mathbb{Z}_2\times\mathbb{Z}_3\cong\mathbb{Z}_6$ הם שני פירוקים **שונים** של אותה חבורה לחבורות ציקליות. למעשה לכל חבורה ציקלית יש אינסוף פירוקים לחבורות ציקליות:

$$\mathbb{Z}_n=\mathbb{Z}_n\times\{e\}=\mathbb{Z}_n\times\{e\}\times\{e\}=...$$

תרגיל: מיינו את כל החבורות <u>האבליות</u> מסדר 50 .

הוכחה: $50=2*5^2$. לכן לפי המשפט היסודי של חבורות אבליות לכן $G=H_5\times H_2$. עכשיו ידוע שכל חבורת p איזומורפיות למכפלה ישרה של חבורות ציקליות במקרה הנ"ל H_5,H_2 חבורות p לכן הם איזומורפיות למכפלה ישרה של חבורות ציקליות והאפשריות הם:

$$H_5\cong\mathbb{Z}_{25},\quad \mathbb{Z}_5\times\mathbb{Z}_5$$
$$H_2\cong\mathbb{Z}_2$$

לכן סך הכל נקבל:

$$G\cong\mathbb{Z}_5\times\mathbb{Z}_5\times\mathbb{Z}_2\quad\vee\quad G\cong\mathbb{Z}_{25}\times\mathbb{Z}_2.$$

תרגיל: מיינו את החבורות האבליות מסדר 40.

תשובה: $40=2^3*5$ לפי המשפט היסודי של חבורות אבליות ניתן לפרק למכפלה של חברות ציקליות.לפי משפט על פירוק לחבורות p סילוא נקבל $G\cong H_2\times H_5$ וכל חבורה היא חבורה p אשר איזומורפית למכפלה ישרה של חבורות ציקליות.

$$H_5\cong\mathbb{Z}_5$$
$$|H_2|=8\Rightarrow H_2\cong\mathbb{Z}_8\vee\mathbb{Z}_4\times\mathbb{Z}_2\vee\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$$

ולכן סך הכל האפשריות הם:

$$G\cong\mathbb{Z}_{40}\times\mathbb{Z}_5\times\mathbb{Z}_8\vee\mathbb{Z}_5\times\mathbb{Z}_4\times\mathbb{Z}_2\vee\mathbb{Z}_5\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$$

שימו לב: בשתי הדוגמאות האחרונות רשמנו את כל האפשרויות עבור חבורות אבליות מסדר 50, 40, אך לא הראינו שכל שתי אפשרויות אינן איזומורפיות זו לזו. לדוגמא, כיצד נוכיח ש $\mathbb{Z}_5\times\mathbb{Z}_4\times\mathbb{Z}_2\ncong\mathbb{Z}_5\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$. ניתן כמובן לרשום את טבלאות הכפל של החבורות, ולבדוק סדרי איברים וכו, אבל אנחנו רוצים דרך יותר פשוטה להראות ששתי תת-חבורות אינן איזומורפיות.

<u>אינוריאנטים:</u>

אינוריאנט הוא מספר (או אוביקט מתמטי אחר) שאנחנו מתאימים לחבורות, כך שאם האינוריאנט של שתי חבורות הוא שונה, אז אנחנו יכולים לדעת שהן לא איזומורפיות. להלן מספר אינוריאנטים של חבורות שכבר ראינו בקורס:

1. סדר החבורה
2. קבוצת סדרי האיברים (לדוגמא אם לחבורה אחת יש סדרי איברים {1,2,3} ולחבורה שניה {1,2,4} אזי החבורות אינן איזומורפיות).
3. מספר ת"ח
4. מספר תח"נ
5. מספר חבורות p-סילוא
6. מספר מחלקות צמידות

נראה בהמשך התרגול שני אינוואריאנטים חדשים (דרגה ומעריך):

<u>הגדרה:</u> דרגה של חבורה נוצרת סופית G היא המספר המינימלי של האיברים היוצרים אותה. הדרגה מסומנת ב $r(G)$.

<u>דוגמאות:</u>

- $r(\mathbb{Z}_m)=1$ (נוצר ע"י 1)
- $G=\mathbb{Z}_k\times\mathbb{Z}_m$ $r(G)=2$
- $r(Q)=r(Q^*)=\infty$

<u>תרגיל:</u> $G\cong H$ אז $r(G)=r(H)$.

