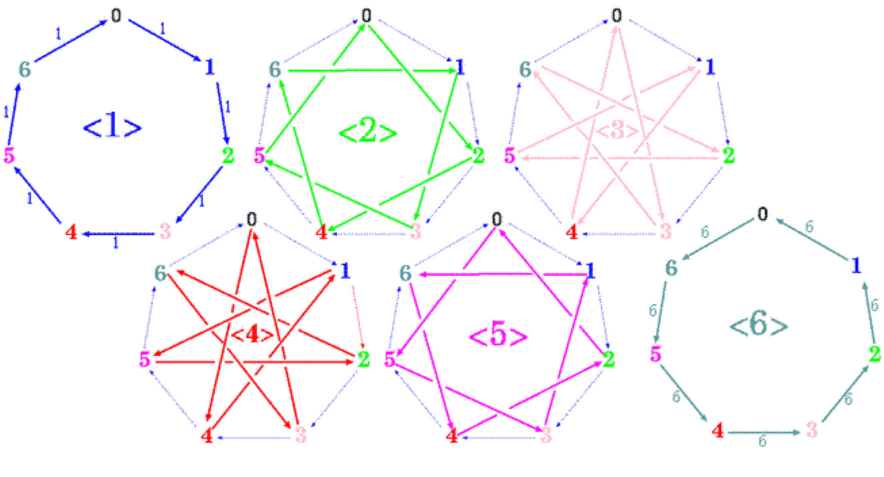
ב"ה

אלגברה מופשטת 1

הקליד וערך: בנימין לוין
מההרצאות של ד"ר רוני ביתן
קיץ תשע"ג

מספר קורס 88-211



כל הזכויות שמורות לבנימין לוין ©

הקדמה ותודות

תודות

תודה לד"ר רוני ביתן על שעבר על כל ההרצאות ושיפר ותיקן אותם.

תודה לדביר חדד, לניר שוורץ ולרועי גוטליב על שהשלימו לי הרצאות כשהחסרתי, ועל כתיבת רוב התרגולים המופיעים בסוף החוברת.

תודה למתרגלת לואי פולב על ההגהות ברוב תרגולים.

הערות

למרות ההגהות הרבות שנעשו, יתכנו טעויות קטנות, אשמח לקבל מייל לגבי הערות ותיקונים levbinyamin@gmail.com.

יש פה סיכומים שלא נעשו על ידי, ולכן קיימים פה ושם שינויים בעיצוב הטקסט, בנוסף התחלתי הסמסטר לכתוב סיכומים במחשב ולכן תוך כדי כתיבה שיניתי קצת את הסגנון.

תודה רבה לכולם.

כל הזכויות שמורות לבנימין לוין ©

הרצאה 1

Rony.bitan@gmail.com

90% מבחן +10% בוחן

מבנים אלגבריים עם פעולה אחת

הגדרה: מערכת אלגברית עם פעולה בינרית אחת היא הזוג $(S,*)$ כאשר S היא קבוצת איברים לא ריקה ו-* היא פעולה בינרית המוגדרת על איברי S. * שומר על סגירות בS

הגדרה: שתי מערכות אלגבריותS,T, עם פעולה אחת * תקראנה שקולות (איזומורפיות) אם קיימת פונקציה חח"ע ועל $f: S \to T$ המשמרת את הפעולה של S, כלומר

$$\forall a, b \in S : f(a * b) = f(a) * f(b)$$

הגדרה: מערכת אלגברית (S,*) תקרא אגודה או חבורה למחצה אם היא מקיימת את החוק האסוציאטיבי (הקיבוץ) אם:
$\forall a, b, c \in S: a * (b * c) = (a * b) * c$

הערה: באגודה מותר להשתמש בחוקי חזקות.

הגדרה: במערכת (S,*) איבר b יקרא נטרלי מימין אם מתקיים $\forall a \in S: a * b = a$

במערכת (S,*) איבר b יקרא נטרלי משמאל אם מתקיים $\forall a \in S: b * a = a$

אבר נטרלי מימין ומשמאל יקרא נטרלי, במקרה זה נסמנו e.

טענה: אם קיים איבר נטרלי מימין b וגם קיים נטרלי משמאל a אזי a=b.

מסקנה: אם קיים איבר נטרלי אזי הוא יחיד.

הגדרה: אגודה עם איבר ניטרלי תיקרא מונואיד.

במונואיד (S,*) איבר a יקרא:

הפיך מימין-אם קיים אבר b כך ש a*b=e

הפיך משמאל-אם קיים אבר b כל ש b*a=e

הפיך: אם קיים אבר b כך ש a*b=b*a=e. אזי נסמן $a = b^{-1}$

טענה: אם לאיבר a במונואיד קיים הופכי מימין b ומשמאל c אזי הם שווים

הוכחה: $c = c * e = c * (a * b) = (c * a) * b = e * b = b$

כל הזכויות שמורות לבנימין לוין ©

הגדרה: א)מונואיד שכל אבריו הפיכים נקרא חבורה group.

ב)נאמר שחבורה (s,*) היא קומוטטיבית או אבלית אם $\forall a,b \in S : a*b=b*a$

ג)חבורה ציקלית היא חבורה שנוצרת מאבר אחד בה

$$\exists g \in G: < g > := \{g^i : i \in Z\}$$

טענה: כל חבורה ציקלית היא בהכרח אבלית

הוכחה: $\forall a,b \in S : a = g^{i\in Z}, b = g^{j\in Z}$

$$a*b = g^i * g^j = g^{i+j} \underbrace{=}_{\text{חוקי חזקות באגודה}} g^j g^i = b*a$$

דוגמאות: 1)קבוצת שורשי היחידה $x^n = 1$ מעל C היא $\Omega_n = \{cis\left(\frac{2\pi k}{n}\right): k = 1,..,n-1\}$

$$\left[cis\left(\frac{2\pi}{n}\right)\right]^k = cis\left(\frac{2\pi k}{n}\right)$$
$$cis\theta_1 * cis\theta_2 = cis(\theta_1 + \theta_2)$$

לכן נסמן $W_n = cis\left(\frac{2\pi}{n}\right)$

$$\Omega_n = < W_n > = \{1, W_n, W_n^2 \dots, w_n^{n-1}\}$$

2) $R^* = R - \{0\}, Q^* = Q - \{0\}$ לגבי כפל הם חבורות אבליות אינסופיות אך אינם ציקליות.

3) $M_n(R)$ לגבי חיבור-חבורה אבלית לא צקלית.

4) $GL_n(R)$ לגבי כפל מטריצות- חבורה לא אבלית.

<u>סימון:</u> עבור מונואיד (M,*) נסמן ב Gr(M,*) את קבוצת כל ההפיכים במונואיד

<u>טענה: Gr(M,*)</u> היא חבורה.

<u>הוכחה:</u> 1)תכונת האסוציאטיביות היא תורשתית מהמונואיד.

2)קיום איבר נטרלי: $e*e=e \to e \in Gr(M,*)$

3) סגירות: $\forall a,b \in Gr(M,*) : (ab)^{-1} = b^{-1}a^{-1} \in Gr(M,*)$

קיום ההופכי: $a \in Gr \to \exists a^{-1} \in M : aa^{-1} = e \to a^{-1} \in Gr$

4) כל האיברים הפיכים : ע"פ הגדרה.

כל הזכויות שמורות לבנימין לוין ©

תת חבורה:

הגדרה: תהא (G,*) חבורה, תת קבוצה $H \subseteq G$ נקראת תת-חבורה ונסמן $H \leq G$, אם H היא חבורה, כלומר אם 1) $e \in H$
2) סגירות 3) $\forall a \in H : a^{-1} \in H$

דוגמאות: 1) $(Z,+)$: $\forall n \in Z : nZ =< n > \leq Z$

$$< 3 >= 3Z = \{0, \pm 3, \pm 6, \dots\}$$

2) $SL_n(R) = \{A \in M_n(R) : |A| = 1\} \leq GL_n(R)$

חבורות קונגרואנציה

הגדרה: עבור $n \in N$ נגדיר את היחס הבא על Z :

$$\forall x, y \in Z : x \overset{mod\, n}{\approx} y \Leftrightarrow x = y \bmod n \Leftrightarrow \exists k \in Z : x - y = k * n$$

למשל $2 = 5 mod 3 = 8 mod 3$

כלומר כל Z מתחלקת לקבוצות זרות = שאריות מודולו n
מסמנים כל מחלקה עם שארית k ע"י $\bar{k}$.

הגדרה: המבנה $Z_n = \{0,1, \dots, n-1\}$ הוא חבורה ונקראת חבורת קונגרואציה, או חבורת השאריות מודולו n.

כל הזכויות שמורות לבנימין לוין ©

הרצאה 2- תכונת הצמצום ומחלקי אפס בחוג

הגדרה: א)במונואיד (s,*) אנו נאמר כי $a \in S$ הוא ניתן לצמצום מימין אם

$$\forall b,c \in S : b*a = c*a \to b = c$$

במונואיד (s,*) אנו נאמר כי $a \in S$ הוא ניתן לצמצום משמאל אם

$$\forall b,c \in S : a*b = a*c \to b = c$$

נאמר שהוא ניתן לצמצום אם הוא ניתן לצמצום מימין וממשמאל.

טענה: במונואיד (M,*) אם $a \in M$ הפיך מכיוון מסוים אז הוא ניתן לצמצום מכיוון זה

הוכחה: נראה רק עבור צמצום מימין

$$ba = ca \to baa^{-1} = caa^{-1} \to b = c$$

הכיוון השני לא נכון, למשל ב(Z,*) חוץ מ-0 כל האיברים ניתנים לצמצום אבל רק 1,-1 הפיכים.

עוד דוגמא: במונואיד $(Z_6, * \; mod6)$ איברים שאינם ניתנים לצמצום: 0,2,3,4 לדוגמא 2*0=2*3 אבל 0 שונה מ-3.

משפט: יהא S מונואיד סופי ויהא $a \in S$ וניתן לצמצום מימין (או משמאל) אזי a הפיך.

הוכחה: כיוון שS סופי אם נכפיל את a בעצמו מספיק פעמים נחזור על איבר שכבר היינו בו, כלומר

$$\exists i < \infty, k : 1 \le k \le i : a^k = a^i$$

כעת נצמצם את a מימין k פעמים ונקבל $a^{i-k} = e \to a^{-1} = a^{i-k-1} \in S$

הגדרה: יהא (R,*) מונואיד בו מוגדרת גם פעולת + (לאו החיבור הרגיל) אזי המבנה (R,*,+) נקרא חוג Ring אם:

1)מתקיים חוק הפילוג $a(b+c) = ab + ac$

$$(b+c)a = ba + ca$$

2) (R,+) חבורה אבלית.

דוגמאות לחוגים: (Z,*,+) חוג לגבי הכפל רק מונואיד.

$(M_n,*,+)$ חוג,לגבי הכפל רק מונואיד.

$\{f: R \to R\},*,+$ כפל וחיבור רגילים.

כל הזכויות שמורות לבנימין לוין ©

הגדרה: אבר בחוג $0 \neq a \in (R,*,+)$ יקרא:

מחלק אפס ימיני: אם $\exists 0 \neq b \in R : b * a = 0$

מחלק אפס שמאלי: אם $\exists 0 \neq b \in R : ab = 0$

מחלק אפס: אם הוא מ"א (מחלק אפס) ימני ושמאלי.
דוגמא: 1) $(Z_6,* \, mod6, +mod6)$ 0=3*2 ולכן 2,3 מחלקי אפס.

משפט: בחוג R איבר a ניתן לצמצום אם"ם הוא אינו מחלק אפס משמאל (וכן לימין)

הוכחה: בכיוון ראשון: יהה $a \in R$ ניתן לצמצום, ונניח בשלילה שהוא מחלק אפס משמאל, אזי
$\exists 0 \neq b \in R : ab = 0 = a * 0 => b = 0$ סתירה

בכיוון ההפוך: נניח $a \in R$ אינו מחלק אפס משמאל, אזי בהינתן ab=ac עבור $b, c \in R$

R חבורה אבלית לגבי + ולכן הפרש מוגדר היטב.

$$ab - ac = 0 \rightarrow a(b-c) = 0 \underbrace{\rightarrow}_{\text{משמאל אפס מחלק אינו } a} b - c = 0 \rightarrow b = c$$

כלומר a ניתן לצמצום משמאל.

מסקנה: בחוג סופי כל איבר הוא או הפיך (לגבי כפל) או מחלק אפס.
דוגמא: $(Z_n,*,+)$ כל איבר או הפיך או מחלק אפס (חוץ מ-0).

הגדרה: איבר באגודה X ניקרא אידמפוטנט אם הוא מקיים $a^2 = a$.
טענה: במונואיד (ק"ו חבורה) עם תכונת הצמצום האדמפוטנט היחיד הוא האיבר הנטרלי e.

הוכחה: $a^2 = a = ae \rightarrow a = e$

לעומת זאת במונואיד $(Z_n,* \, mod \, n)$ יש שתי אידמפוטנטים, 0,1.

במונואיד $(M_2(R),*)$ מעבר לאפס ולאחד יש עוד אידמפוטנטים $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$

טענה: אם x איד' אז גם 1-x איד' (בחוג).הוכחה: $(1-x)^2 = 1 - 2x + x^2 = 1 - 2x + x = 1 - x$

משפט: באגודה X סופית יש לפחות אדמ' אחד.

הוכחה: כיוון ש-X סופית קיימת לה $K \leq X$ תת-אגודה מינימלית (כך ש: $\emptyset \neq K_1 \leq K \rightarrow K_1 = K$

יהא $a \in K$ אזי $aK = \{ak : k \in K\} \leq K$ אבל K מינימלית ולכן aK=K.

מכאן שהקבוצה $A = \{k \in K, ak = a\}$ אינה ריקה.

נשים לב כי $A \leq k$, נראה סגירות:

כל הזכויות שמורות לבנימין לוין ©

$$k_1, k_2 \in A : ak_1 = a, ak_2 = a \to ak_1k_2 = ak_2 = a \to k_1 * k_2 \in K$$

שוב מתוך המינימליות נסיק כי A=K, מכאן שיש לפחות אדמ' אחד.

אם X היה אינסופי, לא בהכרח היתה תת-אגודה מינמלית, למשל X=2Z-{0}. $nZ - \{0\} \leq x$ אך אין בו שום אדמ'.

מבוא לתורת המספרים

הגדרות וסימונים בסיסיים:

1) עבור $a, b \in Z$ נסמן a|b אם a את b, כלומר $\exists q \in Z : aq = b$ לדוגמא 3|6,2|6
2) מספר טבעי p>1 נקרא ראשוני אם המחלקים היחידים שלו הם $\pm 1, \pm p$

<u>המשפט היסודי של הארתמיטקה:</u>
כל מספר טבעי ניתן לייצוג יחיד עד כדי חילוף סדר הגורמים $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

<u>הגדרה:</u> 1) מחלק משותף גדול ביותר (ממג"ב) של שתי מספרים שלמים a,b הוא המספר הגדול ביותר שמחלק את שתיהם. סימון: $\gcd(a, b) = (a, b) = d$

2) כפולה משותפת קטנה ביותר (כמק"ב) של שתי מספרים שלמים a,b הוא המספר הטבעי הקטן ביותר ששתיהם מחלקים אותו. סימון lcm(a,b)=[a,b]
לדוגמא 24=[8,12]

<u>טענה:</u> לכל $a, b \in Z$ מתקיים $(a, b) * [a, b] = |ab|$

<u>הוכחה:</u> $|a| = \prod_{i=1}^{\infty} p_i^{\alpha_i}$

$$|b| = \prod_{i=1}^{\infty} p_i^{\beta_i}$$

$$(a, b) = \prod_{i=1}^{\infty} p_i^{\min\{\alpha_i, \beta_i\}}$$

$$[a, b] = \prod_{i=1}^{\infty} p_i^{\max\{\alpha_i, \beta_i\}}$$

$$(a, b) * [a, b] = \prod_{i=1}^{\infty} p_i^{\alpha_i + \beta_i} = |ab|$$

כל הזכויות שמורות לבנימין לוין ©

הגדרה: חילוק עם שארית: לכל $b, a \in Z \neq 0$ קיימים באופן יחיד $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$

משפט: $(a, b) = d \rightarrow \exists k_1, k_2 \in Z : k_1 a + k_2 b = d$

הוכחה: אלגוריתם אוקלידס למציאת ממב"ג

יהיו $a, b \in Z$

נחשב: $a = bq_1 + r_1$

$$b = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

$$\dots\dots\dots$$

$$r_{k-2} = r_{k-1} q_k + \overbrace{r_k}^{gcd}$$

$$r_{k-1} = r_k q_{k+1}$$

נשים לב כי השאריות r_k הולכות וקטנות, כיוון שהם אי-שליליות התהליך חייב להסתיים, מתוך המשוואה האחרונה נסיק כי $r_k | r_{k-1}$, לכן יחד עם המשוואה הלפני אחרונה נקבל $r_k | r_{k-2}$ נמשיך כך ונקבל ש $r_k | r_1, r_k | r_2$ ולכן גם את b ומכאן ע"פ המשוואה הראשונה גם $r_k | a$.

כעת נותר להראות מקסימליות של r_k כמחלק של a,b

נניח באופן כללי $t | a, t | b$ נרצה להראות $t \leq r_k$

$$t | \overbrace{(a - bq_1)}^{r_1}$$

$$t | \overbrace{(b - r_1 q_2)}^{r_2}$$

$$\dots\dots\dots$$

$$\dots\dots t | r_k \rightarrow t \leq r_k$$

אם כן, נוכל לייצג כל שארית ע"י שאריות קודמות יותר וכך להגיע בסופו של דבר לקומבנציה לינארית של a,b באמצעות מספרים שלמים, שתהיה שווה ל(a,b).

דוגמא: $(594,420) = 6$

$$594 = 420 * 1 + 174$$

$$420 = 174 * 2 + 72$$

$$174 = 72 * 2 + 30$$

$$72 = 30 * 2 + 12$$

$$30 = 12 * 2 + \mathbf{6}$$

$$12 = 6 * 2$$

החבורה הסמטרית

בהינתן קבוצת איברים סופית X, נמספר אותם $X = \{1, \dots, n\}$. כל תמורה (פרמוטציה) של אברי X היא פונקציה חח"ע ועל ולכן הפיכה. $\varphi: X \rightarrow X$

כל הזכויות שמורות לבנימין לוין ©

הרצאה 3

חבורת אוילר (Euler)

הגדרה

שני מספרים שלמים a,b יקראו <u>זרים</u> $\Leftrightarrow (a,b)=1$.

משפט

$$(m,n)=1 \Leftrightarrow \ \exists k_1,k_2 \in \mathbb{Z} : k_1m+k_2n=1$$

הוכחה

הכיוון ⇒ נובע ממשפט כללי יותר שהוכחנו

בכיוון ⇐נניח

$$\exists k_1,k_2 \in \mathbb{Z} : k_1m+k_2n=1$$

ונניח $(m,n)=d$

אזי

$$d|m \wedge d|n \Rightarrow d|(k_1m+k_2n) \Rightarrow d|1 \Rightarrow d=1$$

טענה

כל שתי מספרים טבעיים עוקבים זרים זה לזה

הוכחה

$$1(n+1)-1n=1 \Rightarrow (n+1,n)=1$$

מסקנה

יש אינסוף מספרים ראשוניים

נניח בשלילה כי קבוצת המספרים הראשוניים סופית.

נסמן את מכפלת כל הראשוניים האלו ב-n. לפי הטענה הנ"ל,n+1 זר ל-n כלומר אין להם מחלקים משותפים גדולים מ-1 לפיכך בפירוק של n+1 לגורמים ראשוניים בהכרח יופיעו מספרים ראשוניים אחרים מהרשימה הנ"ל, סתירה.

טענה

איבר $m \in \mathbb{Z}_n$ הוא הפיך לגבי כפל מודולו $\Leftrightarrow$ (m,n)=1

הוכחה

$$(m,n)=1 \Leftrightarrow \exists k_1,k_2 \in \mathbb{Z} : k_1m+k_2n=1 \Leftrightarrow \exists k_1 \in \mathbb{Z}\ k_1m=1 mod\ n$$

הגדרה

חבורת אוילר היא קבוצת ההפיכים ב-$\mathbb{Z}_n$ לגבי כפל מודולו n

$$U_n \coloneqq Gr(\mathbb{Z}, *\ mod\ n)$$

דוגמא

$U_{10}=(\{1,3,7,9\},*\ mod10)$ - צקלית כי $<3>=\{1,3,9,7\}$

$U_8=\{1,3,5,7\}$ לא צקלית

כל הזכויות שמורות לבנימין לוין ©

תרגיל

חשב את 90^{-1} ב- $\mathbb{Z}_{143}$

פתרון

ע"פ אלגוריתם אוקלידס כאשר תחילה נראה כי $(143,90) = 1$, נשחזר את המקדמים כך ש:

$$143 * 17 - 90 * 27 = 1$$

ולכן $90^{-1} = -27 mod 143 = 116 mod 143$

טענה

$$\begin{cases} a \equiv b \bmod n \\ c \equiv d \bmod n \end{cases} \Rightarrow \begin{cases} ac \equiv bd \bmod n \\ a + c \equiv (b + d) \bmod n \end{cases}$$

הוכחה

$$\exists k_1 \in \mathbb{Z} : a = k_1 n + b$$
$$\exists k_2 \in \mathbb{Z} : c = k_2 n + d$$

כאשר מכפילים מודולו או מחברים מודולו את a,b כל מכפלה של n מצטמצמת.

תרגיל

פתור את המשווה $3x = 55$ ב$\mathbb{Z}_{2000}$

פתרון

$$3 * 667 = 2001 = 1 mod 2000$$
$$\Rightarrow 3 * \underbrace{677 * 55}_{x} = 55 mod 2000$$

משפט השאריות הסיני CRT

תהא $\{m_1, \dots, m_k\}$ קבוצת מספרים טבעיים הזרים זה לזה.

נסמן את מכפלתם ב-m. בהינתן קבוצה כלשהי של שאריות $\{a_i mod m_1\}$ קיימת שארית יחידה $x \bmod m$

המהווה פתרון למערכת המשוואות $\begin{cases} x = a_1 mod\, m_1 \\ x = a_2 \bmod m_2 \\ \dots\dots \\ x = a_k \bmod m_k \end{cases}$

דוגמא

מצא פתרון למערכת למערכת $\begin{cases} x = 1 mod 4 \\ x = 2 mod 7 \\ x = 3 mod 15 \end{cases}$

הוכחת המשפט

נבנה בסיס של שאריות $\{e_1, \dots, e_k\}$ כך ש

$$\forall i, j : e_i = \delta_{ij} mod\, m_j = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$$

ואז

$$x = a_1 e_1 + \dots + a_k e_k$$

כל הזכויות שמורות לבנימין לוין ©

הבנייה של $\{e_k\}$ תעשה בצורה הבאה:

לכל $1 \le i \le k$ נגזיר $n_i = \frac{m}{m_i}$. כיוון שכל הm_i זרים אחד לשני, נקבל $(n_i, m_i) = 1$, מכאן ש:

$$\exists s_i, r_i \in \mathbb{Z} : s_i n_i + r_i m_i = 1$$

נגדיר $e_i \coloneqq s_i n_i$ ונקבל $e_i = 1 mod\ m_i$

כמו כן לכל $i \neq j$ $m_j | n_i$ ולכן $e_i = 0 mod\ m_j$, כדרוש,נניח כי קיים פתרון אחר y

אז מתוך מערכת המשוואות נקבל $\forall i :\ m_i | (x-y)$

אבל כל ה$\{m_i\}$ זרים אחד לשני ולכן $m | (x-y)$ ומכאן $x = y\ mod\ m$

הגדרה

תהיינה H,K חבורות עם איברים נטרליים e_H, e_K

<u>המכפלה הישרה</u> H ו-K היא הקבוצה של הזוגות הסדורים

$$H \times K = \{(h,k) : h \in H, k \in K\}$$

יחד עם הפעולה $(h_1, k_1) * (h_2, k_2) = (h_1 h_2, k_1 k_2)$

$H \times K$ היא חבורה.

דוגמא

$$\mathbb{Z}_2 \times \mathbb{Z}_3 =< (1,1) \ge \{(0,0), (1,1), (0,2), (1,0), (0,1), (1,2)\}$$

הגדרה

העתקה בין מונואידים $\varphi: (G,*) \to (H,*)$ היא הומומורפיזם אם היא משמרת פעולה

$$\forall a, b \in G : \varphi(ab) = \varphi(a)\varphi(b)$$

- אם φ היא חח"ע אז היא נקראת <u>מונומורפיזם.</u>
- אם φ היא על אז היא נקראת <u>אפימורפיזם.</u>
- אם φ היא חח"ע ועל אז היא נקראת <u>אזומורפיזם.</u>

דוגמאות

1. $x \mapsto 2x \quad \varphi: \mathbb{Z} \to \mathbb{Z}$ לגבי חיבור – מונומורפיזם
2. $x \mapsto x^2 \quad \varphi: U_{10} \to < 9 >$ אפימורפיזם

$$\mathrm{Im}(\varphi) = \{1,9\} =< 9 >$$

3.

$$\varphi: (\mathbb{R}, +) \to \big((0,\infty), *\big) \quad x \mapsto 2^x$$

$$\varphi(x+y) = 2^{x+y} = \varphi(x)\varphi(y)$$

$$G \cong H$$

כל הזכויות שמורות לבנימין לוין ©

טענה
אם $f: G \to H$ ההומומורפיזם של חבורות אזי

1) $f: 1_G \to 1_H$
2) אם x הפיך ב-G $f(x^{-1}) = f(x)^{-1}$

הוכחה
1) $f(1_G) = f(1_G 1_G) = f(1_G)f(1_G) \Rightarrow f(1_G) = 1_H$
2) $1_H = f(1_G) = f(xx^{-1}) = f(x)f(x^{-1}) \Rightarrow f(x^{-1}) = f(x)^{-1}$

מסקנה
בהינתן איזומורפיזם של מונואידים G ≅ H נקבל איזומורפיזם של חבורות $Gr(G) \cong Gr(H)$

טענה
אם $(n,m) = 1$ אזי $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ וזהו איזומורפיזם של חוגים (לגבי שתי הפעולות).

דוגמא
$$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$$

הוכחה
נסמן $\varphi: \mathbb{Z}_{nm} \to \mathbb{Z}_n \times \mathbb{Z}_m$ ע"י:

$$\varphi(x) = (x \bmod n, x \bmod m)$$

$$\varphi(x+y) = \big((x+y) \bmod n, (x+y) \bmod m\big) = (x \bmod n, x \bmod m) + (y \bmod n, y \bmod m)$$

וכנ"ל לגבי כפל.

תכונות החח"ע ועל של φ נובעות כעת מהזרות של n,m יחס עם משפט השאריות הסיני, שאומר שלכל 2 שאריות $a_1 \bmod n, a_2 \bmod m$ קיים פתרון x יחיד בתוך $\mathbb{Z}_{nm}$.

הגדרה
לכל מספר טבעי n נגדיר את פונקציית אוילר.

$$\varphi(n) = |U_n|$$

לדוגמא
אם p מספר ראשוני אזי $\varphi(p) = p - 1$

$\varphi(p^k) = ?$ מיהם המספרים $1 \le m \le p^k$ שאינם זרים ל-p?

$$\left|\{p, 2p, \ldots, p^2, 2p^2, \ldots, p^k\}\right| = p^{k-1}$$

$$\varphi(p^k) = p^k - p^{k-1}$$

כל הזכויות שמורות לבנימין לוין ©

טענה
אם $(n,m)=1$ אז $\varphi(nm)=\varphi(n)\varphi(m)$

הוכחה
$$\varphi(nm)=|U_{nm}|=|Gr(\mathbb{Z}_{nm})|=|Gr(\mathbb{Z}_n\times\mathbb{Z}_m)|=|Gr(\mathbb{Z}_n)||Gr(\mathbb{Z}_m)|=\varphi(n)\varphi(m)$$

מסקנה – נוסחה לחישוב פונקציית אוילר
בהינתן פירוק של n $n=\prod_{i=1}^{k}p_i^{\alpha_i}$

$$\varphi(n)=\varphi\left(\prod_{i=1}^{k}p_i^{\alpha_i}\right)=\prod_{i=1}^{k}\varphi(p_i^{\alpha_i})=\prod_{i=1}^{k}p_i^{\alpha_i}-p_i^{\alpha_i-1}=\prod_{i=1}^{k}\left(p_i^{\alpha_i}\left(1-\frac{1}{p_i}\right)\right)=n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

לדוגמא
$$\varphi(160)=\varphi(2^5*5)=160\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=64$$

כל הזכויות שמורות לבנימין לוין ©

הרצאה 4

סדר של איבר ושל חבורה

הגדרה

- סדר של חבורה הוא מס' האיברים בה.
- סדר של איבר g בחבורה הוא $o(g)=\begin{cases}\min\{k\in\mathbb{N}: g^k=0\}\\ \infty \ \ if\ there\ is\ no\ such\ k\end{cases}$

דוגמא

ב$U_{10}=\{1,3,7,9\}$ מתקיים $o(9)=2, o(3)=4$

ב$(\mathbb{Z},+)$ מתקיים $o(1)=\infty$

טענה

בחבורה $a^k=e \Leftrightarrow o(a)|k$

הוכחה

בכיוון ראשון

$$o(a)|k \Rightarrow \exists q\in\mathbb{Z}: k=o(a)*q \Rightarrow a^k=\left(a^{o(a)}\right)^q=e^q=e$$

בכיוון הנגדי

$$a^k=e\Rightarrow o(a)\le k$$

נתייחס לפירוק מקסימלי: $0\le r<o(a), k=o(a)*q+r$

נתון: $e=a^k=\left(a^{o(a)}\right)^q a^r\Rightarrow a^r=e$

אבל בהתאם למינימליות של e של הסדר o(a) ‏r=0, ולכן k=o(a)q

הערה

תמונה הומומורפית של חבורה צקלית היא חבורה צקלית.

$$f: \overset{=<a>}{\tilde{G}} \twoheadrightarrow H\Rightarrow H=<f(a)>$$

הוכחה

$$\forall G\in G:\ \ g=a^i\to f(g)=f(a)^i\Rightarrow Im(f)=H=<f(a)>$$

משפט
$\forall n,m \in \mathbb{Z}:\ (n,m)=1 \Leftrightarrow \mathbb{Z}_n \times \mathbb{Z}_m \cong Z_{nm}$ (עבור חיבור)

הוכחה
⇐ הוכחנו באמצעות CRT.

⇒

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong Z_{nm} =< i > \Rightarrow \exists (a,b) \in \mathbb{Z}_n \times \mathbb{Z}_m : o(a,b) = nm$$
$$\Rightarrow (a,b)^{[n,m]} = ([n,m]a,[n,m]b) = (nq_1a, mg_2b) = (0,0)$$
$$o(a,b) = nm \le [n,m] \Rightarrow nm = [n,m] \Leftrightarrow (n,m) = 1$$

מיון חבורת ציקליות

משפט
תהא $G =< a >$ חבורה צקלית, אזי:

א. אם G אינסופית, אזי $G \cong \mathbb{Z}$
ב. אם G מסדר n, אזי $G \cong \mathbb{Z}_n$

הוכחה
א. נגדיר $f{:}\,\mathbb{Z} \to G : k \mapsto a^k$

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

לכן f הומו' (משמר פעולה).
כיוון שניתן להגיע לכל חזקה שלמה של a, $Im(f) =< a >= G$
כלומר f אפי' (על). בנוסף אם $m \ne n$ אז בהכרח $a^m \ne a^n$ שכן אחרת G היית סופית (חזקות חוזרות על עצמן נכנסים ללולאה סופית) בסתירה לנתון, מכאן f מונו' ובסה"כ איזו'.

ב. שוב נגדיר את ההעתקה $f{:}\,\mathbb{Z}_n \to G : k \mapsto a^k$
שימור פעולה: $\forall k_1,k_2 \in: k_1 \oplus k_2 = k_1 + k_2 - \alpha n$

$$f(k_1 \oplus k_2) = k^{k_1 \oplus k_2} = a^{k_1} a^{k_2} (a^{n\alpha}) = a^{k_1} a^{k_2} = f(k_1)f(k_2)$$

כיוון שכל חזקה $0 \le k \le n-1$ מתאפשרת בתמונה, כלומר כל G נפרשת, כלומר f על, ומתוך כך f הוא מונו' (כי $|\mathbb{Z}_n| = |G| = n$).

דוגמא

$$\mathbb{Z} \cong < 1+i > \le \mathbb{C}$$
$$|1+i| \ne 1$$

חבורה צקלית אינסופית.

באופן כללי, החבורה $G =< z = re^{i\theta} \in \mathbb{C} >$ לגבי כפל סופית אם"ם $\frac{\theta}{\pi} \in \mathbb{Q}$, r=1

$$\frac{\theta}{\pi} \in \mathbb{Q} \Leftrightarrow \theta k \in 2\pi\mathbb{Z} \Leftrightarrow \left(cis(\theta)\right)^k = cis(k\theta) = 1,$$

כל הזכויות שמורות לבנימין לוין ©

מיון תת-חבורות של חבורה צקלית

טענה

צקליות היא תכונה תורשתית, כלומר אם G צקלית אזי כל ת"ח $H \leq G$ צקלית

הוכחה

בהינתן $G =< a >$, צ"ל $\exists k \in \mathbb{N} : H =< a^k >$

אם $H = \{e\}$ אזי $H =< e >$

אחרת נגדיר $k \coloneqq \min\{i \in \mathbb{N} : a^i \in H\}$ ונראה כי $H =< a^k >$

אכן יהא $h = a^t \in H$ ונתייחס לפרוק t=kq+r כאשר $0 \leq r < k$. ע"פ הסגירות נקבל $a^r = a^{t-kq} = a^t\left(a^k\right)^{-q} \in H$
אבל r<k, בסתירה למנמליות, ולכן r=0, ולכן $t = kg$ ולכן $a^t \in< a^k >$

טענה 1

תהא חבורה G ואיבר $a \in G$ כך ש $o(a) = n$, אזי :

$$\forall d \leq n : o\left(a^d\right) = \frac{n}{(d,n)}$$

דוגמא

$$1 \in \mathbb{Z}_6, o\left(1^d\right) = o(d) = \frac{6}{(d,6)}$$

הוכחה

1. התיכונות $\left(a^d\right)^{\frac{n}{(d,n)}} = (a^n)^{\frac{d}{(d,n)}} = e$
2. מינימליות : נניח כי $\left(a^d\right)^t = e$ אזי $a^{dt} = e$. ידוע כי o(a)=n ולכן n|dt מכאן שגם: $\frac{n}{(d,n)} \Big| \frac{dt}{(d,n)}$ אבל $\left(\frac{n}{(d,n)} \Big| \frac{d}{(d,n)}\right)$ ולכן $\frac{n}{(d,n)} \Big| t$ ולכן $t \geq \frac{n}{(d,n)}$

תרגיל נחמד:

תהא $G =< a >$, כמה איברים ב-G יוצרים את כל G (כל אחד בנפרד)?

פתרון

$$\mathrm{G} =< a^k > \Leftrightarrow o\left(a^k\right) = n = \frac{n}{(n,k)} \Leftrightarrow (n,k) = 1$$

לדוגמא $\mathbb{Z}_6 =< 1 >$ ולכן התשובה היא $\varphi(n)$

תרגיל

נניח שU_n חבורה צקלית, כמה איברים יפרשו אותה כל אחד לבד?

$$\varphi(|U_n|) = \varphi\left(\varphi(n)\right)$$

טענה 2:
נניח שבחבורה G מתקיימים עבור $g,h\in G$

1. $gh=hg$
2. $(o(g),o(h))=1$

אזי $o(gh)=o(g)\,o(h)$

הוכחה
נסמן $o(gh)=m, o(g)=n, o(h)=k$

צ"ל m=nk

היתכנות: $(gh)^{nk}=(g^n)^k\left(h^k\right)^n=ee=e$

מינימליות : $g^{mk}=g^{mk}e=g^{mk}h^{mk}=(gh)^{mk}=((gh)^m)^k=e\Rightarrow n|mk$

אבל $(n,k)=1$ ולכן $n|m$ ובאותו אופן $k|m$ ומכאן ש $[n,k]|m$ אבל $[n,k]=nk$ ולכן $m\geq nk$ ולכן

$\mathrm{m=nk}$

טענה
יהיו 2 איברים a,b בחבורה כך ש:

$$o(a)=n, o(b)=m, ab=ba$$

אזי

$$o\left((ab)^{(n,m)}\right)=\frac{[n,m]}{(n,m)}$$

הוכחה
מתוך טענה 1 : $o\left(a^{(n,m)}\right)=\frac{n}{(n,m)}$

$$o\left(b^{(n,m)}\right)=\frac{m}{(n,m)}$$

אבל $\left(\frac{n}{(n,m)},\frac{m}{(n,m)}\right)=1$ ולכן ע"פ טענה 2: $o\left((ab)^{(n,m)}\right)=o\left(a^{(n,m)}b^{(n,m)}\right)=\frac{nm}{(n,m)^2}=\frac{[n,m]}{(n,m)}$

קבוצת יוצרים של חבורה

הגדרה
בהינתן חבורה G, תת קבוצה $A\subset G$ נקראית קבוצת יוצרים של G אם $G=<A>$.
אם A סופית אז נאמר כי G נוצרת סופית.

