מבוא לחבורות

מרצה: תמר ציגלר

30 במרץ 2009

תקציר

רשימות אלו הוקלדו במהלך השיעורים של הקורס "מבוא לחבורות" 104172, במהלך סמסטר חורף 2008, בהרצאות מאת ד"ר תמר ציגלר, ומפורסמת ברשותה. **רשימות אלו רחוקות מלהיות מלאות,** הן מכילות, בקירוב, רקמחצית מההרצאות.

המחברת הוקלדה ע"י רונן אברבנאל (ronen@tx.technion.ac.il) ומפורסמת ב־www.technion.ac.il/~ronen. המחברת תתעדכן מעת לעת במיקום זה.

המחברת עלולה לכלול טעויות, חוסרים ואי דיוקים. בפרט, היא אינה מכילה כלל שרטוטים ואיורים שצוירו על הלוח. אני אשתדל לציין מקומות בהם החסרתי שיעור.

תוכן עניינים

1 מבוא . . . 2
1.1 פעולות . . . 2
1.1.1 תכונות של פעולות . . . 2
1.1.2 סימונים . . . 3
1.2 חבורות . . . 4
1.2.1 דוגמאות . . . 4
1.3 תת חבורה . . . 5
1.4 חבורות נגזרות . . . 5
1.5 חבורות איזומורפיות . . . 6
1.5.1 הומומורפיזם . . . 8
1.6 קו־סטים . . . 10
1.6.1 משפט לגרנז' . . . 11
2 חבורות מנה . . . 14
2.0.2 דוגמאות . . . 15
2.1 משפט האוטומטרפיזם הראשון . . . 16
2.1.1 משפט האיזומורפיזם הראשון: $\varphi : G \to G'$ הומומורפיזם, אזי

$$G/_{\ker\varphi} \cong \mathrm{Im}\varphi$$

דוגמאות . . . 16
2.2 משפט האיזומורפיזם השני . . . 17
2.2.1 דוגמאות . . . 17
3 פעולות של חבורה על קבוצה . . . 18
3.0.2 דוגמאות . . . 18
3.1 מסלול של חבורה . . . 18
3.2 מייצב . . . 19
3.2.1 תזכורת . . . 20
3.2.2 דוגמה שדיקלה תאהב . . . 20
3.3 פעולה של חבורה על עצמה . . . 21
3.4 משוואת המחלקה . . . 22
3.4.1 דוגמאות . . . 22
3.5 פעולה על תתי קבוצות . . . 23

1 מבוא

1.1 פעולות

הגדרה 1.1 קבוצה אם פעולה: תהא S קבוצה. פעולה על S זו פונקציה

$$\mu : S \times S \underset{(a,b)\mapsto\mu(a,b)}{\rightarrow} S$$

את $\mu\left(a,b\right)$ כמו $a\times b, a+b, a\circ b, ab$

דוגמאות:

1. כפל מטריצות

$$S=\left\{ \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}|\alpha,\beta,\gamma,\delta\in\mathbb{R}\right\}$$

ו־μ כפל מטריצות

$$\begin{aligned}\mu(a,b)=ab & =\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 3 & 2\end{pmatrix}\\ & =\begin{pmatrix}7 & 4\\ 3 & 2\end{pmatrix}\end{aligned}$$

2. הקבוצה היא פעולה צפידות ששומרות על הריבוע (סיבובים, שיקופים) ־ הפעולה μ ־ הי הרכבה בין הפעולות.

3. אם T קבוצה,

$$S\subset\mathrm{Map}\left(T,T\right)$$

(א) S היא אוסף כל ההעתקות מ־Tל־T. וכאן פעולה יכולה להיות פעולת הרכבה.

4. $S=\left\{ x|\left|x\right|=1\right\}$, כל המעגלים על מעגל היחידה, ופעולה היא כפל. אפשר להסתכל על S בתור

$$S=\left\{ \begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\right\}$$

מתריצה כזו, כשהיא מוכפלת בוקטור, מסובבת אותו ב־$\pm\theta$.

- (דוגמא 0) $S=\mathbb{R},\mathbb{Z},\mathbb{Q}$, $\mu=+,\cdot$, שתיהן פעולות אסוציאטיביות וקומוטטיביות על S.
  - לפעמים מסמנים $(\mathbb{R},+)$, $(\mathbb{R},\cdot)$.

1.1.1 תכונות של פעולות

- פעולה נקראת "**אסוציאטיבית**" אם $a\left(bc\right)=\left(ab\right)c$.
- פעולה נקראת **קומוטטיבית** (חילופית) אם $ab=ba$.

כל הדוגמאות הן אסוציאטיביות, כי ־

- כפל מטריצות אסוציאטיבי (לפי אלגברה א')
- דוגמא 3 ־ הרכבת פונקציות ־ פעולה אסוציאטיבית.

קומוטטיביות היא תכונה נדירה יותר. לפעולה חילופית הרבה פעמים משתמשים בסימון $+$.

- אם משתמשים ב־$+$, תמיד מתכוונים שהפעולה קומטטיבית. ההיפך אינו נכון.

דוגמא הקבוצה T **ו־**$S = \mathbf{Map}\,(T,T)$
במקרה ש־$T = \{a\}$, אז $S = \{i\}$ - העתקת הזהות.
במקרה ש־$T = \{a,b\}$אז
$$S = \begin{Bmatrix} i & i(a)=a & i(b)=b \\ \tau & \tau(a)=b & \tau(b)=a \\ \alpha & \alpha(a)=a & \alpha(b)=a \\ \beta & \beta(a)=b & \beta(b)=b \end{Bmatrix}$$
טבלת הכפל של S, כאשר $\begin{pmatrix} \cdot & v \\ u & u\cdot v \end{pmatrix}$

$\cdot$	i	τ	α	β
τ	i	τ	α	β
τ	τ	i	β	α
α	α	α	α	α
β	β	β	β	β

אסוציאטיביות מאפשר לנו להגדיר באופן יחיד את האיבר $a_1 \circ a_2 \circ .. \circ a_n$ עבור כל $a_1,..,a_n \in S$.
ניתן להגדיר אינדוקטיבית $a_1 \circ ... \circ a_n = (a_1 \circ ... \circ a_{n-1})\, a_n$. (תרגיל הביתה)

- זהות (איבר יחידה) של פעולה הוא איבר ב־S־$e \in S$ שמקיים, לכל $a \in S$, $a \cdot e = e \cdot a = a$. לא לכל פעולה חייב להיות איבר יחידה.

דוגמא: בכפל מטריצות, איבר היחידה היא מטריצת היחידה I, וב־$S = \mathrm{Map}(T)$, איבר היחידה הוא העתקת הזהות ($i : i(x) = x$)

  - אם הפעולה היא חילופית (עם יחידה), הרבה פעמים מסמנים את איבר היחידה ב־0.
  - הרבה פעמים מסמנים את איבר היחידה ב־1.

- S קבוצה עם פעולה אסוציאטיבית ויש לה איבר יחידה. איבר $a \in S$ נקרא **הפיך** אם יש איבר נוסף $b \in S$ כך ש־$ab = ba = 1 (= e)$..
  - נסמן $b = a^{-1}$.

למה 1.2 אם a איבר הפיך ו־$ac = ad$ או $ca = da$, אז $c = d$. (לא ניתן להסיק מסקנה כזו אם a אינו הפיך)

הוכחה: נכפול את שני האגפים משמאל ב־b (ההופכי של a)

$$bac = bad$$
$$1 \cdot c = 1 \cdot d$$

■

$\frac{da}{a}$ הוא סימון שאינו מוגדר היטב, אלא אם כן הפעולה קומטטיבית.
תרגיל: להוכיח יחידות של b.
הערה: אם a, b הפיכים, אז גם ab הפיך ו־$(ab)^{-1} = a^{-1}b^{-1}$ (תרגיל)

1.1.2 סימונים

- a^{-1} הוא a הופכי (inverse)
- $a^n = a \cdot a \cdot ... \cdot a$
- אם מניחים שהקבוצה אסוציאטיבית עם איבר יחידה$a^{-n} = a^{-1} \cdot a^{-1} \cdot ... \cdot a^{-1}$
- חוקי חזקה -$a^{n+m} = a^n \cdot a^m$. $(a^n)^m = a^{nm}$
- חשוב לשים לב ש־$(ab)^n \neq a^n b^n$ (זה לא בהכרח נכון..)

1.2 חבורות

הגדרה 1.3 חבורה היא קבוצה G (group) עם פעולה אסוציאטיבית, שיש לה איבר יחידה ולכל איבר ב־G יש הופכי. (כל איבר ב־G הוא הפיך)

- חבורה נקראת חילופית (קומטטיבית, אבלית) אם הפעולה היא קומטטיבית.
- אם G חבורה סופית ־ כלומר, בקבוצה G מספר סופי של איברים ־ אז מסמנים ב־$|G|$ את מספר האיברים ב־G ו־$|G|$ נקרא **סדר החבורה**