<u>הוכחה:</u> אם $S=\{x_1,x_2,...,x_n\}$ יוצרים של G ו $\varphi:G\to H$ הוא האיזומורפיזם אז $S'=\{\varphi(x_1),\varphi(x_2),...,\varphi(x_n)\}$ יוצרים של H כיכל איבר ב $h\in H$ קיים $g\in G$ הוא מהצורה $g=x_1^{i_1}x_2^{i_2}...x_n^{i_n}$ ו $h=\varphi(g)=\varphi(x_1)^{i_1}*\varphi(x_2)^{i_2}*....*\varphi(x_n)^{i_n}$ כנדרש ולכן $r(G)\ge r(H)$ באותו אופן מוכיחים בעזרת φ^{-1} ש $r(G)\le r(H)\Rightarrow r(G)=r(H)$.

<u>הגדרה:</u> תהי G חבורה. **המעריך** (**אקספוננט**) של G מוגדר כ:

$$\exp(G) = lcm\{|g| \mid g \in G\}$$

<u>דוגמאות:</u>

$$\exp(\mathbb{Z}_2 \times \mathbb{Z}_2) = lcm\{1,2\} = 2 \neq \exp(\mathbb{Z}_4) = lcm\{1,2,4\} = 4$$

$$\exp(S_3) = \exp(\mathbb{Z}_2 \times \mathbb{Z}_3) = \exp(\mathbb{Z}_6) = lcm\{1,2,3\} = 6$$

<u>שימו לב:</u> בשיעור ייתכן וראיתם הגדרה אחרת של המעריך (נסמנה בשם expmax במקום exp כדי למנוע בלבול) והיא:

$$\exp\max(G) = \max\{|g| \mid g \in G\}$$

הגדרה זאת אינה סטנדרטית, והיא מספיק טובה כאשר עובדים רק עם חבורות אבליות, אבל יותר נוח לעבוד עם ההגדרה של המעריך ככפולה המשותפת המינימלית, כי אז ניתן להוכיח את הטענה הבאה (שלא נכונה עבור expmax):

<u>תרגיל בית:</u> exp(G) הוא המספר הכי קטן עבורו מתקיים $g^n = e$ לכל $g \in G$.

<u>מסקנה:</u> $\exp(\mathrm{G}) \le |G|$, כיוון ש $g^{|G|} = e$ לכל $g \in G$. למעשה מתקיים $\exp(\mathrm{G}) \mid |G|$ כיוון ש $|G|$ היא כפולה משותפת של אברי G (מדוע?), וראינו בתחילת הקורס שכפולה משותפת מינימלית מחלקת כל כפולה משותפת.

<u>תרגיל בית:</u> $\exp(\mathrm{G} \times \mathrm{H}) = lcm(\exp(G), \exp(H))$. רמז: נובע מכך שעבור $(x,y) \in G \times H$ מתקיים $o((x,y)) = lcm(o(x), o(y))$.

<u>דוגמא:</u> לדוגמא ב $\exp(\mathbb{Z}_2 \times \mathbb{Z}_2) = 2$ (כי כל האיברים הם מסדר 2), ובאמת לפי הטענה מקבלים $\exp(\mathbb{Z}_2 \times \mathbb{Z}_2) = lcm(\exp(\mathbb{Z}_2), \exp(\mathbb{Z}_2)) = lcm(2,2) = 2$. בדוגמא זאת גם רואים שיכול להיות מצב בו $\exp(G) < |G|$.

<u>תרגיל:</u> אם G חבורה ציקלית אז $\exp(\mathrm{G}) = |G|$.

<u>הוכחה:</u> אם $\exp(\mathrm{G}) < |G|$ אז לכל $g \in G$ מתקיים $|g| \le \exp(G) < |G|$ בסתירה לכך שהחבורה ציקלית (בחבורה ציקלית תמיד קיים איבר מסדר החבורה).

תרגיל: הוכיחו או הפריכו: הכיוון השני של המשפט, כלומר אם $\exp(G)=|G|$ אזי G ציקלית.

פתרון: נפריך ע"י S_3: $\exp(S_3)=lcm(1,2,3)=6=|S_3|$.

תרגיל: אם G חבורת-p אזי G היא ציקלית אם ורק אם $\exp(G)=|G|$.