למשל $\mathbb{Z}^2=<(1,0),(0,1)>$

הערה:
אם G נוצרת סופית אז $|G|\leq\aleph_0$

נחליט על כלשהו של היוצרים, יוצרים אלו הם הא"ב של כל אוסף המילים הסופיות שיכולות להיווצר

כיוון שהא"ב סופי ניתן לסדר את כל המילים לפי סדר לקסיקוגרפי.

כל הזכויות שמורות לבנימין לוין ©

הערה

תיתכן אבל חבורה בת מניה שאינה נוצרת סופית $(\mathbb{Q}^*,*)$

הגדרה

הדרגה של חבורה rank(G) : G היא המס' המינימלי של פורשים יחד את כל G. זהו הגדרה של המרצים בבר אילן, ולא מופיע בספרים וכד' (ואף יש לו משמעות אחרת שנראה בהמשך).

למשל $rank(\mathbb{Z}^n) = n$

חבורה חופשית

כל חבורה ניתנת לכתיבה כקבוצת האיברים היוצרים אותה וקבוצת היחסים ביניהם.

לדוגמא $C_n =< a : a^n = e >$

$$D_n = \{\overbrace{a,b}^{\text{יוצרים}} \mid \overbrace{b^2 = e, a^n = e, ab = b^n a^{n-1}}^{\text{יחסים}}\}$$

הגדרה

יחס טריוויאלי הוא שוויון בין איברי חבורה שנובע מאקסיומות של חבורה, למש $a^3a^4 = a^7, aa^{-1} = e$

הגדרה

קבוצה חופשית (מעל קבוצה X) היא קבוצה הנוצרת ע"י איברי X כך שאין ביניהם שום יחסים לא טריוויאליים.

סימון $G = F(X)$

לדוגמא $G = F(\{a,b\}) = \{a, a^2, ab, ba, bbaba\}$

הגדרה

חבורה אבלית חופשית מעל קבוצה X היא חבורה הנוצרת מאיברי X יחד עם יחס הקומוטטיביות.

מסמנים חבורה אבלית חופשית מעל X היא $G = A(X)$

לדוגמא $G = A(\{a,b\}) \cong \mathbb{Z}^2$

באופן כללי $G = A(X) \cong \mathbb{Z}^{|X|}$

האיזו' מופיע ע"י סידור מסוים של יוצרים, וקיבוץ כל היוצרים בנפרד על שכל מילה מתוארת ע"י

וקטור של חזקות בגודל n.

כל הזכויות שמורות לבנימין לוין ©

הרצאה 5

משפט ווילסון – Wilson

מספר טבעי $n>1$ הוא מספר ראשוני אם"ם $(n-1)!\equiv(-1)(mod\ n)$

הוכחה

<u>בכיוון האחד</u>: עבור $n=p>1$ ראשוני חבורת אוילר היא: $U_p=1,2,...,p-1$. כל איבר $a\in U_p$ ההפוך לעצמו מקיים: $a^2-1=(a-1)(a+1)\equiv 0(\mathrm{mod}\ p)$ כלומר: $a\equiv\pm1(\mathrm{mod}\ p)$. מכאן שלמעט ±1 לכל איבר יש הופכי שהוא אחר ממנו. לכן כיוון שהחבורה אבלית, במכפלת האיברים $m=(p-1)!$ האיבר היחיד שאינו מצטמצם (ע"י סידור כל איבר ליד ההופכי שלו) הוא: $m=p-1\equiv(-1)(\mathrm{mod}\ p)$.

<u>בכיוון ההפוך</u>: נניח בשלילה כי n אינו ראשוני. אם $n=4$ קל לבדוק כי: $(4-1)!=6\equiv 2(\mathrm{mod}\ 4)$. סתירה.

עבור $n>4$: כיוון ש- n אינו ראשוני, ישנו לפחות מספר אחד $1<a\leq n-1$ שמחלק את n.

אם: $a=\sqrt{n}$ אזי: $4<n \Leftarrow 2<a \Leftarrow 2a<a^2=n$ כלומר $a,2a$ מופיעים כ"א במכפלה $(n-1)!$ ומכפלתם מאפסת אותה בסתירה לנתון.

אחרת (a אינו שורש של n) מתקיים: $\exists 0<a\neq b<n: a\cdot b\equiv 0(\mathrm{mod}\ n)$. לכן ab מופיע במכפלה: $(n-1)!$ ושוב מאפס אותה בסתירה לנתון.

תרגיל (מועד א 2007)

הוכח או הפרך:

$71|70!+1$ נכון כי 71 ראשוני ולכן ע"פ משפט ווילסון.

$117|116!+1$ לא נכון כי $117=9*3$ ולכן $117|116!$ $\Rightarrow$ $9*13|116!+1$.

קוסטים ומשפט לגרנז'

הגדרה

תהא חבורה G ות"ח H, שני איברים $x,y\in G$ יקראו קונגרואנטים משמאל מודולו H אם:

$$x\sim^L y \Leftrightarrow \exists h\in H: x=yh$$

(x הוא הזזה של y ע"י איבר מH)

טענה

היחס $x\sim^L y$ הוא יחס שקילות

הוכחה

רפלקסיביות: $x\sim^L x: x=xe$

כל הזכויות שמורות לבנימין לוין ©

סמטריות: $x\sim^L y \Rightarrow x = yh \Rightarrow xh^{-1} = y \Rightarrow y\sim^L x$

טרנזטיביות: $x\sim^L y, y\sim^L z \Rightarrow x = yh_1, y = zh_2 \Rightarrow x = zh_2h_1 = zh_3 \Rightarrow x\sim^L y$

באופן דומה מגדירים גם את $x\sim^R y$

הגדרה

הקוסט השמאלי של $a \in G$ לגבי H הוא אוסף כל האיברים השקולים משמאל ל-a מודולו H, כלומר

$$aH = \{ah: h \in H\}$$

נשים לב כי $a \in H \Leftrightarrow aH = H$

אכן $\Rightarrow$ נובע מתוך סגירות

$\Leftarrow$ אם $a \notin H$ אזי $a^{-1} \notin H$ אז בaH אין e

באופן כללי יחס השקילות מחלק את איברי G למחלקות שקולות זרות aH

דוגמאות

$$H = \{0,2,4\} = 2\mathbb{Z}_6 \leq \mathbb{Z}_6$$

$$0 + H = H$$
$$2 + H = H$$
$$4 + H = H$$

כלומר $\{0,2,4\}$ נציגים של אותו קוסט.

$$\mathrm{H} = \{0,3\} = 3\mathbb{Z}_6 \leq \mathbb{Z}_6$$

כאן יש 3 קוסטים, $0 + H = H, 1 + H = \{1,4\}, 2 + H = \{2,5\}$

באותו אופן מגדירים קוסט ימני בHa.

הגדרה

קבוצת המנה של החלוקה משמאל ב-H היא קבוצת הקוסטים השמאליים:

$$G/_H = \{aH: a \in G\}$$

אפשר גם להגדיר את קבוצת הקוסטים הימניים: $G\backslash_H = \{Ha : a \in G\}$

כל הזכויות שמורות לבנימין לוין ©

טענה

תהא G חבורה ו$H \leq G$, אזי $|G/_H| = |G\backslash_H|$

הוכחה

נגדיר את ההעתקה $\varphi: G/_H \to G\backslash_H$

$$gH \to Hg^{-1}$$

חח"ע: $\mathrm{H}g_1^{-1} = Hg_1^{-1} \Rightarrow H \underbrace{g_1^{-1}g_2}_{\in H} = H \Rightarrow g_2H = g_1H$

ברור שφ על שכן לכל תמונה Hg^{-1} יש מקור gH

נקרא לגודל של קבוצת המנה ה"אינדקס של H ב-G".

נסמן $[G:H] = |G/_H|$

משפט לגראנז'

תהא G חבורה סופית, אזי לכל ת"ח $H \leq G$ מתקיים $[G:H] = \frac{|G|}{|H|}$

הוכחה

לכל $a \in G$ נגדיר את ההעתקה $\varphi_a: H \to Ha$ ע"י $\varphi_a(h) = ha$.

ההעתקה חח"ע שכן $h_1a = h_2a \Rightarrow h_1 = h_2$

וברור שהיא על (מעצם הגדרתו) ולכן $|H| = |Ha|$.

כיוון שהקוסטים הם מחלקות שקילות, G הוא איחוד זר שלהם ולכן $|G| = [G:H]|H|$

מסקנות מידיות (עבור G סופית, $H \leq G$)

1) $[G:H], |H| \mid |G|$
2) $\forall a \in G: o(a) = |<a>| \, | \, |G|$
3) $\forall a \in G : a^{|G|=o(a)q} = e$

משפט (מיון של ת"ח של חבורה ציקליות).

תהא $G =< a >$ חבורה צקלית, אם G מסדר n אזי:

1) $H \leq G \Rightarrow |H| | n$
2) לכל k טבעי, $k|n$, קיימת ת"ח יחידה $H \leq G$ כך ש$|H| = k$

אם G אינסופית הראינו כבר ש$G \cong \mathbb{Z}$ וכל ת"ח של G היא $< a^n >$

הוכחה

1) משפט לגראנז'
2) כל ת"ח של חבורה צקלית היא צקלית, כמו כן לכל $k|n$:

$$o(a^j) = k \Leftrightarrow k = \frac{n}{(j,n)} \Leftrightarrow (j,n) = \frac{n}{k}$$

בפרט עבור $j = \frac{n}{k}$ נקבל קיום של ת"ח מסדר k : $H =< a^{\frac{n}{k}} >$

באופן כללי יותר, אם $j = \frac{n}{t}t$ אז במילא $< a^j > \subseteq < a^{\frac{n}{k}} >$ ומכאן היחידות

משפט אויילר

$$\forall a \in \mathbb{Z}^*, n \in \mathbb{N} : (a,n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 (mod\ n)$$

הוכחה

$$(a,n) = 1 \Rightarrow a \equiv a' \in U_n \Rightarrow a^{\varphi(n)} \equiv a'^{|U_n|} = 1$$

תרגיל

חשב את $9^{121} (mod\ 100)$

$$(9,100) \Rightarrow 9^{\varphi(100)} = 1 (mod\ 100)$$
$$\varphi(100) = \varphi(4)\varphi(25) = 2 * 20 = 40$$
$$9^{40} = 1(100) \Rightarrow 9^{121} = (9^{40})^3 9 = 9(100)$$

מקרה פרטי של משפט אויילר:

$$\forall a \in \mathbb{Z}^*, p : a^{p-1} \equiv 1 (mod\ p)$$

אלגוריתם ההצפנה RSA (ריבסט-שמיר-אדלמן) 1977

אליס מעוניינת שבוב ישלח לה הודעה חסויה באמצעות תקשורת פומבית.

<u>אלגוריתם:</u>

1) אליס בוחרת באקראי שני מספרים ראשוניים גדולים p,q שישארו חסויים אצלה, ומחשבת את $n = pq$ ואת $\varphi(n) = (p-1)(q-1)$.
2) אליס בוחרת d כך ש $(d, \varphi(n)) = 1$ ומחשבת את $e \equiv d^{-1} (mod\ \varphi(n))$ באמצעות אלגוריתם אוקלידס.
3) אליס שולחת לבוב את המפתח הציבורי (n,e).
4) בוב מצפין הודעה M המקיימת (M,n)=1 ע"י $E = m^e (mod\ n)$ ושולח לאליס.
5) אליס משחזרת את M: $E^d = M^{ed} = M^{1+\varphi(n)k} = M\left(M^{\varphi(n)}\right)^k = M$.

הערות:

- אם ימצאו אלגוריתם יעיל למצוא את הפירוק $n = pq$ יוכלו לחשב את $\varphi(n)$ ואת $d \equiv e^{-1}$.
- זוהי שיטה אסימטרית : המצפין לא יודע לפענח.

כל הזכויות שמורות לבנימין לוין ©

תת-חבורה נורמלית וחבורת המנה

הגדרה:

אם $H \leq G$ מקיימת: $\forall g \in G : gH = Hg$

אזי H נקראת תת-חבורה נורמלית, ונסמן $H \lhd G$

אם $G \lhd H$ אזי קבוצת המנה $G\backslash_H$ היא חבורה עם פעולת הכפל המוגדרת ע"י $Hx * Hy = Hxy$

אכן, אם $G \lhd H$ אזי $Hx = xH$ ובהתאם לכך $(Hx)^{-1} = Hx^{-1}$ שכן $HxHx^{-1} = HHxx^{-1} = HH = H$.

H הוא איבר היחידה.

הפעולה $*$ שבאמצעותה הגדרנו את הכפל היא הפעולה המקורית המוגדרת ב-G!

לכן רק באמצעות הנורמליות של $G \leq H$ מתקיים $HxHy = Hxy$

דוגמא

$$G = GL_2(\mathbb{Z}_2) = \{\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}, a = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}, \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}, b = \begin{pmatrix}0 & 1\\1 & 1\end{pmatrix}\}$$

$$a^2 = 1, b^3 = 1$$

$$GL_2(\mathbb{Z}_2) =< a, b > rank(GL_2\mathbb{Z}_2) = 2$$

$$[G:< a >] = \frac{|G|}{|< a >|} = \frac{6}{2} = 3, [G:< b >] = \frac{6}{3} = 2$$

$$G\backslash_{<b>} = \left\{ \overbrace{< b >}^{\{1,b,b^2\}}, \overbrace{a < b >}^{\{a,ab,ab^2\}} \right\}$$

$$G/_{<b>} = \left\{ \underbrace{< b >}_{\{1,b,b^2\}}, \underbrace{< b > a}_{\{a,ba,b^2a=ab\}} \right\}$$

נשים לב כי $a < b >=< b > a$

$$G/_{<a>} = \left\{ \underbrace{< a >}_{\{1,a\}}, \underbrace{b < a >}_{\{b,ba\}}, \underbrace{b^2 < a >}_{\{b^2,b^2a\}} \right\}$$

$$G\backslash_{<a>} = \left\{ \underbrace{< a >}_{\{1,a\}}, \underbrace{< a > b}_{\{b,ab\}}, \underbrace{< a > b^2}_{\{b^2,ab^2\}} \right\}$$

שלא שווים!

$G/_{<b>} \cong \mathbb{Z}_2$ חבורת המנה.

$G/_{<a>}$ קבוצת מנה!

כל הזכויות שמורות לבנימין לוין ©

הרצאה 6 – גרעין ותמונה של הומומורפיזם

G ⊲ H ת"ח נורמלית אם $\forall g \in G : gH = Hg$
$\Leftrightarrow \quad \forall g \in G : gHg^{-1} = H$
$\Leftrightarrow \forall g \in G, h \in H : ghg^{-1} \in H$

למשל אם G אבלית, ברור שכל $H \leq G$ היא $H \lhd$ G

לדוגמא

$$G = \mathbb{Z}, H = n\mathbb{Z} =< n >$$

$$3\mathbb{Z} \leq \mathbb{Z}$$

$$\mathbb{Z}/_{3\mathbb{Z}} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}m2 + \mathbb{Z}\} = \mathbb{Z}_3$$

הגדרה:

יהא $f: G \to H$ הומומורפיזם, הגרעין של f הוא $\ker(f) = \{g \in G : f(g) = 1_H\}$

טענה:

$$\ker(f) \lhd \text{G}$$

הוכחה

$f(1_G) = 1_H \Rightarrow 1_G \in \ker(f)$
$x, y \in \ker(f) \Rightarrow f(x) = f(y) = 1_H \Rightarrow f(xy) = f(x)f(y) = 1_H \quad \Rightarrow xy \in \ker(f)$

ולכן תת חבורה.

לגבי נורמליות:

נסמן $K \coloneqq \ker(f)$, צ"ל $\forall x \in G: xKx^{-1} = K$ כלומר $\forall x \in G, k \in K: xkx^{-1} \in K$

$$f(xkx^{-1}) = f(x)\underbrace{f(k)}_{1_H}\underbrace{f(x^{-1})}_{f(x)^{-1}} = 1_H \Rightarrow xkx^{-1} \in K$$

ולכן $Ker(f) \lhd$ G

טענה

בהינתן $f: G \to H$ הומו', $Im(f) \leq H$.

א. $1_H = f(1_G) \Rightarrow 1_H \in Im(f)$
ב. $h_1, h_2 \in Im(f) \Rightarrow h_1 = f(g_1), h_2 = f(g_2) \Rightarrow f(g_1g_2) = h_1h_2 \Rightarrow h_1h_2 \in Im(f)$

$$h \in Im(f) \Rightarrow h = f(g) \Rightarrow f(g^{-1}) = f(g)^{-1} = h^{-1} \in Im(f)$$

תוצאה

אם G סופית, H סופית, $f: G \to H$, ע"פ לגראנז':

$$|\ker(f)| \mid |G| \wedge |Im(f)| \mid |H|$$

למשל לא ניתן לשכן (מונומורפיזם) את $\mathbb{Z}_3$ בתוך $\mathbb{Z}_{10}$.

$$f: \mathbb{Z}_3 \to \mathbb{Z}_{10}$$

$$|Im(f)| = 3 \nmid 10$$

טענה

הומומורפיזם $f: G \to H$ הוא חח"ע אם"ם $\ker(f) = \{1_G\}$

הוכחה

$$\ker(f) = \{1_G\} \Leftrightarrow (\forall x, y \in G: xy^{-1} \in \ker(f) \Rightarrow x = y)$$
$$\Leftrightarrow (\forall x, y \in G : f(xy^{-1}) = 1_H \Rightarrow x = y) \Leftrightarrow \big(\forall x, y \in G: f(x) = f(y)\big)\text{חח"ע}$$

משפט האיזומורפיזם(!!!) Emmy Nother

טענה

תהא G חבורה ו $H \lhd G$, נגדיר העתקה $\nu: G \to G/_H$ ע"י $\nu(a) = aH$, אזי ν הוא הומומורפיזם ומתקיים $\ker(\nu) = H$.
ν נקרא ההומומורפיזם הטבעי.

הוכחה

$$\forall a, b \in G : \nu(ab) = abH = abHH = aHbH = \nu(a)\nu(b)$$

$$\ker(\nu) = \{a \in G : aH = H\} = H$$

משפט האיזומורפיזם הראשון:

אם $\varphi: G \to H$ אפימורפיזם אז קיים איזומורפיזם $\psi: G/_{\ker(\varphi)} \cong H$ כך ש $\varphi = \psi \circ \nu$ כאשר $\nu: G \to G/_{\ker(\varphi)}$ הוא ההומומורפיזם הטבעי.

דוגמא

$$\varphi: \mathbb{Z} \to \mathbb{Z}_n$$
$$x \mapsto x(mod\ n)$$
$$\ker(\varphi) = n\mathbb{Z}$$
$$\mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}_n$$

הוכחה:

נסמן $K = \ker(\varphi)$ ונגדיר את ההעתקה $\psi: G/H \to H$ ע"י $\psi(Ka) = \varphi(a)$

צ"ל שההעתקה מוגדרת היטב כלומר שהתמונה של Ka לא תלויה בבחירת הנציג.

$$Ka = Kb \Leftrightarrow ab^{-1} \in K \Leftrightarrow \varphi(ab^{-1}) = 1_H \Leftrightarrow \varphi(a) = \varphi(b)$$

נבדוק שψ הומומורפיזם, נעזר בעובדה כי $K \lhd G$:

$$\psi(Ka * Kb) = \psi(Kab) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(Ka)\psi(Kb)$$

 כל הזכויות שמורות לבנימין לוין ©

כעת נבדוק כי ψ חח"ע:

$$\ker(\psi) = \{Ka: a \in G \mid \varphi(a) = 1_H\} = \{Ka: a \in K\} = \{K\}$$

נתון כי φ על כלומר $\forall h \in H \exists a: \exists a \in G: \varphi(a) = h$

לכן מתוך ההגדרה של ψ המקור של h יהיה Ka תחת ψ.

הערה:

$$|G/_{\ker(\varphi)}| = \frac{|G|}{|\ker(\varphi)|} = |H| = |Im(\varphi)|$$

הערה: ניסוח שקול של משפט האיזו' הראשון (בקיצור):

$$G/_{\ker(\varphi)} \cong Im(\varphi)$$

תוצאה של המשפט:

K היא ת"ח נורמלית של G אם"ם קיים אפימורפיזם $f: G \to H$ כך ש: $K = \ker(f)$

דוגמא:

$$D_3 = GL_2(\mathbb{Z}_2) =< a, b: a^2 = b^3 = 1, ab = b^2a$$

שלוש תתי חבורות נורמליות בD_3 : $\{id, < b >, D_3\}$

איזה איזומורפיזם φ מD_3 מתאים ל $\ker(\varphi) = \{id\}$?

$$\varphi: x \mapsto x \quad D_3 \to D_3$$

$\boldsymbol{ker(\varphi)}$	$\boldsymbol{\varphi}$	$\boldsymbol{Im(\varphi)}$
$\{id\}$	$x \mapsto x$	6
$< b >$	$x \mapsto x^3$	2
D_3	$x \mapsto id$	1

תרגיל

תהיינה שתי חבורות G_1, G_2 מסדרים זרים, כמה הומומורפיזם שונים קיימים מG_1 לG_2?

פתרון

$$\varphi: G_1 \to G_2$$

אזי

$$|kar| \,|_{|G_1|} \quad |Im| \,|_{|G_2|}$$

$$G_1/_{\ker(\varphi)} \cong Im(\varphi)$$

$$\frac{|G_1|}{|\ker(\varphi)|} = |Im(\varphi)|$$

$$|Im(\varphi)| |_{|G_2|}$$

כל הזכויות שמורות לבנימין לוין ©

אבל $(|G_1|,|G_2|)$ זרים ולכן $|Im(\varphi)| = 1$ ולכן זוהי ההעתקה הטריוויאלית וזו היחידה.

דוגמאות נוספות

1) $f: GL_n(\mathbb{R}) \to (\mathbb{R}^*,*)$ המוגדר ע"י $f(A) = \det(A)$

הומו' לפי תכונות הדטרמיננטה.

נבדוק על: לכל מספר ממשי שונה מאפס r .

$$\ker(f) = \{A \in GL_n: \det(A) = 1\} = SL_n(\mathbb{R})$$
$$SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$$

לפי משפט איזו I : $|GL_n(\mathbb{R})|/_{SL_n(\mathbb{R})} \cong (\mathbb{R}^*,*)$

2) הוכח כי $\mathbb{R}/_{\mathbb{Z}} \cong \mathbb{T}$

$$\mathbb{T} = \{z \in \mathbb{C}: |z| = 1\}$$

פתרון

נגדיר אפימורפיזם $\varphi: \mathbb{R} \to \mathbb{C}$ כך ש $\ker(\varphi) = \mathbb{Z}$

$$\varphi: r \mapsto cis(2\pi r)$$

$$\ker(\varphi) = \mathbb{Z}$$

$$2\pi r \in 2\pi\mathbb{Z} \Rightarrow r \in \mathbb{Z}$$

3) נגדיר בתוך $G = \mathbb{R}^2$ את $H = \{(x, 3x)\}$, הראה כי $G/_H \cong \mathbb{R}$

נמצא אפימורפיזם $\varphi: (x, y) \mapsto y - 3x \quad \varphi: G \to \mathbb{R}$

$$\ker(\varphi) = H$$

ע"פ איזו I : $\mathbb{R}^2/_H \cong \mathbb{R}$

$$(a, b) + H = \begin{pmatrix} \text{ישר} \\ \text{המקביל} \\ \text{ל} - H \end{pmatrix}$$

כל הזכויות שמורות לבנימין לוין ©

הרצאה 7

משפט האיזומורפיזם השני

תהא G חבורה ו$A \leq G, H \lhd G$ שתי חבורות, אזי מתקיים:

1) $\{ah: a \in A, h \in H\} = AH \leq G$
2) $AH/_H \cong A/_{A\cap H}$

הוכחה

סעיף 1:

1) $1 \in AH$
2) נרצה להראות כי $(AH)(AH)^{-1} \subseteq AH$ (זה בקבוצות, כלומר $\forall a_1 a_2, h_1, h_2: (a_1h_1) * (h_2^{-1}a_2^{-1}) \in AH$

$$(a_1h_1) * (h_2^{-1}a_2^{-1}) = a_1h_3a_2^{-1} = a_1 \underbrace{a_2h_4}_{H\lhd G} \in AH$$

סעיף 2:

א) נתון $H \lhd G \Rightarrow \forall g \in G: gH = Hg$ ובפרט עבור $g = ah \in AH$ ולכן $H \lhd AH$
ב) חיתוך של תתי חבורות הוא גם תת חבורה, לגבי הנורמליות, נסמן $L = A \cap H$ ונראה:

$$\forall a \in A, l \in L: ala^{-1} \in L$$

לכל $g \in G$ ובפרט לכל $a \in A$ מתקיים $aHa^{-1} \in H$ (כי $H \lhd G$). ובפרט עבור $l \in L$ מתקיים $l \in A$ ולכן מתוך סגירות $ala^{-1} \in A \Rightarrow ala^{-1} \in A \cap H = L$.

נמצא אפימורפיזם $\varphi: A \to AH/_H$ כך ש$\ker(\varphi) = A \cap H$

$$\varphi(a) = aH \in AH/_H$$

נראה הומו':

$$\varphi(ab) = abH = a\overbrace{bH} = aHbH = \varphi(a)\varphi(b)$$

φ היא על שכן המקור לכל $ahH = aH$ הוא a

נחשב את הגרעין:

$$\ker(\varphi) = \{a \in A: aH = H\} = \{a \in A: a \in H\} = A \cap H$$

כעת ההוכחה מסתיימת הודות למשפט איזו' הראשון.

הערה

$$H \leq G \Leftrightarrow 1 \in H \wedge \forall x, y \in H: xy^{-1} \in H$$

כל הזכויות שמורות לבנימין לוין ©

דוגמא:

$$a\mathbb{Z}+b\mathbb{Z}=(ab)\mathbb{Z}$$
$$a\mathbb{Z}\cap b\mathbb{Z}=[a,b]\mathbb{Z}$$

$$\forall a,b\in\mathbb{N}:\ {a\mathbb{Z}+b\mathbb{Z}}/{b\mathbb{Z}}\cong {a\mathbb{Z}}/{a\mathbb{Z}\cap b\mathbb{Z}}={a\mathbb{Z}}/{[a,b]\mathbb{Z}}\cong\mathbb{Z}_{\frac{b}{(a,b)}}$$

משפט האיזומורפיזם השלישי

תהא G חבורה ותהיינה $G,N\lhd G$ $H\lhd$ ת"ח כך ש $N\le H$, אזי

$$\left.{G/_N}\middle/{H/_N}\right.\cong G/_H$$

הוכחה

נגדיר את ההעתקה $\varphi: G/_N\to G/_H$ ע"י $gN\mapsto gH$

נראה שההעתקה מוגדרת היטב, כלומר שתמונה אינה תלוייה בנציג של gN

$$g_1N=g_2N\Rightarrow g_2^{-1}g_1\in N\Rightarrow g_2^{-1}g_1\in H\Rightarrow g_2^{-1}g_1H=H\Rightarrow g_1H=g_2H$$

נראה הומו':

$$\varphi(g_1Ng_2N)=\varphi(g_1g_2N)=g_1g_2H=g_1Hg_2H=\varphi(g_1N)\varphi(g_2N)$$

כמו כן היא על שכל לכל תמונה קיים מקור, ולכן היא אפימורפיזם, נחשב את הגרעין

$$\ker(\varphi)=\{gN: g\in G\mid gH=G\}=\{gN: g\in G\}=H/_G$$

דוגמא

החבורה $2\mathbb{Z}/_{6\mathbb{Z}}$ היא ת"ח של $\mathbb{Z}/_{6\mathbb{Z}}$

$$\left.{\mathbb{Z}/_{6\mathbb{Z}}}\middle/{2\mathbb{Z}/_{6\mathbb{Z}}}\right.\cong\mathbb{Z}_2$$

תרגיל נחמד

יהי G חבורה $G,H\lhd G$ $A\le$, הוכח:

$$[G:A\cap H]\le[G:A][G:H]$$

$A/_{A\cap H}\cong AH/_H\le G/_H$
$[A:A\cap H]=[AH:H]\le[G:H]$
$\left.{G/_{A\cap H}}\middle/{A/_{A\cap H}}\right.\cong G/_A\Rightarrow[G:A\cap H]=[A:A\cap H][G:A]\Rightarrow[G:A\cap H]\le[G:A][G:H]$

כל הזכויות שמורות לבנימין לוין ©

כמו כן עפ"י משפט לגרנז': $[G:A\cap H]=\frac{|G|}{|A|}\cdot\frac{|A|}{|A\cap H|}=[G:A]\cdot[A:A\cap H]$ וכך מגיעים לתוצאה הרצויה.

אנדומורפיזם

הגדרה:

בהינתן מונואיד M, הומומורפיזם $f: M \to M$ נקרא אנדומורפיזם (בפרט עבור חבורות).

אם אנדומורפיזם הוא גם איזומורפיזם אז הוא יקרא אוטומורפיזם.

סימון

קבוצת האנדו' של M : $End(M)$.

חבורת האוטומורפיזם של M: $Aut(M) = Gr(End(M))$

דוגמאות

1) $Aut(\mathbb{Z})$, הראינו בתמונה מומומורפית של חבורה צקלית היא צקלית, אם נרצה שהתמונה גם על (באשר חבורת השווה צקלית) נצטרך ש יוצר = $f($יוצר$)$

כיוון שב$\mathbb{Z}$ ישנם שני יוצרים, $< \pm 1 >$, נוצרים שני איזומורפיזם אפשריים:

א) $1 \mapsto 1 \Rightarrow k \mapsto k$ כלומר $f = id$

ב) $1 \mapsto -1 \Rightarrow k \mapsto -k$ כלומר $f = -id$

2) $Aut(\mathbb{Z}_n)$

טענה:

$$\mathbb{Z}_n =< a > \Leftrightarrow (a,n) = 1$$

$$f: 1 \mapsto a \Rightarrow f: k \mapsto ak \Rightarrow \ker(f) = \{k \in \mathbb{Z}_n : aK \equiv 0(mod\ n)\}$$

כעת a אינו מחלק אפס, כלומר$(a,n) = 1$ $\ker(f) = \{0\} \Leftrightarrow$

$$f: 1 \mapsto \{a \in U_n\}$$

נרצה להראות $Aut(\mathbb{Z}_n) \cong U_n$

דוגמאות

1) $\varphi: a \in U_n \mapsto \overbrace{f_a: 1 \mapsto a}^{\in Ant(\mathbb{Z}_n)}$

$$\varphi(ab) = f_{ab}: 1 \mapsto ab, f_{ab}(k) = abk = af_b(k) = f_a\big(f_b(k)\big)$$

$$f_{ab} = f_a \circ f_b = \varphi(a)\varphi(b)$$

כל הזכויות שמורות לבנימין לוין ©

ולכן הומו'. נבדוק חח"ע:

$$\ker(\varphi) = \{a \in U_n : f_a = id = f_1\} = \{1\}$$

כיוון שהראינו $|Ant(\mathbb{Z}_n)| = |U_n|$, זה גורר על ובס"כ $Aut(\mathbb{Z}_n) \cong U_n$

הגדרה

תהא G חבורה, עבור $a \in G$ האוטומורפיזם הפנימי I_a הוא ההעתקה $\forall x \in G : x \mapsto axa^{-1}$

נראה כי היא אכן אוטו':

אנדו $\forall x, y \in G : I_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = I_a(x)I_a(y) \Rightarrow$

חח"ע $\ker(I_a) = \{x \in G : I_a(x) = 1\} = \{x \in G : axa^{-1} = 1\} = \{1\} \Rightarrow$

לכל תמונה $y \in G$ קיימת מקור $a^{-1}ya$ שהרי $I_a(a^{-1}ya) = aa^{-1}yaa^{-1} = y$

ולכן אוטו'.

סימון

קבוצת כל האוטומורפיזמים הפנימיים

$$\mathrm{Inn(G)} = \{\mathrm{I_a} : a \in G\}$$

טענה

$$Inn(G) \lhd Aut(G)$$

הוכחה

תחילה נראה כי היא תת חבורה

1) $I_e = id \in Inn(G)$

2) $\forall I_a, (I_b)^{-1} \in Inn(G) : I_a \circ (I_b)^{-1} \in Inn(G)$

$$I_{b^{-1}} \circ I_b(x) = b^{-1}bxb^{-1}b = x \Rightarrow (I_b)^{-1} = I_{b^{-1}}$$
$$I_a \circ (I_b)^{-1}(x) = I_a \circ I_{b^{-1}}(x) = I_a(b^{-1}xb) = ab^{-1}xba^{-1} \in Inn(G)$$

כעת נראה נורמליות:

$$\forall f \in Ant(G), I_a \in Inn(G), x \in G$$
$$(f \circ I_a \circ f^{-1})(x) = f\left(I_a\left(f^{-1}(x)\right)\right) = f(af^{-1}(x)a^{-1}) = f(a)xf(a^{-1}) = I_{f(a)}(x) \in Inn(G)$$

הגדרה

המרכז (center) של חבורה G הוא הקבוצה $Z(G) \coloneqq \{x \in G : xy = yx \ \forall y \in G\}$

דוגמאות

1) $Z\left(GL_n(\mathbb{R})\right) = \{cI_n : c \in \mathbb{R}^*\} \cong (R^*, *)$

2) $O_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) : AA^t = I_n\}$

$Z\left(O_n(\mathbb{R})\right) = \{\pm I_n\} \cong \mathbb{Z}_2$

3) $Z(D_3) = \{e\}$

כל הזכויות שמורות לבנימין לוין ©

טענה

$$Z(G) \lhd G$$

הוכחה

1) $\forall g \in G: 1g = g1 \Rightarrow 1 \in Z(G)$

2) $\forall z \in Z(G), g \in G: z^{-1}g = (g^{-1}z)^{-1} = gz^{-1} \Rightarrow z \in Z(G)$

3) $z_{1,2} \in Z(G): z_1 z_2 g = z_1 g z_2 = g z_1 z_2 \Rightarrow z_1 z_2 \in Z(G)$

נורמליות:

$$\forall g \in G, z \in Z(G): gzg^{-1} = z \in Z(G) \Rightarrow Z(G) \lhd G$$

טענה

$$G/_{Z(G)} \cong Inn(G)$$

הוכחה

נגדיר העתקה $\varphi: G \to Inn(G),\ \ g \mapsto I_g$

ראינו כבר שזהו הומו', וברור שזה על

$$\ker(\varphi) = \{g \in G: I_g = id\} = \{g \in G: I_g(x) = gxg^{-1} = x\} = \{g \in G: gx = xg\ \forall x \in G\} = Z(G)$$

וההוכחה מסתיימת ע"פ משפט האיזו' הראשון.