1.2.1 דוגמאות

- $(\mathbb{Z},+)$, קבוצת המספרים השלמים עם חיבור ־ היא חבורה. איבר היחידה ־ 0, וההופכי של n הוא $-n$.
- $(\mathbb{Z},\cdot)$ אינה חבורה, כי ההופכי של n ־ $\frac{1}{n}$, אינו ב־$\mathbb{Z}$. האיברים היחידים עם איבר הופכי הם $1,-1$
- $(\mathbb{R},\cdot)$ אינו חבורה, כי ל־0 הן הופכי.
- $(\mathbb{R}^*,\cdot)$ הוא חבורה.
- החבורה הטרוויאלית ־ $G=\{1\},G=\{0\},G=\{I\}$
- $M_n(\mathbb{R})$, אוסף המטריצות $n\times n$ עם איברים מ־$\mathbb{R}$.
  - ביחס לפעולת החיבור ־ זוהי חבורה, שאיבר היחידה הוא מטריצת האפס.
  - ביחס לפעולת הכפל, זו אינה חבורה.
  - $(\{M\in M_n(\mathbb{R}),\det M\neq 0\},\cdot)$, כלומר ־ כל המטריצות ההפיכות עם כפל ־ זוהי חבורה
  - $(\{M\in M_n(\mathbb{R}),\det M=1\},\cdot)$ ־ חבורה
- $T=\{1,2,3,..,N\}$. $S=\mathrm{Map}(T,T)$, עם הפעולה "הרכבה", זו אינה חבורה
  - אם S' הן חח"ע (ולכן ־ בקבוצה סופית, על) ־ אז זו חבורה. חבורה זו היא S_n ־ אוסף התמורות על הקבוצה.
  - $S_1=\{i,\tau\}$. זו חבורה קומטטיבית.
  - S_3 מכילה שישה איברים (אוסף כל התמורות על 3 איברים, $3!$). S_3 אינה קומטטיבית, והיא החבורה הכי קטנה שאינה קומטטיבית.
- S_n אוסף פרמוטציות על n איברים, עם פעולת ההרכבה.
  - צורות כתיב של פרמוטציות $\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$, $\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}$ $\iff$ $(1,2,3)$, $\iff$ $(1,2,4)$ $\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}$
  - כל פרמוטציה על 4 איברים, היא סדרת הרכבות של הפרמוטציות $(1,2)$ ו־$(1,2,3,4)$. (יהיה בתרגיל)
  - S_3 פרמוטציה על 3 איברים $S_3=\{1,c,c^2,\tau,\tau c,\tau c^2\}$ ($\tau=(1,2)$, $c=(1,2,3)$) מתקיים $c^3=1,\tau^2=1,c\tau c\tau=1$.
    - * האם $c\tau c\tau=\tau c\tau c$? S_3 שקולה ל־ $G=\left\{\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\begin{pmatrix}0&1&0\\0&0&1\\1&0&0\end{pmatrix},\begin{pmatrix}0&1&0\\1&0&0\\0&0&1\end{pmatrix}\right\}$ (וכל המכפלות שלהן)
    - * $|S_3|=6$ והיא אינה חילופית. (בדקו!)
- $GL_n(\mathbb{R})$, ־ מטריצות $n\times n$ עם דטרמיננטה שאינה 0. $SL_n(\mathbb{Z})$ ־ אוסף המטריצות $n\times n$ שהדטרמיננטה שלהן 1.
  - $|GL_n(\mathbb{R})|=\infty$.

– $GL_n(\mathbb{Z})$ אינה חבורה כי יש איברים שאין להם הופכי

- שורשי יחידה מסדר n - $G_n = \left\{e^{\frac{2\pi i k}{n}} : k = 0, \dots, n-1\right\}$

– $G_2 = \{1, -1\}$ ו־$G_3 = \left\{1, e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}\right\}$

– $|G_6| = 6$ והיא קומטטיבית. $G_6 = \left\{1, -1, e^{\frac{2\pi i}{3}}, \dots\right\}$ כאשר שאר האיברים בחבורה הם הכפולות שלהם.

1.3 תת חבורה

הגדרה 1.4 תהא G חבורה, תת חבורה H של G היא תת קבוצה של G המקיימת:

- סגירות - $g, h \in H$ אז $gh \in H$.
- $1_G \in H$ (1 הוא איבר היחידה של G)
- $g \in H$ אז $g^{-1} \in H$.

לכל חבורה G יש שתי תתי חבורות טריוויאליות $H = \{1\}$, או G.
אם תת חבורה לא טרוויאלית נקראת **תת־חבורה־ממשי**.
חסר: שיעור שני, 18.11

1.4 חבורות נגזרות

הגדרה 1.5 חסר: התחלה של שיעור, 25.11
G חבורה. $H \subset G$ היא תת חבורה אם $H \subseteq G$ ו־H חבורה ביחס לפעולה ב־G.
- מיינו את תת החבורות של $\mathbb{Z}, *$: כל תת חבורה היא מהצורה $d\mathbb{Z}$ כש־$d \in \mathbb{Z}$ כלשהן
- אם G חבורה ו־$x \in G$, נתבונן ב־$H = \left\{\dots, x^{-2}, x^{-1}, 1, x, x^2 \dots\right\}$זו תת חבורה של G. זו תת חבורה של G הקטנה ביותר שמכילה את x.

שני מקרים:
א. אם $x^n \neq x^m$ לכל $n \neq m$, אז H נקראת התת־חבורה הציקלית ה־∞, הנוצרת על ידי X
ב. יש $n \neq m$ כך ש־$x^n = x^m$, ואז $x^{n-m} = 1$ ו־$n - m \neq 0$ נבתונן ב־$S = \{n \in \mathbb{Z} : x^n = 1\}$
$0 \in S$ יש ב־S איבר $0 \neq$ קל לבדוק ש־S היא תת חבורה של $(\mathbb{Z}, +)$.
$n, m \in S$ אז $x^m = 1$ ו־$x^n = 1$ לכן $x^{n+m} = x^n x^m = 1 \cdot 1 = 1$ לכן $n + m \in S$.
אם $n \in S$ אז $x^n = 1$ לכן $x^{-n} = x^{-n} x^{-n} = 1$ ולכן $-n \in S$. וכן $0 \in S$ כי $x^0 = 1$
לכן $S \in d\mathbb{Z}$ עבור $d > 0$
טענה: $H = \left\{1, x, \dots, x^{d-1}\right\}$ כלומר, לכל $n \in \mathbb{Z}$ קיסם $0 \leq i \leq d - i$ כך ש- $x^n = x^i$.
הוכחה: לכל i, נצג את $n = dq + r$ ו־$0 \leq r \leq d - 1$, $r, q \in \mathbb{Z}$.

$$x^n = x^{dq+r} = \left(x^d\right)^q - x^r =$$

טענה: אם $i \neq j$, $0 \leq i, j \leq d - 1$ **אז** $x^i \leq x^j$
הוכחה: נניח בשלילה ש־$x^i = x^j$ ו־$j > i$. אז $x^{i-j} = 1$ ו־$0 < i - j < d$ ולכן $i - j \notin S$ וזו סתירה

הגדרה 1.6 H נקראת תת־חבורה ציקלית הנוצרת על ידי x, אם H סופית אז $|H|$הוא <u>הסדר</u> של x ב־G.
שקול לכך: הסדר של x הוא השלם החיובי המינימלי d עבורו $x^d = 1$.

דוגמאות:

- תהא G חבורה. אזי יש רק איבר אחד מסדר אחד ב־G.
- $G = S^1$. (S^1, אוסף כל האיברים מהצורה $\cos\theta = i \sin\theta$ או $e^{i\theta}$) אז, $x = \mathrm{cis}\frac{2\pi}{n}$ הוא איבר מסדר n.

  – תרגיל: $e^{i 2\pi \sqrt{2}}$ הוא איבר מסדר ∞.

- $G=S_3$ (חבורת הפרמוטציות על $\{1,2,3\}$) $(1,2,3)$ איבר מסדר 3. $(1,2)$ איבר מסדר 2.
- $G=GL_2\left(R\right)$. $x=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. אז xהוא איבר מסדר ∞ ($x^n=\begin{pmatrix}1 & n\\ 0 & 1\end{pmatrix}$)

הגדרה 1.7 תת חבורה של G הנגזרת ע"י קבוצה $S\subseteq G$, היא תת החבורה הקטנה ביותר המכילה את אברי S. נסמן - $\langle S\rangle$
$\langle S\rangle$ היא הקבוצה שמכילה את כל אברי S, את ההופכיים שלהם, ואת כל המכפלות שאפשר לרשום בעזרת אברי S וההופכיים (ובפרט - את איבר היחידה)

אם G חבורה, ונניח $a,b\in G$, אז $\langle a,b\rangle=\left\{1,a,b,a^{-1},b^{-1},ab,ab^{-1},ab^2,a^{-1}b,ba\ldots\right\}$. $\langle a\rangle\subset\langle a,b\rangle$.

הגדרה 1.8 בפרט, $S\subseteq G$ יוצרת את G, אם $G=\langle S\rangle$,

- אם $G=S_3$, אז $G=\langle\left(1,2\right),\left(1,2,3\right)\rangle$.
- $G=\mathbb{Z}$, ו-$S=\{10,18\}$ אז $\langle S\rangle=2\mathbb{Z}$.
- $\mathbb{R}^2$- $\{(a,b):a,b\in\mathbb{R}\}$ והפעולה - $(a,b)\cdot(c,d)=(a+c,b+d)$. $S=\{(a,0),(0,a):a\in\mathbb{R}\}$. אזי $\mathbb{R}^2=\langle S\rangle$.
- עבור $\mathbb{Z}^2$, $S=\{\left(1,0\right),\left(0,1\right)\}$ אזי $\mathbb{Z}^2=\langle S\rangle$. (עם פעולת החיבור)

הגדרה 1.9 G חבורה נקראת ציקליות (אין סופית אם $|G|=\infty$) אם G נוצרת על ידי איבר יחיד.

- למשל, $\mathbb{Z}$ נוצרת ע"י $\langle 1\rangle$.
  - $\langle 2\rangle$=$\{2^n:n\in\mathbb{Z}\}$(פעולת כפל)
- $\left\{e^{\frac{2\pi k}{n}i}:0\leq k\leq n-1\right\}$ חבורה ציקלית מסדר n. שנוצרת על ידי $\left\langle e^{\frac{2k}{n}i}\right\rangle$.
- כל חבורה ציקלית היא אבלית!
- חבורת קליין - $G=\left\{\begin{pmatrix}\pm1 & 0\\ 0 & \pm1\end{pmatrix}\right\}$. עם כפל מטריצות. $|G|=4$. כל איבר למעט איבר היחידה הוא מסדר 2, ולכן G אינה ציקלית!
- קווטרניונים - $quanternions$ - $1=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, $I=\begin{pmatrix}i & 0\\ 0 & -1\end{pmatrix}$, $J=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$, $K=\begin{pmatrix}0 & i\\ i & 0\end{pmatrix}$ כאשר $H=\{\pm I,\pm i,\pm J,\pm K\}$ לא ציקלית ולא אבלית. I איבר מסדר 4. לבדוק: $H=\langle I,J\rangle$. יש טעות - למצוא כתרגיל

1.5 חבורות איזומורפיות

$G=\left\{\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}:x\in\mathbb{R}\right\}$ עם כפל מטריצות. $\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & y\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & x+y\\ 0 & 1\end{pmatrix}$ מאוד דומה ל-$(\mathbb{R},+)$.
היינו רוצים להגיד ש-G,G' הן "אותה" חבורה, אם קיימת העתקה חח"ע ועל בין החבורות, המקיימת $g,h\in G$, $g',h'\in G$, ו-$gh\mapsto g'h'$, $1_G\mapsto 1_{G'}$ ו-$g^{-1}\mapsto g'^{-1}$.