פתרון: כיוון => הוא מקרה פרטי של התרגיל הלפני אחרון. <=: לפי הגדרה $\exp(G)=lcm\{o(g)\mid g\in G\}$. לפי משפט לגרנג' בחבורת-p מתקיים שלכל $g\in G$ קיים i_g כך ש $o(g)=p^{i_g}$. לכן $\exp(G)=lcm\{p^{i_g}\mid g\in G\}=\max\{p^{i_g}\mid g\in G\}$ כלומר קיים איבר $g\in G$ כך ש $\exp(G)=o(g)$ ומכאן נובעת הטענה.

תרגיל: אם G חבורה לא אבלית מסדר 8 אזי $\exp(G)=4$.

פתרון: $\exp(G)\mid|G|\Rightarrow\exp(G)\mid 8\Rightarrow\exp(G)\in\{1,2,4,8\}$.

נפסול את כל המקרים פרט ל 4:

א. $\exp(G)\neq 1$ כיוון שקיים איבר ב G מסדר 2 לפי משפט קושי, ולכן $\exp(G)\geq 2$.

ב. $\exp(G)\neq 8$ כי אחרת החבורה היא ציקלית, לפי טענה שראינו קודם (כי החבורה היא חבורת-2), ואז אבלית, בסתירה להנחה.

ג. $\exp(G)\neq 2$ כי אחרת כל האיברים שהם לא היחידה הם מסדר 2, וראינו בתחילת הקורס שחבורה בה כל האיברים הם מסדר 2 היא אבלית.

משפט "המעריך": אם $G\cong H$ אז $\exp(G)=\exp(H)$.

תרגיל: הראו ש $\mathbb{Z}_5\times\mathbb{Z}_4\times\mathbb{Z}_2\ncong\mathbb{Z}_5\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.

פתרון: המעריך של החבורה מימין הוא 10, המעריך של החבורה משמאל הוא 20. ולכן החבורות אינן איזומורפיות.

משפט הצמצום: אם $G\times H\cong K\times H$ אזי $G\cong K$ (בצורה דומה ניתן לצמצם משמאל).

תרגיל: הראו ש $\mathbb{Z}_4\times\mathbb{Z}_4\ncong\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2$

פתרון: שימו לב שבמקרה זה המעריכים שני המעריכים שווים ל 4. דוגמא זו מראה שמשפט "המעריך" לא נכון בכיוון ההפוך. אפשר לפתור את התרגיל בעזרת הדרגה של החבורות, או

מספר איברים מסדר 2, אבל אפשר לפתור יותר בקלות בעזרת משפט הצמצום: נניח בשלילה ש $\mathbb{Z}_4\times\mathbb{Z}_4\cong\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2$ ונצמצם $\mathbb{Z}_4$ משמאל, ונקבל $\mathbb{Z}_4\cong\mathbb{Z}_2\times\mathbb{Z}_2$, סתירה (החבורה משמאל היא ציקלית, ומימין היא לא, או החבורה משמאל היא עם מעריך 4, ומימין עם מעריך 2).

<u>תרגיל:</u> תהי G חבורה אבלית מסדר 72 עם 3 איברים מסדר 2 ופחות מ 8 איברים מסדר 3. מצאו את החבורה G.

<u>פתרון:</u> $G\cong H_2\times H_3$ מכפלה ישרה של חבורת 2-סילוא וחבורת 3-סילוא מסדרים $3^2,2^3$ בהתאמה. האפשרויות עבור H_2 הן:

$$H_2\cong\mathbb{Z}_8,\mathbb{Z}_4\times\mathbb{Z}_2,\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$$

האפשרויות עבור H_3 הן:

$$H_3\cong\mathbb{Z}_9,\mathbb{Z}_3\times\mathbb{Z}_3$$

כעת נתחיל לפסול אפשרויות עבור H_2 :

א. $H_2\ncong\mathbb{Z}_8$ כיוון שב $\mathbb{Z}_8$ יש רק איבר אחד מסדר 2. מדוע? נזכר שסדר של איבר $g\neq 0$ ב $\mathbb{Z}_n$ הוא $o(g)=\frac{n}{lcm(n,g)}$. לכן $2=o(g)=\frac{8}{lcm(8,g)}\Rightarrow lcm(8,g)=4\Rightarrow g=4$.