הגדרה

המרכז (Centralizer) של איבר x בחבורה G הוא הקבוצה

$$C(x) = \{y \in G: xy = yx\}$$

טענה

$$\forall x \in G: C(x) \leq g$$

1) $1x = x1 \Rightarrow 1 \in C(x)$

2) $\forall c \in C(x): c^{-1}x = (x^{-1}c)^{-1} = (cx^{-1})^{-1} = xc^{-1} \Rightarrow c^{-1} \in C(x)$

3) $c_{1,2} \in C(x): c_1 c_2 x = x c_1 c_2 \Rightarrow c_1 c_2 \in C(x)$

הערה

$$\bigcap_{x \in G} C(x) = Z(G)$$

כל הזכויות שמורות לבנימין לוין ©

הרצאה 8

החבורה הסמטרית

הגדרות

קבוצת כל התמורות של $X = \{1, \dots, n\}$ נקראת **חבורת הסימטריה** או **החבורה הסמטרית**. ומסומנת ע"י S_X, S_n

עגיל (או מחזור) היא תמורה המציינת מעגל אחד של החלפת מספרים שונים $a_1 \mapsto a_2 \mapsto \cdots \mapsto a_k \mapsto a_1$ ומסומנת ע"י $(a_1\ a_2 \dots a_k)$ למשל $(1\ 3\ 5)$.

ניתן לכתוב כל תמורה בS_n כמכפלה של עגילים זרים אע"פ שבדר"כ מכפלת תמורות או בפרט עגילים אינה קומו' כשמדובר בעגילים זרים, כיוון שכל עגיל פועל על מספרים שונים, אין חשיבות לסדר הופעתו במכפלה.

לדוגמא

$$\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8 \\ 3\,5\,6\,1\,8\,4\,7\,2 \end{pmatrix} = (1\ 3\ 6\ 4)(2\ 5\ 8)(7)$$

טענה

סדר של עגיל שווה לאורכו.

הוכחה

הזזה צקלית r פעמים כאשר r הוא אורך העגיל מחזירה את כל המספרים למקומם.

טענה

בהינתן תמורה כלשהי המוצגת כמכפלה של k עגילים זרים באורכם $\{r_1, \dots, r_k\}$ הסדר של σ הוא הכק"ב של אורכי העגילים $o(\sigma) = [r_1, \dots, r_k]$.

הוכחה

כיוון שהעגילים זרים $\sigma^m = \sigma_1^m \dots \sigma_k^m$

$$\sigma^m = id \Leftrightarrow \forall i :\ \overbrace{r_i}^{o(\sigma_i)}\ | m$$

הm מינימלי שמקיים זאת הוא הכמק"ב של $\{r_i\}_{i=1}^k$

הגדרות

כל עגיל באורך 2 נקרא חילוף.

תמורה תיקרא זוגית אם היא ניתנת לכתיבה כמכפלה של מס' זוגי של חילופים.

אחרת, התמורה נקראת אי זוגית.

טענה

כל עגיל ניתן לכתיבה כמכפלה של $r-1$ חילופים.

כל הזכויות שמורות לבנימין לוין ©

הוכחה

$$(a_1 \dots a_r) = (a_1\ a_2)(a_2\ a_3) \dots (a_{r-1}\ a_r)$$

אלגוריתם לקביעת זוגיות של תמורה

1) S נכתוב את התמורה כמכפלה של עגילים זרים.
2) אם מספר העגילים מסדר זוגי הוא זוגי, אז התמורה זוגית.

הסבר:

כל עגיל מסדר זוגי ניתן לכתיבה כמכפלה של מס' אי-זוגי של חילופים. לעומתו עגיל מסדר אי-זוגי מוסיף למכפלה מס' זוגי של חילופים ולכן לא משפיע על הזוגיות, ולכן אם יש מס' אי-זוגי של עגילים זוגיים אז בסה"כ התמורה תהיה אי-זוגית ולהיפך.

דוגמא

$$\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9 \\ 2\,4\,5\,1\,3\,7\,8\,9\,6 \end{pmatrix} = (1\ 2\ 4)\overbrace{(3\ 5)}^{\text{זוגי}}\overbrace{(6\ 7\ 8\ 9)}^{\text{זוגי}} \Rightarrow \sigma \text{ זוגי}$$

$$o(\sigma) = [4,3,2] = 12$$

טענה

קבוצת כל התמורות הזוגיות ב-S_n היא ת"ח נורמלית ומסומנת ע"י A_n. $\quad A_n \lhd S_n$

הוכחה

א) $id = (1\ 2)(1\ 2) \in A_n$
ב) אם σ זוגית וτ זוגית אז $\sigma\tau$ ניתן לכתיבה כמספר זוגי של חילופים ולכן $\sigma\tau \in A_n$
ג) אם σ היא זוגית, אזי σ^{-1} תהיה כתובת החילופים בסד הפוך ולכן גם מספר החילופים יהיה זוגי ולכן $\sigma^{-1} \in A_n$.

כעת נגדיר העתקה $\sigma \mapsto \sigma(1\ 2)$, $A_n \to \overbrace{S_n - A_n}^{A^c}$. זוהי העתקה חח"ע שכן אם $\sigma_1(1\ 2) = \sigma_2(1\ 2)$ אז $\sigma_1 = \sigma_2$

היא גם על וכן $|A_n| = |A_n^c|$ כלומר $[S_n : A_n] = 2 = \frac{|S_n|}{|A_n|}$ ולכן $A_n \lhd S_n$.

עוד דרך לראות זאת:

להגדיר $sign: S_n \to \mathbb{Z}_2$ ע"י $sign(\sigma) = \begin{cases} 0 & \sigma \text{ זוגי} \\ 1 & \sigma \text{ אי זוגי} \end{cases}$.

זהו הומומורפיזם ולכן $\text{sign}(\sigma\tau) = \begin{cases} 0 & have\ to\ same\ pairity \\ 1 & othewise \end{cases}$

$$\ker(sigh) = A_n \lhd S_n$$

כל הזכויות שמורות לבנימין לוין ©

דוגמא

$$\varphi: \overbrace{O_n(\mathbb{R})}^{\text{אורטוגונליות}} \twoheadrightarrow \{\pm 1\}$$

$$A \mapsto \det(A)$$

$$\ker(\varphi) = SO_n(\mathbb{R})$$

$$[O_n(\mathbb{R}): SO_n(\mathbb{R})] = 2$$

הגדרות:

$$the\ orthgonal\ group = O_n(F) = \{A \in M_n(F): AA^T = I_n\}$$

$$special\ orthgonal\ group = SO_n(F) = \{A \in O_n(F): \det(A) = 1\}$$

דוגמא

$$A_4 = \begin{Bmatrix} id, (1\ 2\ 3), (1\ 3\ 2), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 5), (1\ 4\ 3) \\ (1,2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \end{Bmatrix}$$

$$|A_4| = 12 = \frac{4!}{2}$$

החבורה הדיהדרלית (חבורת קליין)

הגדרה

עבור מספר טבעי k הקבוצה D_k של סיבובים ושיקופים המעתיקים מצולע משוכלל בן k צלעות על עצמו היא חבורת דיהדר.

אם a הוא סיבוב ב$\frac{2\pi}{k}$ ו-b היא שיקוף סביב ציר סמטריה כלשהו של המצולע, אזי:

$$D_k =< a, b : a^k = 1, b^2 = 1, ab = ba^{n-1} = ba^{-1} >= \{1, a, a^2, \dots, a^{k-1}, b, ba, \dots, ba^{k-1}\}$$

כל איבר בD_n הוא למעשה תמורה של קודקודי המצולע ולכן $D_n \leq S_n$.

הגדרה

חבורת הסמטריה של מלבן (אשר צלעותיו הסמוכות באורך שונה) היא חבורת קליין.

$$V_4 = \{1, a, b, ab = ba\} =< a, b: a^2 = b^2, ab = ba >\cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

כל הזכויות שמורות לבנימין לוין ©

טיפוס (מבנה) של תמורה

תהא σ תמורה בS_n. נפרק אותה למכפלה של מספרים זרים $\sigma = (a_{11} \dots a_{1r_1}) \dots, (a_{k1} \dots a_k r_k)$ כך ש $r_1 \geq r_2 \geq \cdots \geq r_k$. אזי הסדרה $(r_1, r_2, \dots, r_k)$ נקראת הטיפוס (type) של σ.

לדוגמא

$$\begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \\ 3\ 4\ 5\ 2\ 1\ 6\ 8\ 7 \end{pmatrix} = (1\ 3\ 5)(2\ 4)(7\ 8)(6)$$

המבנה שלה הוא (3,2,2,1).

טענה

$$\forall \mu \in S_n : \mu(i_1\ i_2 \dots i_k)\mu^{-1} = \big(\mu(i_1)\ \mu(i_2) \dots \mu(i_k)\big)$$

דוגמא

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

$$\mu(1\ 2\ 5\ 4)\mu^{-1} = (1\ 4\ 5\ 3) = \big(\mu(1)\ \mu(2)\ \mu(5)\ \mu(4)\big)$$
$$1 \to 1 \to 2 \to 4$$
$$2 \to 3 \to 3 \to 2$$
$$3 \to 4 \to 1 \to 1$$
$$4 \to 2 \to 5 \to 5$$
$$5 \to 5 \to 4 \to 3$$

הוכחה

נוכיח טענה שקולה:

$$\forall \mu \in S_n : \mu(i_1 \dots i_k) = \big(\mu(i_1) \dots \mu(i_k)\big)\mu$$

אם $i_t \in \{i_1, \dots, i_k\}$ אזי $i_t \mapsto \mu(i_t) \mapsto \mu(i_{t+1})$

באגף שמאל $i_t \mapsto i_{t+1} \mapsto \mu(i_{t+1})$

אם $i_t \notin \{i_1, \dots, i_k\}$ אז בשני האגפים נקבל סה"כ $i_t \mapsto \mu(i_t)$

טענה

את הטענה האחרונה אפשר להרחיב לכל תמורה=מכפלה של עגילים.

$$\mu(i_1 \dots i_k)(j_1 \dots j_l)\mu^{-1} = \mu(i_1 \dots i_k)\mu^{-1}\mu(j_1 \dots j_l)\mu^{-1} = \big(\mu(i_1) \dots \mu(i_k)\big)\big(\mu(j_1) \dots \mu(j_l)\big)$$

דוגמא

הראה כי $V_4 \lhd A_4$

פתרון

V_4 מכיל את כל התמורות מטיפוס (2,2) בA_4. מכאן ש:

$$\forall \sigma \in A_n, \tau \in V_4 : \underbrace{\sigma\tau\sigma^{-1}}_{\substack{\text{טיפוס} \\ (2,2)}} \in V_4 \Rightarrow V_4 \lhd A_4$$

משפט

$\forall n \geq 2 : S_n =< (1\ 2), (1\ 2 \dots n) >$
$rank(S_n) = 2$

הוכחה

כל תמורה ניתנת לכתיבה כמכפלה של חילופים, כמו כן: $\forall (i\ j) = (1\ i)(1\ j)(1\ i)$

ולכן $S_n =< (1\ i) : i \in \{2, \dots, n-1\} >$

$\tau = (1\ 2 \dots n), \sigma = (1\ 2)$

$\tau\sigma\tau^{-1} = (2\ 3)$
$\tau^2\sigma\tau^{-2} = (3\ 4)$
$\dots \dots \dots \dots \dots \dots \dots$
$\tau^{n-2}\sigma\tau^2 = (n-1\ n)$

$(1\ 3) = (1\ 2)(2\ 3)(1\ 2)$
$(1\ 4) = (1\ 3)(3\ 4)(1\ 3)$
$(1\ 5) = (1\ 4)(4\ 5)(1\ 4)$
$\dots \dots \dots \dots \dots \dots \dots \dots \dots \dots \dots$
$(1\ n) = (1\ n-1)(n-1\ n)(1\ n-1)$

כלומר $S_n < \sigma, \tau >$

כל הזכויות שמורות לבנימין לוין ©

הרצאה 9

משפט קיילי | הצגה של חבורות

משפט Cayley

כל חבורה סופית G איזומורפית לתת חבורה של S_G

הוכחה

נגדיר את ההעתקה $\varphi: G \to S_G$ ע"י $a \mapsto l_a$ כאשר $l_a(x) = ax$ (תמורה של אברי G).

l_a היא אכן תמורה שכן זו העתקה חח"ע $G \to G$.

$$\forall x, y \in G : ax = ay \Rightarrow x = y$$

ומתוך סופיות זוהי גם על.

נבדוק שימור פעולה של φ, כלומר נראה כי:

$$\varphi(ab) \overset{?}{=} l_a \circ l_b$$

$$\forall x \in G \ \varphi(ab)(x) = abx = l_a\big(l_b(x)\big) = (l_a \circ l_b)(x)$$

ולכן הומו', נבדוק חח"ע

$$\ker(\varphi) = \{a \in G : l_a = id\} = \{a \in G : ax = x\} = \{e\}$$

ולכן בסה"כ φ מונו' כלומר $G \cong \varphi(G) \leq S_G$

תוצאה:

כל חבורה בעלת n איברים איזומורפית לתת חבורה כלשהיא של S_n.

דוגמא

בחבורה $\mathbb{Z}_2 \times \mathbb{Z}_2$ ישנם ארבעה איברים, לכן ניתן לשיכון בתוך S_4.

$$G = \left\{\overset{1}{(0,0)}, \overset{2}{(0,1)}, \overset{3}{(1,0)}, \overset{4}{(1,1)}\right\}$$

$$(0,1) + G = \left\{\overset{2}{(0,1)}, \overset{1}{(0,0)}, \overset{4}{(1,1)}, \overset{3}{(1,0)}\right\}$$

$$(0,1) \mapsto (1\ 2)(3\ 4) \in S_4$$
$$(1,0) \mapsto (1\ 3)(2\ 4)$$

הערה

נורמליות היא לא טרנזטיבית:

$$A \lhd B \lhd C \ \not\Rightarrow A \lhd C$$

כל הזכויות שמורות לבנימין לוין ©

דוגמא

$$K = \{e, ba\} \lhd \underbrace{V_4}_{\{e,ba,a^2,ba^3\}} \lhd D_4 =< a, b >$$
$$K \ntriangleleft D_4$$

פיצול חבורות

הגדרה

G נקרא מכפלה ישרה פנימית של ת"ח שלה: $X, Y \leq G$ אם:

א) כל איבר ב-G ניתן לכתיבה בצורה יחידה כ$g = xy$ כאשר $x \in X, y \in Y$ ($G = XY \Leftarrow$)

ב) $\forall x \in X, y \in Y: xy = yx$.

משפט

G מכפלה ישרה פנימית אם"ם $G \cong X \times Y$

הוכחה

$\boxed{\Leftarrow}$

נגדיר העתקה $\varphi: X \times Y \to G$ ע"י $(x, y) \mapsto xy$. נראה כי היא משמרת פעולה

$$\varphi\big((x_1, y_1), (x_2, y_2)\big) = \varphi\big((x_1x_2, y_1y_2)\big) = x_1 \underbrace{x_2y_1}_{\text{מתחלפים}} y_2 = x_1y_1x_2y_2 = \varphi(x_1, y_1)\varphi(x_2, y_2)$$

והיא חח"ע ועל שכן:

$$\forall g \in G: \overset{\text{קיים ויחיד}}{\widehat{\exists}}\ x \in X, y \in Y: xy = g$$

$\boxed{\Rightarrow}$

אם $\varphi: G \cong X \times Y$ נגדיר $X' = \varphi^{-1}\big(X \times \{1_y\}\big), Y' = \varphi^{-1}(\{1_X\} \times Y)$.

כיוון φ^{-1} איזו' אזי $X', Y' \leq G$. צ"ל G מכפלה ישרה פנימית של X', Y'.

אכן, כיוון שφ^{-1} איזו', לכל $g \in G$ קיים מקור יחיד (x, y). ומתקיים:

$$g = \varphi^{-1}(x, y) = \varphi^{-1}\big((x, 1_Y)(1_x, y)\big) = \underbrace{\varphi^{-1}(x, 1_Y)}_{\in X'}\underbrace{\varphi^{-1}(1_x, y)}_{\in Y'} = \varphi^{-1}(1_X, y)\varphi^{-1}(x, 1_Y)$$

דוגמא

$$U_8 = (\{1,3,5,7\}, *\ mod\ 8)$$

$$U_8 =< 3,5 >=< 5 >\times< 3 >\cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

כל הזכויות שמורות לבנימין לוין ©

משפט פיצול חבורות

תהא G חבורה עם תתי חבורות X,Y כך ש:

א) $X, Y \lhd G$
ב) $X \cap Y = \{e\}$
ג) $G = XY$

אזי:

$$G \cong X \times Y$$

הוכחה

מתוך $G \lhd X$ נובע בפרט:

$$\forall y \in Y, x \in X: yxy^{-1} \in X$$

ולכן גם $yxy^{-1}x^{-1} \in X$

מתוך $G \lhd Y$ נובע בפרט:

$$\forall y \in Y, x \in X: xy^{-1}x^{-1} \in Y$$

ולכן גם $yxy^{-1}x^{-1} \in Y$

$$yxy^{-1}x^{-1} \in X \cap Y = \{e\} \Rightarrow yxy^{-1}x^{-1} = e \Rightarrow yx = xy$$

זה נכון לכל x, y.

כעת כמו מקודם נוכל להגדיר $\varphi: X \times Y \to XY = G$ וראינו שהיא הומו' ואיזו' ולכן $X \times Y \cong G$

הגדרה

תהא חבורה G עם ת"ח X, Y כך ש:

א) $X \lhd G, Y \leq G$
ב) $X \cap B = \{e\}$
ג) $G = XY$

אזי נאמר כי G היא מכפלה חצי ישרה של X וY ונסמן

$$X \rtimes Y$$

דוגמא

1) $D_3 \cong < a > \rtimes < b >$
2) חבורת Heitenberg. $H = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \right\}$

$$\mathrm{X} = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\}, Y = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \right\}$$

הראו בבית כי $H = \ltimes Y$.

כל הזכויות שמורות לבנימין לוין ©

בחבורה אבלית נהוגה כתיבה חיבורית: במקום x^m כותבים mx.

אם $A =< x_1, \dots, x_k >$ הכוונה $m_1 \in \mathbb{Z}$ $\forall x \in A : x = \sum_{i-1}^{k} m_i x_i$

במכפלה ישרה במקום $A \times B$ כותבים $A \oplus B$ וזה אומר $A \cap B = \{0\}$.

מיון חבורות אבליות נוצרות סופית

למה

תהא A אבלית נוצרת סופית ע"י $\{x_i\}_{i=1}^{k}$. אזי לכל קבוצה של מקדמים טבעיים(או אפס) $\{c_i\}_{i=1}^{k}$ כך ש$\gcd(c_!, \dots, c_k) = 1$ קיימת קבוצה יוצרת $\{y_i\}_{i=1}^{k}$ כך ש$y_1 = c_1x_1 + \cdots + c_kx_k$.

הוכחה

נוכיח ע"י אינדוקציה שלמה על $s = c_1 + \cdots + c_k$.

אם s=1 אזי $k = 1, y = x_1$. נניח נכונות הטענה לכל $m < s$ עבור $s > 1$ כלשהו.

נוכיח עבור s, אז בהכרח $k \geq 2$. נניח $c_1 \geq c_2$ ונקבל $\{x_1, x_1 + x_2, x_3, \dots, x_k\}$.

$$\gcd(c_1 - c_2, c_2, \dots, c_k) = 1$$

$$(c_1 - c_2) + c_2 + \cdots + c_k < s$$

מכאן ע"פ הנחת האינדוקציה קיימת קבוצה $\{y_i\}$ כך ש:

$$y_1 = (c_1 - c_2)x_1 + c_2(x_1 + x_2) + \cdots + c_kx_k = c_1x_1 + c_2x_2 + \cdots + c_kx_k$$

משפט

כל חבורה אבלית נוצרת סופית היא מכפלה ישרה של חבורות ציקליות.

הוכחה (לא יהיה במבחן)

נוכיח ע"י אינדוקציה שלמה על הדרגה k של החבורה A.

אם $k = 1$ סיימנו. אחרת נניח כי $\{x_i\}_{i=1}^{k}$ יוצרים את A.

מכל קבוצות היוצרים האפשריות בגודל k נבחר אחד כזו שx_1 הוא בעל סדר מינימלי. נרצה להראות ש:

$$A =< x_1 > \oplus < x_2, \dots, x_k >$$

נניח בשלילה שלא.כלומר קיים איבר שונה מאפס בחיתוך, קרי קיימת קומבינציה

$m_1x_1 + \cdots + m_kx_k = 0$ עם $m_1x_1 \neq 0$. כלומר $m_1 < o(x_1)$.

ניתן להניח כי כל הm_i אי שליליים. נסמן

$$d = \gcd(m_1, \dots, m_k)$$

$$c_i := \frac{m_i}{d}$$

$$\gcd(c_1, \dots, c_k)$$

ע"פ הלמה הנ"ל קיימת קבוצת יוצרים $\{y_i\}$ כך ש $y_1 = c_1x_1 + \cdots c_kx_k$

$$dy_1 = m_1x_1 + \cdots + m_kx_k = 0$$

כל הזכויות שמורות לבנימין לוין ©

כלומר $o(x_1) \le m_1 \le d \le o(y_1)$ בסתירה לאיך בחרנו את $\{x_i\}$ (x_1 בעל סדר מינימלי).

מסקנה

A אבלית נוצרת סופית.

$$A \cong \underbrace{\mathbb{Z}^r}_{Free} \oplus \underbrace{\mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_k}}_{\text{פיתול } torsion}$$

$rank(A) = r$ (זו לא הדרגה שדיברנו עליה!!!).

הגדרה

חבורה שהסדר שלה הוא חזקה של מס' ראשוני p נקראת חבורת-p.

למשל $\mathbb{Z}_8$ הוא חבורת-2.

לפי משפט שהראינו כל חבורה אבלית מסדר p^r איזומורפית לסכום ישר של תת חבורות-p צקליות (לגראנז').

דוגמא

$$|A| = p^2 \Rightarrow \begin{cases} A \cong \mathbb{Z}_{p^2} \\ \mathbb{Z}_p \oplus \mathbb{Z}_p \end{cases}$$

$$|A| = p^3 \Rightarrow \begin{cases} A \cong \mathbb{Z}_{p^3} \\ \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \\ \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \end{cases}$$

סימון

עבור מספר טבעי r, נסמן ב$\rho(r)$ את מס' הסדרות הסופיות הלא עולות של מספרים טבעיים כולל אפס $(r_1, \dots, r_k)$ כך ש$\sum_{i=1}^{k} r_i = r$

מסקנה

מס' החבורות האבליות הלא איזו' מסדר p^r הוא $\rho(p)$.

דוגמא

$$\begin{array}{ll} \rho(1) = 1 & \\ \rho(2) = 2 & (2,0), (1,1) \\ \rho(3) = 3 & (3,0,0), (2,1,0), (1,1,1) \\ \rho(5) = 7 & (5), (4,1), (3,2), (3,1,1), (2,2,1), (2,1,1,1), (1,1,1,1,1) \end{array}$$

אקספוננט של חבורה

הגדרה

האקספוננט של חבורה G הוא המספר הטבעי הקטן ביותר m כך ש

$$\forall g \in G : g^m = e$$

$$\exp(\mathbb{Z}_n \oplus \mathbb{Z}_m) = [n, m]$$

$$\exp(S_n) = [1,2,3 \dots, n]$$
$$\sigma^m = (\,)^m \dots (\,)^m$$

כל הזכויות שמורות לבנימין לוין ©

הרצאה 10

מיון חבורות אבליות

טענה

תהא G חבורה אבלית מסדר nm כאשר $(n,m)=1$, אזי

$$G = mG \oplus nG$$

הוכחה

א. $mG, nG \lhd G$

ב. $\forall mg_1, ng_2 : mg_1 + ng_2 = ng_2 + mg_1$

ג. $\forall x \in mG \cap nG : x = mg_1 = ng_2 \Rightarrow nx = mx = 0 \Rightarrow o(x)|_{n,m} \Rightarrow \ o(x)|_{(n,m)=1} \Rightarrow x = 0$

ד. צריך להראות כי $G = mG + nG$ אבל $nG + mG = (n,m)G = 1G = g$

הערה

$$mG = \{x = mg : g \in G\} = \{x \in G : nx = 0\} = \{x \in G : o(x)|_n\} =: G_n$$

מסקנה

אם $G = P_1 + P_2$ אבלית באשר $(|P_1|, |P_2|) = (m,n) = 1$, אזי $G = P_1 \oplus P_2$.

הוכחה

$i = 1,2$, $P_i \subseteq G_{|P_i|}$ לכן: $P_1 \oplus P_2 \le G$ אבל: $|P_1 \oplus P_2| = |G| = |P_1| \cdot |P_2|$ לכן: $P_1 \oplus P_2 = G$.

באופן כללי, אם G חבורה אבלית מסדר n עם פירוק למספרים ראשוניים:

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

אנו נראה בהמשך כי לכל $1 \le i \le k$ בהכרח קיימת ל-G ת"ח מסדר $p_i^{\alpha_1}$. ת"ח כזאת נקראת p_i-סילו (על שם Sylow).

מסקנה

אם G חבורה אבלית מסדר n כלשהו, אז היא שווה למכפלה ישרה (פנימית) של ת"ח סילו שלה..

$$G = \prod_{i=1}^{k} P_i \Rightarrow G = \bigoplus_{i=1}^{k} P_k = P_1 \oplus \ldots \oplus P_k$$

כל הזכויות שמורות לבנימין לוין ©

פעולות של חבורות על קבוצות

הגדרה

פעולה (שמאלית) של חבורה G על קבוצה לא ריקה X היא ההעתקה $G \times X \to X : (g, x) \mapsto g * x$

כאשר הפעולה * מקיימת את התכונות הבאות:

1) $\forall x \in X : 1 * x = x$
2) $\forall x \in X, g_1, g_2 \in G : (g_1 g_2) * x = g_1 * (g_2 * x)$

הגדרה

תהא חבורה G הפועלת על קבוצה X, נגדיר יחס על איברי X:

$$x \sim y \Leftrightarrow \exists g \in G : y = g * x$$

טענה

היחס שהגדרנו הוא יחס שקילות

הוכחה

$$x = 1 * x \Rightarrow x \sim x$$

$$x \sim y \Rightarrow \exists g \in G : x = g * y \Rightarrow g^{-1} * x = g^{-1} * (g * y) = (g^{-1} g) * y = 1 * y = y \Rightarrow y \sim x$$

$$x \sim y \wedge y \sim z \Rightarrow \exists g_1, g_2 \in G : x = g_1 y \wedge y = g_2 z \Rightarrow x = g_1 * (g_2 * z) \Rightarrow (g_1 * g_2) * z \Rightarrow x \sim z$$

מסקנה

X הוא איחוד זר של מחלקות שקילות. כל מחלקת שקילות נקראת מסלול (Orbit).

דוגמא

בהינתן חבורה G, פעולת <u>ההצמדה</u>, היא פעולה של החבורה על עצמה $G \times G \to G : (g_1, g_2) \mapsto g_1 g_2 g^{-1}$

נבדוק שהפעולה מוגדרת היטב

1) $\forall g \in G : 1 * g = 1 g 1^{-1} = g$
2) $\forall g_1, g_2 \in G : (g_1 g_2) * x = g_1 \underbrace{g_2 x g_2^{-1}} g_1^{-1} = g_1 * (g_2 x)$

תחת פעולת ההצמדה של G על עצמה, המסלולים שנוצרים נקראים מחלקות צמידות.

משפט

$\sigma, \tau \in S_n \Leftrightarrow$ הן מאותו טיפוס הן צמודות

הוכחה

הוכחנו ש $\tau \sigma \tau^{-1}$ יש את אותו טיפוס כמו של σ. צ"ל שאם σ, τ מאותו טיפוס אז הן בהכרח צמודות.

נמצא γ כך ש: $\tau = \gamma \sigma \gamma^{-1}$.

נניח: $\sigma = (a_{11} \dots a_{1r_1}) \dots (a_{k1} \dots a_{kr_k}), \tau = (b_{11} \dots b_{1r_1}) \dots (b_{k1} \dots b_{kr_k})$

נגדיר $\gamma = \begin{pmatrix} a_{11} \dots a_{1r_1} \dots a_{k1} \dots a_{kr_k} \\ b_{11} \dots br_{1r_1} \dots b_{k1} \dots b_{br_k} \end{pmatrix}$. ע"פ טענה שהוכחנו $\gamma \sigma \gamma^{-1} = (\gamma(a_{11}) \dots \gamma(a_{kr_k})) = \tau$

כל הזכויות שמורות לבנימין לוין ©

דוגמא

מצא γ כך ש-$\gamma(1\ 2\ 3) = (3\ 4\ 5)\gamma$

פתרון

$$\gamma = \begin{pmatrix} 1\ 2\ 3\ 4\ 5 \\ 3\ 4\ 5\ 2\ 1 \end{pmatrix} \Rightarrow \gamma(1\ 2\ 3) = (1\ 4\ 2\ 5) = (3\ 4\ 5)\gamma$$

תרגיל

כמה מחלקות שקילות יש ב-S_4, A_4?

פתרון

ב-S_n מספר הטיפוסים הוא כמספר מחלקות השקילות ולכן ב-S_4 מס' מחלקות השקילות הוא $\rho(4) = 5$

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

ב-S_4 $(1\ 3\ 2) \sim (1\ 2\ 3)$ אבל ב-A_4 $(1\ 3\ 2) \nsim (1\ 2\ 3)$ שכן המצמיד $(2{,}3) \notin A_4$

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

(3 1)

(1 2 3)
(1 4 2)
(1 3 4)
(2 4 3)

(1 3 2)
(1 2 4)
(1 4 3)
(2 3 5)

(1 1 1 1)

(2 2)

כמה מחלקות שקילות יש ב-A_4? תשובה 4.

מי שלא הבין (אהמ אריאל) שיעשה בבית עבור A_6

הגדרה

תהא G חבורה הפועלת על קבוצה X, <u>המייצב</u> (stabilizer) של $x \in X$ הוא הקבוצה:

$$Stb(x) = \{g \in G : g * x = x\}$$

טענה

$$\forall x \in X : Stb(x) \leq G$$

הוכחה

א) $1 * x = x \Rightarrow 1 \in Stb(x)$

ב) $g \in Stb(G) \Rightarrow g * x = x \Rightarrow g^{-1} * x = g^{-1} * (g * x) = (g^{-1}g) * x = 1 * x = x \Rightarrow g^{-1} \in Std(x)$

ג) $\forall g_1, g_2 \in Stb(X) : (g_1 g_2) * x = g_1 * (g_2 * x) = g_1 * x = x \Rightarrow g_1 g_2 \in Stb(x)$

כל הזכויות שמורות לבנימין לוין ©

משפט

תהא G חבורה הפועלת על X, אזי

$$\forall x \in X : |G * x| = [G: Std(x)]$$

הוכחה

$$\forall x \in X : \varphi: G * x \to G/_{Stb(x)}, \quad g * x \mapsto gStb(x)$$

נראה שההעתקה מוגדרת היטב

$$g_1 * x = g_2 * x \Rightarrow (g_2^{-1}g_1) * x = x \Rightarrow g_2^{-1}g_1 \in Stb(x) \Rightarrow g_2^{-1}g_1Stb(x) = Stb(x)$$
$$\Rightarrow g_1Stb(x) = g_2Stb(x)$$

נראה שφ חח"ע:

$$g_1Stb(x) = g_2Stb(x) \Rightarrow (g_2^{-1}g_1)Stb(x) \Rightarrow (g_2^{-1}g_1) * x = x \Rightarrow g_1 * x = g_2 * x$$

על ברור, לכל $gStb(x)$ המקור הוא $g * x$.

דוגמא

$$\sigma = \begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8 \\ 3\ 6\ 5\ 8\ 1\ 2\ 7\ 4 \end{pmatrix} \in S_8, X = \{i\}_{i=1}^{8}$$

מצא מסלולים ומייצבים שנוצרים מהפעולה $G =< \sigma >$ על X המוגדרת ע"י $\sigma^i * x = \sigma^i(x)$

פתרון

$\sigma = (1\ 3\ 5)(2\ 6)(4\ 8)(7)$, $o(\sigma) = [3,2] = 6$. $G = \{\sigma^i\}_{i=0}^{5}$.

המסלולים שנוצרים הם $\{1,3,5\}, \{2,6\}, \{4,8\}, \{7\}$

$$Stb(1) = \{1, \sigma^3\} = Stb(3) = Stb(5)$$
$$Stb(2) = \{1, \sigma^2, \sigma^4\} = Stb(6) = Stb(4) = Stb(8)$$

כל הזכויות שמורות לבנימין לוין ©

הרצאה 11

נוסחת המחלקה

תהא G חבורה סופית, אזי:

$$|G| = |Z(G)| + \sum_{\substack{x\ represent \\ \notin Z(G)}} \frac{|G|}{|C(x)|}$$

הוכחה

נתייחס לפעולת הצמדה של G לעצמה

$$\forall x \in G : Stb(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = gx\} = C(x)$$

$$\forall x \in G : |G * x| = [G: stb(x)] = \frac{|G|}{|C(x)|}$$

G איחוד זר של מחלקות צמידות, ולכן

$$|G| = \sum_{x\ rep} |G * x| = \sum_{x\ rep} \frac{|G|}{|C(x)|} \underset{\text{במרכז כל איבר הוא מחלקת צמידות של עצמו כלומר באורך1}}{\overset{ש}{=}} |Z(G)| + \sum_{\substack{x\ rep \\ \neq Z(G)}} \frac{|G|}{|C(x)|}$$

תוצאה

תהא G חבורת p, כלומר $|G| = p^n$ כאשר p ראשוני,n טבעי. אזי $Z(G) \neq \{e\}$

הוכחה

ע"י נוסחת המחלקה:

$$|Z(G)| = |G| - \sum_{\substack{x\ rep \\ \notin Z(G)}} \frac{|G|}{|C(x)|} = p^n - \sum p^{r_i > 0}$$

כלומר $|Z(G)|$ $p|$ולכן לא טריוויאלי.

$$x \notin Z(G): |C(x)| < |G| \Rightarrow r_i > 0$$

תוצאה

תהא G חבורה מסדר p^2 עבור p ראשוני, אז בהכרח G אבלית.

הוכחה

לפי מה שהראינו $Z(G) \neq \{e\}$ ולכן ע"פ לגראנז':

$|Z(G)| \in \{p, p^2\}$. G אבלית $\Leftrightarrow |Z(G)| = p^2$.

כל הזכויות שמורות לבנימין לוין ©

נניח בשלילה $|Z(G)| = p$. אזי בהכרח $\left|G/_{Z(G)}\right| = p$ וזה לא יתכן, מכיוון:

$$e \neq a \in Z(G) \Rightarrow < a >= Z(G)$$

$$b \in G - Z(G) : o(b) \in \{p, p^2\}$$

אם $o(b) = p^2$ אזי G צקלית בסתירה להנחה, לכן נניח $o(b) = p$ ואז $< a, b >$ צקלית.

$< a, b >$ אבלית שכן $a \in Z(G)$ ולכן בפרט $ab = ba$. $Z(G) \subset < a, b >$ ולכן $G = < a, b >$ אבלית, בסתירה.

הגדרה

תהא G חבורה פועלת על קבוצה X, קבוצת נק' השבת של $g \in G$ היא:

$$X_g = \{x \in X : g * x = x\}$$

משפט (למת) Burnside

תהא G חבורה סופית הפועלת על קבוצה סופית X. מספר המסלולים שG יוצרת ב-X הוא

$$k = \frac{1}{|G|}\sum_{g \in G}|X_g|$$

הוכחה

הרעיון הוא לבנות "טבלת נקודות שבת" ולמלא אותה באמצעות הפונקציה:

$$T(g,x) = \begin{cases} 0 & g * x \neq x \\ 1 & g * x = x \end{cases}$$

לדוגמא:

$G \backslash X$	x_1	x_2	…	…	…	x_m
g_1	1		1			1
g_2		1				1
…	0	0				0
…						
…	1	0				0
g_l	1	0				1

נספור את כל ה-1 בטבלה, לא משנה לפי עמודות או שורות.

כל הזכויות שמורות לבנימין לוין ©

$$\underbrace{\sum_{g\in G}|X_g|}_{\text{סך נקודות השבת}} = \sum_{x\in X}|Stb(x)| = \sum_{i=1}^{k}\sum_{x\in G*x_i}|Stb(x_i)| = \sum_{i=1}^{k}|G*x_i|\frac{|G|}{|G*x_i|} = \sum_{i=1}^{k}|G| = |G|k$$

תרגיל

שני לוחות בגודל 3×3 משבצות, יחשבו שקולים אם ניתן להגיע לשני ע"י סיבוב, חשב כמה לוחות שונים לא שקולים קיימים, אם ניתן לצבוע כל משבצת באחד משלושה צבעים.