הגדרה 1.10 יהיו G,G' חבורות. נאמר ש-G,G' איזומורפיות אם קיימת העתקה $\phi:G\to G'$ חד-חד ערכית ועל המקיימת $\varphi\left(g\cdot h\right)=\varphi(g)\cdot\varphi(h)$.

הערה: אם קיימת העתקה $\varphi^{-1}:G'\to G$ כך ש-$\varphi\circ\varphi^{-1}=\varphi^{-1}\circ\varphi$ וכך-$\varphi^{[1}\left(g'\cdot h'\right)=\varphi^{-1}\left(h\right)\varphi^{-1}(h)$.

למה 1.11 $\varphi(1_G)=1_{G'}$ ו-$\varphi(a^{-1})=\left(\varphi\left(a\right)\right)^{-1}$.

הוכחה: יחידה: $a\in G$, אז $\varphi(a)=\varphi(a\cdot 1)=\varphi(a)\varphi(1)$ נכפול משמאל ב־$\varphi\left(a^{-1}\right)$ ונקבל -

$$1_{G'}=\varphi\left(1_G\right)$$

הופכי: $1=\varphi(1)=\varphi\left(a\cdot a^{-1}\right)=\varphi(a)\cdot\varphi(a^{-1})$ נכפול ב־$\left(\varphi(a)\right)^{-1}$ משמאל ולכן:

$$\varphi\left(a^{-1}\right)=\left(\varphi(a)\right)^{-1}$$

■

הגדרה 1.12 העתקה כזו φ נקראת "איזומורפיזם" ומסמנים $G\simeq G'$

דוגמאות:

- $\{2^n:n\in\mathbb{Z}\}\simeq\mathbb{Z}^+$. נקח $\varphi:\mathbb{Z}\to\{2^n:n\in Z\}$ ו־$n\mapsto 2^n$
- $G=\left\{\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}:x\in\mathbb{R}\right\}$ עם כפל מטריצות. $G\simeq\mathbb{R}$.

  – $\phi:\mathbb{R}\to G$ ע"י $\varphi(x)=\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}$.

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

- אם G,G' 2 חבורות ציקליות מסדר n, G,G' איזומורפיות.

  הוכחה: $G=\langle x\rangle$, $G'=\langle y\rangle$. כי G,G' ציקליות וכן $x^n=1_G$ ו־$y^n=1_{G'}$.

  נגדיר $\varphi:G\to G'$: $\varphi(x)=y$. (תרגיל: לסיים) ■

הגדרה 1.13 אוסף כל החבורות G' האיזומורפיות לחבורה נתונה G נקראת מחלקת האיזומורפיזם של G (אם G',G'' איזומורפיות ל־G, אז $G'\simeq G''$. תרגיל)

דוגמאות:

- יש רק מחלקת שקילות אחת לחבורות מסדר 3 , איזומורפית לחבורה ציקלית, $H=\left\{x^3=1\right\}$ ($e^{\frac{2\pi}{3}}$)
- יש שתי מחלקות שקילות לחבורות מסדר 4. כלומר - כל חבורה מסדר 4 איזומורפית לחבורה ציקלית או לחבורת קליין.

הגדרה 1.14 איזומורפיזם מ־$G\to G$ נקרא אוטומורפיזם.

דוגמאות:

- $\varphi:G\to G$ - הזהות הוא אוטומורפיזם
-

$$\varphi:\mathbb{R}\to\mathbb{R}$$
$$\varphi(x)=-x$$

היא איזומורפיזם. היא בוודאי חח"ע ועל, צריך להראות ש־$\varphi(x+y)=-x-y=\varphi(x)+\varphi(y)$

- $G=\{1,x,x^2\}$, $x^3=1$, G ציקליות מסדר 3 .

$$\varphi: G\to G$$
$$\varphi(x)=x^2$$

$$\varphi(1)=1,\ \varphi(x)=x^2 \text{ ו־} \varphi(x)=\left(x^2\right)^2=x$$

- האוטומורפיזם החשוב ביותר: **הצמדה** - $a\in G$. נגדיר את אוטומורפיזם ההצמדה ב־a:

$$\varphi_a(g)=aga^{-1}$$

אם $a\in G$, אז aga^{-1} נקרא **איבר צמוד** של g.

– תרגיל: לבדוק שזה אוטומורפיזם - להראות שזה חח"ע ועל (או להראות שיש לפונקציה פונקציה הפוכה - $\varphi^{-1}(g)=a^{-1}ga$ אז $\varphi^{-1}\circ\varphi(g)=\varphi^{-1}(aga^{-1})=a^{-1}aga^{-1}a=g$. ו־$\varphi_a(gh)=agha^{-1}=aga^{-1}aha=\varphi(g)\varphi(h)$

– אם $g\in G$ אז כל איבר מהצורה aga^{-1} עבור $a\in G$ נקאה איבר צמוד של g. g,aga^{-1} נקראים "איברים צמודים".

למה 1.15 אם $g,h\in G$ צמודים, אז יש להם את אותו הסדר. $\left(aga^{-1}\right)^n=ag^na^{-1}$

$$\left(aga^{-1}\right)^n=ag\underbrace{a^{-1}a}_{1}ga^{-1}\dots aga^{-1}=ag^na^{-1}$$

הגדרה 1.16 עבור $g\in G$, $\left\{aga^{-1}:a\in G\right\}$, נקראת מחלקת הצמידות של g.

– אם G חבורה אבלית, $a\in G$ אז $\varphi_a(g)=aga^{-1}=g$ כלומר, φ_a היא פונקצית זהות.
– אם $g\in G$ אז מחלקת הצמידות של g היא $\{g\}$

1.5.1 הומומורפיזם

הגדרה 1.17 יהיו G,G' שתי חבורות. $\varphi:G\to G'$ נקראה הומומורפיזם אם $\varphi\left(gh\right)=\varphi(g)\varphi(h)$ לכל $g,h\in G$.

הערה 1.18 אם φ הוא הומומורפיזם, אז $\varphi(1_G)=1_{G'}$. $\varphi\left(a^{-1}\right)=\varphi^{-1}(a)$.

דוגמאות:

- ההומומורפיזם הטריוויאלי: $\varphi:G\to G'$ $\varphi(g)=1$ לכל $g\in G$.

  – זה הומומורפיזם כי $1=\varphi(g\cdot h)=1\cdot 1=\varphi(g)\cdot\varphi(h)$

- כל $\varphi:G\to G'$ שהוא איזומורפיזם, הוא בודאי הומומורפיזם

  – $\varphi:G\to G$, $\varphi(g)=g$ הוא איזומורפיזם, ולכן הומומורפיזם

- $G=GL_n\left(\mathbb{R}\right)$ (מטריצות הפיכות,) אז $\varphi:G\to\mathbb{R}^\star$, $\varphi(g)=\det(g)$. אנחנו יודיעם כי

$$|A\cdot B|=|A|\cdot|B|$$

  – (כשמסמנים $\mathbb{R}^\star$, הכוונה היא ל־$\mathbb{R}\setminus\{0\}$, ולכן הפעולה היא כפל)

- $G=S_n$, תמורות על n איברים. סימן/זוגיות של תמורה $\operatorname{sign}\left(\sigma\right)$, $\sigma\in S_n$, הוא זוגיות מספר החילופים שמגדירים את σ. - $(-1)^{\text{number of swaping}}$.

– אם $\sigma \in S_n$, $\text{sign}\sigma = (-1)^{(\#\text{ of swapps})}$. בתרגיל - יהיה להראות שזה מוגדר היטב

–

$$\varphi : S_n \to \{-1, 1\}$$

$\{1,-1\}$ היא חבורה עם כפל. הטענה: $\phi(\sigma) = \text{sign}(\sigma)$ הוא איזומורפיזם. יהיה בתרגיל בית. רמז: הקשר לדטרמיננטים, ויצוג של תמורה כמטריצה, אז הדטרמיננט של המטריצה המייצגת של התמורה היא דטרמיננטה.

- G חבורה, $a \in G$, $\varphi_a : \mathbb{Z} \to G$ יוגדר כ־$\varphi_a(n) = a^n$ הוא הומומורפיזם. התמונה של φ_a היא תת חבורה ציקלית הנוצרת על ידי a.
- אם $H \subset G$ תת חבורה, אז $i = \varphi : H \to G$ ההכלה - $i(h) = h$.

אם $\varphi : G \to G'$ הוא הומומורפיזם, אז φ מגדירה שתי תתי חבורות חשובות:

1. $\text{Im}\varphi$ - התמונה של φ - אוסף כל האיברים $\{g' \in G' : g' = \varphi(g), g \in G\}$.
   - נוודא שזה תת חבורה: $1_{G'} \in \text{Im}\varphi$ כי $1_{G'} = \varphi(1_G)$
   - סגירות לכפל: אם $g', h' \in \varphi(g)$ אז $g' = \varphi(g)$ ו־$h' = \varphi(h)$ לכן $\varphi(g \cdot h) = g'h'$.
   - סגירות להופכי: $g' \in \text{Im}\varphi$ אז $g' = \varphi(g)$ ל־$g \in G$ אז $\varphi(g^{-1}) = g'^{-1}$.
2. הגרעין של φ - $\ker\varphi = \{g \in G : \varphi(g) = 1\}$
   (א) $\varphi(1) = 1$ לכן $1 \in \ker\varphi$
   (ב) אם $g, h \in \ker\varphi$ אז $\varphi(g) = \varphi(h) = 1$ לכן $\varphi(gh) = \varphi(g) \cdot \varphi(h) = 1 \cdot 1 = 1$
   (ג) אם $g \in \ker\varphi$ אז $\varphi(g) = 1$ לכן גם $\varphi(g^{-1}) = \varphi(g)^{-1} = 1^{-1} = 1$

דוגמאות

- אם φ הוא המומומורפיזם הטריויאלי, אז $\text{Im}\varphi = \{1\}$ ו־$\ker\varphi = G$
- אם $\varphi : G \to G'$ הוא איזומורפיזם, אז $\text{Im}\varphi = G'$ ו־$\ker\varphi = \{1\}$
- אם $G = GL_n(\mathbb{R})$, $\varphi(g) = \det G$ אז $\text{Im}\varphi = \mathbb{R}^\star$ ו־$\ker\varphi = \{g : \det g = 1\} = SL_n(\mathbb{R})$
- עם $\varphi : S_n \to \{-1, 1\}$ אז התמונה היא $\{1, -1\}$ והגרעין הוא $\ker\varphi = \{\sigma \in S_n : \text{sign}\sigma = 1\} = A_n$

הערה 1.19 אם $\varphi : G \to G'$ הומומורפיזם, ו־$g \in \ker\varphi$, אז לכל $a \in G$, $aga^{-1} \in \ker\varphi$ כי

$$\begin{aligned}
\varphi(aga^{-1}) &= \varphi(a)\varphi(g)\varphi(g^{-1}) \\
&= \varphi(a)\varphi(g)\varphi(g)^{-1} \\
&= \varphi(a) \cdot 1 \cdot \varphi(g)^{-1} \\
&= 1
\end{aligned}$$

הגדרה 1.20 תהא G חבורה, ותהא $N \subset G$ תת חבורה. N נקראת **תת חבורה נורמלית של** G אם לכל $g \in N$, $aga^{-1} \in N$ לכל $a \in G$.