ב. $H_2\ncong\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ כי מספר האיברים מסדר 2 ב $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$ הוא 7 (כל האיברים פרט ליחידה הם מסדר 2).

ניתן לראות שב $\mathbb{Z}_4\times\mathbb{Z}_2$ יש 3 איברים מסדר 2 (הם $(2,0),(2,1),(0,1)$), לכן קיבלנו שבהכרח $H_2\cong\mathbb{Z}_4\times\mathbb{Z}_2$.

בצורה דומה עבור H_3 ניתן לפסול את $\mathbb{Z}_3\times\mathbb{Z}_3$ כיוון שיש בה 8 איברים מסדר 3, וב $\mathbb{Z}_9$ יש 2 איברים מסדר 3 (והם 3,6). לכן בהכרח $H_3\cong\mathbb{Z}_9$.

לכן בסה"כ קיבלנו שבהכרח $G\cong\mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_9\cong\mathbb{Z}_2\times\mathbb{Z}_{36}\cong\mathbb{Z}_4\times\mathbb{Z}_{18}$.

תרגול 13

תרגיל: תהי G חבורה אבלית ו $H \le G$ כך ש G/H היא ציקלית אינסופית. הראו שקיימת $K < G$ כך ש $G \cong K \times H$.

פתרון: לפי משפט "מכפלה פנימית מכפלה חיצונית" מספיק להראות שקיימת $K \le G$ כך ש $G = KH$ וגם $K \cap H = \{e\}$. $G/H \cong <xH>$ לפי הנחה. נגדיר $K =< x >$. לכל $g \in G$ מתקיים $g \in x^i H \Rightarrow \exists h \in H, g = x^i h \Rightarrow g \in KH$. לכן $G = KH$. אם $K \cap H \neq \{e\}$ אזי קיים $x^i \in H$, אבל אז $|xH| \le i$ בסתירה לכך ש $<xH>$ היא ציקלית אינסופית.

בתרגיל הבא נראה שיטת הוכחה בה משתמשים הרבה בנושא של סדרות הרכב וחבורות פתירות:

תרגיל: הראו שבחבורת-p סופית מסדר p^n קיימות תת-חבורות נורמליות מכל סדר p^k, $0 \le k \le n$.

הוכחה: אם החבורה אבלית, אז הטענה היא מסקנה פשוטה ממשפט סילוא 1.

אם החבורה אינה אבלית, נוכיח באינדוקציה:

הטענה ברורה עבור n=1.

נניח שהטענה מתקיימת עבור n-1,...,1, ונוכיח עבור n:

אנחנו יודעים ש $Z(G) \lhd G$ וגם $Z(G) \neq \{e\}, G$. בגלל לגרנג' נקבל $|Z(G)| = p^i$, כך ש $i \ge 1$.

כעת לכל $0 \le k \le i$ קיימות תת-חבורות נורמליות מסדר p^k, כיוון שלפי סילוא 1 קיימת ת"ח מסדר p^k של $Z(G)$ והיא נורמלית ב G, כי כל ת"ח של המרכז היא נורמלית (**מדוע**?).

יהי $i < k \le n$:

כעת $|G/Z(G)| < p^n$, ולכן לפי הנחת האינדוקציה, קיימת לה ת"ח נורמלית K מסדר p^{k-i}.

נסתכל על ההומ' הטבעי $\pi : G \to G/Z(G)$, אזי $H := \pi^{-1}(K) \lhd G$ (כיוון שתמונה הפוכה של ת"ח נורמלית היא נורמלית). מה הסדר של H?

$\frac{|H|}{p^i} = \frac{|H|}{|Z(G)|} = \frac{|H|}{|Ker\varphi|} = [H : Ker\varphi] = |K| = p^{k-i}$ ומכאן נקבל $|H| = p^k$.

<u>תרגיל:</u> הראו ש Q_8 (חבורת הקווטרניונים) אינה ניתנת לשיכון ב-S_4.