פתרון

כל משבצת ניתנת לצביעה ע"י אחד מ-3 צבעים, ולכן נגדיר את מרחב הפעולה:

$$X = \{f:(1,2,\dots,9)\to(b,g,r)\}$$

החבורה $G =< \sigma >$ פועלת על X כאשר:

$$\sigma = \begin{pmatrix}1&2&3&4&5&6&7&8&9\\3&6&9&2&5&8&1&4&7\end{pmatrix} = (1\ 3\ 9\ 7)(2\ 6\ 8\ 4)(5)$$

$$o(\sigma) = [4,1] = 4$$

נחשב את קבוצת נקודות השבת:

$$\sigma^2 = (1\ 9)(3\ 7)(2\ 8)(6\ 5)(5)$$
$$\sigma^3 = (7\ 9\ 3\ 1)(4\ 8\ 6\ 2)(5)$$

$g\backslash X_G$	$\|X_g\|$
id	3^9
σ,σ^3	3^3
σ^2	3^5

$$k = \frac{1}{4}(3^9 + 3^2 * 2 + 3^5) = 4995$$

הערה

אם היו אומרים לנו שיש גם ששקילות נוצרת גם ע"י שיקוף, אז היינו לוקחים את D_4 שתפעל על X.

כל הזכויות שמורות לבנימין לוין ©

תזכורת

G חבורה אבלית מסדר nm כאשר $(n,m)=1$, אזי:

$$G = nG \oplus mG = G_m \oplus G_n = \{g \in G : o(g)|m) \oplus \{g \in G : o(g)|n)$$

ולכן אם $G = P_1 + P_2$ אבלית כאשר $(|P_1|,|P_2|)=1$ אזי $P_1 \oplus P_2 = G$

משפטי סילו (Sylow)

טענה

תהא G חבורה אבלית סופית כך ש $p \mid |G|$, p ראשוני, אזי קיים ב-G איבר מסדר p.

הוכחה

נכתוב $|G| = p^r m$ כאשר $(p,m)=1$ ונקבל $G \cong P \oplus M$ כאשר P סכום ישר של ת"ח צקליות מסדר p^{r_i}.

אם כן יוצר a של $\mathrm{H}_i \cong \mathbb{Z}_{p^{r_i}} \leq P$ ונקבל

$$o\left(a^{p^{r_i-1}}\right) = \frac{p^{r_i}}{(p^{r_i-1}, p^{r_i})} = \frac{p^{r_i}}{p^{r_i-1}} = p$$

משפט סילו 1:

נראה באינדוקציה על $|G|$.

בדיקת התחלה: $|G| = p$ אז G עצמה p-סילו.

הנחה: הטענה נכונה עבור כל G מסדר $|G| < p^n m$

צ"ל: נכונה עבור $|G| = p^n m$

ישנם שני ממקרים בלבד:

א) קיימת ת"ח $H \leq G$ כך ש: $|H| = p^n m_1$, $m_1 < m$. לפי הנחת האינדוקציה יש בתוך H ת"ח p-סילו ב-G.
ב) לא קיימת ת"ח $H \leq G$ מסדר $p^n m_1$, $m_1 < m$.
כלומר כל ת"ח היא מסדר $p^{n_1<n} m$ באופן כללי יתכן גם: $m_1 \leq m$

$$\forall H \leq G : p|[G:H] = \frac{|G|}{|H|}$$

מכאן ע"פ נוסחת המחלקה:

$$p^n m = \underbrace{|G|}_{\text{מתחלק ב}p} = |Z(G)| + \underbrace{\sum_{\substack{x\ rep \\ \notin Z(G)}} [G:C(x)]}_{\text{מתחלק ב}p} \Rightarrow p|\,|Z(G)| \Rightarrow Z(G) \neq \{e\}$$

כעת כיוון $Z(G)$ אבלית ו $p \mid |Z(G)|$ קיים איבר מסדר p (טענה קודמת),נשים לב כי:

$$(a \in Z(G))\ \ H =< a > \lhd G$$

$$|G/_H| = \frac{p^n m}{p} = p^{n-1} m$$

ע"פ הנחת האינדוקציה, יש ל $G/_H$ תת-חבורה p-סילו, כלומר $\exists A \leq G/_H$ כך ש: $|A| = p^{n-1}$

כל הזכויות שמורות לבנימין לוין ©

$$H \lhd G \Rightarrow \text{קיים אפי}: \nu: G \to G/_H\ , \qquad g \mapsto gH$$

נסמן: $A^* = \nu^{-1}(A) \le G$. נמצם את ν ל:

$$\nu_0: A^* \to A$$

$$e \in A \Rightarrow \ker(\nu) = \ker(\nu_0) = H$$

לפי משפט איזו' 1:

$$A^*/_{\ker(\nu_0)} = A^*/_H \cong A$$

$$|A^*| = |H||A| = pp^{n-1} = p^n$$

הערה

באותו אופן אפשר להראות כי לכל חבורת pמסדר p^n, יש ת"ח מסדר p^k לכל $1 \le k \le n$.

הוכחה

נניח באינדוקציה שנכון לכל $|G| \le p^{n-1}$

צ"ל עבור $|G| = p^n$ (ההתחלה ברורה).

$$p \mid |Z(G)|$$

ולכן בתוך $Z(G)$ כחבורה אבלית יש איבר a מסדר p , נתייחס ל$G \rhd H \ge a >$ ולהעתקה $\nu: G \to G/_H$.

ע"פ הנחת האינדוקציה יש ב$G/_H$ (מסדר p^{k-1}) כל ת"ח מסדר p^k, נניח $|A| = p^k$ ונסמן $\nu^{-1}(A) = A^* \le G$. ונצמצם את ν: $\nu_0: A^* \to A$ ומכאן ע"י איזו' 1.

תוצאה – משפט קושי

תהא G כך ש: $p| \ |G|$ ראשוני כלשהו, אזי קיים ב-G איבר מסדר p.

הוכחה

נרשום $|G| = p^n m$ כאשר $(n, m) = 1$ ונקבל ע"פ סילו 1 שקיימת ת"ח מסדר p^n ולכן יש בה ת"ח מסדר $p^{1 \le k \le n}$ בפרט עבור $k = 1$.

כל הזכויות שמורות לבנימין לוין ©

הרצאה 12

משפטי סילו'

הבהרה לגבי מה שלמדנו בפעם שעברה

אמרנו לפי משפט קושי, אם $p\mid |G|$ אז בהכרח קיים איבר מסדר p בתוך G.

אמרנו שזה למעשה מקרה פרטי של טענה כללית יותר שאם $p^k \mid |G|$ אז יש ת"ח מסדר p^k ב-G.

הוכחנו ע"י:

1) משפט סילו 1 אומר שקיים ת"ח p-סילו (חזקה מקסימלית)
2) בתוך כל חבורת pיש ת"ח מסדר p^k לכל $1 \le k \le n$.

<u>אבל זה לא אומר שיש איבר מסדר</u> p^k למשל ב$\mathbb{Z}_p^2$ יש ת"ח מסדר p^2 אבל אין איבר מסדר זה!

כשמדובר בp^1 זה כן שקול כי $\mathbb{Z}_p$ צקלית בהכרח.

משפט

חבורה G אבלית סופית איזומורפית לסכום ישר של חבורות הp-סילו שלה.

הוכחה

$$|G| = \prod_{i=1}^{k} p_i^{\alpha_i}$$

נסיק ע"פ טענה קודמת כי:

$$G = \overbrace{G_{p_1^{\alpha_1}}}^{P_1=\{g\in G: o(g)\mid p_1^{\alpha_1}\}} \oplus \dots \oplus G_{p_k^{\alpha_k}}$$

ע"פ משפט סילו 1 לכל P_i קיימת ת"ח p_i-סילו וזו מקיימת $P_i \le G_{p_i^{\alpha_i}}$. מכאן שהחיתוך של כל שני ת"ח p_i-סילו הוא טריוויאלי, יחד עם האבליות נסיק (תנאי משפט פיצול חבורות) כי:

$$\bigoplus_i P_i \le G$$

אבל $|\bigoplus_i P_i| = |G|$ ולכן $G = \bigoplus_i P_i$

מסקנה

בהינתן מספר טבעי $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ מס' החבורות האבליות הלא איזומורפיות הוא:

$$\rho(\alpha_1) \dots \rho(\alpha_k)$$

הידעתם:

פרופ' רואן הוא זה שהגה את התוכנית שלכם (של התיכוניסטים).

הסבר

ע"פ המשפט האחרון G הוא סכום ישר של ת"ח p-סילו שלה.

<u>בתוך</u> כל חבורת p-סילו מס' האפשרויות לפצל לסכום ישר של ת"ח צקליות הוא כמספר הטיפוסים של החזקה של p, כלומר $\rho(\alpha)$ (ולא חשוב מהו p).

דוגמא

כמה חבורות אבליות לא איזו' יש מסדר 18,000?

$$1800 = 2^4 3^3 5^3$$

$$\rho(4)\rho(2)\rho(3) = 5 * 2 * 3 = 30$$

הערה

לפרופסור רואן יש משקפי שמש גדולות והוא נסחב עם צ'לו

הגדרה

תהא G חבורה הפועלת על חבורה X

- נקודת שבת היא איבר $x \in X$ כל ש $\forall g \in G: g * x = x$
- קבוצת נקודות השבת היא

$$\underbrace{F}_{Fixed} = \left\{ x \in X : \underbrace{G * x = x}_{\text{בעלות מסלול מאורך } 1} \right\}$$

בפרט, אם G, X סופיות, נוכל לנסח את נוסחת המחלקה הכללית:

$$|X| = |F| + \sum_{\substack{x\ rep \\ \notin F}} |G * x| = |F| + \sum_{\substack{x\ rep \\ \notin F}} [G: Stb(x)]$$

X אחוד זר של מסלולים (המרכז מקרה פרטי כשהפעולה היא הצמדה!).

מליצה

אנלוגיה לחיים: אתם לא מכירים אנשים שאף אחד לא יוציא אותם מהבית? הם כמו נקודת שבת.

מקרה כללי: אפשר ללמוד על בני אדם ע"י שבודקים לאן סיטואציות חיצוניות בחיים לוקחות אותם. מתמטיקה≡חיים.

הגדרה

פעולה נקראת טרנזטיבית (או הומוגנית) אם היא יוצרת רק מסלול אחד.

דוגמא

S_n פועלת על $X = \{1, \dots, n\}$

$\mathbb{Z}_n$ פועלת על עצמה באמצעות חיבור $\forall x, y \in X : \exists g: x = g * y$

למשל $X \ni 1$ יכול להגיע ל$s \in X$ ע"י $5 = (1,5) * 1$

כל הזכויות שמורות לבנימין לוין ©

משפט סילו 2:

תחת התנאים של משפט סילו 1 $((p,m)=1, |G|=p^n m)$:

א) כל ת"ח $H\le G$ מסדר p^k כאשר $1\le k\le n$ מוכלת באיזשהי ת"ח p-סילו.
ב) כל שני ת"ח p-סילו הם צמודות.

הוכחה

תהא $H\le G$ עם $|H|=p^k$.

קבוצת ת"ח p- סילו= Syl_p

ע"פ משפט סילו 1:

$$Syl_p\neq\phi$$

תהא $P\in Syl_p$ ונגדיר פעולה $H\times G/_p\to G/_p$ ע"י $(h,xP)\mapsto hxP$

פעולת H מחלקת את איברי $G/_P$ למסלולים זרים. נזכר כי H היא חבורת p, ולכן:

$$m=|G/_P|=\sum_{x\,rep}|H*xp|=\sum_{x\,rep}[H:Stb(xp)]=\sum_{x\,rep}p^{r_x}$$

<u>אבל</u> $(m,p)=1$ ולכן בהכרח לפחות $r_x=0$ עבור x אחד, כלומר קיימת לפחות נקודת שבת אחת, כלומר קיים xP כל שלכל $h\in H$

$$hxP=xP\Leftrightarrow x^{-1}hxP=x^{-1}xP=P\Leftrightarrow x^{-1}hx\in P\Leftrightarrow h\in xPx^{-1}\Rightarrow H\subseteq xPx^{-1}$$

$$|xPx^{-1}|=|P|=p^n$$

ב)

ע"פ סעיף קודם בפרט עבור $P_1\in SyL_p(G)$ (מסדר p^n) קיימת $P_2\in SyL_p(G)$ כך ש: $P_1\subseteq xP_2x^{-1}$ עבור x כלשהו.

אבל $|xP_2x^{-1}|=|P_2|=p^n=|P_1|$ ולכן $P_1=xP_2x^{-1}$.

ההצמדה לא משנה את גודל הקבוצה!.

לכל $|H|=p^k$ יכולנו להתחיל עם $P\in SyL_p(G)$

$H\times G/_P$ אתה יכול להתחיל עם כל P שאתה רוצה ותקבל

$$H\subseteq xPx^{-1}$$

תוצאה

$$Syl_p(G)=\{P\}\Leftrightarrow P\lhd G$$

הוכחה

$$Syl_p(G)=\{P\}\Leftrightarrow\forall x\in G: xPx^{-1}=P\Leftrightarrow\forall x\in G: xP=Px$$

כל הזכויות שמורות לבנימין לוין ©

דוגמא

$$\left|Syl_p(G)\right| \coloneqq n_p$$

ב D_3 : $|D_3| = 6 = 2 * 3$

$n_2 = 3$(3 סילו), $n_3 = 1$

$$< a > \lhd D_3$$

$$|D_3| = 1 + 1(3-1) + 3(2-1) = 6$$

e נמצא בכל ת"ח ולכן סוכמים אותו רק פעם אחת.

הבהרה (משאלה של סטודנט)

בחבורה אבלית זה לא שיש רק ת"ח p-סילו אחת, אלא שלכל p יש ת"ח p-סילו אחת.

הגדרה

תהא G חבורה ו-$H \le G$. הנורמילטור של H ב-G הוא:

$$N_G(H) \coloneqq \{g \in G : gH = Hg\}$$

טענה

$$\mathrm{N_G}(H) \le G$$

הוכחה

1. $e \in N_G(H)$
2. $\forall x, y \in N_G(H) : xy^{-1}H = xHy^{-1} = Hxy^{-1} \Rightarrow xy^{-1} \in N_G(H)$

משפט סילו 3

עבור חבורה G נסמן $n_p = |Syl_p(G)|$

א) $n_p = [G:N_G(P)]$

ב) $n_p \equiv 1(mod\ p)$

ג) $n_p = (1+kp)|_m$ כאשר $k \in \mathbb{N} \cup \{0\}, (m,p) = 1, m = \frac{|G|}{p^n}$

הוכחה

א) נגדיר את הפעולה $G \times Syl_p(G) \to Syl_P(G)$ ע"י $(g,P) \mapsto g * P = gPg^{-1}$.

ע"פ משפט סילו 2 הפעולה היא הומוגנית (יש מסלול אחד).

לכן $n_p = |G * P| = [G: Stb(P)] = [G: N_G(P)]$

כי $Stb(P) = \{g \in G: gPg^{-1} = P\} = N_G(P)$

ב) תהא $P \in Syl_P(G)$ ונתייחס לצמצום של פעולת ההצמדה לפעולת P בלבד. כעת הפעולה כבר לא בהכרח הומוגנית!

$$P \times Syl_p(G) \to Syl_g(G) : (p, P_1) \mapsto pP_1p^{-1}$$

גודל כל מסלול: $\forall Q \in Syl_g(G):\ |P * Q| = [P: Stb(Q)]$ מחלק את $|P| = p^n$, כלומר אורך כל מסלול הוא מאורך 1 או חזקה של p.

ומכאן ע"פ נוסחת המחלקה הכללית:

$$|Syl_g(G)| = |X| = |F| + \sum_{\substack{Q\ rep \\ \notin F}} [P: Stb(Q)] = \frac{p^n}{p^{r<n}}$$

ונקבל כי $|F| \equiv n_p(mod\ p)$

אנו נראה כי $F = \{P\}$ (P היא נקודת השבת היחידה).

מצד אחת $P \in F$ כן $P * P = \{pPp^{-1} : p \in P\} = \{P\}$

מצד שני, יהי $Q \in Syl_g(G)$ כך ש $Q \in F$, אזי $P \le N_G(Q)$ שכן Q היא נקודת שבת תחת הצמדה של אברי P: $\forall p \in P: pQp^{-1} = Q$ ולכן $P, Q \le N_G(Q)$.

קבלנו שתי ת"ח p-סילו ב$N_G(Q)$. אבל $Q \lhd N_G(Q)$ ולכן היא היחידה, כלומר $P = Q$.

<u>מסקנה:</u>

$$|F| = 1 \Rightarrow n_p \equiv |F|(mod\ p) = 1$$

ג) ע"פ לגראנז':

$$[G:P] = \frac{|G|}{|P|} = \frac{|G|}{|N_G(p)|}\frac{|N_G(P)|}{|P|} = [G:N_G(P)][N_G(P):P]$$

$$\Rightarrow n_p|_{\frac{|G|}{|P|}=m}$$

צריך להזכיר שעפ"י סעיף א': $n_p = [G:N_G(P)]$.

כל הזכויות שמורות לבנימין לוין ©

הגדרה
חבורה נקראת פשוטה simple אם אין לה שום ת"ח נורמליות לא טריוויאלות.

דוגמאות:
$\mathbb{Z}_p$ עבור p טבעי

כל חבורה מסדר 20 אינה פשוטה,שהרי $20 = 2^2 * 5$

$$n_2 = 1 + 2k|5 \Rightarrow k = 0,1$$

$$n_5 = 1 + 5k|4 = 1 \Rightarrow H_5 \lhd G$$

כי היא 5-סילו ויחידה ולכן G לא פשוטה.

תרגיל
תהא G חבורה מסדר 30. הראה כי היא אינה פשוטה

פתרון

$$30 = 2 * 3 * 5$$

$$n_3 = 1 + 3k|10 = 1,10$$

$$n_5 = 1 + 5k|6 = 1,6$$

נניח בשלילה כי גם $n_2 = 10$ וגם $n_5 = 6$

נסכום את האיברים שאלו תורמים:

$$1 + 10(3 - 1) + 6(5 - 1) = 45 > 30$$

ולכן $n_3 = 1$ או $n_5 = 1$ ולכן G אינה פשוטה.

כל הזכויות שמורות לבנימין לוין ©

הרצאה 13: חבורות פתירות solvable

הגדרה

- חבורה G תקרא <u>פתירה</u> אם קיימת לה סדרה נורמלית שכל גורמיה אבליים, כלומר קיימים סדרה:

$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{e\}$ כך שלכל k חבורת המנה $G_k/_{G_{k+1}}$ אבלית.

- סדרה נורמלית אחת היא <u>עידון</u> של סדרה נורמלית אחרת אם היא תוצאה של הוספת ת"ח לסדרה.
- סדרה נורמלית נקראת <u>סדרת הרכב</u> אם לא ניתן לעדן אותה, כלומר שכל גורמיה פשוטים.

דוגמאות

1) כל חבורה אבלית היא פתירה. $G \rhd \{e\}$.
2) D_n פתירה: $D_n \rhd < a > \rhd \{e\}$ (הגורמים צקליים ולכן אבליים). $D_n/_{<a>} \cong \mathbb{Z}_2, < a >/_{\{e\}} \cong < a >$

סדרת ההרכב היא $D_4 \rhd < a > \rhd < a^2 > \rhd \{e\}$

3) S_4 פתירה: $S_4 \rhd A_4 \rhd V_4 \rhd \{e\}$

סדרת ההרכב $S_4 \rhd A_4 \rhd \underbrace{V_4}_{\{(1\,2)(3\,4),(1\,3)(2\,4)\}} \rhd < (1\,2)(3\,4) > \rhd \{e\}$

משפט

כל חבורת p פתירה

טענת עזר

תהא G חבורת p מסדר p^n (p ראשוני), אזי לכל $1 \le k \le n$ קיימת ת"ח נורמלית ב-G מסדר p^k.

הוכחת טענת העזר

באינדוקציה על $|G| = p^n$

<u>התחלה:</u> אם $|G| = p$ אז ניקח את G עצמה.

<u>הנחה:</u> נניח שהטענה נכונה לכל G כך ש$|G| < p^n$, צ"ל עבור $|G| = p^n$.

בחבורת p המרכז $Z(G)$ לא טריוויאלי.

כחבורה אבלית ב$Z(G)$ יש איבר a מסדר p.

נסמן $H = < a >$. כיוון ש$H \le Z(G)$, $H \lhd G$. נתבונן באפימורפיזם הטבעי $\nu: G \to G/_H, g \mapsto gH$.

ע"פ לגראנז' $|G/_H| = p^{n-1}$ ולכן עפ"י ההנחה לכל $1 \le k \le n$ קיימת ת"ח נורמלית $A \lhd G/_H$, $|A| = p^{k-1}$.

נתבונן ב$\tilde{A} = \nu^{-1}(A)$. כיוון שν הומ', $\tilde{A} \lhd G$. ע"פ משפט איזו' I: $\tilde{A}/_{H=\ker\nu} \cong A$ (גם בצמצום של ν ל$\tilde{A}$ הגרעין H נשאר).

ולכן $|\tilde{A}| = |H||A| = pp^{k-1} = p^k$ ■

הוכחת המשפט

ע"פ טענת העזר נוכל לבנות סדרה נורמלית

$$G \rhd G_1 \rhd G_2 \rhd \cdots \rhd \{e\}$$

כך שאם $|G| = p^n$ אז $|G_1| = p^{n-1}$ $|G_2| = p^{n-2}$,

ונקבל $G_k/_{G_{k+1}} \cong \mathbb{Z}_p$ ולכן צקלית ולכן אבלית.

כל הזכויות שמורות לבנימין לוין ©

טענה

A_5 אינה פתירה.

טענה

מספיק להראות כי A_5 פשוטה.

נתאר את מחלקות הצמידות של A_5. ראשית נכתוב את הטיפוסים בS_5, מתוכם נוריד את המחלקות בהם התמורות אי-זוגיות, ונבדוק פיצול אפשרי של מחלקה:

$$S_5: (5), (4\ 1), (3\ 2), (3\ 1\ 1), (2\ 2\ 1), (2\ 1\ 1\ 1), (1\ 1\ 1\ 1\ 1)$$

$$A_5: (5), (3\ 1\ 1), (2\ 2\ 1), (1\ 1\ 1\ 1\ 1)$$

Type	$(5)_1$	$(5)_2$	$(3\ 1\ 1)$	$(2\ 2\ 1)$	$(1\ 1\ 1\ 1\ 1)$
Class	$(a\ b\ c\ d\ e)$	$(a\ b\ c\ e\ d)$	$(a\ b\ c)(d)(e)$	$(a\ b)(c\ d)(e)$	$(a)(b)(c)(d)(e)$
Card	$\frac{4!}{2} = 12$	$\frac{4!}{2} = 12$	$\binom{5}{3} 2! = 20$	$\binom{5}{2}\binom{3}{2}\frac{1}{2} = 15$	1

כדי ש$H \leq A_5$ תהיה נורמלית בA_5 היא צריכה להכיל מחלקות צמידות בשלמותם שכן הן מהוות את המסלולים של פעולת ההצמדה, ולכן אם H מכילה חלקית מסלול קיימת הצמדה $ghg^1 \notin H$. (H חייבת להכיל את id)

$$|H| = 1 + c_1 12 + c_2 12 + c_3 15 + c_4 20$$

ע"פ לגראנז' $|H|| 60$. שתי האפשרויות היחידות המקיימות זאת הן $|H| = 1, |H| = 60$ ולכן A פשוטה.

מסקנה: A_5 אינה פתירה.

משפט (מיון של ת"ח של חבורה ציקליות).

תהא $G =< a >$ חבורה צקלית, אם G מסדר n אזי:

3) $H \leq G \Rightarrow |H||n$
4) לכל k טבעי, $k|n$, קיימת ת"ח יחידה $H \leq G$ כך ש$|H| = k$

אם G אינסופית הראינו כבר ש$G \cong \mathbb{Z}$ וכל ת"ח של G היא $< a^n >$

הוכחה

3) משפט לגראנז'
4) כל ת"ח של חבורה צקלית היא צקלית, כמו כן לכל $k|n$:

$$o(a^j) = k \Leftrightarrow k = \frac{n}{(j,n)} \Leftrightarrow (j,n) = \frac{n}{k}$$

בפרט עבור $j = \frac{n}{k}$ נקבל קיום של ת"ח מסדר k : $H =< a^{\frac{n}{k}} >$

באופן כללי יותר, אם $j = \frac{n}{t} t$ אז במילא $< a^j > \subseteq < a^{\frac{n}{k}} >$ ומכאן היחידות

דוגמא

תאר את כל ת"ח של $\mathbb{Z}_{70}$.

לכל מספר שמחלק את 70 קיים ת"ח אחת מסדר זה, כלומר:

$$< 1 >, < 2 >, < 5 >, < 7 >, < 10 >, < 14 >, < 35 >, < 70 >$$

כל הזכויות שמורות לבנימין לוין ©

נגזרת של חבורה

הגדרה

תהא חבורה G, לכל $a,b\in G$, הקומוטטור הוא האיבר:

$$[a,b]\coloneqq aba^{-1}b^{-1}$$

$$(ab=ba\Leftrightarrow[a,b]=e)$$

הגדרה

תהא חבורה G, חבורת הקומוטטרים של G היא ת"ח שנוצרת מהם:

$$G'=<\{[a,b]:a,b\in G\}>$$

קוראים לזה נגזרת של G

משפט

לכל חבורה G מתקיים:

א) $G'\lhd G$
ב) $G/_{G'}$ אבלית

הוכחה

א)

$$\forall g,a,b\in G:$$
$$g[a,b]g^{-1}=gaba^{-1}b^{-1}g^{-1}=\underbrace{gag^{-1}}\underbrace{gbg^{-1}}\underbrace{ga^{-1}g^{-1}}\underbrace{gb^{-1}g^{-1}}=[gag^{-1},gbg^{-1}]\in G$$

ב) צ"ל: $\forall x,y\in G:xG'yG'=yG'xG'$
מתוך הנורמליות

$$xyG'=yxG'\Leftrightarrow x^{-1}y^{-1}xyG'=G'$$

אבל $[x^{-1},y^{-1}]=x^{-1}y^{-1}xy\in G'$.

למעשה G' היא ת"ח נורמלית הקטנה ביותר כך ש: $G/_{G'}$ אבלית.

מסקנה

אם $G^{(n)}=\{e\}$ עבור $n\in\mathbb{N}$ כלשהו אסי G פתירה, גם ההיפך נכון.

דוגמאות:

1) סיבוב $<a\geq<a>=(D_3)'$ שכן $[a,b]=aba^{-1}b^{-1}=a(ab^{-1})b=aab^{-1}b=a^2=a^{-1}$
2) $(D_4)'=<a^2>$

תרגיל

הנגזרת של חבורת Heisenberg (מעל שדה F, יכול להיות גם סופי כמו $\mathbf{Z}_p$ עבור p ראשוני):

$$\left\{\begin{pmatrix}1&x&y\\0&1&z\\0&0&1\end{pmatrix}:x,y,z\in F\right\}$$

$H=\left\{\begin{pmatrix}1&0&*\\0&1&0\\0&0&1\end{pmatrix}:*\in F\right\}$ זוהי חבורה אבלית, ולכן H פתירה!

כל הזכויות שמורות לבנימין לוין ©

בס"ד

שאלה: תהא D_7 פועלת על קבוצה בת 19 איברים. האם בהכרח יש נקודת שבת ?

פתרון: לא. בנוסחת המחלקה הכללית מתאפשרת הקומבינציה הבאה של אורכי מסלולים:

$$19=|X|=|F|+\sum_{x\ rep.\notin F}|D_7*x|=|F|+\sum_{x\ rep.\notin F}\left[D_7:Stb(x)\right]=2\cdot 6+1\cdot 7$$

כלומר יתכנו 6 מסלולים באורך 2 כ"א ומסלול אחד באורך 7 ואז אין נקודות שבת: $F=\varnothing$.

למשל בצורה מפורשת: נגדיר את הפעולה של $D_7=\left\langle a,b:a^7=e,b^2=e,ab=ba^6\right\rangle$ על: $X=\{1,2,...,19\}$ ע"י:

b מזיז רק את המספרים $1\le i\le 12$ בהתאם למסלולים:

$(1 2),(3 4),(5 6),(7 8),(9\ 10),(11\ 12)$.

לעומתו a מזיז רק את המספרים $13\le i\le 19$ בהתאם למסלול: $(13\ 14\ 15\ 16\ 17\ 18\ 19)$.

קל לבדוק שההגדרה הזו מקיימת את האקסיומות של פעולה, כלומר ש:

1. $\forall i:\ \ e*i=i$
2. $\forall i,g_1,g_2\in D_7:\ \ g_1*(g_2*i)=(g_1\cdot g_2)*i$.

אלגברה מופשטת 1 – תרגול 1

שם המתרגלת לואי פולב. התרגול ינוהל דרך הmath-wiki.com. הציון הסופי יהיה מורכב מ- 90% בחינה ו10% בוחן. הבוחן יערך בערך בשבוע הרביעי. הוא יכלול תרגילים משיעורי הבית-וזו המוטיבציה להכין את ש״ב. מהתרגילים שאחרי הבוחן יורכב המבחן. חשוב מאוד להכיר את כל ההגדרות בעל פה.

תורת החבורות-הגדרות:

1. תהי S קבוצה לא ריקה. פעולה בינארית על S היא פונקציה דו מקומית * היא $*: SxS \to S$.
2. קבוצה לא ריקה אסוציאטיבית עם פעולה בינארית אסוציאטיביות נקרת אגודה (חבורה למחצה).
3. אגודה S שבה יש איבר יחידה (e) נקראת מונואיד. ז״א ש- $\forall a : e * a = a * e = a$
4. איבר a ב-S נקרא הפיך מימין אם קיים איבר b $a * b = e$.
5. איבר a ב-S נקרא הפיך אם הוא הפיך מימין וגם הפיך משמאל.
6. מבנה S עם פעולה בינארית (סימון: (S,*)) נקרא חבורה אם הוא מונואיד שבו כל איבר הפיך.
   על מנת לבדוק שמבנה כלשהו הוא חבורה יש לבדוק:
   א. סגירות הפעולה.
   ב. אסוציאטיביות.
   ג. קיום איבר יחידה.
   ד. קיום איבר נייטרלי.
   ה. קיום הופכי לכל איבר.

הערה בקשר לפעולה הבינארית: ניתן להגדיר פעולה בינארית (פ״ב) ע״י לוח כפל. למשל, אם יש לנו מבנה S={a,b} ניתן להגדיר את הפעולה משמאל. תמיד תמיד תמיד נניח שמדובר בקבוצה שאינה ריקה.

*	a	b
a	b	b
b	b	a

הפעולה אינה אסוציאטיבית שכן מתקיים

$$(a*b)*b = b*b = a$$
$$a*(b*b) = a*a = b$$

דוגמאות:

1. תהי X קבוצה כלשהו. נביט ב-$(P(X), \cap)$. יש לה סגירות ואסוציאטיביות באופן ברור, וקיים לה איבר נייטרלי שהוא X. כעת כבר יש לנו מונואיד. נבדוק אם קיים לכל איבר איבר הופכי, כדי שהוא יהפוך לחבורה. צריך להוכיח שלא קיים כזה ולכן אין היא חבורה. (בהנחה שמדובר בקבוצה לא ריקה כמובן) ולכן $(P(X), \cap)$ הוא מונואיד. (תשימו לב ש $A \cap A = A$)
2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ הן חבורות ביחס לחיבור.
3. $\mathbb{Z}_n$ ולכל $a,b \in \mathbb{Z}_n$ מגדירים פעולה מודולו n כך:
   א. $a \oplus b = \underbrace{a + b(mod(n))}_{\text{לוקחים שארית מודולו n}}$. נובע מההגדרה כי $a \equiv b$ או״א $\exists k: a - b = kn$
   ב. $a \odot b = a \cdot b\ (modn)$.

   איזה סוג של יצור הוא $(\mathbb{Z}_n, \cdot)$? ניתן לראות שהוא מונואיד, אך אינו חבורה.
4. $(M_n(\mathbb{F}), +)$ חבורה.
5. $(M_n(\mathbb{F}), \cdot)$ מונואיד, לא כל המטריצות הפיכות. (איבר יחידה זה I)

6. עבור שדה כלשהו k נסמן $k^* = k\backslash\{0\}$. נביט בk^* כמבנה כפלי. זאת חבורה.
מה קורה אם נעשה אותו דבר למבנה שהוא לא שדה? $(\mathbb{Z}_n^*,\cdot)$ יכול להיות בכלל לא מבנה אלגברי.(אם n ראשוני הוא הופך לחבורה).למשל: $\mathbb{Z}_6^*$ אינו מבנה אלגברי כי אין סגירות, לדוגמה 2 כפול 3 נותן אפס, שבכלל לא שייך לקבוצה.
7. $n\mathbb{Z} = \{na|a \in \mathbb{Z}\}$. והוא חבורה. (n טבעי)

תרגיל: האם קיים מונואיד שיש בו איבר הפיך מימין אך לא הפיך משמאל?

פתרון: $V = \mathbb{F}^N = \{(x_1, x_2, \dots .)|x_i \in \mathbb{F}\}$. נגדיר $Hom(V) = \{T: V \to V|\text{T העל}\}$. נראה ש$(Hom(V), \circ)$ מונואיד. היא אסוציאטיבית, קומוטטיבית, ואיבר היחידה היא העתקת הזהות. נביט בשני איברים במונואיד הזה: $U(x_1, x_2, \dots) = (0, x_1, x_2, \dots), D(x_1, x_2, \dots) = (x_2, x_3, \dots)$.

הבה נביט ב-$UD(x_1, x_2, \dots) = (0, x_2, x_3 \dots), DU(x_1, x_2, x_3, \dots) = (x_1, x_2, x_3, \dots)$. בעצם, D הפיך מימין, אבל לא אמרנו כלום לגבי ההפיך משמאל.

העובדה ש$\text{UD} \neq id$ לא מחייבת שD אינו הפיך משמאל . D אינו הפיך משמאל משתי סיבות.

א. אם היה לD הופכי משמאל אז זה היה U (הוכחנו בשיעור את יחידות ההופכיים במבנים אסוציאטיביים)
ב. אם D היה הפיך גם משמאל, אז הוא היה הפיך. אך D אינו הפיך מאחר ואינו חד חד ערכי שכן $\ker(D) \neq 0$. מ.ש.ל. ■.

תרגיל: $Map(X, X)$ קבוצת כל הפונקציות מX לX כאשר X קבוצה אינסופית. מיינו את ההפיכים משמאל ואת ההפיכים מימין.

פתרון:
פונקציה היא הפיכה משמאל או״א היא חח״ע. פונקציה היא הפיכה מימין או״א היא על. (הוכחנו את המשפט/ים בבדידה).

- שימו לב שתרגיל זה פותר לנו בעצם את התרגיל הקודם.

השאלה נשאלת , למה קבוצה אינסופית? כי אם זו קבוצה סופית, כל פונקציה חד חד ערכית היא גם על. ולכן, על מי שהפיך מימין הפיך גם משמאל (הפיך בכללי בצעם)

מ.ש.ל. ■.

תרגיל: האם קיימת אגודה שיש בה איבר יחידה משמאל אך אין איבר יחידה מימין?

פתרון: נתבונן באגודה $S = \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} : a, b \in R\right\}$. ביחס לכפל מטריצות, (S,·). ישנם אינסוף איברי יחידה משמאל, כי לכל x בR המטריצה $\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix}$ היא האיבר יחידה משמאל של $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ וז״א שמתקיים $\begin{pmatrix} 1 & x \\ 0 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$. אנחנו מניחים שאין איבר יחידה מימין. נניח בשלילה שיש וננסה למצוא אותו. נסמנו ב-$\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix}$.לכל $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ אמור להתקיים $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$. בפרט, נחפש הפיך ל$\begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}$. נקבל מהחישוב שx=1 וy=b ולכן האיבר יחידה תלוי ב-b בכל מטריצה ומטריצה ואינו יחיד, זה אינו ייתכן. מכאן שאין איבר יחידה מימין.

הוכחה ב׳: נניח שיש איבר יחידה מימין, ולכן בגלל שהאגודה אסוציאטיבית נקבל שכל איברי היחידה משמאל שווים אליו, ולכן כל איברי היחידה משמאל שווים, בסתירה למה שמצאנו. מ.ש.ל. ■.