- דוגמא:
  אם $\varphi : G \to G'$ הוא הומומורפיזם, אז $\ker\varphi$ הוא תת חבורה נורמלית של G

הערה 1.21 אם G אבלית, אז כל תת חבורה של G היא נורמלית.

(להשלים: שיעור שני, 2.12)

1.6 קו־סטים

- כל יחס שקילות על קבוצה S, מגדיר חלוקה של S ־ למחלקות שקילות
- ולהפך, כל חלוקה של S מגדירה יחס שקילות על S.

אם $\varphi : S \to S'$, פונקציה, אז φ משרה יחס שקילות על S, על ידי הסיבים שלה: $a \sim b$ אם $\varphi(a) = \varphi(b)$ והקבוצה

$$\{a : \varphi(a) = \alpha\} = \varphi^{-1}(\alpha)$$

הוא סיב של φ . נקבל התאמה חח"ע ועל בין התמונה של φ לבין מחלקות השקילות של היחס ש־φמשרה.
אם נסמן את קבוצת תת מחלקות השקילות ב־$\bar{S}$ (או $S/\sim$) ההתאמה היא $\bar{S} \to \mathrm{Im}\varphi$, $\bar{S} \mapsto \varphi(S)$
מקרה פרטי: אם $\varphi : G \to G'$ היא הומומורפיזם, אז φ משרה יחס שקילות על G.
לדוגמא,

1. $\varphi : \mathbb{C}^\star \to \mathbb{R}^\star$, $|a| \mapsto a$, אז φ הומומורפיזם, ומשרה חלוקה על $\mathbb{C}^\star$ למחלקות שקילות שהן מעגלים קו(נ)צנטרים.
2. $\varphi : \mathbb{Z} \to C_m = \left\{1, x, x^2, \ldots x^{m-1}\right\}$ $n \mapsto x^n$, מחלקות השיקלות
   מחלקות השקילות תחת φ ־ $n \sim k$ אם $x^n = x^k \iff k^{n-k} = 1 \iff m|n-k$.
   יש m מחלקות ששילות:

$$\begin{aligned}
\bar{0} &= \{0, m, -m, 2m - 2m, \ldots\} \\
\bar{1} &= \{1, m+1, -m+1, 2m+1, -2m+1\} \\
m \bar{-} 1 &= \{m-1, 2m-1, -1, \ldots\}
\end{aligned}$$

כל המחלקות שקילות מתקבלות על ידי הזזה של מחלקת שקילות של 0.

טענה 1.22 נניח ש־$\varphi : G \to G'$ הומומורפיזם, ויהי $N = \ker\varphi$. אז $a \sim b$ תחת φ ($\varphi(a) = \varphi(b)$) אם ורק אם $a^{-1}b \in N$.

הוכחה: נניח $\varphi(a) = \varphi(b)$, φ הוא הומומורפיזם, לכן

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

ו־$a^{-1}b$ בגרעין.
בכיוון השני, נניח $a^{-1}b \in N$, אז $a^{-1}b = n$ עבור $n \in N$. נכפול את 2 האגפים ב־ a ונקבל

$$\begin{aligned}
b &= an \\
\varphi(b) &= \varphi(a) \cdot \varphi(n) = \varphi(a)
\end{aligned}$$

קבוצת כל הנקודות $aN = \{an : n \in N\}$, נקראת מחלקת השקילות של a.
aN ־ מהווים את הסיבים של ההעתקה φ. ∎

דוגמא: אם ההעתקה φ היא חח"ע, לכל מחלקת שקילות יש רק איבר אחד, ובפרט, $\ker\varphi = \{1\}$

הערה 1.23 לכל a, g, יש התאמה חח"ע ועל בין N ל־ aN:

$$\begin{aligned}
N &\to aN \\
g &\mapsto ag
\end{aligned}$$

- בניה כללית ־ $H \subset G$, אפשר להגדיר יחס שקילות על G בעזרת H:$a \sim b$ אם $a^{-1}b \in H \iff b = ah$ עבור איזה $h \in H$.
  - נבדוק שזה יחס שקילות:

* טרנזיטיביות - נניח $a\sim b, b\sim c$ $b=ah$ וגם $c=bh'$ (עבור $h,h'\in H$ כלשהם) , נציב ונקבל $c=ahh'$ אבל לפי הסגירות של תת החבורה H, $hh'\in H$.
* סימטריות - אם $a\sim b$ אז $b=ah$ עבור איזה $h\in H$, נכפול ב-h^{-1} ונקבל $a=bh^{-1}$, אבל $h^{-1}\in h$ ולכן $b\sim a$.
* רפלקסיביות: $a=a\cdot 1$ ו-$1\in H$.

הגדרה 1.24 הקו־סטים השמאליים של H הם מחלקות השקילות $aH=\{ah : h\in H\}$.

מכוון שאלה מחלקות שקילות, נובע שאם $aH\cap bH\neq\emptyset$, אז $aH=bH$.

דוגמאות:

- המקרים הטריוויאלים:
  - $H=\{1\}$, אז הקוסטים השמאליים של H הם $\{a\}$עבור $a\in G$
  - $H=G$, אז יש רק קו־סט שמאלי אחד - G.
- $G=\mathbb{C}^{\star}$, ו-$H=S^{1}$ (אוסף כל האיברים בגודל 1) -
  - כל קוסט של H הוא מהצורה $r\in\mathbb{R}$, $c_r=\left\{rz : z\in S^{1}\right\}$.

טענה 1.25 יש התאמה חח"ע ועל בין H ל-aH לכל $a\in G$ (הוכחנו בע"פ)

מסקנה 1.26 כל הקוסטים הם מאותו גודל

הגדרה 1.27 האינדקס H ב-G הוא מספר הקוסטים השמאליים של H ב-G (לא חייב להיות סופי). מסומן ב-$[G:H]$.

מסקנה 1.28 אם G חבורה סופית את $|G|=|H|\,[G:H]$ (נכון גם אם G לא סופית)

1.6.1 משפט לגרנז'

משפט 1.29 משפט לגרנז'
(לגרנז') - אם $H<G$ אז $|H|\mid|G|$

מסקנה 1.30 אם לG0 יש מספר איברים ראשוני (כלומר $|G|$ ראשוני) אז יש לה רק תתי חבורות טריוויאליות

מסקנה 1.31 אם G חבורה $|G|$-ראשוני, אז G ציקלית.

הוכחה: נקח $1\neq g\in G$. נניח כי $|G|\geq 2$.
נתבונן ב-$H=\langle g\rangle$. $|H|>1$ ולכן $H\neq 1$ ולכן $\langle g\rangle=G$. ■

הערה 1.32 הצלחנו למיין את כל החבורות מסדר ראשוני

מסקנה 1.33 יש $a\in G$ סופית אז $|a|\mid|G|$ (כש-$|a|=|\langle a\rangle|$)

מסקנה 1.34 אם $\varphi:G\to G'$ הומומורפיזם של חבורות סופיות, אז $|G|=|\ker\varphi|\cdot|\mathrm{Im}\varphi|$

הוכחה: יחס שקילות המוגדר על ידי φ הוא בדיוק מספר השקיליות המוגדר על ידי התת חבורה $\ker\varphi$, ולכן $|\mathrm{Im}\varphi|=[G:\ker\varphi]$ ■

מסקנה 1.35 נובע מכך ש-$|G|\,/\,|G||\ker\varphi|\,/\,|\mathrm{Im}\varphi|$ וכן $|\mathrm{Im}\varphi|\,/\,|G'|$

הערה 1.36 (הערכה כללית): בהנתן $H<G$, ניתן להתבונן ביחס השקילות "הימני" $b\sim a$ הוא $b=ha$ עבור איזה $b\in H$.

שאלה: מתי אוסף הקוסטים השמאליים שווה לאוסף הקוסטים הימניים?
תשובה: לא תמיד. אך אם החבורה אבלית ־ אז כן.

הגדרה 1.37 קוסטים ימניים ־ $\{Ha\}_{a\in G}$. זו לא תמיד ואתה חלוקה כמו קוסטים ימניים
$|H| = |aH|$ לכל $a \in G$ ולכן $|G| / |A|$ אם $|H|$ ו־$|G|$ סופית ו־

$$G = \bigcup_{a\in G} aH$$

שאלה: מתי החלוקה השמאלית היא זהה לחלוקה הימנית?