<u>פתרון:</u> $|S_4| = 24 = 2^3 \times 3$. אם Q_8 (שהיא מסדר 8) ניתנת לשיכון ב-S_4 אזי היא איזומורפית לת"ח 2-סילוא של S_4. ידוע שניתן לשכן את D_4 (החבורה הדיהדרלית של סימטריות הריבוע) ב- S_4 (כל סימטריה על הריבוע היא תמורה של הקדקדים). לכן קיימת ל S_4 ת"ח איזומורפית ל D_4 והיא מסדר 8, כלומר אחת מת"ח 2-סילוא של S_4. אבל לפי טענה מהתרגול הקודם, כל ת"ח 2-סילוא הן צמודות ולכן איזומורפיות, כלומר נקבל ש Q_8 איזומורפית ל D_4, סתירה (הראיתם בתרגול בית שהן אינן איזומורפיות).

<u>סדרות נורמליות וסדרות הרכב:</u>

<u>הגדרה:</u> **סדרה נורמלית** של חבורה G היא סדרה של תת חבורות נורמליות:

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright ... \triangleright G_k = \{e\}$$

חבורות המנה $0 \le i < k$, G_i / G_{i+1} נקראות ה**גורמים** של הסדרה.

<u>דוגמאות:</u>

1. לכל חבורה G, $G \triangleright \{e\}$ סדרה נורמלית. הגורם היחיד הוא $G/\{e\} \cong G$.

2. $G = S_3$, $N := \langle (1,2,3) \rangle \triangleleft G$. נקבל $\{e\} \triangleleft N \triangleleft G$ היא סדרה נורמלית. הגורמים הם $G/N \cong \mathbb{Z}_2$ וגם $N/\{e\} \cong \mathbb{Z}_3$.

<u>הגדרה:</u> **עידון של סדרה נורמלית** $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright ... \triangleright G_k = \{e\}$ היא סדרה $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright ... \triangleright G_i \triangleright ... \triangleright G_{i+1} \triangleright ... \triangleright G_k = \{e\}$ (כלומר הוספנו עוד אברים בסדרה).

<u>עידון ממש</u> של סידרה היא סדרה נורמלית המהווה עידון שאינו טריויאלי (כלומר לא הוספנו גורמים טריויאליים $G_i / G_{i+1} = \{e\}$ לסדרה).

<u>הגדרה:</u> **סדרת הרכב** היא סדרה נורמלית שאין לה עידונים ממש.

<u>משפט:</u> סדרה נורמלית היא סדרת הרכב אם ורק אם כל הגורמים של הסדרה הם פשוטים.

<u>הערה:</u> חבורה אבלית היא פשוטה אם ורק אם היא ציקלית סופית מסדר ראשוני (זה מאפשר לנו לדעת בקלות שאם אחד הגורמים הוא אבלי, אך אינו ציקלי סופי מסדר ראשוני, אזי הסדרה **אינה** סדרת הרכב).

<u>דוגמאות:</u>

$$Z^4 = Z\times Z\times Z\times Z \rhd Z^3\times\{e\} \rhd \{e\}\times\{e\}\times\{e\}\times\{e\}$$

עידון של ממש הוא

$$Z^4 \rhd Z^3\times\{e\} \rhd Z^2\times\{e\}\times\{e\} \rhd \{e\}\times\{e\}\times\{e\}\times\{e\}$$

$S_n \rhd A_n \rhd \{Id\}, n\geq 5$ סדרת הרכב כי כל הגורמים הם חבורות פשוטות.

$S_4 \rhd A_4 \rhd \{Id\}$ לא סדרת הרכב כי

$A_4 \rhd V_4 = \{Id,(1\quad 2)(3\quad 4),(1\quad 3)(2\quad 4),(1\quad 4)(2\quad 3)\}$ ועדיין $S_4 \rhd A_4 \rhd V_4 \rhd \{e\}$

אינה סדרת הרכב כי אפשר לעדן אותה ע"י $V_4 \rhd U := \{e,(1\quad 2)(3\quad 4)\}$. שימו לב: $U \ntriangleleft A_4, S_4$. לבסוף קיבלנו את הסדרה הנורמלית $S_4 \rhd A_4 \rhd V_4 \rhd U \rhd \{e\}$ וזאת סדרת הרכב כי כל הגורמים הם מסדר 2 ולכן איזומורפיים ל $\mathbb{Z}_2$.

$Z \rhd 2Z \rhd 4Z \rhd 8Z \rhd \ldots \rhd 2^m Z \rhd \{0\}$ אין סדרת הרכב (תמיד אפשר לעדן אותה).