תרגיל ממבחן:

א. הוכיחו כי לכל מונואיד $(X,\cdot)$ הקבוצה $P_*(X)$ (כל תת קבוצה של X חוץ מהקבוצה הריקה) מגדירה מונואיד ביחד לפעולה טבעית $\circ$: $A \circ B = \{a \cdot b \mid a \in A, b \in B\}$
ב. מה הם האיברים ההפיכים של $(P_*(X), \circ)$.

פתרון:

א. נבדוק את התנאים למונואיד:
1. נבדוק אם $(P_*(X), \circ)$ מונואיד. ראשית נראה שהיא אינה ריקה, כי {e} הנקודון של איבר היחידה שייך לה.
2. סגירות: ברור. (נובעת מהיות X מונואיד)
3. אסוציאטיבית (שוב, מהיות X מונואיד)
4. איבר נייטרלי: שוב, הנקודון $\{e\}$.

ב. מה הם האיברים ההפיכים של $(P_*(X), \circ)$?
טענה: ההפיכים הם $A=\{a\}$ כאשר a הפיכים בX. צריך להסביר למה $A = \{a_1, a_2\}$ לא הפיכה אם a_1, a_2 הפיכים? אם היא היתה הפיכה, היה קיים איבר שהפיך לשניהם (לa_2 ולa_1) ולכן נקבל ש$a_1 = a_2$.

<u>חבורת האיברים ההפיכים:</u>

בהינתן מונואיד $(M,\cdot)$ נסמן ב$Gr(M)$ את אוסף האיברים ההפיכים של M.

דוגמה (1): $\mathrm{G}r\big(M_n(\mathbb{F})\big) = (GLn(\mathbb{F}),\cdot)$

דוגמה (2): $\mathrm{G}r(Z,\cdot) = \{1,-1\}$

דוגמה (3): $\mathrm{G}r(\mathbb{Z},+) = \mathbb{Z}$ ולכן היא חבורה.

<u>הגדרה</u>: נאמר ש* היא פעולה אבלית אם היא קומוטטיבית.

$(S,*)$ חבורה אבלית אם $\forall \mathrm{a},\mathrm{b} \in \mathrm{S} : \mathrm{a} * \mathrm{b} = \mathrm{b} * \mathrm{a}$.

דוגמה (1): לא אבלית $(GLn(\mathbb{F}),\cdot)$

דוגמה (2): אבלית $(\mathrm{Mat_n}(\mathbb{F}),+)$.

תרגיל: תהי $(G,\cdot)$ חבורה כך שלכל x שייך לG מתקיים $x \cdot x = x^2 = e$. הוכיחו שG היא חבורה אבלית.

הוכחה: צריך להוכיח שלכל $\forall x,y \in G : xy = yx$.

נוכיח $xyxy = yxxy \rightarrow (xy)^2 = e \rightarrow (xy)^2 = x^2y^2 \rightarrow xyxy = xxyy \rightarrow yxy = xyy \rightarrow xy = yx$
מ.ש.ל. ■

אלגברה מופשטת 1 – תרגול 2

הקדמה לתורת המספרים:

הגדרה: יהי n טבעי נגדיר את $nZ=\{0,\pm n,\pm 2n,\dots\}$ להיות אוסף כל המספרים השלמים שמתחלקים ב n.

הגדרה: עבור $a,b\in\mathbb{Z}$ נאמר ש-a מחלק את b ונכתוב $a|b$ אם קיים $n\in\mathbb{Z}$ כך ש-na=b.

הגדרה: המחלק המשותף המקסימלי של $n,m\in\mathbb{Z}$ מסומן בgcd (Greatest Common Divisor) או ב(m,n)=gcd(m,n) ומוגדר להיות $(m,n)=\max\{d\in N: d|m\wedge d|n\}$. אם (n,m)=1 נאמר ש-m ו-n זרים.

הערה: אם d|a וd|b אזי d מחלק כל צירוף לינארי של a ו-b.

טענה: אם $n=qm+r$ אזי (n,m)=(m,r).

הוכחה: נסמן d=(n,m). אנחנו יודעים מכאן ש d|n וגם d|m. כעת, מכיוון ש-r הוא צירוף ליניארי של n,m נקבל d|r. ולכן $d\le(m,r)$.

כעת נראה את הכיוון השני. (m,r)|r וגם (m,r)|m ז״א (m,r)|n וגם ידוע ש-(m,r)|n וגם (m,r)|m. לכן $d\le$(m,r). ובסה״כ קיבלנו כי (m,r)=d=(n,m). מ.ש.ל. ■

אלגוריתם אוקלידס:

יהיו $m,n\in\mathbb{Z}$. ניתן להניח כי $0\le m<n$. אם m=0 ברור ש-(m,n)=0. אחרת (m>0), ניתן לכתוב n=qm+r כאשר $0\le r<m$ ואז מתקיים (n,m)=(m,r).

דוגמה (1): חישוב GCD באמצעות אלגוריתם אוקלידס: $(6,5)=(5,1)=1 \underbrace{=}_{7\cdot 6+5} (47,6) \overset{1\cdot 47+6}{=} (53,47)$.

דוגמה (2): $(28,7)=7 \overset{1\cdot 28+7}{=} (35,28) \overset{1\cdot 35+28}{=} (63,35) \overset{3\cdot 63+35}{=} (224,63)$.

משפט איפיון הgcd.

מתקיים $u,v\in Z$, $\gcd(a,b)=\min\{ua+vb>0\}$. ובפרט, קיימים $u,v\in Z$ כך ש-(a,b)=ua+vb.

תרגיל: הוכיח שלכל a,b,c שלמים מתקיים: (a,b)=1 וכן a|bc אזי a|c.

פתרון: ידוע כי (a,b)=1. לכן קיימים $\alpha,\beta\in Z$ כך ש$\alpha a+\beta b=1$. נכפול את שתי האגפים ב-c, וקיבלנו $a|\alpha ca\wedge a|\beta cb\to a|\alpha ca+\beta cb\to a|c$. מ.ש.ל. ■.

תכונות של הGCD:

1. d=(m,n) ויהי t כך ש t|m וגם t|n אזי t|d.
2. (am,an)=a(m,n)
3. אם p ראשוני וp|ab אזי p|a או p|b. (נובע מהתרגיל האחרון)

הגדרה: כפולה משותפת מינימלית (LCM=Least Common Multiple). ההגדרה הפורמלית הינה: $lcm(m,n)=[m,n]=\min\{d: n|d\wedge m|d\}$.

<u>תכונות של הLCM:</u>

1. אם m|a וגם n|a אזי [m,n]||a
2. [n,m]·(n,m)=|nm|

תרגיל:

א. פתרו את המשוואה 7x=12(mod34) ;
ב. מצאו את הספרה האחרונה של 333^{333}.

פתרון:

א. נכפיל בהופכי, כמו בהרצאה, ונקבל $7x = 12mod34 \to 35x = 60mod34 \to x = 26mod34$.

אתנחתא קלה: מציאת ההופכי של a ב-Z_n : זהו בעצם אותו a שמקיים ax-nk=1 עבור ax=1(mod(n))

ב. $3^{333}111^{333} = x\ mod(10) \equiv 333^{333}$ אבל $111^{333}mod10 = 1^{333}mod10 = 1mod10$= לכן ניתן לכתוב $3^{333} = x\ mod10$. שוב נפרק ונקבל $x\ mod10 = 3^{4\cdot 83+1} = 81^{83}\cdot 3 = 1^{83}\cdot 3$. פתרנו.

<u>חבורות ציקליות ותתי חבורות:</u>

הגדרה: תהי G חבורה ויהי a ששייך ל-G. אם כל איבר ב-G מתקבל כחזקה חיובית או שלילית של a נאמר ש-G נוצרת ע"י a ונקרא ל-G חבורה ציקלית. סימון: $G =< a >= \{a^k | k \in Z\}$.

דוגמאות:

1. Z נוצרת ע"י 1 ו-1-.
2. *kZ=<k>*
3. $Z_6 =< 1 >=< 5 >$ כל חבורה ציקלית הנוצרת ע"י איבר ניתן ליצור אותה גם בעזרת ההופכי.

<u>הגדרה</u>: תהי *(G,*)* חבורה. אם $\emptyset \neq H \subseteq G$ כך ש-*(H,*)* היא בעצמה חבורה (ביחס לאותה הפעולה!) אזי *H* היא תת חבורה של *G* ונסמן $H \leq G$.

הקריטריון המקוצר לבדיקת היותו של *H* תת חבורה הינו:

1. $\emptyset \neq H \subseteq G$ .2 $\forall a, b \in H : ab^{-1} \in H$.

דוגמה (1): $4Z \leq 2Z \leq Z \leq Q \leq R \leq C$. כל זה לגבי חיבור..

דוגמה (2): האם Z_n ת"ח של *Z*? לא! כי לא מדובר באותה פעולה בכלל (וזאת גם לא תת קבוצה).

דוגמה (3): תהי *G* חבורה ויהי *a* שייך לה. אזי $< a > \leq G$ היא תת החבורה הציקלית הנוצרת על ידי *a*.

דוגמה (4): $SLn(F) \leq GLn(F)$. (מטריצות עם דטרמיננטות 1)

תרגיל: $\Omega_n = \left\{cis\left(\frac{2\pi k}{n}\right) : 0 \leq k \leq n-1\right\}$. אוסף כל שורשי היחידה מסדר *n*.
צריך להוכיח כי: 1. $\Omega_n \leq (C^*,\cdot)$ .2 *m*/*n* אזי $\Omega_m \leq \Omega_n$.

פתרון:

1. נוכיח לפי הקריטריון המקוצר. זה מוכל, בוודאות. זה לא ריק כי 1 שייך אליו. התנאי הראשון הוכח. עבור התנאי השני $(\forall a, b \in H : ab^{-1} \in H)$

מתקיים: $(ab^{-1})^n = a^n(b^n)^{-1} = 1 \cdot 1 = 1$. ולכן זוהי תת חבורה.

2. אם $m|n$ אזי $\Omega_m \leq \Omega_n$. בעצם נוכיח תחילה שזה מוכל, שזהו התנאי הראשון של הקריטריון המקוצר. נניח ש $a \in \Omega_m$ אבל בגלל ש-$m|n$ ניתן לרשום $n=mk$ ולכן $a^m = 1$.

$a^{mk} = (a^m)^k = 1^k = 1$ לסיכום, ראינו ש Ω_m היא תת קבוצה, בנוסף בסעיף א׳ ראינו ש Ω_m היא בעצמה חבורה, לכן לפי ההגדרה (אפילו לא לפי הקריטריון המקוצר!) נקבל שΩ_m תת חבורה של Ω_n. ומ.ש.ל.

תרגיל: הוכיחו באמצעות לוחות כפל שכל חבורה עם שני איברים וכל חבורה עם 3 איברים היא ציקלית.

פתרון: $S=\{e,a\}$

$\langle a \rangle = S$

*	e	a
e	e	a
a	a	e

עבור $S=\{e,a,b\}$

$S=\langle a \rangle=\langle b \rangle$

$aa=b$ כי לא יכול להיות ש$aa=e$!

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

אלגברה מופשטת 1 – תרגול 3

הגדרה: $\mathrm{U_n} = \{$כל האיברים בין 1 לn כך שk זר ל$n\}$

דוגמה: $\mathrm{U}_{12} = \{1,5,7,11\}, |U_{12}| = 4$

שאלה: האם 5 נמצא בU_{10}?

פתרון: לא. 5 מחלק את 10.

הערה: ניתן בקלות להראות ש$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$

ולכן $\varphi\left(p_1^{k_1}p_2^{k_2}\dots p_m^{k_m}\right) = \varphi\left(p_1^{k_1}\right)\cdots\varphi\left(p_m^{k_m}\right) = p_1^{k_1}\dots p_m^{k_m}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_m}\right)$

שאלה: $\varphi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 16$

הגדרה: סדר של חבורה הוא מספר האיברים בחבורה ומסומן ב$|G|$.

הגדרה: סדר של איבר בG הוא $O(a) = \min\{n \in \mathbb{N} | a^n = 1\}$ ואם לא קיים n כזה אז $O(a) = \infty$.

דוגמאות:

1. $U_6 = \{1,5\}, O(1) = 1, O(5) = 2$
2. $\mathrm{Gln}(\mathbb{R}), n = 2, b = \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}, b^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \to O(b) = 3$

הערה: אם G סופית אזי לכל a בG מתקיים: $O(a)|G$.

הערה: בהינתן חבורה סופית מסדר n, אם קיים איבר a בG כך ש$O(a)=n$ אזי G נקראת ציקלית.

דוגמה: U_6 ציקלית $\mathrm{U}_6 = \{1,5\}, |U_6| = 2, O(5) = 2 \to$

תרגיל: תהי G חבורה $\mathrm{H} \leq G$ תת קבוצה סגורה לכפל מגודל סופי ולא ריקה. הוכיחו כי H היא תת חבורה של G.

תזכורת: תת חבורה מקיימת את התנאים הבאים:

1. H מכילה את איבר היחידה
2. H סגורה לכפל
3. H מכילה את ההפכיים של עצמה.

פתרון: נתון שהיא סגורה לכפל, וגם שהיא לא ריקה. נביט באיבר b שבH. נביט בקבוצה $\{b^n : n \in \mathbb{N}\} \subset H$ זו קבוצה סופית, ולכן קיימים n,m: $b^n = b^m$. אם נכפול את שתי האגפים b^{-m-1} נקבל כי האיבר ההופכי של b הוא $b^{-1} = b^{n-m-1}$.

מצד שני, $n-m-1>0$ כי אם זה שווה ל0 נקבל ש$b=1$ ואז אין משמעות לחזקות, כולן חוזרות ל1, בסתירה להנחה שלנו.

קיבלנו שלכל איבר בH יש גם את ההופכי שלו.

ראינו גם כי איבר היחידה נמצא בH, כי H סגורה לכפל ולכל מספר יש הופכי, לכן יש גם יחידה. מ.ש.ל. ■

תרגיל: תהי G חבורה אבלית. הוכיח שאוסף האיברים מסר סופי הוא תת חבורה.

פתרון: איבר היחידה מסדר סופי, לכן הוא נמצא ועניינו על הקריטריון הראשון.

נביט בשני איברים מסדר סופי a,b בG, ונראה שהמכפלה שלהם מסדר סופי. נניח כי $\mathrm{O(a) = n\,, O(b) = m}$ ‏$\mathrm{(ab)^{nm}} = (a^n)^m(b^m)^n = 1 \cdot 1$.

ניקח איבר מסדר סופי b כך שO(b)=k. מתקיים כי $b^{k-1} = b^{-1} \rightarrow b^k = 1 = b \cdot b^{k-1} = 1$.

והוכחנו כי שלושת התנאים מתקיימים. מ.ש.ל. ■

<u>חיתוך ואיחוד של חבורות</u>

<u>משפט</u>: חיתוך של תת חבורות (לאו דווקא סופי) הוא תת חבורה.

הוכחה: G חבורה $\{\mathrm{H_i}\}_{i\in I}$ אוסף של תתי חבורות. האם $\mathrm{H} = \bigcap_{\mathrm{i\in I}} H_i$. לכל i בו $\mathrm{H_i}$ היא תת חבורה, ולכן איבר היחידה שייך לחיתוך. $a, b \in \bigcap_{i\in I} H_i \rightarrow \forall i \in I : a, b \in H_i \rightarrow a \cdot b \in H_i \rightarrow a \cdot b \in \bigcap_{i\in I} H_i$ והוכחנו סגירות לכפל. כעת נוכיח באופן דומה כי לכל איבר קיים הפיך. נניח *b* שייך לאיחוד $\bigcap_{\mathrm{i\in I}} H_i$ לכן לכל *i* שנבחר $b \in H_i$ אבל $\mathrm{H_i}$ תת חבורה, ולכן $\forall i \in I : b^{-1} \in H_i \rightarrow \forall b \in \bigcap_{i\in I} H_i : b^{-1} \in \bigcap_{i\in I} H_i$. והוכחנו כי לכל איבר קיים הופכי. מ.ש.ל. ■.

תרגיל: תנו דוגמה לכך שאיחוד של שתי תתי חבורות הוא לאו דווקא תת חבורה.

פתרון: נביט בחבורה $(\mathbb{Z}_6, +)$. ובתתי החבורות $2\mathbb{Z}_6 = \{0,2,4\}, 3\mathbb{Z}_6 = \{0,3\} \rightarrow 2\mathbb{Z}_6 \cup 3\mathbb{Z}_6 = \{0,2,3,4\}$ אבל אין כאן סגירות, כי *3+4* לא בתת חבורה.

תזכורת: בהינתן שתי חבורות *B,A* מגדירים $A \times B = \{(a, b): a \in A, b \in B\}$

$(a, b) \cdot (c, d) = (a \cdot_A c, b \cdot_B d)$.

תרגיל: עבור *n>1* האם $\mathbb{Z}_n \times \mathbb{Z}_n$ ציקלית?

פתרון: הסדר של החבורה הוא n^2, האם קיים איבר מסדר כזה? נבדוק.

צריך להתקיים ש$\mathrm{n(a,b)} = (na, nb) = (0,0) \rightarrow O\big((a, b)\big) \le n < n^2$ ולכן היא אינה ציקלית ■.

תרגיל: תהי *G* חבורה, ו*a,b* איברים בה. אם *a,b* מסדר סופי, האם גם המכפלה שלהם $(\mathrm{a \cdot b})$ היא מסדר סופי?

פתרון: באופן כללי התשובה היא לא. חשוב לדעת שבמקרה שמדובר בחבורה אבלית, התשובה היא דווקא כן. מקרה שבו המכפלה של שתי איברים מסדר סופי היא לא מסדר סופי ניתן למצוא בחבורה $G = GL_2(\mathbb{R})$.

נביט במטריצות $\mathrm{a} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}. O(a) = 4, O(b) = 3. a \cdot b = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ואנחנו יודעים שלכל *n* טבעי מתקיים כי $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ ולכן הסדר של המכפלה הוא ∞. מ.ש.ל. ■.

<u>כמה הערות על סדרים</u>:

א. אם *G* חבורה, $g \in G$ עבור *n* טבעי $\mathrm{g^n} = 1$ אז *O(g)|n*.
ב. אם *G=<a>* ציקלית מסדר *n*. אזי לכל *g* ב*G* מתקיים $g^n = 1$.

ג. בחבורה סופית הסדר של איבר הוא סופי.
ד. $O\left(a^i\right) \leq O(a)$
ה. $O(a) = O(a^{-1})$

נוכיח את תכונה (ה׳):

1. נניח כי $O(a)=n$ (לא אינסוף). אזי $(a^{-1})^n = (a^n)^{-1} = 1^{-1} = 1$ ונותר להוכיח שn הוא מינימלי. נניח בשלילה שn לא מינימאלי. אזי קיים $n>m$ כך ש$(a^{-1})^m = (a^m)^{-1} = 1$. כעת נכפול ב$a^m$ את שני האגפים, ונקבל $\mathrm{a}^\mathrm{m} = 1$ בסתירה לכך ש$O(a)=n$.
2. כעת נניח כי $O(a) = \infty$. נניח בשלילה ש$O(a^{-1}) = n < \infty$. ז״א, ע״פ הגדרה ש$(a^{-1})^n = 1$ ואם נכפול בשתי האגפים ב a^n נקבל כי $\mathrm{a}^\mathrm{n} = 1$ בסתירה להנחה.

מ.ש.ל. ■

אלגברה מופשטת 1 – תרגול 4

הבוחן יתקיים ב6.8 בשעה 13:00 (יום שלישי). הבוחן הוא שעה וחצי, שלוש שאלות. בבניין 507 אולם 7. יורכב ברובו מתרגילי הבית, יכול להיות שתהיה שאלה חדשה, וכו'. בהצלחה!!!

תרגיל: יהי a=cis(30) מתקיים כי $< a > \leq C^*$. חשבו את |<a>|.

פתרון: |<a>|=o(a) בעצם מחפשים n כך ש $a^n = 1$. ניתן לחשב מיידית שעבור n=12 התנאי מתקיים. כעת נותר להראות ש12 הוא ה-n המינימלי. נמצא את ה-k הMin עבורו 30t=360k כי $a^t = 1 = cis(360k)$. ולכן עבור ...k=1,2,3 ברור שהמינימאלי הוא עבור k=1. הוא לא יכול להיות שלילי (כי הסדר הוא טבעי או אפס) או אפס (כי a אינו נייטרלי).

לכן, 12=|<a>|. מ.ש.ל. ■

<u>משפט</u>: תהא G חבורה ציקלית מסדר n אזי לכל t שלם מתקיים $o(a^t) = \frac{n}{(n,t)}$ עבור G=<a>.

שאלה: כמה יוצרים יש לחבורה ציקלית?

פתרון: לפי משפט, אם (t,n)=1 אזי $o(a^t) = 1$ ואז a^t הוא יוצר החבורה. לכן מספר היוצרים הוא $\varphi(n)$.

- אם G ציקלית אינסופית אזי G איזומורפית ל-Z ($G \cong Z$) ולכן יש לה 2 יוצרים. Z=<1>=<-1>

דוגמה: נתבונן ב$\Omega_{40} =< w >$ כאשר $w = cis\left(\frac{2\pi}{40}\right)$.

א. מהו הסדר של w^{14}?
$o(w^{14}) = \frac{40}{(40,14)} = \frac{40}{2} = 20.$

ב. כמה יוצרים יש ל $\Omega_{40} =< w >$?
מספר היוצרים של $\Omega_{40} =< w >$ הוא $16 = 40\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = \varphi(40)$. מ.ש.ל. ■

<u>חבורת הסימטריה</u>: (החבורה הסימטרית או חבורת התמורות)

הגדרה: S_n אוסף כל הפונקציות החח"ע ועל מקבוצה {1,2,..,n} לעצמה. איברי S_n נקראים תמורות. בS_3 תמורה היא פונקציה. (1 2) , $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, f(1)=2,f(2)=1,f(3)=3.

התמורות של S_3 הן:

$$id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \tau\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

מה חשוב לנו לחיים? לדעת לחשב סדר, לכפול אותם, ולחשב הופכי.

- <u>כפל</u>: $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$=(1 2 3)(1 2) .

תרגיל: $(4\ 3\ 1\ 2) = (1\ 2\ 4\ 3) = (4\ 1\ 3\ )(1\ 3)(1\ 2\ 4)$. למדנו את זה בלינארית (חישוב דטרמיננטות). חשוב לדעת את זה טוב טוב!

- <u>הופכי של מחזור</u>: $(i_1, i_2, \dots, i_n)^{-1} = (i_n, i_{n-1}, \dots, i_1)$.
- <u>מחזורים זרים</u>: נאמר שמחזורים $(i_1, \dots, i_n), (j_1, \dots, j_n)$ הם זרים אם $\{j_1, \dots, j_n\} \cap \{i_1, \dots i_n) = \emptyset$ מחזורים זרים זהם מתחלפים.

-דביר, זה לאו דווקא מחזורים באותו אורך... תשנה את אחד ה-n-ים ל- k או משהו כזה...

<u>תכונות מעניינות וחשובות:</u>

1. החל מ-n=3 החבורה S_n אינה אבלית. איך נראה את זה? נראה שיש שתי תמורות שאינן מתחלפות. לדוגמה, נביט ב (13)(12) וב(12)(13). קיבלנו שהראשון הוא (132) והשני הוא (123) ולכן שתי התמורות הללו אינן מתחלפות, ולכן S_n (החל מ- $n=3$) היא אינה אבלית (שכן, שתי התמורות הללו נמצאות בכל S_n כנ"ל).
2. החל מ-n=3 חבורת התמורות אינה ציקלית. זה ברור כי כל ציקלית היא אבלית, ואם היא אינה אבלית אין היא ציקלית.
3. $|S_n| = n!$.

תרגיל: פתרו את המשוואה: $(\ 1\ 2\ 3\ )^2 x = (12)(132)^{-1}$.

פתרון: נפשט את הביטוי ונחפש את x: $(1\ 3\ 2)x = (1\ 2)(2\ 3\ 1) = (2\ 3)$. כעת נכפול בהופכי את שני האגפים, ונקבל (2 1)=(3 2) (1 3 2) = x. מ.ש.ל. ■

<u>הגדרה: חבורה נוצרת על ידי מספר איברים:</u> תהי G חבורה ותהי $A \leq G$ ת"ק (לאו דווקא ת"ח, נכון, אז למה השתמשת בסימון של תת חבורה ☺ תחליף את הקטן-שווה בהכלה?!...) לא ריקה של איברים מ-G. תת החבורה הנוצרת על ידי A היא תת החבורה הקטנה ביותר של G המכילה את A, ונסמנה ב<A>.

אם G=<A> נאמר ש-G נוצרת על ידי A.

<u>דוגמאות:</u>

1. נתבונן ב- $G = \square$, A={2,3}. ?=<A>=<2,3>. ז"א $< 2,3 >= \{2k_1 + 3k_2 | k_1, k_2 \in Z\}$. נוכיח שזה ממש כל Z על ידי הכלה דו כיוונית. ברור לנו ש-

$< 2,3 > \subseteq Z$. את הכיוון השני קצת יותר קשה להראות. ניתן להראות ש$a = -2a + 3a$ ולכן אין בעיה בכלל להראות גם את הכיוון השני.

2. נמשיך עם אותה G. A={4,6}. ניתן להראות ש<4,6>=2Z=<2>. להוכיח בבית!

<u>הערה</u>: אם G חבורה אבלית ו$A = \{x_1, x_2, \dots, x_n\}$ אזי $< A >= \{x_1^{i_1} x_2^{i_2}, \dots\}$.

<u>הגדרה</u>: חבורה G נוצרת סופית אם יש לה קבוצת יוצרים סופית.

כלומר, קיימים $a_1, \dots, a_n \in G$ כך ש$< a_1, a_2, \dots, a_n >= G$.

- כל חבורה ציקלית נוצרת סופית על ידי איבר אחד.
- כל חבורה סופית נוצרת סופית (על ידי כל איבריה, למשל).

תרגיל: ראינו את החבורה של שורשי היחידה ה-n-ים. נגדיר $\Omega_\infty = \cup_{n=1}^{\infty}\Omega_n$. (זהו אוסף כל שורשי היחידה). הוכיחו כי Ω_∞ אינה נוצרת סופית.

פתרון: נניח בשלילה כי Ω_∞ נוצרת סופית. כלומר קיימים $a_n, \dots, a_k \in \Omega_\infty$

כך ש $\langle a_1, \dots, a_k \rangle = \{a_1^{j_1} a_2^{j_2} \dots a_k^{j_k} | 1 \le i \le k, 0 \le j_i \le o(a_i) < \infty\}$ כי a_i שייך ל Ω_n כלשהו ולכן סדרו סופי.

כלומר, כל קבוצה סופית ב Ω_∞ יוצרת חבורה סופית שכן $|\langle a_1, .., a_k \rangle| \le o(a_1)o(a_2)\dots o(a_k) < \infty$

אבל ב Ω_∞ יש ∞ איברים ולכן זו סתירה. מכאן ש Ω_∞ אינה נוצרת סופית. מ.ש.ל. ■

<u>דוגמאות</u>:

1. $Z \times Z = \{(a,b) | a, b \in Z\}$ נוצרת סופית ע״י <(1,0),(0,1)>. כי לכל g ב-$Z \times Z$ קיימים m,n כך ש-g=(m,n) וז״א g=m(1,0)+n(0,1).
2. S_n נוצרת סופית? מתקיים כי $Rank(S_2) = 2$ אבל גם $S_2 = \langle (12), (123 \dots n) \rangle$. נראה ונוכיח בהמשך הקורס.דביר – זה אמור להיות S_n בכל הדוגמה הזאת...

תרגיל: הוכיחו כי החבורות הבאות אינן נוצרות סופית.

א. $(R, +, 0)$
ב. $(Q^*, \cdot, 1)$

מישהו שאל למה יש גם את האיבר הטבעי ביחס לפעולה בצד ימין בסוגריים, התשובה היא שזאת אופציה נוספת לסמן חבורה ולהדגיש את האיבר הנייטרלי.

פתרון:

א. נניח בשלילה ש-R נוצרת סופית. ז״א קיימים $a_1, \dots, a_n \in \mathbb{R}$ כך ש-

$R = \langle a_1, a_2, \dots, a_n \rangle = \{a_1^{i_1}, \dots, a_n^{i_n}\}: i, j \in Z, 1 \le i_j \le n$ אבל הבעיה היא של $a_n^{i_n}$ יש $\aleph_0$ אפשרויות, ולכן בסה״כ יש $\aleph_0 = (\aleph_0)^n$ איברים, ועם זאת, R אינה בת מניה בכלל. מ.ש.ל.

נניח בשלילה ש $\mathbb{Q}^*$ נוצרת סופית. $Q^* = \langle \left(\frac{a_1}{b_1}\right), \dots, \left(\frac{a_n}{b_n}\right) \rangle \geq$

$$\left\{ \left(\frac{a_1}{b_1}\right)^{i_1} \left(\frac{a_2}{b_2}\right)^{i_2} \dots \left(\frac{a_n}{b_n}\right)^{i_n} \middle| \begin{matrix} 1 \le j \le n \\ i_j \in Z \end{matrix} \right\}$$

מ.ש.ל. ■לא הבנתי את התשובה לב'... אנחנו לא מוכיחים למקרה כללי =) מוכיחים בדיוק למה שצריך ☺

א. הגורמים הראשוניים במכנים של האיברים הנוצרים מוגבלים לקבוצת הגורמים הראשוניים של $b_1, \dots, b_n$, אבל זאת קבוצה סופית, ולכן לא ניתן לקבל את כל השברים ב $(\mathbb{Q}^*, \cdot, 1)$, סתירה.

<u>אתגר (כי פרנקנטל ממש ביקש יפה)</u> : (MANN מהספר של רוטמן). G חבורה סופית. S,T הן תתי קבוצות (לאו דווקא תתי חבורות) לא ריקות. אזי מתקיים או G=ST (כפל איבר איבר בקבוצות ולא בחבורות) או ש $|G| \geq |S| + |T|$.

דביר חדד

<u>אלגברה מופשטת 1 – תרגול 5</u>

<u>החבורה הדיהדרלית</u>

D_n- חבורת הסיבובים והשיקופים של מצולע משוכלל בעל n צלעות.

למשל: החבורה D_3 היא חבורה הנוצרת מסיבוב (σ) בזווית 120 מעלות, ושיקוף (τ).

מתקיימים היחסים: $\tau\sigma\tau = \sigma^{-1}$, $\sigma^2 = \tau^2 = id$.

איברי החבורה הם: $D_3 = \{id, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. האם $\sigma\tau \in D_3$?

מתקיים:

$$\tau\sigma\tau = \sigma^{-1} \; / \, \tau$$
$$\sigma\tau = \tau\sigma^{-1} \;\; / \, \sigma^3$$
$$\sigma\tau\sigma^3 = \tau\sigma^2$$
$$\sigma\tau = \tau\sigma^2$$

מכאן רואים שלכל $n \geq 3$ החבורה D_n אינה אבלית, שכן (למשל) $\sigma\tau \neq \tau\sigma$.

באופן דומה D_n נוצרת על ידי σ, τ (באשר σ הוא סיבוב של $\frac{360^\circ}{n}$) כאשר $\tau\sigma\tau = \sigma^{-1}, \sigma^n = \tau^2 = id$.

איברי $D_n = \left\{id, \sigma, \sigma^2, ..., \sigma^{n-1}, \tau, \tau\sigma, ..., \tau\sigma^{n-1}\right\}$.

מתקיים $|D_n| = 2n$.

תרגיל: תהי G חבורה סופית ויהיו $a, b \in G$ האם יכול להיות ש$o(a)o(b) > o(ab)$?

פתרון: כן. D_3. נבחר $a = \tau$, $b = \tau\sigma$. כעת $o(\tau\sigma) = 2$, $o(\tau) = 2$. אבל מה הסדר של $ab = \tau\tau\sigma$? הוא בדיוק זה של σ, ולכן זה שלוש. קיבלנו דוגמה שמקיימת $o(a)o(b) > o(ab)$.

<u>מחלקות / קוסטים (*cosets*) בחבורה</u>

הגדרה: תהי G חבורה ו$H \leq G$ תת חבורה. עבור $a \in G$:

1. המחלקה השמאלית של a בH היא $aH = \{ah | h \in H\}$
2. המחלקה הימנית של a בH היא $Ha = \{ha | h \in H\}$

הערה: אם החבורה אבלית אזי $Ha = aH$.

דוגמאות:

1. קוסטים של $3\mathbb{Z}$ כתת חבורה של $\mathbb{Z}$: $3\mathbb{Z} + 8 = 3\mathbb{Z} + 2 = 2 + 3\mathbb{Z}$.

2. כעת נביט ב$G = S_3 = \{id, (12), (13), (23), (123), (132)\}$. ונתבונן בקוסטים השמאליים של תת החבורה $H = \langle (12) \rangle = \{id, (12)\}$.

$\mathrm{idH} = \{(12), \mathrm{id}\} = H$

$(123)H = \{(13), (123)\}, (132)H = \{(23), (132)\},$

$(23)H = \{(132), (13)\}, (13)H = \{(123), (13)\}, (12)H = \{id, (12)\}.$

<u>תזכורת</u>:

הקוסטים הם מחלקות שקילות. למשל, או ששתי מחלקות זרות או שהן שוות. וגם מתקיים שהחבורה היא איחוד זר של מחלקות השקילות הללו. בדוגמה שלנו: $S_3 = H \cup (13)H \cup (132)H$

3. $G = \mathrm{GL}_2(\mathbb{Q})$. נגדיר $H = \left\{\begin{pmatrix}1 & n\\0 & 1\end{pmatrix} : n \in \mathbb{Z}\right\}$ ותבדקו בבית ש$H \le G$. עבור איבר $g = \begin{pmatrix}5 & 0\\0 & 1\end{pmatrix} \in G$ הקוסטים הם $gH = \left\{\begin{pmatrix}5 & 5n\\0 & 1\end{pmatrix} : n \in \mathbb{Z}\right\}$. $Hg = \left\{\begin{pmatrix}5 & n\\0 & 1\end{pmatrix} : n \in \mathbb{Z}\right\}$. מתקיים כי $Hg \neq gH$.

<u>הערות</u>:

1. לכל תת חבורה $H \le G$ מתקיים כי H היא מחלקה שמאלית וגם מחלקה ימנית $e_G H = He_G = H$
2. קיימת התאמה חח״ע ועל בין המחלקות הימניות למחלקות השמאליות $Hg \longmapsto g^{-1}H$.

הגדרה: תהי G חבורה, $H \le G$ תת חבורה. נסמן את האינדקס של H בG כך: $[G:H]$ וזהו מספר המחלקות השמאליות (ימניות) של H בG.

למשל: מתקיים $[G:H] = 3$: $G = S_3,\ H = <(12)>$.

תרגיל: מצאו חבורה G ות״ח $H \le G$ כך ש-

1. $[G:H] = \aleph_0$
2. $[G:H] = \aleph$

פתרון:

1. $G = \mathbb{Z} \times \mathbb{Z}$. $H = \mathbb{Z} \times \{0\}$. ולכן $[G:H] = \aleph_0$. כל הקוסטים הם $\{Z \times \{x\}\}_{x \in \mathbb{Z}}$.
2. $[GL_2(\mathbb{R}), GL_2(\mathbb{Q})] = \aleph$. דוגמה הרבה יותר אלגנטית $G = \mathbb{R} \times \mathbb{R}, H = \mathbb{R} \times \{0\}$.

<u>משפט לגרנג' ומסקנותיו:</u>

תהי G חבורה סופית ו$H \le G$ תת חבורה. אזי $|G| = [G:H] \cdot |H|$.

מסקנה: מתקיים כי $|H|$ מחלק את $|G|$ כלומר, הסדר של תת חבורה מחלק את סדר החבורה. בפרט, סדר של כל איבר בחבורה מחלק את סדר החבורה. כי $\forall a \in G : o(a) = |<a>|$.

נשים לב: הסדר של איבר הוא סדר של ת״ח הציקלית שהוא יוצר. וראינו שסדר של הת״ח מחלק את סדר החבורה.

מסקנה: G סופית, $K \le H \le G$ מתקיים $[G:K] = [G:H][H:K]$.