טענה 1.38 G חבורה, $H < G$, אז החלוקות ש־H משרה זהות $\iff$ H נורמלית ב־G

הוכחה: אם $H \triangleright G$ כלומר, אם H נורמלית ב־G, נראה ש־ $aH = Ha$ לכל $a \in G$.
אם $a \in aH$ אז $g = ah$ לאיזה $h \in H$.

$$g = ah = aha^{-1}a$$

אבל $aha^{-1} \in H$, כלומר $aha^{-1} = h'$ ולכן

$$ah = h'a \in Ha$$

כלומר, $aH \subseteq Ha$.
הכיוון השני דומה ־ $Ha \subseteq aH$, ולכן $aH = Ha$.
הכיוון השני ־ צ"ל אם החלוקות זהות אז H נורמלית.
נוכיח בשלילה. נראה כי אם H לא נורמלית אז החלוקות לא זהות.
נשים לב שאם החלוקת זהות אז בפרט, $aH = Ha$ כי $a \in aH$ ו־$a \in Ha$.
נראה כי קיים $a \in G$ עבורו $aH \neq Ha$.
H לא נורמלית, לכן **יש** איזשהו $h \in H$ ו־$a \in G$, כך ש־$a^{-1}ha \notin H$. כלומר $Ha \ni ha \notin aH$. ■

טענה 1.39 G חבורה. נניח $K, H < G$. אז $K \cap H < H$, אם K נורמלית ב־G, אז $H \cap K$ נורמלית ב־H.

מסקנה 1.40 אם $(|H|, |K|) = 1$, אז $\{1\} = H \cap K$

הוכחה: $K \cap H < H$ ו־$K \cap H \subset K$ ולכן $|H| / |K \cap H|$ ו־$|K| / |K \cap H|$ ולכן $|K \cap H| = 1$.
$K \cap H < H$. מספיק לבודק ש־$K \cap H$ חבורה ביחס לכפל ב־$\cdot$.
נראה ש־$K \triangleleft G$ אז $K \cap H \triangleleft H$ (לא אומר ש־$K \cap H \triangleleft G$).
נקח $h \in H$ ו־$k \in K \cap H$. אז

$$h^{-1}kh \in K$$

כי K נורמלית ב־G. מצד שני,

$$h^{-1}kh \in H$$

בגלל הסגירות לכפל ב־H, לכן $h^{-1}kh \in K \cap H$. ■

הערה 1.41 אם גם H נורמלית ב־G, אז $K \cap H \triangleleft G$, כי אם $K \in K \cap H$ ו ־ $g \in G$ אז

$$H \ni gkg^{-1} \in K$$

כי $k \in K$ ו־$k \in H$, ובגלל ש־K, H נורמליות, ולכן $gkg^{-1} \in H \cap K$.

הגדרה 1.42 $\varphi : G \to G'$ הומומורפיזם ו־$H < G$ תת חבורה.
הצמצום של φ ל־H:

$$\varphi|_H : H \to G'$$

היא פונקציה המוגדרת על ידי $\varphi|_H(h) = \varphi(h)$.

טענה 1.43

$$\ker \varphi|_H = \ker \varphi \cap H$$

טענה 1.44 אם $(|G|, |G'|) = 1$ אז $\varphi(H) = \{1\}$ (נניח, H, G' סופיות)

הוכחה: $\varphi(H)$ היא התמונה של $\varphi|_H$. לכן, $|\varphi(H)| / H$ וגם $|\varphi(H)| / |G'|$ ■

דוגמה: $\varphi : S_n \to \{\pm 1\}$. $\varphi(\sigma) = \text{sign}\sigma$.
H ־ תת חבורה של תמורות זוגיות, אז $H \subseteq A_n$.
תרגיל: מה הקשר? $(-$:.

טענה 1.45 $\varphi : G \to G'$ הומומורפיזם. נניח $H' < G'$

$$\tilde{H} = \varphi^{-1}(H) = \{x \in G | \varphi(x) \in H'\}$$

אזי

1. $\tilde{H} < G$
2. אם $H' \triangleleft G'$ אז $\tilde{H} \triangleleft G$
3. $\ker \varphi \subseteq \tilde{H}$
4. $\varphi|_{\tilde{H}} = \tilde{H} \to H'$ היא הומומורפיזם , $\ker \varphi|_H = \ker \varphi$

(יופיע בתרגיל בית)

דוגמא: $\varphi : GL_n(\mathbb{R}) \to \mathbb{R}^\star$, כאשר $g \mapsto \det g$. $P < \mathbb{R}^\star$ כך ש־$P = \{x : x > 0\}$.
אז $P \triangleleft \mathbb{R}^\star$.
מסקנה: $\varphi^{-1}(P)$ היא תת חבורה נורמלית של $GL_n(\mathbb{R})$. נובע מטענה (2) ־ כל המטריצות g עם $\det g > 0$ הם תת חבורה נורמלית של $GL_n(\mathbb{R})$.
להשלים משיעור קודם
רצינו תנאי למתי $G \cong H \times J$ כאשר H, K תתי חבורות שלה

טענה 1.46 אם G חבורה, $H, K \triangleleft G$ (H, K נורמליות ב־G) וגם $H \cap K = \{1\}$, $G = HK = \{\, h \cdot k \mid h \in H, k \in K \,\}$ אז

$$G \cong \underbrace{H \times K}_{(1)}$$

(1) ־ מכפלה ישרה.

הוכחה: (נזכיר כי אם $H \triangleleft G$ אז HK תת חבורה.)
אם גם H וגם K נורמליות, אז לכל $H \ni h, k \in K$ וגם החיתוך הוא טריוויאלי , מתקיים $hk = kh$ **(זה לא אומר שאחת מהן קומטטיבית)**.
כי

$$hkh^{-1}k^{-1}$$

אם הביטוי שווה ל־1, אז h,k מתחלפים

$$\underbrace{\underbrace{hkh^{-1}}_{\in K}k^{-1}}_{\in K}$$

ומצד שני

$$hkh^{-1}k^{-1}=h\left(kh^{-1}k^{-1}\right)=hh'\in H$$

מסגירות, כלומר, האיבר הוא גם ב־K וגם ב־H, אבל האיבר היחיד בחיתוך הוא "1" ולכן,

$$\begin{aligned}hkh^{-1}k^{-1}&=1\\ hk&=kh\end{aligned}$$

נגדיר העתקה,

$$\begin{aligned}\varphi:H\times K&\to G\\ (h,k)&\mapsto h\cdot k\end{aligned}$$

אזי φ על כי $HK=G$. נראה ש־φ הומומורפיזם ושהגרעין טריוויאלי.

$$\varphi\left((h,k)\left(h',k'\right)\right)=\varphi\left(\left(hh',kk'\right)\right)=hh'kk'=hkh'k'=\varphi\left((h,k)\right)\varphi\left(\left(h',k'\right)\right)$$

נסתכל על הגרעין של φ: אם $\varphi\left((h,k)\right)=1$ אז $hk=1$, אז $H\ni h=k^{-1}\in K$ אבל יש רק איבר אחד שנמצא גם ב־H וגם ב־K, והוא 1, ולכן $h=k=1$. ■

2 חבורות מנה

נזכור סימונים -

$aN=\{an:n\in N\}$ - קוסטים שמאליים של N (אם N נורמלית, אז $aN=Na$)

אם A,B תתי קבוצות של G, אז $A\cdot B=\{\,a\cdot b\mid a\in A,b\in B\,\}$

למה 2.1 תהא G חבורה, ו־$N\lhd G$ (N תת חבורה נורמלית של G)

$$aN\cdot bN=\{anbn'|n,n'\in N\}=abN$$

(כאשר השוויון הוא שוויון של קבוצות)

הוכחה: $bN=Nb$ (כקבוצות, בגלל ש־N נורמלית)

$$a\cdot N\cdot b\cdot N=a\cdot b\cdot N\cdot N$$

אז, נותר להוכיח ש־ $N\cdot N=N$.

מצד אחד, $N\subseteq N\cdot N$ מתוך סגירות.

מצד שני, $N\cdot N\subseteq N$ כי $1\in N$. ■

מסקנה 2.2 אם $N\lhd G$ אז ניתן להגדיר מכפלה על אוסף הקוסטים (השמאליים) של N: אם c_1,c_2 הם שני קוסטים של N, אז $C_1=aN$ לאיזה $a\in G$, $C_2=bN$ לאיזה $b\in G$, אז

$$C_1\cdot C_2=ab\cdot N$$

קוסט שמאלי של N.

2.0.2 דוגמאות

- נקח את $G=\mathbb{Z}$ ואת $N=n\mathbb{Z}$ עבור $n\in\mathbb{N}$, אז הקוסטים של N הם מהצורה

$$a+n\mathbb{Z}$$

עבור $a\in\mathbb{Z}$, ופעולת הכפל (חיבור) על הקוסטים היא על ידי $(a+n\mathbb{Z})+(b+n\mathbb{Z})=(a+b)+n\mathbb{Z}$.
אז

$$\bar{a}+\bar{b}=(a\bar{+}b)$$

- $G=\mathbb{C}^{\star}$ (בלי ה־0) ואת $N=S^1$ (מעגל היחידה) , אז קוסטים של N הם מהצורה $r\cdot S^1,\ r\in\mathbb{R}^{\star}$ ($C_r=\{\,r\cdot z\mid |z|=1\,\}$) אזי

$$C_r\cdot C_s=C_{r\cdot s}$$

- $G=S_3$, $|G|=6$.

$$\begin{aligned}N&=\langle(1,2,3)\rangle\\&=\left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},(1,2,3)^2=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},(1,2,3)=e\right\}\end{aligned}$$

נבדוק: $N\lhd G$ (תרגיל בית)

$$[G:N]=2$$

מחלקות השקילות: $H=\{\,N,(1,2)\,N\,\}$. נראה שזו חבורה. נגדיר פעולה: $((1,2)\,N)\,((1,2)\,N)=(1,2)\,(1,2)\,N=N\in H$

- אם N לא נורמלית, אז הפעולה שהגדרנו היא לא טובה: אם N לא נורמלית, קיים איבר $a\in G$ כך ש־$aN\neq Na$, כלומר

$$aNa^{-1}\neq N$$

אבל, אם הגדרת הפעולה היתה עובדת במקרה הזה, אש $aN\cdot a^{-1}N=aa^{-1}N=N$

הגדרה 2.3 אם $N\lhd G$ אז מסמנים את אוסף הקוסטים של N ב־G ע"י ${}^{G}\!/_{N}$ (או, אם יש רק תת חבור נורמלית אחת שאפשר לדבר עליה - $\bar{G}$).