נראה סדרות נורמליות של D_4 (זיכרו שסימנו ב σ סיבוב ב 90 מעלות, וב τ את אחד השיקופים): $D_4 \ \triangleright\ <\sigma^2>\ \triangleright\ \{1\}$ (מספיק להראות ש $<\sigma^2>$ היא אינוריאנטית תחת הצמדה ע"י היוצרים. נראה זאת עבור τ: $\tau\sigma\tau = \sigma^{-1} \Rightarrow \tau\sigma^2\tau = \sigma^{-2} = \sigma^2$). זאת אינה סדרת הרכב: $\left|D_4/<\sigma^2>\right| = 4$ וחבורה מסדר 4 אינה פשוטה (**<u>תרגיל בית:</u>** בדקו לאיזו אחת משתי החבורות מסדר 4 איזומורפית החבורה $D_4/<\sigma^2>$). ניתן לעדן את הסדרה ולקבל $D_4 \ \triangleright\ <\sigma>\ \triangleright\ <\sigma^2>\ \triangleright\ \{1\}$. כאן כל הגורמים הם איזומורפיים ל $\mathbb{Z}_2$ ולכן הסדרה היא סדרת הרכב. זאת לא סדרת ההרכב היחידה. לדוגמא:

$D_4 \ \triangleright\ <\sigma^2,\tau>\ \triangleright\ <\tau>\ \triangleright\ \{1\}$ (שימו לב: במקרה זה $<\tau> \ntriangleleft D_4$).

<u>הגדרה:</u> שתי סדרות נורמליות של חבורה G

$$G = G_0 \rhd G_1 \rhd G_2 \rhd \ldots \rhd G_k = \{e\}$$
$$G = H_0 \rhd H_1 \rhd H_2 \rhd \ldots \rhd H_m = \{e\}$$

נקראות **שקולות** אם $k=m$ והגורמים איזומורפיים עד כדי תמורה: כלומר $\pi\in S_k$ כך ש-

$G_{i-1}/G_i \cong H_{\pi(i)-1}/H_{\pi(i)}$ (כאשר $1\leq i\leq k$).

<u>משפט ז'ורדן-הולדר:</u> אם ל G יש סדרות הרכב אז כל שתי סדרות הרכב שקולות.

<u>דוגמא:</u> נמצא שתי סדרות הרכב עבור D_6:

$$\{1\} \lhd <\sigma^2> \lhd <\sigma> \lhd D_6$$
$$\{1\} \lhd <\sigma^3> \lhd <\sigma^3,\tau> \lhd D_6$$

נסמן את החבורות בסדרה הראשונה ב G_i(כאשר $G_0 = D_6$) ואת החבורות בסדר השניה ב $\tilde{G}_i$.

אזי נחשב את הגורמים: $G_0/G_1 \cong \mathbb{Z}_2,\ G_1/G_2 \cong \mathbb{Z}_2,\ G_2/G_3 \cong \mathbb{Z}_3$.

$\tilde{G}_0/\tilde{G}_1 \cong \mathbb{Z}_3,\ \tilde{G}_1/\tilde{G}_2 \cong \mathbb{Z}_2,\ \tilde{G}_2/\tilde{G}_3 \cong \mathbb{Z}_2$.

נקבל שתמורה מתאימה למשפט ז'ורדן-הולדר היא $\pi = (1,3)$ (מחליפים את הגורם הראשון בגורם השלישי).

<u>דוגמא:</u> שתי חבורות עם סדרות הרכב בעלות אותם גורמים (עד כדי תמורה של סדרם) לא בהכרח איזומורפיות. לדוגמא: $D_p \ncong \mathbb{Z}_{2p}$ אבל סדרות ההרכב הן:

$$\{1\} \lhd <\sigma> \lhd D_p,$$
$$\{1\} \lhd <2> \lhd \mathbb{Z}_{2p}$$

והגורמים הם: $\mathbb{Z}_p, \mathbb{Z}_2$.

<u>חבורות פתירות:</u>

<u>הגדרה:</u> חבורה היא **פתירה** אם יש לה סדרה נורמלית (לאו דווקא סדרת הרכב) כך שכל הגורמים אבלים.

<u>דוגמא:</u>

כל חבורה אבלית פתירה מכיוון ש $G \rhd \{e\}$ שהגורם היחיד בה הוא $G/\{e\} \cong G$ אבלי.