הערה: $a^{|G|} = e$ לכל $a \in G$.

תרגיל: תהא G חבורה מסדר 8. הוכיחו שקיימת ב-G תת חבורה ציקלית מסדר 4.

פתרון: יש רק איבר אחד מסדר 1 (היחידה). לא יתכן שכל שאר האיברים (חוץ מהנייטרלי) הם מסדר 2, כי אז היא אבלית (הוכחנו את הטענה: אם בחבורה כל איבר (חוץ מהנייטרלי) הוא מסדר 2, אזי החבורה אבלית).

אין איבר מסדר 8, כי אם היה G הייתה ציקלית ולכן אבלית. מכאן שקיים איבר מסדר 4 שיוצר את תת החבורה הדרושה. מ.ש.ל. ■

טענה (הכללה של התרגיל): תהא G חבורה לא אבלית מסדר 2^t $(t > 2)$ אזי קיימת בG תת חבורה ציקלית מסדר 4.

הוכחה: לפי לגרנג' הסדרים האפשריים של אברים ב-G הם: 2^k, $k = \{0,1,2,\dots,t\}$.

- יש רק איבר 1 מסדר 1
- לא כולם מסדר 2 כי אז G אבלית
- אין איבר מסדר 2^t כי אז G ציקלית ולכן אבלית.

לכן, קיים איבר a בG כך ש $o(a) = 2^k, 2 \le k < t$.

אנו יודעים כי $|<a>| = 2^k$. אנחנו טוענים שבתת חבורה הזו ניתן לייצר איבר מסדר 4.

להזכירם: $o(g^t) = \frac{n}{(n,t)}$, $|G| = n$, $<g> = G$. וכעת נבחר $a^j \in <a>$ כך ש $o(a^j) = \frac{2^k}{(2^k,j)} = 4$.

נבחר $j = 2^{k-2}$. כלומר, בתוך <a> נבחר את האיבר $a^{2^{k-2}} \in <a>$ וקל לראות $o\left(a^{2^{k-2}}\right) = 4$. ולכן $a^{2^{k-2}}$ יוצר את תת החבורה הציקלית הדרושה. מ.ש.ל. ■

תרגיל: הוכיחו: תהא G חבורה סופית אזי G מסדר זוגי או"א קיים ב-G איבר מסדר 2.

פתרון: $\rightarrow$: כיוון פשוט, ע"פ לגרנג' הסדר של על איבר מחלק את סדר החבורה, ולכן סדר החבורה הוא זוגי.

$\leftarrow$: שימו לב: איבר מסדר 2 הוא איבר שהופכי לעצמו. נניח שבשלילה שאין אף איבר בG שהוא ההופכי של עצמו. (חוץ מהיחידה, e, כמובן). ניתן להצמיד כל איבר להפכי שלו (שהוא איבר שונה ממנו). ביחד עם איבר היחידה, נקבל מספר אי-זוגי. מ.ש.ל■

<u>הערה</u>: לחבורה מסדר זוגי יש מספר אי זוגי של איברים מסדר 2. (המשפט של ארד ☺).

<u>משפט אוילר 2</u>:

לכל $a \in U_n$ מתקיים $a^{\varphi(n)} \equiv 1\big(mod(n)\big)$.

מסקנה:

זהו למעשה זהו משפט פרמה הקטן שאומר: אם $a \in U_p$ כאשר p ראשוני אזי $a^{p-1} \equiv 1(modp)$.

תרגיל: חשבו את שתי הספרות אחרונות של $8073767^{1999}+2013$.

פתרון: נפעיל mod100 ונקבל:

$67^{1999}+13=67^{50\cdot 40-1}+13\equiv(67^{\varphi(100)})^{50}67^{-1}+13\equiv 67^{-1}+13$ נשתמש באלגוריתם למציאת הופכי, שתרגלנו בשיעורים הקודמים, ונקבל $67^{-1}=3$. ולכן שתי הספרות האחרונות הן 3+13=16.

תזכורת לאלגוריתם למציאת ההופכי:

אנו יודעים שיש הופכי ל-67 בחבורה $\mathbb{Z}_{100}$ כי הם זרים. כלומר ישנו פתרון למשוואה $67x\equiv 1 (\mathrm{mod}\, 100)$ אם ורק אם קיים $k\in\mathbb{Z}$ כך ש- $100k+67x=1$. נשתמש באלגוריתם אוקלידס כדי למצוא את x, כלומר למצוא ביטוי של $\gcd(100,67)$ כצירוף לינארי של 67 ושל 100: $(100,67)\underset{100=1\cdot 67+33}{=}(67,33)\underset{67=2\cdot 33+1}{=}(33,1)=1$

ומהצבה לאחור נקבל $1=67-2\cdot 33=-2\cdot 100+3\cdot 67$ ולכן $x=3$.

מ.ש.ל. ■

__אתגר:__

ידוע כי עבור $H_1,H_2\le G$ ועבור $H\le G$ מתקיים ש$H_1\cup H_2$ לא בהכרח תת חבורה.

הוכיחו תחילה את הטענה הבאה: אם $H\subseteq H_1\cup H_2$ אזי $H\subseteq H_1$ או $H\subseteq H_2$.

לעומת זאת, כשמדובר בשלוש תת חבורות באיחוד, המצב משתנה.

יהיו $H,H_1,H_2,H_3\le G$ (כולן תתי חבורות) מצאו דוגמה שבה מתקיים:

א. $H\subseteq H_1\cup H_2\cup H_3$;

ב. H לא מוכלת באף H_i ובאף איחוד של שתיים $H_i\cup H_j$.

אלגברה מופשטת 1 – תרגול 6

תרגיל: תהא G חבורה סופית $|G|=n$, יהי k טבעי כך ש-k/n. האם קיים בהכרח איבר מסדר k ב-G?

פתרון: לא. נביט ב-$G=\mathbb{Z}_4\times\mathbb{Z}_4$. מתקיים כי $|G|=16$ אבל אנחנו טוענים כי אין איבר ב-G מסדר 8 (למשל).
למעשה, לכל $(a,b)\in G$ מתקיים כי $(a,b)^4=(4a,4b)=(0,0)$ ולכן $O\big((a,b)\big)\le 4$. מ.ש.ל. ■

אגב, הראינו ש-G אינה ציקלית (כי בשביל שהיא תהיה ציקלית, צריך איבר מסדר 16).

<u>תת חבורה נורמלית (תח״נ)</u>

הגדרה: תהא G חבורה $H\le G$ נקראת תח״נ אם $\forall g\in G: gH=Hg$ ונסמן $H\lhd G$.

משפט: התנאים הבאים שקולים:

1. $H\lhd G$;
2. $\forall g\in G\ gHg^{-1}=H$;
3. $\forall g\in G\ gHg^{-1}\subseteq H$ (פרוש: $\forall g\in G\forall h\in H\ ghg^{-1}\in H$).

דוגמאות:

1. בחבורה אבלית, כל ת״ח היא נורמלית.
2. בחבורה לא אבלית, זה לא בהכרח נכון. למשל, $G=S_3$ ו-$H=<(12)>=\{(12),id\}$ וראינו כי $(13)H\neq H(13)$ ולכן H אינה נורמלית ב-G.
3. $SL_n(\mathbb{R})\lhd GL_n(\mathbb{R})$.

טענה: תהא G חבורה, $H\le G$ אם [G:H]=2 אזי $H\lhd G$.

הוכחה: נניח [G:H]=2. מכאן שקיימים שני קוסטים ימניים שונים, $H, Ha_{a\notin H}$. (שימו לב ש$H=Ha$ או״א a שייך לH (ו-Hx=Hy או״א $xy^{-1}\in H$) כלומר, $G=H\uplus_{\text{איחוד זר}}Ha$.

כעת מתקיים $H\neq aH$ ולכן $G=H\uplus_{\text{איחוד זר}}aH$. ומכאן ש$H\uplus Ha=H\uplus aH$ ולכן לכל a שלא שייך לH מתקיים כי aH=Ha, אבל אם a שייך לH ברור שHa=H=aH ולכן זה לכל a. מ.ש.ל. ■

<u>דוגמית לתרגיל</u>: $|D_n|=2n$ ראינו שעבור $\sigma\in D_n$(סיבוב) מתקיים $o(\sigma)=n$. ולכן $|<\sigma>|=n$. מכאן ש-$<\sigma>\lhd D_n\to[D_n:<\sigma>]=2=\frac{|D_n|}{|<\sigma>|}$.

<u>הגדרה</u>: תהא G חבורה. $a,b\in G$ יקראו <u>צמודים</u> אם קיים $x\in G$ כך ש$a=xbx^{-1}$.

<u>ננסח מחדש את הגדרת הנורמליות:</u>

$H\le G$ תח״נ אם היא סגורה להצמדות , כלומר, לכל h שייך ל-H ולכל g שייך ל-G מתקיים $ghg^{-1}\in H$.

תרגיל: תהא G חבורה, $H\le G$ ו-$N\lhd G$ אזי $N\cap H\lhd H$.

פתרון: צ״ל $\forall h\in H: h(N\cap H)h^{-1}\subseteq N\cap H$.

- שימו לב ש-$N\cap H$ אכן ת״ח של H שכן ראינו שחיתוך של ת״ח הוא ת״ח

במילים אחרות, צ״ל: לכל h שייך ל-H ולכל $x\in N\cap H$ מתקיים $hxh^{-1}\in N\cap H$.

קודם כל, נניח ש-$x \in N \cap H$, ולכן x שייך ל-H. ולכן $hxh^{-1} \in H$ בגלל הסגירות של ת״ח H. שנית, x שייך ל-N, ולכן $hxh^{-1} \in N$ כי $N \lhd G$ ולכן $hxh^{-1} \in N \cap H$. מ.ש.ל. ■

<u>הגדרה</u>: יהיו $N, H \leq G$ נגדיר את המכפלה $HN = \{hn | h \in H, n \in N\}$.

תרגיל: בבית תוכיחו את הטענה הבאה: אם $N, H \lhd G$ אזי $HN \lhd G$.

עכשיו הראו שאם H,N ת״ח לא נורמליות אז HN אינה בהכרח ת״ח של G.

פתרון :ב- D_3 נבחר: $N =< \tau >= \{\tau, id\}$, $H =< \tau\sigma >= \{\tau\sigma, id\}$. N אינה נורמלית שכן $N\sigma \neq \sigma N$. גם H אינה נורמלית, מכיוון ש-$\tau H \neq H\tau$.

עכשיו נראה ש-HN אינה ת״ח של G. $HN = \{\tau\tau\sigma, \tau, \tau\sigma, id\} = \{\sigma, \tau, \tau\sigma, id\}$ וזו לא תת חבורה של D_3 בגלל שתי סיבות:

א. לגרנג׳: הסדר שלה בכלל לא מחלק את 6 (4 לא מחלק את 6)
ב. אין בה סגירות: $\sigma^2 \notin HN$.

מ.ש.ל. ■.

<u>הומומורפיזמים</u>

תהיינה H,G חבורות . העתקה $\varphi: G \to H$ תקרא הומומורפיזם אם $\forall a, b \in G : \varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$.

תכונות:

1. $\varphi(e_G) = e_H$
2. $\forall n \in \mathbb{Z} : \varphi(a^n) = \varphi(a)^n$ ובפרט $\left(\varphi(a^{-1})\right) = \varphi(a)^{-1}$
3. $\forall a \in G : O(\varphi(a)) \mid O(a)$
4. אם G אבלית אזי $\varphi(G) \leq H$ היא אבלית.

- <u>איזומורפיזם</u>: הומומורפיזם חח״ע ועל .
  הוא שומר על:
  א. סדר של חבורה
  ב. סדר של כל איבר
  ג. אבליות
  ד. ציקליות

דוגמאות:

1. האם $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_4$?
   לא! מכיוון ש$\mathbb{Z}_4$ ציקלית ו$\mathbb{Z}_2 \times \mathbb{Z}_2$ לא.
2. האם בין כל שתי חבורות G,H ניתן למצוא הומומורפיזם?
   כן. הומומורפיזם טריוויאלי. $\varphi: G \to H$ כך ש$\forall a \in G : \varphi(a) = e_H$.
3. תהא G חבורה אבלית. יהי n שלם. האם $\varphi: G \to G$ המוגדרת על ידי $\varphi(x) = x^n$ היא הומומורפיזם?
   כן. $\varphi(xy) = (xy)^n \overset{\text{אבליות}}{=} x^n y^n = \varphi(x)\varphi(y)$

4. האם $\mathbb{Q} \cong \mathbb{R}$?
לא. משיקולי עוצמות ידוע כי $|\mathbb{R}| \neq |\mathbb{Q}|$.
5. האם $5\mathbb{Z} \cong \mathbb{Z}$?
כן. כל החבורות הציקליות האינסופיות הן איזומורפיות זו לזו. האיזומורפיזם הדרוש הוא $\varphi: \mathbb{Z} \to 5\mathbb{Z}$, $\varphi(n) = 5n$.
6. האם $\mathbb{Z}_6 \cong D_3$?
לא. משיקולי אבליות.
7. האם $S_3 \cong D_3$? תחשבו על זה, נענה על זה בהמשך הקורס ☺

תרגיל: יהי $\varphi: G \to H$ אפימורפיזם. הוכיח שאם G ציקלית אזי H ציקלית.

פתרון: G ציקלית ולכן קיים g ב-G כך ש-$\langle g\rangle=G$. נסמן $\varphi(g) = h$. נרצה להראות $\langle h\rangle=H$. יהי x ב-H וצ״ל שקיים i כך ש-$x = h^i$. עבור x ששייך ל-H קיים a שייך ל-G כך ש-$\varphi(a) = x$ כי φ אפימורפיזם. $a \in \langle g \rangle$ ולכן קיים i כך ש-$a = g^i$ ולכן $x = \varphi(a) = \varphi(g^i) = \varphi(g)^i = h^i$. מ.ש.ל. ■.

<u>הערה</u>: אפימורפיזם מעביר קבוצת יוצרים לקבוצת יוצרים.

תרגיל:

הוכיחו/הפריכו:

1. קיים איזומורפיזם $f: (\mathbb{Q}^+,\cdot) \to (\mathbb{Q},+)$
2. קיים אפימורפיזם $f: H \to \mathbb{Z}_3 \times \mathbb{Z}_3$ כאשר $H = \langle 5 \rangle \leq (\mathbb{R}^*,\cdot)$
3. קיים מונומורפיזם $f: (GL_2(\mathbb{Q}),\cdot) \to (\mathbb{Q}^{10},+)$

פתרון:

1. נניח בשלילה שקיים איזומורפיזם. קיים C ב-$\mathbb{Q}$ כך ש-f(5)=C. אבל f אפי׳ ולכן קיים מקור ל-$\frac{C}{2}$ שנסמנו ב-x: $f(x) = \frac{C}{2}$. אמור להתקיים $f(x^2) = f(x \cdot x) = f(x) + f(x) = C = f(5)$ אבל f חח״ע ולכן $x^2 = 5$ וזאת סתירה.
2. H ציקלית, ו$\mathbb{Z}_3 \times \mathbb{Z}_3$ לא ציקלית (הראנו במהלך השיעור כי הסדר של כל איבר הוא לכל היותר 3 ולכן אין איבר מסדר 9). ולכן זו הפרכה, אין אפימורפיזם.
3. הפרכה: ראשית נסכים על הטענה שעבור $f: G \to H$ מונו׳ אזי ההעתקה על התמונה $G \to f(G)$ היא איזומורפיזם. אם קיים מונומורפיזם כנ״ל, אזי קיים איזומורפיזם לתת חבורה של $(\mathbb{Q}^{10},+)$, אבל זאת סתירה, כי $(\mathbb{Q}^{10},+)$ אבלית ועם זאת ידוע לנו כי $(GL_2(\mathbb{Q}),\cdot)$ אינה אבלית.

<u>**כולם הפרכות! בסתירה ללוגיקה של גיא ☺**</u>

<u>גרעין ותמונה:</u>

יהי $\varphi: G \to H$ הומומורפיזם

- $ker\varphi = \{g \in G: \varphi(g) = e_H\}$
- $Im\varphi = \{\varphi(g): g \in G\} = \{h \in H: \exists g \in G : \varphi(g) = h\}$,

ראינו בשיעור שמתקיים $\ker(f) \lhd G$, $\mathrm{Im}\varphi \leq H$.

<u>דוגמאות</u>:

1. $\varphi:\mathbb{Z}\times\mathbb{Z}_6\to\mathbb{Z}\times\mathbb{Z}_6$. $\varphi(n,k)=\big(2n,2k(\text{mod}6)\big)$.
$ker\varphi=\{0\}\times\{0,3\}, Im\varphi=2\mathbb{Z}\times\{0,2,4\}.$
2. $\mathbb{R}_3[x]$ החבורה החיבורית של פולינומים במקדמים ממשיים עד דרגה 3 כולל.
נגדיר $f:\mathbb{R}_3[x]\to\mathbb{R}_3[x]$ כך ש$f\big(p(x)\big)=p'(x)$
הפולינומים הקבועים $\ker(f)=\{c : c\in\mathbb{R}\}$
ועבור התמונה ברור כי $\text{Im(f)}\cong\mathbb{R}_2[x]$

- <u>צמודים (אתגר)</u>:
אם הסדר של חבורה G הוא אי זוגי , אזי אף איבר (פרט ליחידה) אינו צמוד להופכי שלו!

מופשטת 1, קיץ 2013

תרגול 7

הגדרה

תהי חבורה G. המרכז (center) של G הוא $Z(G)=\{g\in G|\forall x\in G: gx=xg\}$

כלומר, המרכז מורכב מאיברי G שמתחלפים עם כל אברי G.

מתקיים $Z(G)\lhd G$ וכן Z(G) אבלית

G אבלית $\Leftrightarrow G=Z(G)$.

שימו לב: המרכז תמיד לא ריק, שכן $e\in Z(G)$.

חבורת המנה

תהי G חבורה. $H\lhd G$. ניתן להגדיר מבנה חבורי על קבוצת המנה:

נסתכל באוסף הקוסטים השמאליים $G/_H=\{gH\mid g\in G\}$ שמוגדר כקבוצה לכל $H\le G$ (אך מוגדר כחבורה אמ"ם $H\lhd G$). הפעולה שמגדירים על $G/_H$ היא $aH\cdot bH=ab\cdot H$. איבר היחידה של $G/_H$ הוא: $e_GH=H$.

דוגמאות

א) תהא $G=(\mathbb{R}^2,+)$, נתבונן בתח"ג $H=R\times\{0\}$

$$\mathbb{R}^2/_H=\{(a,b)+H:(a,b)\in\mathbb{R}^2\}\cong\{\mathbb{R}\times\{b\}\}_{b\in\mathbb{R}}$$

זהו אוסף כל הישרים המקבילים לציר הX.

הערה:

תהא G חבורה סופית, $H\lhd G$, אזי האוסף $G/_H$ הוא כל המחלקות השמאליות ולכן מתקיים $|G/_H|=[G:H]=\frac{|G|}{|H|}$

תרגיל

תהי G חבורה וכן $H\lhd G$. נניח $[G:H]=n$. הראו כי לכל $a\in G$ מתקיים $a^n\in H$.

הוכחה

$G/_H$ חבורת מנה וכן $|G/_H| = n$. יהי $a \in G$ אזי $aH \in G/_H$. הוכחנו ש $\forall a \in G, a^{|G|} = e$ וכן לפי לגראנז׳

$(aH)^n = a^n H = H$ ולכן $H = a^n H \Rightarrow a^n \in H$.

תרגיל

תהא G ≥ H ת״ח מאינדקס 2 אזי $G/_H$ היא חבורה אבלית.

הוכחה

ראינו כי אם $[G:H] = 2$, אזי $G \triangleright H$ ולכן אנחנו יודעים כי $G/_H$ חבורה וגם $|G/_H| = 2$ ולכן $G/_H$ חבורה ציקלית ולכן אבלית. למעשה $G/_H \cong \mathbb{Z}_2$ כיוון שיש רק חבורה אחת מסדר 2 עד כדי איזומורפיזם.

תזכורת: $\Omega_\infty = \{z \in \mathbb{C}^* \mid \exists n \in N: z^n = 1\}$

תרגיל

תהי $\{z \in \mathbb{C}^* | \exists n \in \mathbb{N}: z^n = 1\} = \Omega_\infty$. הראו כי אם $a \in \mathbb{C}^*/_{\Omega_\infty}$ אינו איבר היחידה, אז הוא מסדר אינסופי

הוכחה

נניח בשלילה שקיים $a \in \mathbb{C}^*/_{\Omega_\infty}$ שאינו איבר היחידה והוא מסדר סופי. כלומר

1) a איננו איבר היחידה: $(a \in \mathbb{C}^*/_{\Omega_\infty} \to a = z\Omega_\infty)$ בפרט $a \notin \Omega_\infty \Rightarrow z \neq \Omega_\infty$.
2) a מסדר סופי ולכן קיים $k \in \mathbb{N}$ כך ש: $a^k = \Omega_\infty$. בפרט:

$$(z\Omega_\infty)^k = z^k\Omega_\infty = \Omega_\infty \Rightarrow z^k \in \Omega_\infty \Rightarrow \exists m \in \mathbb{N}: (z^k)^m = z^{kn} = 1$$

אבל זה בפרט גורר ש $z \in \Omega_\infty$ בסתירה להנחה.

מ.ש.ל ■

משפט האיזומורפיזם הראשון

תהיינה G, H חבורות, ויהי $\varphi: G \to H$ אפימורפיזם, אז $G/_{\ker(\varphi)} \cong H$.

(גרסה נוספת) אם φ הוא הומו׳ אז $G/_{\ker(\varphi)} \cong Im(\varphi)$.

תרגיל

נניח וקיים הומומורפיזם $f: \mathbb{Z}_{14} \to D_{10}$. מה יכול להיות הסדר של $\ker(f)$?

פתרון

נזכר כי $\mathbb{Z}_{14} \rhd \ker(f)$ ולכן יתקיים $|\ker(f)| \mid |\mathbb{Z}_{14}|$ ז״א $|\ker(f)| \in \{1,2,7,14\}$.

נבדוק את האפשרויות:

- $|\ker(f)| = 1 \Leftarrow$ f חח״ע
  $\mathbb{Z}_{14}/_{\ker f} \cong Im(f) \leq D_{10}$, ולכן $|\mathbb{Z}_{14}/_{kerf}| = |Im(f)| \mid |D_{10}| = 20$ אבל $14 \nmid 20$ בסתירה.
  אפשרות זו לא אפשרית.
- $|\ker(f)| = 2$ ואז $|\mathbb{Z}_{14}/_{\ker(f)}| = \frac{|\mathbb{Z}_{14}|}{|\ker(f)|} = \frac{14}{2} = 7$ אבל $7 \nmid 20$.
- $|ker(f)| = 7$ ואז $|\mathbb{Z}_{14}/_{\ker(f)}| = 2 \mid 20$. נראה כי אכן קיימת תת חבורה כזו, לדוגמא $H = \{e, \tau\} \leq D_{10}$

צריך לבנות אפימורפיזם $\varphi: \mathbb{Z}_{14} \to H$ (נניח $k \mapsto \tau^k$). הגרעין יהיה תת חבורה מסדר 7, ולכן $\ker(f) \cong \mathbb{Z}_7$

- $|\ker(f)| = 14$ במקרה זה מקבלים $\ker(f) \cong \mathbb{Z}_{14}$ כלומר מקבלים את ההומומורפיזם הטריוויאלי.($k \mapsto id$).

מ.ש.ל.

טענה

תהי G חבורה, נניח כי חבורת המנה $G/_{Z(G)}$ היא צקלית, אז היא חבורת המנה הטריוויאלית (נקבל $|G/_{Z(G)}| = 1$).

בניסוח שונה: אם G איננה אבלית אז חבורת המנה $G/_{Z(G)}$ איננה ציקלית לא-טריוויאלית.

הוכחה

נניח ש- $G/Z(G)$ ציקלית, ונוכיח ש- G אבלית (כלומר, $G = Z(G)$).

$G/_{Z(G)}$ ציקלית ולכן קיים $a \in G$ כך ש $G/_{Z(G)} = \langle aZ(G) \rangle$ ושימו לב כי כיוון ו $Z(G) \leq G$ וכן $xZ(G)$ הם קוסטים וכל חבורה היא איחוד זר של הקוסטים שלה מתקיים

$$G = \bigsqcup_{x \in G} xZ(G)$$

כ״כ $xZ(G) \in G/_{Z(G)} \Leftarrow xZ(G) = (aZ(G))^i = a^i Z(G)$ $\exists i:$ ולכן

$$G=\bigsqcup_{i\in\mathbb{Z}} a^iZ(G)$$

כעת נראה שG אבלית: יהיו $b,c\in G$ וצ"ל $bc=cb$. כיוון ו$b,c\in G$

$$\exists i,j: b\in a^iZ(G), c\in a^jZ(G) \Rightarrow \exists k,t\in Z(G): b=a^ik, c=a^jt$$

ונובע:

$$bc=a^ika^jt=a^ikta^j=a^itka^j=cb$$

ולכן G אבלית כדרוש. ■

משפט האיזומורפיזם השני

תהי G חבורה, $H\le G, N\lhd G$, אזי:

א) $H\cap N\lhd H$

ב) $H/_{H\cap N}\cong HN/_N$

תרגיל

תהי G חבורה סופית, תהאG ⊲ H תח"נ כך ש $\gcd(|H|,[G:H])=1$. הוכח כי H היא תת חבורה שמכילה כל מה שהיא יכולה, או ליתר דיוק, הראו כי תת חבורה שהסדר שלה מחלק את $|H|$, מוכלת ב-H.

הסיקו כי H היא תת החבורה היחידה מסדר |H|.

פתרון

תהא $K\le G$. נניח $|K|\,|\,|H|$. $H\lhd G\Rightarrow HK\le G$ כמו כן ברור כי $H\cap K$ ת"ח של H,K,G.

מכפליות האינדקס נקבל כי

$$[G:H]=[G:HK][HK:H]$$

מכאן רואים כי $[HK:H]|\,[G:H]$

מפני ש-$HK\lhd H$ נפעיל את איזו השני ונקבל כי $HK/_H\cong H/_{K\cap H}$. בפרט $[HK:H]=[H:H\cap K]$ ומכאן $[KH:H]\,\big|\,|K|\,\big|\,|H|$ וגם $[HK:H]\,|\,|K|$. על פי הנתון $\gcd(|H|,[G:H])=1$

מכאן $[HK:H]=1=[H:H\cap K]$.

כלומר $K = K \cap H$ והוכחנו כי $K \leq H$. מכאן אפשר להסיק כי אם $|H| = |K|$, אז $\mathrm{K} = \mathrm{H}$. כלומר H היא תת החבורה היחידה מסדר $|H|$.

מ.ש.ל.

מסקנה נחמדה מהתרגיל: לכל $x \in G$, אם $x^{|H|} = e_G$ אזי $x \in H$.

הגדרה

תהי G חבורה, אזי $Aut(G) = \{f: G \to G | \text{איזומורפיזם } f\}$ שהיא חבורת האוטומורפיזמים של G. זו חבורה ביחס לפעולת ההרכבה ואיבר היחידה בה הוא העתקת הזהות.

דוגמא

תהא G אבלית מסדר n. יהי $k \in \mathbb{N}$ כך ש $(n,k) = 1$. העתקה $f: G \to G$ המוגדרת לפי $f(x) = x^k$ היא איזומורפיזם, ולכן f היא אוטומורפיזם. למשל $U_9 = \{1,2,4,5,7,8\}$, נשים לב ש $|U_9| = 6$. ולכן $x \mapsto x^5$ הוא אוטומורפיזם של U_9.

טענות (ראיתם בכיתה)

א) $Ant(\mathbb{Z}) \cong \mathbb{Z}_2$

ב) $Ant(\mathbb{Z}_n) \cong U_n$

תרגיל

הראו כי $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$.

<u>הוכחה</u>:

תחילה $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$. כל אוטומורפיזם שולח את $(0,0)$ לעצמו ואת הקבוצה $\{a,b,c\}$ לעצמה. האוטו׳ חח״ע ועל ולכן כל אוטומורפיזם הוא למעשה <u>תמורה</u> על קבוצה $\{a,b,c\}$, כלומר בפרט $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2)$ היא אכן ת״ח של S_3. כמו כן כל תמורה בS_3 מגדירה אוטומורפיזם (בדקו!). מ.ש.ל. ■

אלגברה מופשטת 1

תרגול 8

הגדרה: $\varphi : A \to A$ פונקציה. איבר $a \in A$ נקרא נקודת שבת אם $\varphi(a) = a$.

תרגיל:

תהא G חבורה סופית ו$\varphi \in Aut(G)$ אוטומורפיזם שנקודת השבת היחידה שלו היא איבר היחידה של G. הוכיחו:

א.לכל $g \in G$ קיים $x \in G$ כך ש$g = x^{-1}\varphi(x)$;

ב.אם $\varphi \circ \varphi = Id_G$ אזי G אבלית.

פתרון:

א. נתבונן בפונקציה $f : G \to G$ המוגדרת ע"י $f(x) = x^{-1}\varphi(x)$. נוכיח שf חח"ע: נניח שf(a)=f(b) כלומר $a^{-1}\varphi(a) = b^{-1}\varphi(b)$

$\Leftarrow ba^{-1} = \varphi(b)\varphi(a)^{-1}$ וז"א $\varphi(ba^{-1}) = ba^{-1} \Leftarrow ba^{-1}$ היא נקודת שבת של φ ולכן $ba^{-1} = e$

ולכן $b = a \Leftarrow$ f חח"ע ולכן f על ולכן לכל $g \in G$ קיים $x \in G$ כך ש $f(x) = g \Rightarrow x^{-1}\varphi(x) = g$.

ב. $g = x^{-1}\varphi(x)$. נפעיל φ: $\varphi(g) = \varphi(x^{-1}\varphi(x)) = \varphi(x^{-1})\varphi(\varphi(x)) = \varphi(x^{-1})x =$ $\varphi(x)^{-1}x = (x^{-1}\varphi(x))^{-1} = g^{-1} \Leftarrow \varphi(g) = g^{-1}$.

יהיו $a, b \in G$ וצ"ל: $ba = ab$.

$\varphi((ab)^{-1}) = ab$ ומצד שני $\varphi((ab)^{-1}) = \varphi(b^{-1}a^{-1}) = \varphi(b^{-1}) \cdot \varphi(a)^{-1} = ba \Leftarrow ab = ba$.

מ.ש.ל □.

אוטומורפיזמים פנימיים - Inner Automorphisms

הגדרה: תהא G חבורה, $a \in G$. אוטומורפיזם $\gamma_a(x) = axa^{-1}$ נקרא אוטומורפיזם פנימי או אוטו' ההצמדה. נסמן: $Inn(G) = \{\gamma_a : a \in G\}$. הוכחתם בהרצאה: $Inn(G) \triangleleft Aut(G)$.

טענה: ניתן להגדיר הומומורפיזם: $F : G \to Inn(G), a \mapsto \gamma_a$ (כאשר γ_a פונקציה)

$Ker(F) = \{a \in G : \gamma_a = Id_g\} = \{a \in G : \gamma_a(x) = x \forall x \in G\} =$

$$\{a\in G: axa^{-1}=x\forall x\in G\}=\{a\in G: ax=xa\forall x\in G\}=Z(G)$$

לפי איזו 1:

$G/_{Z(G)}\cong Inn(G)$ כאשר $Z(G)=\{g\in G: gx=xg\forall x\in G\}$ ←זה אומר למשל ש$Inn(G)$ אינה ציקלית! [כי הוכחנו ש$G/_{Z(G)}$איננה ציקלית].

<u>תרגיל:</u>

תהא $\left\{\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}: a,b,c\in\mathbb{Z}_3\right\}=G$. חשבו $|Inn(G)|$.

<u>פתרון:</u>

למעשה נחשב $|G/_{Z(G)}|=?$. $|G|=27$. נראה מהו $|Z(G)|$:

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

- $|Z(G)|\neq 27$ כי החבורה איננה אבלית.
- $|Z(G)|\neq 1$ כי למשל $\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix},\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}\in G$ (בדקו !)
- אם $|Z(G)|=9$ אז $|G/_{Z(G)}|=\frac{27}{9}=3$ לא יתכן כי כל חבורה מסדר ראשוני היא ציקלית ו$G/_{Z(G)}$ איננה ציקלית.
- נובע כי $|Z(G)|=3$ ולכן $|Inn(G)|=9$.

<u>סדרי איברים בחבורת התמורות</u>

עבור מחזור $\sigma\in S_n$באורך k מתקיים $o(\sigma)=k$ למשל $o\begin{pmatrix}1&2&4&7\end{pmatrix}=4$.

<u>טענה:</u> (הוכחתם בהרצאה)

תהא G חבורה, $a,b\in G$ כך ש$ab=ba$ ו־$<a>\cap<b>=e_G$ אזי $o(ab)=lcm(o(a),o(b))$.

<u>מסקנה:</u> סדר מכפלת מחזורים זרים הוא הכפולה המשותפת המינימלית של סדרי המחזורים.

$$o\left(\underbrace{\begin{pmatrix}1 & 2 & 3\end{pmatrix}}_{=a}\underbrace{\begin{pmatrix}4 & 5\end{pmatrix}}_{=b}\right)=lcm(3,2)=6$$

<u>תרגיל:</u> מצאו ת"ח מסדר 45 בS_{15}.

<u>פתרון:</u>

$$a=\begin{pmatrix}1 & 2 & 3 & 4 & 5\end{pmatrix}(\begin{matrix}6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14\end{matrix})$$
$$o(a)=lcm(9,5)=45$$

ולכן $H=\langle a\rangle$ היא ת"ח מסדר 45 של S_{15}. מ.ש.ל

<u>הערה:</u>

כל מחזור ב־S_nניתן לכתיבה כמכפלה של חילופים:

$$\begin{pmatrix}a_1 & a_2 & \dots & a_r\end{pmatrix}=\begin{pmatrix}a_1 & a_2\end{pmatrix}\begin{pmatrix}a_2 & a_3\end{pmatrix}\cdots\begin{pmatrix}a_{r-1} & a_r\end{pmatrix}$$ ולכן $$S_n=\left\langle\begin{pmatrix}i & j\end{pmatrix}:1\le i,j\le n\right\rangle$$

כלומר S_n נוצרת ע"י חילופים.

<u>תרגיל:</u> כמה מחזורים מסדר r יש בS_n?

<u>פתרון:</u>

ראשית יש לבחור r איברים מתוך n ויש $\binom{n}{r}$ דרכים לעשות זאת. שנית, את r האיברים שבחרנו ניתן לסדר ב$r!$דרכים שונות.

עם זאת המחזורים $\begin{pmatrix}a_1 & a_2 & \dots & a_r\end{pmatrix},\begin{pmatrix}a_2 & \dots & a_r & a_1\end{pmatrix},\begin{pmatrix}a_r & a_1 & \dots & a_{r-1}\end{pmatrix}$ הם שווים ולכן יש לחלק ב r את מספר האפשרויות.

בסהכ נקבל שיש $\binom{n}{r}\cdot\frac{r!}{r}=\binom{n}{r}\cdot(r-1)!$ מחזורים שונים.

<u>תרגיל:</u>

מהם הסדרים האפשריים של איברים ב־S_4? בS_5?

<u>פתרון:</u>

<u>S_4: להלן הסדרים האפשריים</u>

סדר	איבר לדוגמה
1	id
2	(1,2)
3	(1,3,2)
4	(1,2,3,4)

לגבי S_5:

סדר	איבר לדוגמה
1	id
2	$(35)(14)$
3	(1345)
4	(12345)
5	$(12)(345)$
6	$(12)(345)$

<u>מסקנה:</u>

האם $D_{12} \cong S_4$? לא כי יש בD_{12}יש איבר מסדר 12 ($O(\sigma)=12$) ובS_4אין איבר שכזה.

<u>טענה:</u>

ראיתם בכיתה:

<u>1. תמורות הן צמודות $\Leftrightarrow$יש להן אותו מבנה מחזורים.</u>

2.תהי $\mu \in S_n$ אזי $\mu(\ i_1 \quad i_2 \quad \ldots \quad i_k\ )\mu^{-1} = (\ \mu(i_1) \quad \ldots \quad \mu(i_k)\ )$.

למשל: $(132)(12)(132)^{-1} = (31)$. התמורה (12) צמודה ל(31).