דוגמה - אם $G=\mathbb{Z}$ ו־$N=n\mathbb{Z}$ אז ${}^{G}\!/_{N}={}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$
אם $N\lhd G$ אז יש העתקה טבעית $\varphi:G\to{}^{G}\!/_{N}$ שמוגדרת כ־ $g\mapsto\bar{g}=gN$ נקראת ההעתקה הקאנונית.
ההעתקה הקאנונית φ היא הומומורפיזם והגרעין שלה הוא N

משפט 2.4 תהא G חבורה. $N\lhd G$, אז ${}^{G}\!/_{L}$ היא חבורה תחת פעולת הכפל שהגדרנו. הסדר של ${}^{G}\!/_{N}$ הוא $[G:N]$ והגרעין של ההעתקה הקאנונית הוא N

מסקנה 2.5 כל תת חבורה נורמלית של G היא גרעין של הומומורפיזם.

להשלים, שיעור ראשון מה־ 23.12

2.1 משפט האוטומטרפרפיזם הראשון

2.1.1 משפט האיזומורפיזם הראשון: $\varphi : G \to G'$ הומומורפיזם, אזי

$$G/\ker\varphi \cong \mathbf{Im}\varphi$$

דוגמאות

•

$$\begin{aligned}\varphi : \mathbb{R} &\to S^1 = \left\{e^{2\pi i\theta} | 0 < \theta \leq 1\right\}\\ x &\mapsto e^{2\pi i x}\end{aligned}$$

אזי

$$\begin{aligned}&\mathrm{Im}\varphi = S^1\\ &\ker\varphi = \left\{\ x : e^{2\pi i x} = 1\ \right\} = \mathbb{Z}\end{aligned}$$

מסקנה - חבורת המנה, $\mathbb{R}/\mathbb{Z} \cong S^1$. $\mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$ - היא טורוס (דונאט)

•

$$G = \left\{ \begin{pmatrix} 1 & x & z\\ 0 & 1 & y\\ 0 & 0 & 1\end{pmatrix} \middle| \ x, y, z \in \mathbb{R} \right\}$$

(G נקראת חבורת היזנברג של $\mathbb{R}$ - $\mathbb{H}^{(\mathbb{R})}$)

• וההעתקה

$$\begin{aligned}\varphi &: G \to \mathbb{R}^2\\ \begin{pmatrix} 1 & x & z\\ 0 & 1 & y\\ 0 & 0 & 1\end{pmatrix} &\mapsto (x, y)\end{aligned}$$

אזי φ הומומורפיזם (לבדוק).

$$\begin{aligned}\mathrm{Im}\varphi &= \mathbb{R}^2\\ N = \ker\varphi &= \left\{ \begin{pmatrix} 1 & 0 & z\\ 0 & 1 & 0\\ 0 & 0 & 1\end{pmatrix} \middle| \ z \in \mathbb{R} \right\}\end{aligned}$$

אז המסקנה חבורת איזנברג $\mathbb{H}^{(\mathbb{R})}/N \cong \mathbb{R}^2$ (ו-$N \cong \mathbb{R}$)

• נתבונן בחבורה $G = S_4$. יש 3 חלוקות של הקבוצה $\{1,2,3,4\}$ לזוגות.

$$\begin{aligned}c_1 &= \{1,2\}, \{3,4\}\\ c_2 &= \{1,3\}, \{2,4\}\\ c_3 &= \{1,4\}, \{2,3\}\end{aligned}$$

כל תמורה של S_4 משרה תמורה על אוסף החלוקות $\{c_1, c_2, c_3\}$. למשל, אם נקח את התמורה $\begin{pmatrix} 1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}$ - אזי $\begin{cases} c_3 \mapsto c_2\\ c_2 \mapsto c_1\\ c_1 \mapsto c_3\end{cases}$. נתבונן בהעתקה $\begin{aligned}\varphi : S_4 &\to S_3\\ \sigma &\mapsto \mathcal{X}\end{aligned}$ כאשר $\mathcal{X}$ היא התמורה המושרה על אוסף הזוגות. בדקו - φ הומומורפיזם ועל.

טענה - $\ker\varphi = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3), I\}$ ו-$\ker\varphi \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ - חבורת קליין.

מסקנה -

$$S_4/\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \cong S_3$$

2.2 משפט האיזומורפיזם השני

משפט 2.6 תהא G חבורה ו־$H, N < G$ ו־$N \lhd G$, אזי $H/_{H\cap N} \cong HN/_N$

הוכחה: HN היא תת חבורה של G כי N נורמלית (מכפלה של תת חבורה נורמלית עם תת חבורה).
ו־N נירמלית ב־HN (כי היא נורמלית ב־ G) לכן, אגף ימין מוגדר היטב.
נתבונן בהעתקה הקאנונית:

$$\varphi : G \to G/_N$$

ראינו ש־φ הומומורפיזם. כעת, נתבונן בצימצום של φ ל־H: אזי, $\varphi|_H : H \to G/_N$.
מה הגרעין של $\varphi|_H$: $\varphi|_H(h) = 1 \iff \varphi(h) = hN = N$ ו־$h \in H$.
$\iff h \in N$ ($h \cdot 1 \in h \cdot N$ לכן, $h \in N$)
$\iff h \in H \cap N$
מה התמונה של $\varphi|_H$? התמונה היא אוסף הקוסטים -

$$\{\, hN \mid h \in N \,\} = \{\, hnN \mid h \in H, n \in N \,\} = HN/_N$$

ולכן, לפי משפט האיזומורפיזם הראשון -

$$H/_{\ker \varphi|_H} \cong HN/_N$$

■

2.2.1 דוגמאות

- G תהיה חבורת איזנברג־ $\mathbb{H}(\mathbb{R}) = G = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \middle| \, x, y, z \in \mathbb{R} \right\}$.

$$N = \left\{ \begin{pmatrix} 1 & 0 & z \\ & 1 & 0 \\ & & 1 \end{pmatrix} \middle| \, z \in \mathbb{R} \right\}$$

$$H = \left\{ \begin{pmatrix} 1 & m & k \\ & 1 & n \\ & & 1 \end{pmatrix} \middle| \, n, m, k \in \mathbb{Z} \right\}$$

בדקו - H לא נורמלית ב־G. ממשפט האיזומורפיזם השני - $H/_{H\cap N} \cong HN/_N$ ($\cong \mathbb{Z}^2$).

$$H \cap N = \left\{ \begin{pmatrix} 1 & 0 & z \\ & 1 & 0 \\ & & 1 \end{pmatrix} \middle| \, z \in \mathbb{Z} \right\}$$

$$HN = \left\{ \begin{pmatrix} 1 & m & z \\ & 1 & n \\ & & 1 \end{pmatrix} \middle| \, m, n \in \mathbb{Z}, z \in \mathbb{R} \right\}$$

$$HN/_N = \{ \ \}$$

להשלים שיעור, 30/12

3 פעולות של חבורה על קבוצה

הגדרה 3.1 תהא S קבוצה, ו־G חבורה, אז פעולה של Gעל S היא פונקציה

$$G\times S\to S$$
$$(g,s)\mapsto g\cdot s$$

שמקיימת:

- $1_G\cdot s=s$
- $g\left(hs\right)=\left(gh\right)s$ ($s\in S$, $g,h\in G$)

הערה 3.2 לכל $g\in G$, נקבל העתקה $m_g:S\to S$ המוגדרת על ידי ־ $m_g(s)=gs$. m_g היא חח"ע ועל ־ $gs=gs'\iff g^{-1}\left(gs\right)=g^{-1}\left(gs'\right)\iff s=s'$.
על ־ בהנתן $s'\in S$, צריך להראות שיש $s\in S$ כך ש־$gs=s'$. נקח את $s=g^{-1}s'$, ולכן $gs=g\left(g^{-1}s'\right)=s'$

3.0.2 דוגמאות

- $S=S^1=\{z\in\mathbb{C}|\,|z|=1\}$. $\lambda\in S'$. λ משרה פעולה של $G=\mathbb{Z}$ על s' על ידי

$$(n,z)=\lambda^n z$$

(דומה ל־$S={}^{\mathbb{R}}/_{\mathbb{Z}}$, $\alpha\in R$, $\mathbb{Z}$ פועל על ${}^{R}/_{\mathbb{Z}}$ על ידי $(n,x+\mathbb{Z})=x+n\alpha+\mathbb{Z}$)

- $S=\mathbb{R}^2$, G הוא אוסף העתקות ה<u>צפידות</u> על $\mathbb{R}^2$. ־ העתקות צפידות שומרות מרחקים.
(טענה, לא נוכיח) ־ כל ההעתקות הנ"ל הן מהצורה $v\in\mathbb{R}^2$, $gv=Ov+b$ כאשר $O\in M_2\left(\mathbb{R}\right)$ מטריצה המקיימת $O\cdot O^t=1$. מטריצות כאלו כוללות סיבובים ושיקופים. b ב־$\mathbb{R}^2$
G פועלת על $\mathbb{R}^2$, אבל גם על אוסף הישרים ב־$\mathbb{R}^2$, G גם פועלת על אוסף המשולשים במישור.

3.1 מסלול של חבורה

הגדרה 3.3 תהא G חבורה ו־S היא G־קבוצה, אז **המסלול** של $s\in S$ הוא $O_s=\{\ gs\mid g\in G\ \}=\{\ s'\mid \exists g\in G,gs=s'\ \}$

דוגמאות ־

- $S=\mathbb{R}^n$, $G=GL_n\left(\mathbb{R}\right)$.
  - המסלול של $\vec{0}$, $O_{\vec{0}}=\left\{\vec{0}\right\}$
  - אם $\vec{v}\neq\vec{0}$, אז $O_{\vec{v}}=\mathbb{R}^n\setminus\{0\}$
- $S=\mathbb{C}$, $G=C_2$ $gz=\bar{z}$. אזי $O_0=\{0\}$ ו־$O_z=\{z,\bar{z}\}$.

המסלולים של פעול G על S, משרים על S יחס שקילות: $s\sim s'$ אם $s'=gs$ לאיזה $g\in G$, כלומר־ $s\sim s'\iff O_s=O_{s'}$.