<u>תרגיל:</u> הראו ש D_n פתירה.

<u>פתרון:</u> נסמן ב σ את היוצר של ת"ח הסיבובים. $<\sigma>$ מסדר n, ו $[D_n,<\sigma>]=2$ ולכן $D_n \rhd <\sigma>$. לכן $\{e\} \lhd <\sigma> \lhd D_n$ היא סידרה נורמלית בה הגורמים הם: $D_n/<\sigma> \cong \mathbb{Z}_2$ וגם $<\sigma>/\{e\} \cong \mathbb{Z}_n$. לכן D_n פתירה.

<u>תרגיל:</u> הוכח S_4 פתירה.

<u>הוכחה:</u> $S_4 \rhd A_4 \rhd V_4 \rhd \{e\}$, וכל הגורמים הם אבליים.

<u>דוגמא:</u>

נסתכל על $GL_2(F)$ (F שדה). נגדיר $H=\left\{\begin{bmatrix} a & b\\ 0 & 1\end{bmatrix} \mid a\in F^*, b\in F\right\}$. בקיצור נרשום $H=\left\{\begin{bmatrix} * & *\\ 0 & 1\end{bmatrix}\right\}$. אזי $H\le GL_2(F)$ (בדקו זאת). כעת ניתן להגדיר את הסדרה הנורמלית:

$$\left\{\begin{bmatrix} 1 & 0\\ 0 & 1\end{bmatrix}\right\} \triangleleft \left\{\begin{bmatrix} 1 & *\\ 0 & 1\end{bmatrix}\right\} \triangleleft \left\{\begin{bmatrix} * & *\\ 0 & 1\end{bmatrix}\right\}$$

אכן מדובר בסדרה נורמלית, משמאל זאת החבורה הטריויאלית, והחבורה האמצעית היא הגרעין של ההומ' $\varphi: H\to (F^*,\cdot,1)$ המוגדר ע"י $\varphi\left(\begin{bmatrix} a & b\\ 0 & 1\end{bmatrix}\right)=a$. הגורמים הם (משמאל לימין) $(F,+,0)$ ו- $(F^*,\cdot,1)$. הגורמים הם אבליים, ולכן החבורה פתירה. החבורה לאו דווקא בעלת סדרת הרכב (**מדוע?**).

<u>משפט:</u> כל חבורת-p היא פתירה (ההוכחה כמעט זהה לתרגיל מתחילת התרגול).

<u>משפט:</u> כל חבורה מסדר pq כאשר p,q ראשוניים היא פתירה.

<u>"הוכחה":</u> ראינו בתרגול הקודם שחבורה מסדר pq אינה פשוטה, וקיימת לה תח"נ מסדר p או q. אם כך הגורמים יהיו של הסדרה הנורמלית יהיו $\mathbb{Z}_p,\mathbb{Z}_q$ ואלה גורמים אבליים, ולכן החבורה פתירה.

<u>! משפט:</u> יהיו $N\triangleleft G$. אזי G פתירה אם ורק אם N פתירה וגם G/N פתירה.

<u>תרגיל:</u> הראו שכל חבורה G מסדר $p^a q^b$ כאשר p,q ראשוניים, $a,b\in\mathbb{N}$, וגם $q^t\not\equiv 1(\bmod p)$ לכל $t=1,2,...,b$, אזי G פתירה.

<u>פתרון:</u> $r_p\equiv 1\ (\bmod p)\ \wedge\ r_p\mid q^b$. לפי תנאי התרגיל נקבל שבהכרח $r_p=1$. לכן H_p ת"ח p-סילוא של G היא ת"ח נורמלית. לכן H_p היא פתירה כי היא חבורת-p, וגם $\left|G/H_p\right|=q^b$, כלומר G/H_p היא חבורת-q ולכן פתירה. אם כך לפי המשפט נקבל ש G פתירה.

<u>תרגיל:</u> הראו שחבורה G מסדר pqr, כך ש $p<q<r$ וגם $pq<r$ היא חבורה פתירה. (r,p,q ראשוניים).