עוד דוגמה שמוכיחה את חשיבות הנוסחה (ניתן להעזר לגבי תתי חבורות נורמליות ולגבי חישוב מי המתחלף עם תמורה ואזי מי המרכז):

$(132)(1354)(132)^{-1} = (3254)$

- למשל התמורה $(132)(54)$אינה צמודה ל(13254).

<u>דוגמה:</u>

יהיו $\alpha=(245), \beta=(135), \sigma=(35)$. חשבו:

א.$\alpha\sigma\alpha^{-1}=?$

ב.$\alpha\beta\alpha^{-1}=?$

<u>פתרונות:</u>

א.(32)

ב.(132)

<u>תרגיל:</u> הוכיחו $S_n = \left\langle (12) \begin{pmatrix} 1 & 2 & 3 & ... & n \end{pmatrix} \right\rangle$

<u>פתרון:</u> הוכח בהרצאה.

<u>הגדרה:</u>סימן של תמורה יהי σ מחזור באורך k, אזי $sign(\sigma) = (-1)^{k+1}$. הסימן הוא פונקציה כפלית. $sign(\sigma\tau) = sign(\sigma)sign(\tau)$.

<u>למשל:</u>

- $sign(132) = 1$
- $sign((13)(56)) = 1$

הגדרת ת"ח של S_n: $A_n = \{\sigma \in S_n : sign(\sigma) = 1\}$ וראיתם:

א. $A_n \triangleleft S_n$

ב. $| A_n |= \frac{n!}{2}$

<u>למשל:</u> $\left\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \right\rangle = A_3 = \{id, (123), (132)\}$

<u>תרגיל:</u>

מהם סידרי האיברים בA_4? האם $A_4 \cong D_6$?

<u>פתרון:</u>

$A_4 = \{id, (--)(--), (---)\}$. הסדרים האפשריים: 1,2,3. $A_4 \ncong D_6$ כי ב־D_6 יש איבר יחידה מסדר 6.

<u>תרגיל מאוד מאוד מאוד חשוב משבוע שעבר על אוטומורפימים</u>

<u>תרגיל:</u>

הוכיחו את הטענה הבאה: לכל שתי חבורות G, H קיים שיכון: $Aut(G) \times Aut(H) \hookrightarrow Aut(G \times H)$.

(*) השיכון הנ"ל הוא איזומורפיזם, אם מתקיים $\left(|G| \quad |H| \right) = 1$. ההוכחה קצת ארוכה ואתם מוזמנים לנסות בבית.

<u>הוכחה:</u>

נרצה למצוא מונומורפיזם $F : Aut(G) \times Aut(h) \to Aut(G \times H)$ כך ש- $F(\varphi, \psi) = \varphi \times \psi$ כאשר $\varphi \times \psi(g, h) = (\varphi(g), \psi(h))$.

<u>יש להראות:</u>

<u>1.</u> $\varphi \times \psi \in Aut(G \times H)$ (מוגדרות של F)

2. F הומומורפיזם

3. F חח"ע

<u>נוכיח את 2:</u> מה צ"ל?

$$(\varphi_1 \circ \varphi_2) \times (\psi_1 \circ \psi_2) = F(\varphi_1 \circ \varphi_2, \psi_1 \circ \psi_2) = F(\varphi_1, \psi_1)(\varphi_2, \psi_2)) = F(\varphi_1, \psi_1) \circ F(\varphi_2, \psi_2)$$

$\Rightarrow (\varphi_1 \times \psi_1) \circ (\varphi_2 \times \psi_2) = (\varphi_1 \circ \varphi_2) \times (\psi_1 \circ \psi_2)$. נראה ששתי הפונקציות מתלכדות.

צ"ל:

$$(\varphi_1 \times \psi_1) \circ (\varphi_2 \times \psi_2)(g, h) = (\varphi_1 \circ \varphi_2) \times (\psi_1 \circ \psi_2)(g, h) \forall (g, h) \in G \times H$$

כלומר:

$$(\varphi_1 \times \psi_1) \circ (\varphi_2 \times \psi_2)(g, h) = (\psi_1 \times \psi_1)(\varphi_2(g), \psi_2(h)) = (\psi_1 \psi_2(g), \psi_1 \psi_2(h))$$

$$(\varphi_1 \circ \varphi_2) \times (\psi_1 \circ \psi_2)(g, h) = (\psi_1 \psi_2(g), \psi_1 \psi_2(h))$$

וניתן להראות שהפונקציות אכן שוות.

מ.ש.ל $\square$

נ.ב: בבית ניתן להוכיח חחע עפ"י החחע של φ, ψ ומכפלה של חחע ועל היא חחע ועל.

אלגברה מופשטת 1, קיץ 2013
תרגול 9

תרגיל:

הוכיחו שהמרכז של החבורה הסימטרית S_n עבור $n \geq 3$ הוא טריוויאלי. $(Z(S_n) = \{id\})$

פתרון:

נניח בשלילה שקיים $id \neq a \in Z(S_n)$. $Z(S_n) \lhd S_n$. $a \neq b \in S_n$: $\underline{bab^{-1} \in Z(S_n)}$.
יש ל־a מבנה מחזורים מסוים, יש ב S_n, $a \neq b \in S_n$ עם אותו מבנה מחזורים. לכן, a ו b צמודות. לכן קיימת c : $cac^{-1} = b$ אבל $cac^{-1} = acc^{-1}$ כיוון ש $a \in Z(S_n)$. ז"א $acc^{-1} = b \Leftarrow a = b$. בסתירה לכך שבחרנו $a \neq b$. לכן המרכז טריוויאלי.
מ.ש.ל $\square$

הערה:

$H \lhd G \Leftrightarrow \forall g \in G \forall h \in H: ghg^{-1} \in H$ ב S_n: אם $H \rhd S_n$ אזי היא מכילה את כל התמורות ממבנה מחזורים של תמורותיה. אם H "רוצה להיות" נורמלית ב S_{10} והיא מכילה את התמורה $(123)(57)$ אז היא אמורה להכיל את כל אלו: $(---)(--)$.

תרגיל:

הוכיחו של A_4 אין תת חבורה מסדר 6.

פתרון:

$|A_4| = 12$. נניח בשלילה שקיימת ת"ח $H \leq A_4$ כך ש $|H| = 6$. $\frac{|A_4|}{|H|} = \Leftarrow$ $[A_4 : H] = 2$ $H \lhd A_4$. יהי $\sigma \in A_4$ מחזור באורך 3 $\Leftarrow \sigma^2 \in H$ ($[G:H] = m$ אזי לכל $a \in G$: $a^m \in H$). H ת"ח ולכן גם $\sigma = \sigma^4 = \sigma^2\sigma^2 \in H \Rightarrow \sigma \in H$. כלומר כל מחזור באורך 3 שייך ל H אך יש $\binom{4}{3}2! = 8$ מחזורים מאורך, וזו סתירה כי $|H| = 6 < 8$. לכן, אין ל A_4 ת"ח מסדר 6. מ.ש.ל

התרגיל המרכזי

מיינו את כל החבורות מסדר 6.

פתרון:

נוכיח: $|G| = 6 \leftarrow G \cong \mathbb{Z}_6$ או $G \cong D_3$. תהא G חבורה מסדר 6.

- אם קיים איבר מסדר 6 אזי G ציקלית ולכן $G \cong \mathbb{Z}_6$.
- נניח שאין איבר מסדר 6.

- אם כל האיברים מסדר 2 אזי:

- סתירה ראשונה: G אבלית . כל האיברים מסדר 2 ואז היא איזומרפית למ"ו מעל $\mathbb{Z}_2$ ולכן הגודל שלה חזקה של 2 אבל 6 לא חזקה של 2 ולכן קיבלנו סתירה.

- סתירה אחרת:G אבלית. ניקח $1 \neq a \neq b \in G$ שני איברים מסדר 2. נתבונן במבנה $H = \{1, a, b, ab\}$. נשים לב שזו היא למעשה תת חבורה, אבל $|H| = 4 \nmid 6$ וזו סתירה למשפט לגרנז'⇐לא כל האיברים הם מסדר 2.

- <u>קיים איבר $a \in G$מסדר 3:</u> יהי $b \notin < a >$ ($|\langle a \rangle| = 3$)אזי $b^2 \in \langle a \rangle$ (כי $[G : \langle a \rangle] = 2$).

  טענה:$b^2 = 1$

- הוכחה: יש לפסול שני מקרים:

- $1.b^2 = a$

- $2.b^2 = a^2$

נתייחס לכל מקרה לגופו:

<u>מקרה 1</u>

אם $b^2 = a$אזי $b^6 = 1$. לכן, הסדר של $b = 1, 2, 3, 6$.

6 לא יתכן. הנחנו שאין איבר מסדר 6.

2 לא יתכן(כיא אזי $a = b^2 = 1 \Leftarrow a = 1$)

1 לא יתכן כי $b \neq 1$

3 לא יתכן כי אזי:$b^2 = ab \Leftarrow ba = 1$ונובע ש$b \in < a >$כי הוא ההופכי של a.

<u>מקרה 2</u>

$b^2 = a^2$לא יתכן באותו אופן כמו (1). בדקו בבית.

$\Leftarrow b^2 = 1$ומ.ש.ל הטענה

כעת יש לנו איבר מסדר 3 ואיבר מסדר 2 ונראה אילו יחסים הם מקיימים:

$bab^{-1} \in \langle a \rangle$(כי $\langle a \rangle \triangleleft G$)⇐$bab^{-1} \in \{1, a, a^2\}$

א. $bab^{-1} = 1 \Rightarrow ba = b \Rightarrow a = 1$וזו סתירה.

ב.$bab^{-1} = a \Leftarrow$

- $ba = ab$

- $\langle a \rangle \cap \langle b \rangle = \{1\}$

$o(ab)=lcm(3,2)=6\Leftarrow$אבל הנחנו שאין איבר מסדר 6 ולכן מקרה זה לא אפשרי.

(ג.זה המקרה הנותר: $bab^{-1}=a^2$ [מסגר]. נובע:

$$b\notin\langle a\rangle\wedge[G:\langle a\rangle]=2\Rightarrow G=\langle a\rangle\cup b\langle a\rangle=\{1,a,a^2,b,ba,ba^2\}$$

ומתקיימים היחסים: $b^2=a^3=1$וכן $bab^{-1}=a^2$. לכן $G\cong D_3$.

תרגיל:

העזרו בהוכחת משפט קיילי על מנת לשכן את D_4בS_8.

פתרון:

כאן נשכן איבר אחד (על אף שבבית ניתן לשכן את כל השמונה):

לפי קיילי קיים מונומורפיזם $D_4\to S_8$.

נמספר את איברי החבורה במספרים בין 1 ל8 באופן הבא:

$$D_4=\begin{matrix}1&2&3&4&5&6&7&8\\ \{id,&\tau,&\sigma,&\tau\sigma,&\tau\sigma^2,&\tau\sigma^3,&\tau\sigma^4,&\tau\sigma^5\}\end{matrix}$$

המטרה: לבדוק לאיזו תמורה בS_8עובר האיבר τ.

לפי קיילי: $l_\tau\mapsto\tau$, $l_\tau(x)=\tau x$. על מנת למצוא את l_τ נבדוק אילו ערכים היא מקבלת על כל אחד מאיברי D_4.

$$l_\tau(id)=\tau id=\tau,1\to 2$$
$$l_\tau(\tau)=\tau\tau=id,2\to 1$$
$$l_\tau(\sigma)\tau\sigma,3\to 6$$
$$l_\tau(\sigma^2)=\tau\sigma^2,4\to 7$$
$$l_\tau(\sigma^3)=\tau\sigma^3,5\to 8$$
$$l_\tau(\tau\sigma)=\tau\tau\sigma=\sigma,6\to 3$$
$$l_\tau(\tau\sigma^2)=\sigma^2,7\to 4$$
$$l_\tau(\tau\sigma^3)=\sigma^3,8\to 5$$

כלומר:

$$\tau\to(12)(36)(47)(58)$$

מ.ש.ל □

פירוק חבורות אבליות

טענה 1

תהא G חבורה אבלית מסדר $p_1...p_k$(ראשוניים שונים). אזי $G \cong \mathbb{Z}_{p_1} \times ... \times \mathbb{Z}_{p_k}$.

למשל: חבורה אבלית מסדר 15 איזומורפית ל$\mathbb{Z}_3 \times \mathbb{Z}_5$.

טענה 2:

תהא G חבורה אבלית מסדר p^nאזי קיימים $m_1 + ... + m_k = n$כך ש: $G \cong \mathbb{Z}_p m_1 \times ... \times \mathbb{Z}_p m_k$ למשל, אם G אבלית מסדר 27 אזי:

$$G \cong \begin{cases} \nearrow & \mathbb{Z}_{27} \\ \rightarrow & \mathbb{Z}_9 \times \mathbb{Z}_3 \\ \searrow & \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \end{cases}$$

הגדרה:

עבור $n \in \mathbb{N}$נסמן ב$\rho(n)$את מספר הסדרות הלא עולות $\{s_i\}_{i=1}^r$: $S_1 \geq S_2 \geq ... \geq .S_r$

למשל:$\rho(4) = 5$ שכן האפשרויות הן:

$(1,1,1,1)$

$(1,1,2)$

$(1,3)$

$(2,2)$

(4)

טענה 3:

מס' החבורות האבליות עד כדי איזו' מסדר p^nהוא $\rho(n)$.

לסיכום:

כל חבורה אבלית מסדר $p_1^{k_1} \cdot ... \cdot p_n^{k_n}$ איזומורפית למכפלה $Hp_1 \times ... \times Hp_n$.

כאשר Hp_iהן ת"ח שאיזומורפיות לחבורה אבלית מסדר $p_i^{k_i}$.

תרגיל:

הוכיחו:$\mathbb{Z}_{100} \oplus \mathbb{Z}_{40} \cong \mathbb{Z}_{200} \oplus \mathbb{Z}_{20}$.

פתרון:

הקדמה:

$100 = 25 \cdot 4, 40 = 5 \cdot 8, 200 = 25 \cdot 8, 20 = 5 \cdot 4, (m,n) = 1 \Leftrightarrow \mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

ולכן:

$\mathbb{Z}_{25} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_8 = \mathbb{Z}_{25} \oplus \mathbb{Z}_{20} \oplus \mathbb{Z}_8 =_{(25,8)=1}= \mathbb{Z}_{200} \oplus \mathbb{Z}_{20}$. מ.ש.ל

תזכורת:

נניח $(m,n) = 1$אזי $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. הפונקציות המפורשות הן:

$.f(x) = (x(\mod m), x(\mod n))$,$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ $g : \mathbb{Z}_m \times \mathbb{Z}_n \to$
$\mathbb{Z}_{mn}$, $g(\underline{x}, y) = \beta\underline{n}x + \alpha my$ כאשר $.\alpha m + \beta n = 1$

<u>תרגיל:</u>

מצאו איזומורפיזם מפורש מ$A = \mathbb{Z}_{77} \times \mathbb{Z}_5$ ל$.B = \mathbb{Z}_{11} \times \mathbb{Z}_{35}$

<u>פתרון:</u>

שלב ראשון: הפונקציה $f : \mathbb{Z}_{77} \to \mathbb{Z}_{11} \times \mathbb{Z}_7$ המוגדרת ע"י $f(x) = (x \mod 11, x \mod 7)$
היא איזומורפיזם.לכן גם הפונקציה $h_1 : \mathbb{Z}_{77} \times \mathbb{Z}_5 \to \mathbb{Z}_{11} \times \mathbb{Z}_7 \times \mathbb{Z}_5$ המוגדרת ע"י
$h_1(x, y) = (x \mod 11, x \mod 7, y)$ היא איזומורפיזם (ברכיב הראשון היא
fוברכיב השני היא פונקציה קבועה).

שלב שני:הפונקציה $g : \mathbb{Z}_7 \times \mathbb{Z}_5 \to \mathbb{Z}_{35}$ המוגדרת ע"י $g(x, y) = 15x - 14y$ היא
איזומורפיזם לפי התרגיל הקודם (אכן, שימו לב שמתקיים $1 = 5 \cdot (3) + 7 \cdot (-2)$).
לכן גם הפונקציה $h_2 : \mathbb{Z}_{11} \times \mathbb{Z}_7 \to \mathbb{Z}_5 \times \mathbb{Z}_{11} \times \mathbb{Z}_{35}$המוגדרת ע"י
$h_2(x, y, z) = (x, 15y - 14z)$ היא איזומורפיזם.

שלב שלישי: האיזומורפיזם הדרוש הוא ההרכבה $h_2 \circ h_1$ המוגדרת ע"י
$(x, y) \mapsto (x, 15x - 14y)$

מ.ש.ל $\square$

<u>מכפלה חצי ישרה (ישרה למחצה) פנימית</u>

<u>הגדרה:</u> אם $K, Q \leq G$ הן ת"ח המקיימות:

1. $K \lhd G$
2. $K \cap Q = \{1\}$
3. $G = KQ$

אזי אומרים ש־G היא מכפלה ישרה למחצה פנימית של K בQ. סימון: $G = K \rtimes Q$.

אגב, אם גם $Q \lhd G$ אזי מקבלים את ההגדרה של המכפלה הישרה הפנימית.

<u>תרגיל:</u>

הוכיחו שחבורת המטריצות $G = \left\{ \begin{pmatrix} x & a \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F}^*, a \in F \right\}$ היא מכפלה
ישרה למחצה פנימית: $\underbrace{\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} : a \in \mathbb{F} \right\}}_{=A} \rtimes \underbrace{\left\{ \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} : x \in \mathbb{F}^+ \right\}}_{=B}$

<u>פתרון:</u>

1. צל A,B ת"ח ←קל (בדקו בבית).

2. $A \triangleleft G$: יהי $G \ni \begin{pmatrix} x & b \\ 0 & 1 \end{pmatrix} = g$ אזי

$$gAg^{-1} = \left\{ \begin{pmatrix} x & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{x} & \frac{-b}{x} \\ 0 & 1 \end{pmatrix} ... \right\} = \left\{ \begin{pmatrix} x & xa+b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{1}{x} & \frac{-b}{x} \\ 0 & 1 \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & xa \\ 0 & 1 \end{pmatrix} \right\} = A$$

3. $A \cap B = \{id\}$ ⇐קל. (בדקו בבית).

4. $G = AB$:

$$G \ni \begin{pmatrix} x & a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}$$

והוכחנו את הדרוש.

■

אלגברה מופשטת 1,קיץ 2013

תרגיל 10

תזכורת: תהא G חבורה. G תקרא מכפלה ישרה למחצה של H ב־K אם:

1.$K \triangleleft G$

2.$K \cap H = \{e\}$

3.$KH = G$

ומסמנים $G = K \rtimes H$.

תרגיל:

הראו כי החבורות $\mathbb{Z}_6$,S_3 הן מכפלות ישרות למחצה של תת חבורות שלהן מגודל 2 ו־3.

פתרון:

כל החבורות מסדר 2 איזו' ל־$\mathbb{Z}_2$ וכל החבורות מסדר 3 איזו' ל־$\mathbb{Z}_3$.

א. $\mathbb{Z}_6 = \{0,2,4\} \rtimes \{0,3\}$. במקרה זה מפני שהחבורה $\mathbb{Z}_6$ אבלית, ודאי ש$\{0,2,4\} \triangleleft \mathbb{Z}_6$. כמו כן ע"י חישוב ישיר $\{0,2,4\} \cap \{0,3\} = \{0\}$ וגם $\mathbb{Z}_6 = \{0,2,4\} + \{0,3\}$.

ב. $S_3 = \left\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \right\rangle_{=K} \rtimes \left\langle \begin{pmatrix} 1 & 2 \end{pmatrix} \right\rangle_{=H}$. נבדוק נורמליות: $[S_3 : K] = 2$ (לפי לגראנז') ואזי $K \triangleleft S_3$. חישוב ישיר יראה כי $K \cap H = \{id\}$. הראנו בתרגול הקודם ש$S_3 = KH$. S_3 היא מכפלה ישרה למחצה פנימית של ת"ח מסדר 3 בת"ח מסדר 2. שימו לב שהיא **לא** מכפלה ישרה למחצה פנימית של ת"ח מסדר 2 בת"ח מסדר 3, שכן אין לה תתי חבורות נורמליות מסדר 2.

מחלקות צמידות

הגדרה:תהי G חבורה ויהי $x \in G$ אז מחלקת הצמידות של x ב־G היא

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

תכונות:

1.מחלקות צמידות הן יחס שקילות. (הוכח בהרצאה).

2.$x \in conj(x)$.

3.Gאבלית ⇔לכל $x \in G$מתקיים $conj(x) = \{x\}$.

4.(הכללה ל3) $x \in Z(G) \Leftrightarrow conj(x) = \{x\}$.

5. $conj(e) = \{e\}$.

תרגיל:

מצאו את מספר התמורות הצמודות לתמורה הבאה:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \end{pmatrix}\begin{pmatrix} 5 & 6 \end{pmatrix}\begin{pmatrix} 7 & 8 \end{pmatrix} \in S_8$$

פתרון:אנו נדרשים לחשב את $|\ conj(\pi)\ |$. האיברים ב$conj(\pi)$ הן תמורות צמודות ל־π ולכן בעלות אותו מבנה מחזורים. כלומר יש לבחור 4 מספרים למחזור מסדר 4 וכאלו יש לנו $\binom{8}{4}\cdot 3!$. יש לבחור את החילוף הראשון, ויש לנו $\binom{4}{2}$ אפשרויות והחילוף השני נקבע לחלוטין. סדר החילופים לא חשוב ולכן צריך לחלק ב־2 את מספר האפשרויות. סה"כ קיבלנו $\frac{\binom{8}{3}\cdot 3!\cdot\binom{4}{2}}{2!}$ תמורות שצמודות לπ.

הערות:

א.מחלקות הצמידות, פרט למקרה הטריוויאלי של איבר היחידה, אינן תת חבורות (לדוגמה אין את איבר היחידה באף אחת מהן).

ב.תהא G סופית אזי $|conj(x)|\ |\ |G|$. (נראה הסבר בהמשך. מדובר באינדקס המייצב של xביחס לפעולת ההצמדה)

תרגיל:

כמה מחלקות צמידות יש בחבורות הבאות:

א.S_4

ב.A_4

פתרון:

(נפתר גם בהרצאה אצל רוני).

א. מחלקות הצמידות הן: $conj(id), conj((**)), conj((***)), conj((**)(**)), conj((****))$

. סה"כ $\rho(4)=5$ מחלקות צמידות.

ב. האיברים בA_4הם מהצורות: $id, (***), (**)(**)$. תמיד יש את $conj(id)$. כעת נסתכל על $\sigma = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix} \in A_4$. ב־$S_4$יש ל$\sigma$ עוד 2 איברים במחלקת הצמידות שלה ־ $\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix}$או$\begin{pmatrix} 1 & 4 \end{pmatrix}\begin{pmatrix} 2 & 3 \end{pmatrix}$. כך גם ב$A_4$. לדוגמה נחפש $\pi \in A_4$כך ש: $\begin{pmatrix} 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 4 \end{pmatrix} = \pi\sigma\pi^{-1} = \begin{pmatrix} \pi_1 & \pi_2 \end{pmatrix}\begin{pmatrix} \pi_3 & \pi_4 \end{pmatrix}$. הדבר מתקיים עבור $\pi_1 = 3, \pi_2 = 1, \pi_3 = 2, \pi_4 = 4$ ולכן $\pi = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$. באופן דומה יש πכך ש$(14)(23) = \pi\sigma\pi^{-1}$. סה"כ $|\ conj(\sigma)\ | = 3$. נסתכל על תמורות של

מחזורים מאורך 3 ונניח $\tau \in A_4$

$| A_4 |= \sum | conj(x) |$ ולכן $| A_4 | - | conj(id) | - | conj(\sigma) |$ אבל $8 =| A_4 | - | conj(id) | - | conj(\sigma) |$ אבל $8 \nmid 12$

לכן סדר מחלקת הצמידות של τקטן מ־8.

בחישוב ישיר: $u = (132) \in A_4$, אז $conj(u) = \{(132),(124),(234),(143)\}$ (ניתן לעצור אחרי מציאת ארבעה איברים). יהי $v = (123) \in A_4$, $conj(v) = \{(123)(134)(142)(243)\}$.

סה:כ $| conj(u) |=| conj(v) |= 4$ בעוד ש־u, vצמודים בS_4,הם אינם צמודים בA_4. קיבלנו שישנן 4 מחלקות צמידות בA_4.

<u>תרגיל:</u> תהא G חבורה סופית כך ש־ $|G| = p$ עבור p ראשוני. כמה מחלקות צמידות יש ב־G?

<u>פתרון:</u> ישנן p מחלקות צמידות. $| G |= p \Leftarrow G \cong Z$ ולכן ציקלית ולכן אבלית ולכן לכל $x \in G$, $conj(x) = \{x\}$. מכאן שישנן $| G |$מחלקות צמידות.

הסבר נוסף: במקרה שלא ידענו כי G אבלית, תמיד $conj(id) = \{id\}$ולכל $x \in G$ מתקיים $|G| = p$ | $|conj(x)| < p$ ולכן $| conj(x) |= 1$. מ.ש.ל

<u>תרגיל:</u>

תהא G חבורה, $\{e\} \neq N \lhd G$. תהא C מחלקת צמידות בG. הוכיחו: $N \cap C = \phi$או $C \subseteq N$.

<u>פתרון:</u>

אם $N \cap C = \phi$, אז סיימנו. אחרת, נניח $x \in N \cap C$. מתקיים $x \in C$ ולכן $C = [x] = conj(x) = \{gxg^{-1} : g \in G\}$. אבל לכל $g \in G$ מתקיים $gxg^{-1} \in N$ כי $x \in N$ולכן $C \subseteq N$. מ.ש.ל

<u>מסקנה:</u> תח"נ היא איחוד זר של מחלקות הצמידות של איבריה

<u>פעולה של חבורה על קבוצה</u>

<u>הגדרה:</u> תהא G חבורה, X קבוצה. פעולה של G על X היא פונקציה דו מקומית $G \times X \to X, (g,x) \mapsto g * x$כך שמתקיים:

א.$(gh) * x = g * (h * x)$

ב.$e * x = x$

<u>דוגמאות:</u>

1.פעולת הכפל משמאל: אם $X=G$, אז אפשר להגדיר את הפעולה לפי $g*x=gx$.

2.$G=S_n$, $X=F[x_1,...,x_n]$ (X היא קבוצת הפולינומים ב־ n משתנים מעל F). נגדיר את הפעולה לפי:

$G*f(x_1,...,x_n)=f(x_{\sigma_1},x_{\sigma_2}...x_{\sigma_n})$.

<u>הגדרה:</u>מסלול (Orbit) של איבר $x\in X$ הוא $orb(x)=[x]=G*x=\{g*x:g\in G\}$.

למשל, עבור $X=G$ ופעולת ההצמדה, המסלול של כל איבר הוא מחלקת הצמידות שלו.

<u>הערה:</u>מסלולים הם מחלקות שקילות.

<u>הגדרה:</u> המייצב (Stabilizer) של $x\in X$ הוא $Stb(x)=\{g\in G:g*x=x\}$.

<u>הגדרה:</u> אם קיים $x\in X$ כך ש$G*x=X$ אז נאמר כי הפעולה טרנזיטיבית (אצל מגרל:הומוגנית).

<u>טענה:</u> $Stb(x)\leq G$ לכל$x\in X$ (הוכחתם בהרצאה).

<u>משפט:</u>לכל <u>$x\in X$</u> מתקיים מתקיים $[G:Stb(x)]=|G*x|$. אם G סופית, אז $|G*x|=\frac{|G|}{|Stb(x)|}$.

<u>מסקנה:</u><u>$|conj(x)|\mid|G|$</u> לפי המשפט לעיל ביחס לפעולת ההצמדה.

<u>דוגמה:</u>תהא $X=F[x_1,x_2,x_3],G=S_3$ עם הפעולה שהוגדרה קודם. נמצא את המסלול של האיבר $f(x_1,x_2,x_3)=x_1x_2+x_1x_3$ ונשים לב כי $f=x_1(x_2+x_3)$. ניתן לשים לב כי $\begin{pmatrix}2&3\end{pmatrix},id\in Stbc(f)$ כי הפעולה שלהם לא משנה את f. האיברים במסלול של f יהיו:$G*f=\{x_1(x_2+x_3),x_2(x_3+x_1),x_3(x_1+x_2)\}$. נשים לב שאכן מתקיים $6=|G|=|Stb(f)|\cdot|G*f|=2\cdot3$.

<u>תרגיל:</u>

תהא G חבורה ונתון שקיים $e\neq g\in G$ עם מחלקת צמידות בת שני איברים. הוכיחו כי בG ישנה תת חבורה נורמלית לא טריוויאלית.

<u>פתרון:</u>

לפי פעולת ההצמדה של G על עצמה נקבל כי $[G:Stb(g)]=2$ ולכן $Stb(g)\lhd G$.

<u>תרגיל:</u>

תהא חבורת p סופית, כלומר $|G|=p^k$, עבור p ראשוני ונניח $H\lhd G$ כך ש$|H|=p$.

הוכיחו כי $H\subset Z(G)$.

פתרון:

$|H| = p$ ולכן ציקלית. נרשום $H = \langle a \rangle = \left\{e, a, a^2, ..., a^{p-1}\right\}$. מכיוון שH תח"נ, לפי תרגיל קודם כל הצמודים של a שייכים לH. לכן יהיה $g \in G$, אז קיים $1 \leq i \leq p-1$ כך ש$gag^{-1} = a^i \in H$. מכאן שמספר הצמודים השונים של aהוא לכל היותר p-1. מצד שני, מספר הצמודים של a מחלק את $|G| = p^k$. לכן האפשרות היחידה היא שיש ל־a רק צמוד אחד. לכן $a \in Z(G)$ ולכן $H \subseteq Z(G)$.

מ.ש.ל. □

תרגיל: חשבו את מספר התמורות המתחלפות עם $\in S_n$ $\beta = \begin{pmatrix} 1 & 2 \end{pmatrix}\begin{pmatrix} 3 & 4 \end{pmatrix}$.

פתרון:

נסתכל עם פעולת ההצמדה של S_nעל עצמה: $\sigma * \beta = \sigma\beta\sigma^{-1}$. כעת נותר לחשב את $| Stb(\beta) |$. הרי $| Stb(\beta) |= \frac{|S_n|}{|S_n * \beta|}$ והרי $| S_n * p |$הוא גודל מחלקת הצמידות של p.

$S_n * \beta$ מכסה את כל התמורות מן המבנה $(**)(**)$. כמה כאלו יש?

$\frac{1}{2!}\binom{n}{2}\binom{n-2}{2}$ ועל כן סה"כ: $| Stb(\beta) |= \frac{|S_n|}{|S_n * \beta|} = \frac{n!}{\frac{1}{2}\binom{n}{2}\binom{n-2}{2}} = 8 \cdot (n-4)!$.

מ.ש.ל ■

<u>אלגברה מופשטת 1 קיץ 2013</u>

<u>תרגול 11</u>

הערה: אפריורית אין בחבילות הבסיס של $LaTeX$סימן של איחוד זר (אני עצמי עצלן מכדי לתכנת פונקציה שתעשה זאת) ולכן סימנתי אותו כ$\sqcup$.
הערה נוספת:בכל מקום בו לא ניקדתי, סימן שמדובר במֶרְכָּז $Z(G)$ ולא במְרַכֵּז C_a

<u>הגדרה:</u>

1.תהי G חבורה הפועלת על קבוצה X. נקודת שבת של g∈Gהיא נקודה $x \in X$ כך שמתקיים $g * x = x$.

2.עבור $g \in G$נסמן בX_gאת אוסף נקודות השבת של g: $X_g = \{x \in X : g * x = x\}$ למשל $X_e = X$

3. נאמר ש$x \in X$ היא נקודת שבת של Gאם לכל $g \in G$, $g * x = x$.
(נקראת גם "נקודת שבת משותפת")

<u>תרגיל:</u>

נתונה הפעולה $G \times X \to X$, כאשר $|G| = 49$, $|X| = 23$. הוכיחו שקיימת לפעולה זו נק' שבת משותפת. (הערה:לפעולה של כפל משמאל (נדבר עליה בהמשך) אין נקודות שבת משותפות. אין נקודה שכל החבורה לא מזיזה אותה.($G \times G \to G$ כך ש$g * h = gh$ אזי $\nexists h \in G : \forall g \in G, gh = h$)

לגבי מסלול $orb(x) = G * x = \{g * x \mid g \in G\}$ ידוע ש$|G * x| \mid |G|$ (כי $|G * x| = \sum [G : Stb(x)]$).

הערה: X הוא איחוד זר של המסלולים כלומר $X = \bigsqcup_{x_i \in X} G * x_i$.$\Leftarrow$ $|X| = \sum |G * x_i|$.

<u>שימו לב:</u> אם $|G * x_i| = 1$ אזי x_iהיא נקודת שבת משותפת. לכן נוכיח שקיים x_iשכזה.

לכל x_i: $|G * x_i| \mid |G|$. לכן $|X|$ הוא סכום $23 = |X| = n \cdot 1 + m \cdot 7 + k \cdot 49$. כמובן $k = 0$. $23 = n \cdot 1 + m \cdot 7$. לא יתכן ש$n = 0$ שכן $7 \nmid 23$ולכן $n > 0$.

לכן יש לפחות מסלול אחד באורך 1 $\Leftarrow$קיימת לפחות נק' שבת משותפת אחת. מ.ש.ל.$\square$.

<u>קצת סדר לגבי מונחים מרכזיים:</u>$G \times X \to X$

-מסלול $[x] = orb(x) = G * x = \{g * x \mid g \in G\}$.

-$X = \bigsqcup_{x_i \in X} G * x_i$

־$|G| \mid |G * x_i|$.

־המייצב: $G \geq Stb(x) = \{g \in G : g * x = x\}$.

־$|G * x_i| = [G : Stb(x)]$

־פעולת ההצמדה:

למסלול תחת פעולת ההצמדה נקרא $G * x_i = conj(x) = \{gxg^{-1} : g \in G\}$

למייצב תחת פעולת ההצמדה אנו קוראים המֶרכֵז

$Stb(x) = C_x = \{g \in G : gxg^{-1} = x\}$ וכמו כן: $Z(G) \subseteq C_x$.

<u>הלמה של ברנסייד Burnside</u>

תהא G חבורה סופית הפועלת על קבוצה X. נסמן: k־ מס' המסלולים של הפעולה, אזי: $k = \frac{1}{|G|} \sum |X_g|$.

<u>תרגיל:</u>

אנו מעוניינים לצבוע סרט עם 6 משבצות ב־4 צבעים. שני סרטים הם שקולים אם אפשר להגיע מאחד לשני ע"י שיקוף. מצאו את מספר האפשרויות השונות לצביעת הסרט (עד כדי שקילות).

<u>פתרון:</u>

נגדיר את המבנים $\underline{G = \mathbb{Z}_2, X = (\mathbb{Z}_4)^6}$ (כאשר X קבוצה עליה אנו מפעילים את החבורה G)

$0 * (x_1, x_2, x_3, x_4, x_5, x_6) = (x_1, x_2, x_3, x_4, x_5, x_6)$

וכן מתקיים:

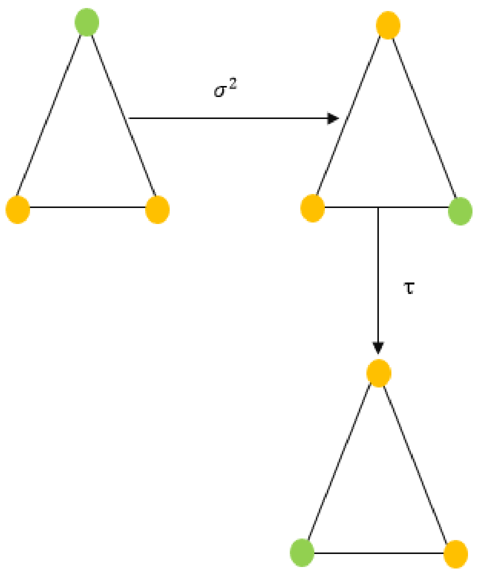
$1 * (x_1, x_2, x_3, x_4, x_5, x_6) = (x_6, x_5, x_4, x_3, x_2, x_1)$

מחפשים את מספר המסלולים של הפעולה: $k = \frac{1}{2}(|X_0| + |X_1|)$.