דוגמה: $S=SL_2\left(\mathbb{R}\right)$, אוסף כל המטריצות 2×2 עם דטרמיננטה ־ "1", $m=\begin{pmatrix}v_1\\v_2\end{pmatrix}=\begin{pmatrix}v_{11}&v_{12}\\v_{21}&v_{22}\end{pmatrix}$. נאמר ש־$\Gamma$ הוא **שריג** ב־$\mathbb{R}^2$, אם $\Gamma=\{mv_1+nv_2|m,n\in\mathbb{Z}\}$. Γ הוא השריג הנוצר על ידי v_1,v_2.
$SL_2\left(\mathbb{Z}\right)$ פועל על S על ידי כפל מטריצות ־ $M\in SL_2\left(\mathbb{Z}\right)$ ו־$N\in SL_2\left(\mathbb{R}\right)$ אז $(M,N)\to MN$.
טענה: מסלול של $N=\begin{pmatrix}v_1\\v_2\end{pmatrix}$ הוא אוסף הזוגות של וקטורים שיוצרים את אותו השריג, כמו v_1,v_2.

הגדרה 3.4 לאוסף מחלקות השקילות ב־S נקרא "המסלולים של G".

הגדרה 3.5 הפעולה של G נקראת טרנזטיבית אם יש ל־G רק מסלול אחד. כלומר, לכל $s,s'\in S$, יש $g\in G$ כך ש־$gs=s'$.

דוגמאות ־

- $S=\{1,2,3\}$, $G=S_4$ אז G פועלת טרנזטיבית על S. (לכל i,j יש תמורה $\sigma\in S_4$ המקיימת ־ $\sigma\left(i\right)=j$)
- $S={}^{\mathbb{R}^n}/_{\{0\}}$ אז $G=GL_n\left(\mathbb{R}\right)$ פועלת טרנזטיבית על S (תרגיל)

3.2 מייצב

הגדרה 3.6 תהא S G-קבוצה. יהא $s\in S$. **המייצב** של s, $G_s=\{g\in G|gs=s\}$.
G_s היא תת חבורה של G.

(להשלים מ-6.1)
G חבורה הפועלת על קבוצה S.

$$\begin{aligned}O_s&=\{gs|g\in G\}\\&=\{s':g'=gs\,,g\in G\}\end{aligned}$$

(המסלול של s תחת הפעולה g)
יש התאמה בין $O_s\to {}^{G}/_{G_s}:\varphi$ חד חד ערכית ועל ששומרת על הפעולה של G. G פועלת על ${}^{G}/_{G_S}$ - $g\left(hG_s\right)=ghG_s$.
G פועלת על O_s דרך הפעולה שלה על S.

$$\begin{aligned}s'&=hs\\gs'&=g\left(hs\right)=\left(gh\right)s\in O_s\\G\times O_S&\to G\\\left(g,s'\right)&\mapsto gs'\end{aligned}$$

$$\begin{array}{ccc}{}^{G}/_{G_s}&\xrightarrow{g}&{}^{G}/_{G_s}\\\downarrow_{\varphi}&&\downarrow_{\varphi}\\O_S&\xrightarrow{g}&O_s\end{array}$$

$$\begin{array}{ccc}hGs&\mapsto&ghG_s\\\downarrow&&\downarrow\\\varphi\left(gG_s\right)&\mapsto&g\varphi\left(hG_s\right)\end{array}$$

כלומר , $g\varphi\left(hG_s\right)=\varphi\left(ghG_s\right)$ כאשר משמאל, זו הפעולה של G על O_s ומימין זו הפעולה של G על ${}^{G}/_{G_s}$.
$S=\bigcup_{s\in S}O_s$, אבל O_S היא תת קבוצה של S. כאשר $O_{s'}=O_s$ או $O_s\cap O_{s'}=\emptyset$.
הפעולה של G על S משרה יחס שקילות על S. $s\sim s'$ אם $s'=gs$ עבור איזשהו $g\in G$.
דרך אחרת לומר זאת - $s'\in O_s$.
מכאן מקבלים חלוקה למחלקות שקילות (המסלולים של G)

$$\begin{aligned}G\times S&\to S\\\left(g,s\right)&\mapsto gs\end{aligned}$$

אם קובעים את g, מקבלים פונקציה $m_G:S\to S$.
$G\geq G_S=\{g|G:gs=s\}$. למה זה תת חבורה?

$$\begin{aligned}gs&=s\\hs&=s\\ghs&=g\left(hs\right)=g\left(s\right)=s\end{aligned}$$

אם $gs=s$, אז $s=g^{-1}s\underbrace{\left(g^{-1}g\right)}_{1}$.

3.7 מסקנה

$$|O_S| = |{}^G/_{G_s}| = [G : G_s]$$
$$[G : G_s] \mid |G|$$

ולכן, לכל $s \in S$, $|O_s| \mid |G|$ - $|G| = |O_s| \cdot |G_s|$.

3.2.1 תזכורת

אם $H \le G$, אז $G = \bigcup_{a \in G} aH$ (בלי קשר לאם H נורמלית או לא). סימנו את מספר מחלקות השקילות ב־$[G : H]$.
יש העתקה חח"ע ועל בין מחלקת שקילות אחת לשניה, ולכן כל מחלקות השקילות הן באותו גודל, אז $G = [G : H] \cdot |aH|$.

3.2.2 דוגמה שדיקלה תאהב

יש לנו דודקהדרון (עם 12 פאות). מהו אוסף כל הסיבובים שמחזיר את הפאה בדיוק לעצמה. יש 5 סיבובים אפשריים. אז גודל המייצב הוא 5 (כולל הזהות). כל פאה יכולה להגיע לכל פאה אחרת, אז גודל המסלול הוא 12, וגודל החבורה הוא 60.

המיצב של קודקוד הוא מגודל 3, יש 20 קודקודים, ולכן שוב־ הגענו ל־20 חבורות סיבוב.

ולהפיך - המייצב של צלע הוא 2, וסדר החבורה הוא 60, ולכן יש 30 צלעות.

3.8 הערה $|S| = \sum_{\substack{s \in S \\ O_s \neq O_{s'}}} |O_s|$

במקרה של הדודקהידרון - נתבונן בפעולה של המייצב של מספר 1 (G_1, תת חבורה) . (שגודלו 5) על S - אוסף הפאות.

$$|S| = 12 = 1_{O_1} + 1_{O_{12}} + 5_{O_3} + 5_{O_2} = 12$$

אם נתבונן בפעולת כל הסיבובים על S - הפאות, המשוואה שתתקבל היא $12 = |S| = 12$ כי G פועלת <u>טרנזיטיבית</u> על S

3.9 הגדרה פעולה טרנזטיבית - לכל $s, s' \in S$ יש $g \in G$ כך ש־$gs = s'$ או לחילופין - ל־G יש רק מסלול 1 .

גדלי כל המסלולים צריכים לחלק את גודל המייצב, ולכן המסלולים האפשריים כאן הם מגודל 5 או 1 .

3.10 הערה אם לאיזה $s \in S$, $|O_s| = 1$ אז $gs = s$ לכל $g \in G$ כי $s \in O_s$ (כי $1 \in G$, $1s = s$)
אם $|O_s| =$ אז רק $s \in O_s$, כלומר $gs = s$ לכ ל $g \in G$.

להשלים - 13.1

S קבוצה, G פועלת על S. את הפעולה של G משרה ההומומורפיזם

$$\varphi : G \to \mathrm{Perm}\,(s)$$

כאשר Perm הם ההעתקות החח"ע ועל $S \to S$.
אם φ היא חח"ע אומרי שהפעולה של G על S <u>נאמנה</u>.
דוגמה: $\mathbb{Z}_2$, נתבונן בחבורה $G = GL_2(\mathbb{Z}_2)$. ($\mathbb{Z}_2 = \mathbb{F}_2$)
טענה: $G \cong S_3$. אם נמצא קבוצה $|S| = 3$ ש־G פועלת עליה, אז נקבל הומומורפיזם $\varphi : G \to S_3$.
תזכורת: חישבנו את גודל החבורה $|G| = 6$ -
אם נמצא קבוצה S כזו - שהפעולה של G עליה נאמנה, אז סיימנו - כי אז φ חח"ע (ומשיקולי ממימדים - גם על)
G פועלת על וקטורי עמודה מעל $\mathbb{F}_2$. $\tilde{S} = \left\{ \begin{pmatrix} a \\ b \end{pmatrix} : a, b \in \mathbb{Z}_2 \right\}$, כאשר $\left|\tilde{S}\right| = 4$.

אבל G גם פועלת על $S = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$. כדי לראות אם זו העתקה נאמנה (חח"ע), יש לבחון האם קיימת מטריצה המשאירה את כל האיברים במקום (מלבד מטריצת הזהות) - ואין כזו. ולכן סיימנו.
תרגיל (מודרך): - להראות ש־$S_3 \cong \mathrm{Aut} S_3$.

3.3 פעולה של חבורה על עצמה

במקרה זה, $S=G$ ו־G פועלת על G. אנחנו נתעניין בשתי פעולות של G על G.

•

$$\begin{aligned} G\times G&\to G\\ (g,h)&\mapsto gh \end{aligned}$$

G פועלת על עצמה על ידי כפל משמאל. נקבל הומומורפיזם $\varphi:G\to \mathrm{Perm}(G)$. אם $|G|=n$, נקבל הומומורפיזם $\varphi:G\to S_n$.

– פעולת G היא נאמנה. אם $\varphi(g)=m_g=1$, אז $gh=h$ לכל $h\in G$, אז $g=1_G$. (m_g ־ פרמוטצית הזהות)

מסקנה 3.11 (משפט קיילי)

כל חבורה סופית G איזומורפית לתת חבורה של S_n לאיזה $n\in\mathbb{N}$.

הוכחה: אם $|G|\in n$, אז $\varphi:G\to S_n$ הצגת פרמוטציה עבור פעולת G על עצמה משמאל ־ היא חח"ע ועל התמונה שלה. כלומר, $G\cong \mathrm{Im}\varphi$, אבל $\mathrm{Im}\varphi\le S_n$ ■

• G פועלת על עצמה על ידי הצמדה

$$\begin{aligned} G\times G&\to G\\ (g,h)&\mapsto ghg^{-1}=m_g(h) \end{aligned}$$

– המייצב של נקודה $x\in G$, $Z(x)$ (הממרכז של x) הוא אוסף כל האיברים

$$G\ge Z\left(x\right)=\left\{\, g\in G \;\middle|\; x=gxg^{-1} \,\right\}=\{g\in g|xg=gx\}$$

* אם החבורה היא אבלית ־ $Z(x)=G$ לכל $x\in G$.
* אם $x\in Z(G)$, אז $Z(x)=G$
* המסלול של $x\in G$ ־

$$C_x=\left\{h\in G|h=gxg^{-1}\right\}$$

והוא מכונה מחלקת הצמידות של x.