<u>פתרון:</u> $r_r\mid pq \Rightarrow r_r\in\{1,p,q,pq\}$ אבל p,q,pq כולם קטנים מ r ולכן שונים מ 1 מודולו r. לכן $r_r=1$, ונקבל שת"ח r-סילוא H_r היא ת"ח נורמלית מסדר r ולכן היא ציקלית, ולכן פתירה. כעת G/H_r היא חבורה מסדר pq ומראים בצורה דומה שגם היא פתירה.

<u>הקומוטטור:</u>

<u>הגדרה:</u> תהי $a,b\in G$ הקומוטטור של a,b מוגדר כ $[a,b]=aba^{-1}b^{-1}$ תהי G חבורה.

<u>תת-חבורה הקומטטור</u> מוגדרת כ $G':=<\{[a,b]\,|\,a,b\in G\}>$ - כלומר התת חבורה הנוצרת ע"י כל הקומוטטרים.

<u>שאלה:</u> מתי $[a,b]=e$? תשובה אם"ם $ab=ba$.

<u>משפט:</u> G אבלית אם ורק אם $G'=\{e\}$.

<u>שאלה:</u> $[a,b]^{-1}$? תשובה: $[a,b]^{-1}=(aba^{-1}b^{-1})^{-1}=bab^{-1}a^{-1}=[b,a]$.

<u>משפט:</u> $G'\lhd G$

<u>טענה:</u> אם G חבורה פשוטה שאינה אבלית אז $G'=G$.

<u>הוכחה:</u> $G'\lhd G$ לפי משפט קודם בנוסף מכיוון ש G אינה אבלית אז $G'\neq\{e\}$ ולכן מכיוון ש G פשוטה אז $G'=\{\not{e}\}\vee G=G$.

<u>משפט:</u> לכל חבורה G , חבורת המנה G/G' אבלית.

<u>משפט:</u> אם $H\leq G$ אז $H'\leq G'$.

<u>משפט:</u> אם $N\lhd G$ וגם G/N אבלית אז $G'\leq N$ (נובע מכך ש $G'\leq Ker\pi=N$ כאשר $\pi:G\to G/N$ הוא ההומ' הטבעי).

<u>הגדרה:</u> **סדרת הקומטטור** של חבורה G מוגדרת באינדוקציה ע"י $G^{(0)}=G,G^{(i+1)}=(G^{(i)})'$.

<u>משפט:</u> G חבורה פתירה אם"ם קיים t סופי כך ש $G^{(t)}=\{e\}$.

<u>משפט:</u> $(S_n)'=A_n$ עבור $n\geq 5$.

<u>משפט</u> $(A_n)'=A_n, n\geq 5$ כי לפי משפט A_n חבורה פשוטה.

<u>! משפט:</u> לכן לפי משפט קודם אין t סופי שעבורו $(S_n)^{(t)}=\{e\}$ ולכן לפי משפטים קודמים S_n אינה פתירה עבור $5\leq n$.

<u>תרגיל:</u> הוכיחו או הפריכו: כל חבורה מסדר 60 היא פתירה. נפריך: A_5 היא חבורה מסדר 60, ואינה פתירה, כיוון שהסדרה $A_5\rhd\{1\}$ היא סדרת הרכב (A_5 היא פשוטה) ולכן לא קיימת לא סדרה בה הגורמים הם חבורות אבליות.

<u>תרגיל:</u> הוכיחו שהחבורה הבאה פתירה: $G=\left\{\begin{bmatrix}1&a&b\\0&1&c\\0&0&1\end{bmatrix}\,\middle|\,a,b,c\in F\right\}$ כאשר F שדה.

פתרון: הערה: אם השדה F סופי (עובדה: כל שדה סופי הוא מסדר p^k כאשר p ראשוני) אזי הסדר של G הוא p^{3k} ואז החבורה היא חבורת p ולכן החבורה פתירה.

נסמן בכתיב מקוצר $(a,b,c)=\begin{bmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{bmatrix}$. נקבל לפי כפל המטריצות ש:

$(a,b,c)*(d,e,f)=(a+d,e+b+af,c+f)$. כיוון שהיחידה היא $(0,0,0)$ נקבל ש

$(a,b,c)^{-1}=(-a,ac-b,-c)$. לכן נקבל ש:

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

לכן $G'=\left\{\begin{bmatrix}1 & 0 & b\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} | b\in F\right\}$. החבורה G' היא אבלית, ולכן $G''=\{1\}$, ולכן החבורה פתירה.