* אם $x\in Z(G)$, אז $C_X=\{x\}$ ובפרט, $|C_x|=1$ ולהיפך ־ אם $|C_x|=1$ אז $C_x=\{x\}$ ולכן $x=gxg^{-1}$ לכל $g\in G$, ולכן ־ $x\in Z(G)$.

$$|G|=|Z(x)|\,|C_x|$$

זה תמיד נכון, בגלל ההתאמה שמתקבלת בין המסלול לבין G "מוד" המייצב.
אם G פועלת על S, אז S היא איחוד של מסלולים של G כאשר שני מסלולים הם או זהים ־ או שחיתוכם ריק.
במקרה שלנו ־ $S=G$, אז $G=\bigcup C_x$, ולכן מתקבלת

3.4 משוואת המחלקה

$$|G| = \sum |C_x|$$

כאשר C_x מחלקות צמידות זרות.
נשים לב ש־$|C_{1_G}| = 1$.

טענה 3.12 אם G חבורת־p, כלומר ־ $|G| = p^k$, עבור איזה ראשוני וטבעי k אז המרכז ל G לא טריויאלי.

הוכחה: נשתמש במשוואת המחלקה ־
נקבל,

$$\begin{aligned} p^k = |G| &= \sum_{C_x} |C_x| \\ &= 1 + \sum_{C_x \setminus C_1} |C_x| \end{aligned}$$

(כאשר הסכימה היא רק על מחלקות צמידות זרות)
אבל, לכל $G \ni x \neq 1_g$, $|C_x| \, | \, |G|$ ולכן, $|C_x| = p^j$ לאיזה $0 \leq j < k$. כלומר ־ כל המספרים המופיעים בסכום הם חזקות של p.
אסם לכל x, $|C_x| = p^j$ עבור $j > 0$, אז $p^k = 1 + (c \cdot p)$ (עבור c שלם כלשהו)
וזה לא יתכן. לכן, קיים $x \neq 1_g$ עבורו $|C_x| = 1$. כלומר ־ $x \in Z(G)$. ■

3.4.1 דוגמאות

- נסתכל על $D_{2 \cdot 3}$ ־ טרנספורמציות צפידות של משולש.

$$D_6 = \left\{1, x, x,^2, y, xy, x^2 y\right\}$$

מחלקות הצמידות ־

$$\{1\}, \left\{x, x^2\right\}, \left\{y, xy, x^2 y\right\}$$

אזי לפי משוואת המחלקה ־

$$6 = 1 + 2 + 3$$

- נחשב את משוואת המחלקה של חבורת הסיבובים של הדודקהדרון. (יודעים שהיא מסדר 60)
  - לכל קודקוד ־ המייצב הוא חבורה מסדר 3, יש ל־G לפחות 10 תתי חבורות מסדר 3. החיתוך בין שתי תתי חבורות הוא טריוויאלי ־ כלומר, $\{1_G\}$ (כי חיתוך הוא תת חבורה של כל אחת מהם, כלומר תת חבורה של חבורה מסדר 3, ואז הוא מסדר 3 או טריוויאלי) לכן, יש לפחות 20 איברים מסדר 3
  - מאותו שיקול ־ יש $4 \cdot 6 = 24$ איברים מסדר 5 (יש 6 חבורות מסדר 5 ־ המייצבים של פאות, עם חיתוך טריוויאלי)
  - יש 15 איברים מסדר 2 ,(יש 15 חבורות מסדר 2, חבורה לכל זוג צלעות נגדיות)
  - יש 60 איברים ־ 20 מסדר 3, 24 מסדר 5, 15 מסדר 2 ו־ 1 מסדר 1.
  - משוואת המחלקה

$$\boxed{60 = \underbrace{1}_{C_{1_g}} + \ldots}$$

כל תתי החבורות מסדר 2 הן צמודות. כלומר, H ו־K צמודות אם קיים $g \in G$

$$gHg^{-1} = K$$

* [תזכורת: אם s, s' נמצאות באותו מסלול, כלומר - $s' = as$, אז

$$G_{s'} = a^{-1} G_s a$$

(אולי $aG_s a^{-1}$)]

כי כל הצלעות הן במסלול של G הפועלות על צלעות הדודקהדרון. לכן, כל האיברים מסדר 2 - צמודים.

$$\boxed{60 = 1 + 15 + \ldots}$$

- באותו אופן, כל תתי החבורות מסדר 3 צמודות, וגם, כל התתי־חבורות מסדר 5 צמודות, אך, זהירות! אי אפשר להסיק מכך שכל האיברים מסדר 3 צמודים, וכל האיברים מסדר 5 צמודים. זה אפילו לא נכון.
- **תרגיל**: להדפיס דודהידרון - ולבנות אותו. לבדוק שיש שתי מחלקות צמידות של איברים מסדר 5, ואחת של איברים מסדר 3.

$$\boxed{60 = 1 + 15 + 20 + 12 + 12}$$

(מלכתכילה, יכולנו לדעת שלא יכולה היתה להיות מחלקת צמידות גגודל 24, כי 24 לא מחלק את 6)

למה 3.13 אם N תת חבורה נורמלית של G, ו־$x \in N$, אז $C_x \subseteq N$.

הוכחה: (אם $g \in G$, ו־$x \in N$ אז $gxg^{-1} \in N$ מהנורמליות של N. ■

מסקנה 3.14 G, חבורת הסיבובים של הדודקהדרון היא פשוטה. - אין לה תת חבורות נורמליות לא טריוויאליות.

הוכחה: אם $N \triangleleft G$ ולא טריוויאלית, אז $1 \neq |N| \neq |G|$ ו־$|N|\,|\,|G|$. מהלמה, ומשוואת המחלקה - ומכך ש־$1_G \in N$, נקבל שלא יתכן שהסדר של N הוא סכום חלקי של המספרים 1,15,20,12,12, שמכיל את 1.

■

חזרה נסמן ב־G את חבורת הסיבובים של הדודקהדרון, אז הראנו (עד כדי תרגיל) של־G פשוטה. כלומר, ל־G אין תתי חבורות נורמליות לא טריוויאליות.

טענה 3.15 $G \cong A_5$ - A_5- פרמוטציות זוגיות ב־S_5

נבחר צלע, ונסתכל על הצלע הנגדים ועל קודקודיה. אז G פועלת על חמש התיבות בתוך הדודקהדרון, ולכן מקבלים הומומורפיזם $\varphi : G \to S_5$. φ היא חח"ע כי G פשוטה. G איזומורפית לתמונה שלה ב־S_5.
נסמן את תמונת G ב־$\varphi(G)$. נתבונן בהומומורפיזם $\mathrm{sign}|_{\varphi(G)} : \varphi(G) \to \{\pm 1\}$.
הגרעין הוא תת חבורה נורמלית של $\varphi(G)$, לכן הגרעין הוא או כל $\varphi(G)$, או 1, כי $\varphi(G)$ פשוטה.
מצד שני, $|\ker\varphi|\,|30$. לכן $\ker\left(\mathrm{sign}|_{\varphi(G)}\right) = \varphi(G)$.
כלומר, $\mathrm{sign}\varphi(g) = 1$ לכל g, ולכן כל התמורות ב־$\varphi(G)$ הן זוגיות.
למה $|A_5| = 60$? $\mathrm{sign} S_5 \to \{\pm 1\}$. $|S_5| = 120$, $|\mathrm{Imsign}| = 2$ ולכן $60 = \frac{120}{2} = |\ker \mathrm{sign}| = |A_5|$

3.5 פעולה על תתי קבוצות

אם G פועלת על S , אז G פועלת על אוסף כל תתי הקבוצות של S - $U \subseteq S$, אז

$$gU = \{gu | u \in U\}$$

מכיוון שפעולת $g \in G$ היא פרמוטציה על S (כל איבר ספציפי פועל באופן חח"ע ועל) אז g פועלת על תתי הקבוצות של S מגודל קבוע.
(g תעביר תת קבוצה מגודל 2 לתת קבוצה מגודל 2, וכו')

המייצב של תת תקבוצה U מוגדר להיות $\{g \in G : gU = U\}$.

דוגמה

- נתבונן ב־D_8 ־ סמטריות של ריבוע ־ $\frac{1}{3}\square\frac{2}{4}$. נתבונן בפעולת D_8 על אוסף הזוגות של S־

  $$\{1,2\}\,,\{1,3\}\,,\{1,4\}\,,\{2,3\}\,,\{2,3\}\,,\{3,4\}$$

  מה המסלולים של פעות D_8 על הזוגות?

  המסלול של $\{1,2\}$ ־ $\{\{1,2\}\,,\{1,3\}\,,\{3,4\}\,,\{2,4\}\}$

  המסלול של $\{2,3\}$ הוא מה שנשאר ־ $\{\{2,3\}\,,\{1,4\}\}$.

טענה 3.16 תהא G חבורה הפועלת על קבוצה S, ותהא G תת קבוצה של S, אז G מייצבת את U $\iff$ U היא איחוד של מסלולים של G בפעולתה על S.

- S קודקודי המתומן ־ ◯ . $H = \{1, \text{reflaction respsect to axis 1-s}\}$.

  $$\{1,2,3,4,6,8\} = \bigcup = \{2,8\} \cup \{6,4\} \cup \{1\}$$

זה יעניין אותנו במקרה ש־U היא גם תת חבורה.

טענה 3.17 תהא G חבורה ונתבונן בפעולת G על עצמה על ידי כפל משמאל. תהא U תת חבורה של G, אז הסדר של המייצב של U מחלק את סדר הסדר של U.

הוכחה: נסמן את H להיות המייצב של U. אז מהטענה הקודמת, U היא איחוד של מסלולים של H בפעולתה על G. מסלול של H בפעולתה על G הוא מהצורה Hg. כלומר, זה קו־סט ימני של H. לכן, כל המסלולים הנ"ל הם מאותו גודל, ולכן הסדר של $|H|\,|\,|U|$ ■

מסקנה 3.18 אם $(|U|\,,|G|) = 1$, ו־H המייצב של U, אז $|H| = \{1\}$, כי $|H|\,|\,|U|$ וגם $|H|\,|\,|G|$.