נשים לב ש: $X_0 = X \Rightarrow |X_0| = 4^6$ (כיוון שאין הגבלות על בחירת הצבע כי הזהות לא מזיזה), $|X_1| = 4^3$. כלומר $k = \frac{1}{2}(4^3 + 4^6)$.) מ.ש.ל.

<u>תרגיל:</u>מצאו את מספר המשולשים השונים (עד כדי סיבוב ושיקוף) אשר מתקבלים ממשולש משוכלל נתון, אם מותר לצבוע כל קודקוד בשלושה צבעים שונים.

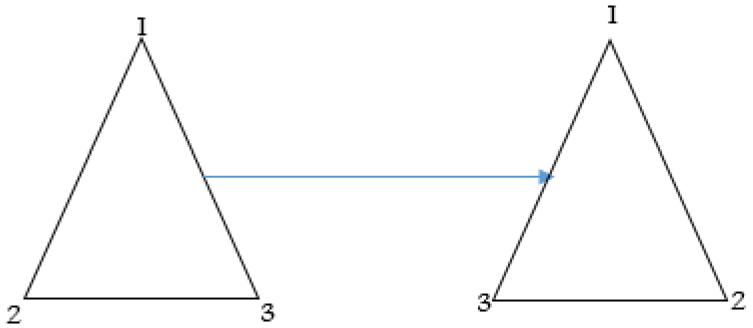
שרטוט להמחשת התרגיל:



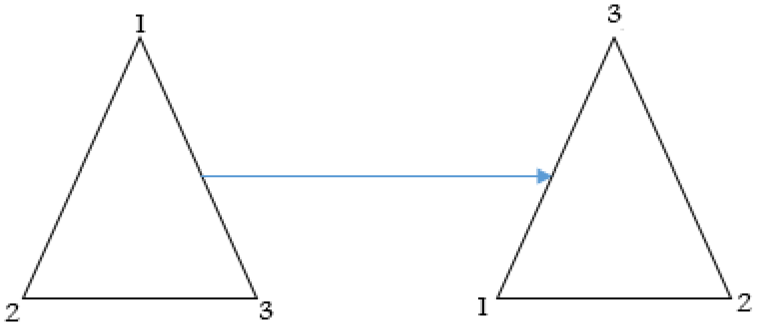
$G = D_3, X = (\mathbb{Z}_3)^3$ (כאשר ה3 התחתי מיועד למס' הצבעים והעילי למס' הקודקודים).

$|X_{id}| = |X| = 3^3$

$|X_\tau| = 3^2 = |X_{\tau\sigma}| = |X_{\tau\sigma^2}|$ כמו שניתן לראות לדוגמה בציור הבא:



$|X_\sigma| = 3 = |X_{\sigma^2}|$ (השיוויון נובע כיוון שσ^2היא סיבוב בכיוון הנגדי).



לכן מס' הצביעות (המסלולים) השונות הוא:

$k = \frac{1}{6}(3^3 + 3 \cdot 3^2 + 2 \cdot 3)$. מ.ש.ל

חבורות p

הגדרה: Gהיא חבורת p אם $|G| = p^n$.

[חזרה טובה] נוכיח שהמרכז של חבורת pהוא לא טריוויאלי:

תהא G חבורת p:$|G| = p^n$. נחקור את מחלקות הצמידות והמרכז שלה. נתבונן בפעולה של Gעל עצמה ע"י הצמדה: $G \times G \to G$.

$g * x \mapsto gxg^{-1}$. לפעולה זו יש מסלולים $x_i \in G : conj(x_i)$ומתקיים $G = \bigsqcup conj(x_i)$. נזכיר: $x_i \in Z(G) \Leftrightarrow conj(x_i) = \{x_i\}$.

$G = Z(G) \cup \bigsqcup_{x \notin Z(G)} conj(x_i) \Rightarrow |G| = |Z(G)| + \sum_{x_i \notin Z(G)} |conj(x_i)|$. המרכז הוא ת"ח ולכן הסדר שלו חזקה של p. כל אחד מהקונג'ים מחלק את הסדר של החבורה ולכן גם הם חזקה של p, ז"א: $p^n = p^\alpha + \sum \beta_i p^{\alpha_i}$. אם נניח בשלילה שהמרכז אכן טריוויאלי נקבל:

$p^n - 1 = \sum \beta_i p^{\alpha_i}$. לא יתכן כיוון ש$p \mid \sum \beta_i p^{\alpha_i}$ אבל $p \nmid p^n - 1$ וזו סתירה.

לסיכום: אם G חבורת p אזי $Z(G) \neq \{e\}$.

משוואת המחלקות

$|G| = |Z(G)| + \sum_{a \notin Z(G)} [G : C_a]$.

תרגיל:

כתבו את משוואת המחלקות של החבורה S_3.

פתרון:

המרכז של S_nעבור $n \geq 3$ הוא טריוויאלי $Z(S_n) = \{id\}$. כמו כן מס' מחלקות הצמידות

הוא $\rho(3) = 3$.

הסבר: נזכור שתמורות ב־S_n הן צמודות אמ"ם יש להן אותו מבנה מחזורים. לכן מספר מחלקות הצמידות הוא כמספר מבני המחזורים. אצלנו מבני המחזורים הם $(---), (--)(-), (-)(-)(-)$. לכן: $6 = 1 + 3 + 2$.

תרגיל (שימושי בש"ב): תהא G חבורה לא אבלית מסדר p^3 ונניח $a \notin Z(G)$. הוכיחו:

א. $|Z(G)| = p$

ב. $|C_a| = p^2$.

ג. $|conj(a)| = p$

פתרון:

א. האפשרויות לסדרי המרכז הן $|Z(G)| = \{1, p, p^2, p^3\}$. נפסול אותן להנאתנו:

- p^3 לא יתכן כיוון וG לא אבלית
- 1 לא יתכן כיוון שהמרכז של חבורת p הוא לא טריוויאלי.
- אם $|Z(G)| = p^2 \Leftarrow |\, G/_{Z(G)} \,| = p$ ולכן $G/_{Z(G)}$ ציקלית בסתירה לטענה שהוכחנו.

לכן, $|Z(G)| = p$.

ב. $|C_a| = ?$.

$|C_a| \neq p^3$ כי אם $C_a = G$ אזי $a \in Z(G)$ בסתירה לנתון. מתקיים $|C_a| \geq |\{a\} \cup Z(G)| < p \Leftarrow C_a \subseteq \{a\} \cup Z(G)$ ולכן $|C_a| = p^2$.

ג. $|conj(a)| = ?$

$|conj(a)| = [G : C_a] = \frac{p^3}{p^2} = p$.

מ.ש.ל

דוגמה לתרגיל:

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}_5 \right\}$$ אזי $|G| = 5^3$ ועל כן: $|Z(G)| = 5$.

תרגיל :

תהי Gחבורה מסדר $p^n, (n \geq 1)$. תהי $\{e\} \neq N \triangleleft G$. הוכיחו ש- $N \cap Z(G) \neq \{e\}$.

פתרון:

אם $x \in Z(G)$ אזי $conj(x) = \{x\}$. על מנת להראות שהחיתוך הנ"ל אינו טריוויאלי מ"ל שקיים $e \neq y \in N$ כך ש-$conj(y) = \{y\}$ ($|conj(y)| = 1$).

תזכורת: כל תח"נ היא איחוד זר של מחלקות הצמידות של איבריה (לא נכון לגבי ת"ח רגילה!). לכן: $N = \bigsqcup_{x_i \in N} conj(x_i)$. $|N| = \sum_{x_i \in N} |conj(x_i)|$. $N \leq G \Leftarrow$ קיים $1 \leq k \leq n$: $|N| = p^k$.

$p^k = \sum_{x_i \in N} |conj(x_i)| = 1 + \sum_{e \neq x_i \in N} |conj(x_i)|$ ואזי $p^k - 1 = \sum \beta_i p^{\alpha_i}$ אם כל ה$\alpha_i > 0$נקבל סתירה. לכן קיים i: $\alpha_i = 0$ אך אז מקבלים שקיים $x_i \in N$כך ש: $|conj(x_i)| = 1 \Rightarrow x_i \in Z(G) \Rightarrow e \neq x_i \in N \cap Z(G)$ וזה מוכיח את הדרוש. מ.ש.ל

משפט קושי (השימושי והפשוט ביותר בתחום):

תהא Gחבורה סופית ויהי p כך ש$p \mid |G|$ אזי קיים בGאיבר מסדר p.

למשל בחבורה מסדר 28 יש איבר מסדר 7 ויש איבר מסדר 2.

משפטי סילו Sylow

תהא G חבורה כך ש־$|G| = p^k m$ כאשר $(m,p) = 1$. ת"ח p־סילו של G היא $H \leq G$ כך ש־$|H| = p^k$

דוגמה:

לדוגמה נביט ב־$|S_3| = 2 \cdot 3$.

ת"ח 3־סילו: $<(123)>=<(132)>$ (הופכים אחד של השני).

ת"ח 2־סילו: $<(23)>, <(13)>, <(12)>$.

משפט סילו 1:

תהא G חבורה סופית. אם $p \mid |G|$ אז קיימת ל־G ת"ח p־סילו.

טענה: בחבורת p יש תת חבורה מכל סדר שמחלק את סדר החבורה.

מסקנה (מהטענה ומסילו):

לכל חבורה סופית G, אם $p^k \mid |G|$, אזי יש ל־G ת"ח מסדר p^k.

דוגמה:

נסתכל לדוגמה ב־D_4. $|D_4| = 8 = 2^3$.

ת"ח 2־ סילו של D_4 היא D_4 בעצמה.

לפי המסקנה קיימת תת חבורה מסדר 4: למשל $<\sigma>$ ות"ח מסדר 2: למשל $<\tau>$.

הערה חשובה: חבורת p־ סילו היא חבורת p המקסימלית.

מופשטת 1,קיץ 2013
תרגול 12

משפט סילו 2
1. כל תתי חבורות p־סילו של חבורה סופית Gצמודות זו לזו.
2. כל תת חבורה־p של Gמוכלת בת"ח p־סילו כלשהי.

הסבר ל־1: $H,K \leq G$ הן ת"ח p־סילו אזי קיים $g \in G : gHg^{-1} = K$.
הערה:שימו לב:אם $H \leq G$ ת"ח p־סילו אזי גם gHg^{-1} p־סילו שכן $|gHg^{-1}| = |H|$.
מסקנה:ת"ח p־סילו היא יחידה אמ"מ היא נורמלית.
הוכחה:
($\Leftarrow$) יש ת"ח p־סילו Pוהיא יחידה. לכל $g \in G$: gPg^{-1} היא גם p־סילו ולכן $P \lhd G \Leftarrow gPg^{-1} = P$.
($\Rightarrow$)$P \lhd G$ p־סילו נורמלית. נניח שהיא לא יחידה, כלומר קיים $K \leq G$ת"ח p־סילו אזי קיים $g \in G$: $gPg^{-1} = K$ אבל $gPg^{-1} = P$ולכן $P = K$. מ.ש.ל

משפט סילו 3
יהי n_p מס' תתי חבורות p־סילו של חבורה סופית G.
א. $n_p \mid |G|$
ב. $n_p = 1(\mod p)$
הערה:נניח $|G| = p^k m$. $(m,p) = 1$ אזי $n_p \mid m$ (כי מתנאי ב' רואים ש־n_pזר ל־p ולכן לא מחלק את p^k).
מסקנה:תת חבורה p־סילו היא נורמלית $\Leftrightarrow n_p = 1$.
תרגיל:
הראו שחבורה מסדר 45 אינה פשוטה.
פתרון:
$|G| = 45 = 3^2 \cdot 5$. יש ל־G תת חבורה 5־סילו נסמנה P_5. כמו כן יש ל־G ת"ח 3־סילו נסמנה P_3. נבדוק אם אחת מהן נורמלית:
נתחיל עם n_3.
$n_3 \equiv 1(\mod 3) \wedge n_3 \mid 5$
$n_3 \in \{1,5\}$אבל נפסול את 5 כיוון ש$5 \not\equiv 1(\mod 3)$. לכן $n_3 = 1 \Rightarrow P_3 \lhd G$ לכן G לא פשוטה.
הערה: אותו הליך היה עובד גם עם P_5:
n_5:
$n_5 = 1(\mod 5) \wedge n_5 \mid 9$ ואזי $n_5 \in \{1,3,9\}$ נפסול שוב את 3,9 כיוון שהם לא שקולים ל$1 \mod 5$.
הערה: כל שתי ת"ח p־סילו שונות מסדר ראשוני p נחתכות טריוויאליות.
הסבר: אפשרויות לגודל החיתוך הן אך ורק אלו המחלקות את המס' (סדר החיתוך או כסדר החבורה [שלא מתקיים כיוון שהן שונות] או טריוויאלי). מצד שני אם הסדר לא ראשוני יתכן והחיתוך לא טריוויאלי (לדוג' אם הסדר של שתיהן היה 5 הסדר היה יכול להיות 1 או 5 אבל אם היה לדוגמה 5^2, סדרהחיתוך היה להיות גם 5)
תרגיל (ספירת איברים): נמצא את מס' ת"ח p־סילו של חבורה G לא אבלית מסדר 21.
פתרון:
$|G| = 21 = 3 \cdot 7$יש ל־G ת"ח 3־סילו P_3 ות"ח 7־סילו P_7. שואלים כמה ת"ח 3 סילו או 7 סילו יש?

$n_3: n_3 \equiv 1 (\mod 3) \wedge n_3 \mid 7 \Rightarrow n_3 \in \{1,7\}$

ועבור n_7 באופן דומה:

$n_7 = 1 (\mod 7) \wedge n_7 \mid 3 \Rightarrow n_7 \in \{1\}$ (3 נפסל) ולכן $n_7 = 1$. יש ת"ח 7־סילו יחידה.

ספירת איברים:

סדר של איבר	מס' איברים מסדר זה
1	1
3	$14(\star)$
7	6 (כי בP_7 ישנם 7 איברים ו1 מהם הוא איבר היחידה ועוד 6 איברים מסדר 7)
21	0 (כי אחרת G הייתה ציקלית ואז אבלית)

$(\star)$: אם $n_3 = 1$ אזי היו לנו 2 איברים מסדר 3 ואז בספירת האיברים לא היינו מגיעים ל־21.

לכן $n_3 = 7$ ואז יש $2 \cdot 7 = 14$ איברים מסדר 3. מ.ש.ל.

תזכורת/הבהרה: כל איבר מסדר p "יושב" בתוך ת"ח p־סילו כלשהיא.

הערות:

א. באותו אופן ניתן להראות כי לכל חבורה $|G| = pq$ עבור $q > p$ ראשוניים אם $p \not\equiv 1 (\mod q)$ אזי G ציקלית.

ב. אם $p = 1 (\mod q)$ אזי G אינה בהכרח ציקלית.

למשל: $|S_3| = 2 \cdot 3$ ואז $3 \equiv 1 (\mod 2)$ ו S_3 איננה ציקלית.

הערה:

אם $H \leq G$ ת"ח p־סילו, $K \leq G$ ת"ח q־סילו (p,q ראשונים שונים) אזי $H \cap K = \{e\}$.

תרגיל: הוכיחו כי לכל חבורה מסדר pq עבור $p > q$ ראשוניים, אם $p \not\equiv 1 (\mod q)$ אזי G ציקלית.

פתרון:

עבור n_p:

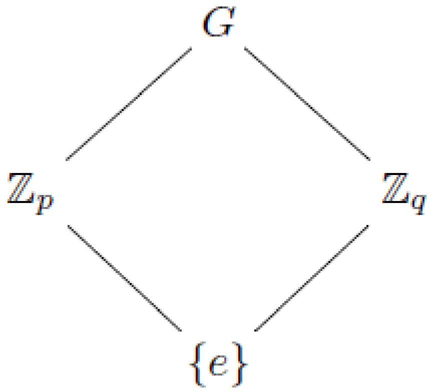
$n_p \equiv 1 (\mod p) \wedge n_p \mid q$ כלומר לכאורה $n_p \in \{1, q\}$ אבל $q \not\equiv 1 (\mod p)$ כי $p > q \Leftarrow n_p = 1 \Leftarrow P \triangleright G$ ת"ח p־סילו $P \cong \mathbb{Z}$.

ננקוט באופן דומה עבור n_q:

$n_q \equiv 1 (\mod q) \wedge n_q \mid p$ ושוב לכאורה $n_q \in \{1, p\}$ אבל $p \not\equiv 1 (\mod q)$ לפני הנתון $n_q = 1 \Leftarrow$.

$Q \triangleleft G$ ת"ח p־סילו ומתקיים $Q \cong \mathbb{Z}_q$.

היינו רוצים:



וכן $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$.
נראה שG היא מכפלה ישרה פנימית של ת"ח שלה P, Q. לשם כך יש להראות כי :
1. $P \cap Q = \{e\}$
2. $P, Q \triangleleft G$ - הוכחנו.
3. $P \cdot Q = G$ - נוכיח זאת כעת.
אזי לפי משפט מההרצאה נקבל ש- $G \cong P \times Q$וזו התוצאה הדרושה.
$P, Q \triangleleft G \Leftarrow H = PQ \leq G$ (סימון) H לפי ההגדרה היא מכפלה ישרה פנימית של Pו־Q.
לכן: $H \cong P \times Q$ולפי מכפלה של קבוצות:
$|H| = |P| \times |Q| = pq$.
$H \leq G$ וגם $|H| = pq \Leftarrow H = G \Leftarrow PQ = G$.
נסכם: $G = PQ$ ולכן $G \cong P \times Q$ אבל $P \cong \mathbb{Z}_p$, $Q \cong \mathbb{Z}_q \Leftarrow G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$
כאשר המעבר האחרון נובע מכך ש$(p, q) = 1$. על כן G ציקלית. מ.ש.ל.
<u>הערה:</u> דרכים נוספות להוכיח את הטענה:
1. ספירת איברים כמו שעשינו עם $|G| = 21$.
2.(דרך אלגנטית) להראות ישירות שיש איבר מסדר pq. {שני איברים מתחלפים ולכן הם זרים
וסדר המכפלה הוא מכפלת הסדרים. מופיע בשיעורי הבית.}.
<u>תרגיל:</u>
הראו שלא קיימת חבורה פשוטה מסדר 132.
<u>פתרון:</u>
$|G| = 132 = 2^2 \cdot 3 \cdot 11$
n_{11}
$n_{11} \mid 12 \wedge n_{11} \equiv 1 (\mod 11)$ ונוכל לפסול 2,3,4,6 להסיק $n_{11} \in \{1, 12\}$.
n_3
$n_3 \mid 44 \wedge n_3 \equiv 1 (\mod 3)$
$n_3 \in \{1, 4, 22\}$
n_2
$n_2 \mid 33 \wedge n_2 \equiv 1 (\mod 2)$ ושום אופציה לא נפסלת $n_2 \in \{1, 3, 11, 33\}$.
אם $n_{11} = 1$או $n_2 = 1$ או $n_3 = 1$ סיימנו ולכן נניח שהם לא 1. ההנחה באופן מפורש היא:

$$n_{11} = 12$$
$$n_3 \in \{4, 22\}$$
$$n_2 \in \{3, 11, 33\}$$

- $n_{11} = 12$ (כל חבורה 11 סילו היא מסדר 11 ויש בה 11 איברים 10 מסדר 11 ואיבר היחידה) לכן יש 120 איברים מסדר 11.
- האם יתכן ש$n_3 = 22$? לא. כי אז יש $2 \cdot 22 = 44$ איברים מסדר 3 ואז אנחנו חורגים מהסדר של החבורה. לכן: $n_3 = 4$ ולכן יש 8 איברים מסדר 3.

<u>סיכומון:</u>

איבר 1 מסדר 1, 120 איברים מסדר 11, 8 איברים מסדר 3. לכן ספרנו עד עכשיו 129 איברים.
נותר מקום ל־3 איברים מסדר 2. אבל חבורת 2- סילו היא מסדר 4 ולכן יש בה 3 איברים מסדר 2. כלומר יש ת"ח 2- סילו יחידה! ולכן היא נורמלית והחבורה G איננה פשוטה.
מ.ש.ל

<u>תרגיל:</u>תהא G חבורה מסדר p^2q עבור p,q ראשוניים שונים. הוכיחו ש-G אינה פשוטה.

<u>פתרון:</u>

$n_p: n_p \equiv 1(\mod p) \wedge n_p \mid q \Rightarrow n_p \in \{1,q\}$. אם $n_p = 1$ סיימנו ולכן נניח $n_p = q$.

$n_q = 1(\mod q) \wedge n_q \mid p^2, n_q \in \{1,p,p^2\}$.

אם $n_q = 1$ סיימנו.

- אם $n_q = p^2$:
  כמה איברים מסדרq יש ? $p^2(q-1) = p^2q - p^2$ איברים מסדר q. אבל אז יש מקום רק לחבורת $p-$סילו אחת שכן חבורת $p-$סילו היא מסדר $p^2 \Leftarrow n_p = 1$וסיימנו.

- אם $n_q = p$ אזי $p \equiv 1(\mod q)$. אבל שימו לב שאנו תחת ההנחה ש- $n_p = q$ כלומר $q \equiv 1(\mod p)$ כלומר יש שני תנאים:
  $p \equiv 1(\mod q)$ וגם $q = 1(\mod p)$ אבל

שימו לב שמכיוון ש$p \neq q$ מתקיים ב.ה.כ ש$p > q$ ואזי $q \not\equiv 1(\mod p)$. סתירה.

מ.ש.ל

<u>דוגמה:</u>

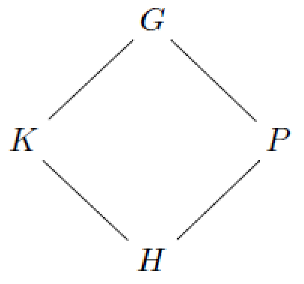
$99 = 3^2 \cdot 11$ לא פשוטה.

<u>תרגיל:</u>

תהא G חבורה סופית ותהא $K \leq G$ ת"ח. תהא $H \leq K$ ת"ח $p-$סילו של K.

הוכיחו שקיימת ת"ח $P \leq G$ $p-$סילו של Gכ ש$H = P \cap K$.

שרטוט מסייע:



<u>פתרון:</u>

H ת"ח של K ולכן הסדר שלה הוא חזקת p. לכן Hת"ח p של G.

לכן היא מוכלת בת"ח $p-$סילו של G שנסמנה P. כלומר $H \leq P$ ⇐$H \leq P \cap K$.

נוכיח ש- $|H| = |P \cap K|$

וכך נקבל את הדרוש.

$P \cap K \leq K$ היא ת"ח p של K.לכן $P \cap K$ מוכלת באחד מהצמודים של H (מוכלת באחד מהסילואים שכולם צמודים לH). כלומר קיים g:

$P \cap K \leq gHg^{-1} \Rightarrow |P \cap K| \leq |gHg^{-1}| = |H|$ וקיבלנו הדרוש. (שכן כבר ראינו ש$|H| \leq |P \cap K|$

ולכן בסה"כ נקבל $|H| = |P \cap K|$. מ.ש.ל.

<u>תזכורת:</u> ראינו שלכל $H \leq G$ מתקיים $H \lhd N(H)$ כאשר $N(H) = \{g \in G : gHg^{-1} = H\}$

<u>תרגיל:</u>

תהא H- ת"ח $p-$סילו של G. הוכיחו ש-Hהיא ת"ח p-סילו יחידה של $N(H)$.

<u>פתרון:</u>

למעשה מספיק להוכיח שהיא ת"ח $p-$סילו של $N(H)$ שכן כיוון ש$H \lhd N(H)$נקבל שהיא יחידה.

נניח $|G| = p^k m$ אזי $|H| = p^k$ מתקיים $H \leq N(H) \leq G$ ולכן קיים $t \mid m$: $|N(H)| = p^k t$ ולכן H ת"ח $p-$סילו של $N(H)$. מ.ש.ל.

תרגיל משמעותי בתרגול:

טענה: אם כל ת"ח הסילו של G הן נורמליות, אזי G היא מכפלה ישרה פנימית שלהן.

שימוש: בהנתן חבורה G בעלת סדר $|G| = 1235 = 5 * 13 * 19$. מתקיים $n_5 = n_{13} = n_{19} = 1$. כל תת"ח שלה נורמליות ולכן $G \cong \mathbb{Z}_5 \times \mathbb{Z}_{13} \times \mathbb{Z}_{19} \cong \mathbb{Z}_{1235}$.

המסקנה הנובעת היא שכל חבורה מסדר 1235 היא ציקלית

הוכחה:

שימו לב שהגדרנו מכפלה ישרה פנימית ל־2 ת"ח . ההגדרה למס' ת"ח היא:

G מכפלה פנימית של $A_1...A_n \leq G$ אם:

1. $\forall 1 \leq i \leq n : A_i \triangleleft G$
2. $\{e\} = A_j \cap (\prod_{i \neq j} A_i)$
3. $\prod_{i=1}^{n} A_i = G$.

למה:

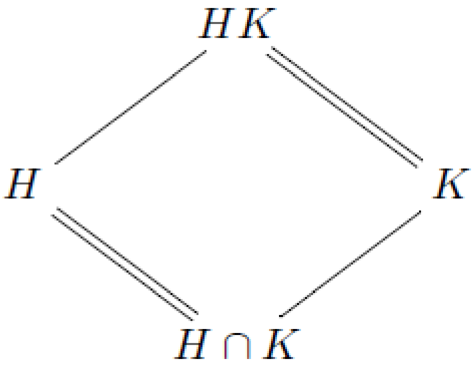
אם $A_1, ..., A_n \triangleleft G$ מסדרים זרים בזוגות אזי: $|A_1 \cdot A_2 ... \cdot A_n| = |A| \cdot |A_2| ... \cdot |A_n|$.

הוכחה:

באינדוקציה על n:

אם $n = 1$ הטענה ברורה.

עבור $n = 2$ לפי איזו' II:



$|A_1 A_2| = \frac{|A_1| \cdot |A_2|}{|A_1 \cap A_2|}$. אצלנו $|A_1 \cap A_2| = 1$ ונקבל הדרוש.

נניח נכונות ל־n ונוכיח ל $n + 1$:

לפי המקרה של $n = 2$ וכיוון ש $|A_1 \cdot ... \cdot A_n| = |A_1| ... |A_n|$

$|A_!....A_n \cdot A_{n+1}| = |A_1 \cdot ... A_n| \cdot |A_{n+1}| = |A_1| \cdot |A_2| ... |A_n| \cdot |A_{n+1}|$.

מ.ש.ל ללמה.

בחזרה לטענה שלנו:

נניח $|G| = p_1^{k_1} ... p_t^{k_t}$ ונסמן את ת"ח p-סילו ב$P_1 ... P_t$ הן נורמליות (לפי הנתון) והסדרים שלהם זרים בזוגות. לכן: יהי i כלשהו. מתקיים:

$(|P_i|, |\prod_{j \neq i} P_j|) = 1$ ולכן $\{e\} = P_i \cap (\prod_{j \neq i} P_j)$.

כמו כן:

$|G| = \prod_{i=1}^{t} |P_i| = |\prod_{i=1}^{t} P_i|$ ולכן $\prod_{i=1}^{t} P_i = G$. מ.ש.ל.

מופשטת 1 קיץ 2013,תרגול 13

29 באוגוסט 2013

סדרות נורמליות וסדרות הרכב

הגדרה: סדרה נורמלית של חבורה G היא סידרה של ת"ח נומרליות:
$G = G_1 \rhd G_2 \rhd .... \rhd G_k = \{e\}$

- שימו לב שכל ת"ח נומרלית בזו שלפניה ולאו דווקא נורמלית ב־G.

חבורות המנה $G_i/_{G_{i+1}}$ נקראות גורמים או מנות של הסדרה.

דוגמאות:

1. לכל חבורה יש סדרה נורמלית $G \rhd \{e\}$ ואז המנה היחידה של הסדרה $G \cong G/_{\{e\}}$.
2. $S_3 \rhd < (123) > \rhd \{id\}$.

מנות: $S_3/_{<(123)>} \cong \mathbb{Z}_2$ וכן $< (123) > /_{\{e\}} = \mathbb{Z}_3$.

הגדרה: עידון של סדרה נורמלית

תהי $G = G_1 \rhd G_2 \rhd ... \rhd G_k = \{e\}$ סדרה נורמלית. עידון שלה הוא סדרה מהצורה
$G = G_1 \rhd G_2 \rhd ... \rhd G_i \rhd G_i^* \rhd G_{i+1} \rhd ... \rhd G_k = \{e\}$
כאשר הגורמים של האיברים שהוספנו הם לא טריוויאלים:
$G_i^*/_{G_{i+1}} \neq \{e\}, G_i/_{G_i^*} \neq \{e\}$

הגדרה: סדרת הרכב היא סדרה נורמלית שאין לה עידונים.

משפט: סדרה נורמלית היא סדרת הרכב אמ"מ כל הגורמים של הסדרה הם פשוטים (כלומר המנות הן חבורות פשוטות).

הערה: חבורה אבלית היא פשוטה אמ"מ היא ציקלית מסדר ראשוני. לכן, אם אחד הגורמים בסדרה הוא אבלי אך אינו ציקלי מסדר ראשוני אזי הסדרה אינה סדרת הרכב.

דוגמאות:

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

נתבונן ב$G \rhd \mathbb{Z}_2 \times \{0\} \rhd \{0\} \times \{0\}$. זוהי סדרה נורמלית אך לא סדרת הרכב. הגורם הראשון: $|\mathbb{Z}_2 \times \mathbb{Z}_4/_{\mathbb{Z}_2 \times \{0\}}| = 4$ אבלי מסדר שאינו ראשוני ולכן גורם זה אינו פשוט.

ננסה סדרה נוספת:

$G \rhd \{0\} \times \mathbb{Z}_4 \rhd \{0\} \times 2\mathbb{Z}_4 \rhd \{0\} \times \{0\}$.

איזומורפיזם של גורמים:

$G/_{\{0\} \times Z_4} \cong \mathbb{Z}_2,$

$\{0\} \times \mathbb{Z}_4/_{\{0\} \times 2\mathbb{Z}_4} \cong \mathbb{Z}_2$.

הגורמים הם פשוטים ולכן זוהי סדרת הרכב.

2. $n \geq 5$: $S_n \rhd A_n \rhd \{id\}$.

$S_n/_{A_n} \cong \mathbb{Z}_2$ וכן $A_n/_{\{id\}} \cong A_n$ כאשר A_n זאת חבורה פשוטה. לכן כל הגורמים פשוטים ולכן זוהי סדרת הרכב.

3. למשל הסדרה $S_4 \triangleright A_4 \triangleright \{id\}$ לא סדרת הרכב כי הגורם $A_4 \cong A_4/_{\{id\}}$ אינו פשוט.
נעדן את הסדרה:

$$\begin{array}{ccccccc} & & \mathbb{Z}_2 & & \mathbb{Z}_3 & & \\ & & | & & | & & \\ S_4 & \triangleright & A_4 & \triangleright & K & \triangleright & \{id\} \\ & & & & \| \wr & & \\ & & & & K \cong \mathbb{Z}_2 \times \mathbb{Z}_2 & & \end{array}$$

$V_4 = K = \{(12)(34),(13)(24),(14)(23),id\}$. הגורם האחרון אינו פשוט ולכן זוהי עדיין איננה סדרת הרכב.

<u>נעדן שוב:</u>

$$\begin{array}{ccccccccc} S_4 & \triangleright & A_4 & \triangleright & K & \triangleright & W & \triangleright & \{id\} \\ & | & & | & & | & & | & \\ & \mathbb{Z}_2 & & \mathbb{Z}_3 & & \mathbb{Z}_2 & & \mathbb{Z}_2 & \end{array}$$

כאשר $W = \{id,(12)(34)\}$ כל הגורמים הם פשוטים ולכן זוהי סדרת הרכב.

<u>חבורות פתירות</u>

<u>הגדרה:</u> חבורה היא פתירה אם יש לה סדרה נורמלית (לאו דווקא סדרת הרכב) כך שכל הגורמים הם אבלים.

<u>דוגמאות:</u>

1. כל חבורה אבלית היא פתירה. יש לה ס"נ $G \triangleright \{e\}$ והגורם היחיד הוא אבלי ($G \cong G/_{\{e\}}$).
2. כל החבורות הדיהרליות הן פתירות:

$$\begin{array}{ccccc} D_n & \triangleright & \langle\sigma\rangle & \triangleright & \{id\} \\ & \downarrow & & \downarrow & \\ & \mathbb{Z}_2 & & \langle\sigma\rangle/_{\{id\}} \cong \langle\sigma\rangle & \end{array} .$$

לכן גורם זה הוא ציקלי ולכן אבלי.

3. חבורות שאינן פתירות: A_n, S_n עבור $n \geq 5$.
$S_n \triangleright A_n \triangleright \{id\}$. ($A_n$איננה אבלית).

<u>תרגיל :</u>

הראו שהחבורה הבאה היא פתירה: $A = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a,b,c \in \mathbb{Z}_p \right\}$.

<u>פתרון:</u>

תחילה נמצא את סדר החבורה $|A| = p^3$. זוהי חבורת p ולכן יש לה מרכז לא טריוויאלי: $|Z(A)| \neq 1$, $A/_{Z(A)}$ איננה ציקלית לא טריוויאלית ולכן $|Z(A)| = p$. נתבונן בסדרה

$$\begin{array}{ccccc} A & \triangleright & Z(A) & \triangleright & \{id\} \\ & | & & | & \\ & |A/_{Z(A)}| = p^2 & & |Z(A)/_{\{id\}}| = p & \end{array}$$

לכן החבורה פתירה כדרוש. מ.ש.ל

<u>משפט:</u> כל חבורת p היא פתירה.

<u>טענה:</u> תהא Gחבורה מסדר pq (עבור p,qראשוניים) אזי G פתירה.

<u>הוכחה:</u>ננסה למצוא תתי חבורות נורמליות. נבדוק תת חבורה $p-$סילו ו$q-$סילו.
$n_p \equiv 1 \pmod p \wedge n_p \mid q : n_p \in \{1,q\}$. באופן דומה $n_q \in \{1,p\}$.

- אם $p=q$ אזי G אבלית כי היא מסדר p^2. אחרת $p\neq q$ ונניח ב.ה.כ כי

$$\Leftarrow n_q=1 \Leftarrow q\not\equiv 1(\mod q) \Leftarrow p<q$$

יש לנו תת חבורה $q-$סילו נורמלית, נסמנה Q.

$$\begin{array}{ccccc} G & \triangleright & Q & \triangleright & \{e\} \\ & \| \wr & & & \\ & \mathbb{Z}_p & & & \end{array}$$

לכן הגורמים הם אבלים ולכן החבורה פתירה.

<u>תרגיל:</u> הוכיחו שכל חבורה מסדר 1089 היא פתירה

<u>פתרון:</u> $n_{11}=1 \Leftarrow n_{11}\in\{1,3,9\} \Leftarrow n_{11}\equiv 1(\mod 11)\wedge n_{11}\mid 3^2, 1089=3^2\cdot 11^2$
ולכן תת חבורה 11־ סילו P_{11}היא נורמלית ולכן החבורה פתירה.

$$\begin{array}{ccccc} G & \triangleright & P_{11} & \triangleright & \{e\} \\ & | & & | & \\ & |G/_{P_{11}}|=3^2 & & |P_{11}/_{\{e\}}|=11^2 & \end{array} .$$

<u>הקומוטטור:</u>

<u>הגדרה:</u> תהי G חבורה ויהיו $a,b\in G$.
1. הקומוטטור של b,a מוגדר להיות $[a,b]=aba^{-1}b^{-1}$.
2. תת חבורת הקומוטטור מוגדרת כ־ $G\prime=\langle\{[a,b]\mid a,b\in G\}\rangle$.

<u>תרגיל:</u> מתי $[a,b]=e$?

<u>פתרון:</u> הדבר מתרחש אמ"ם a,b מתחלפים, כלומר $\Leftrightarrow ab=ba$.

<u>משפט:</u> G אבלית $\Leftrightarrow G\prime=\{e\}$.

<u>תרגיל:</u> מהו $[a,b]^{-1}$?

<u>פתרון:</u> $[a,b]^{-1}=[b,a]$ ואכן $[a,b]\cdot[b,a]=aba^{-1}b^{-1}bab^{-1}a^{-1}=e$.

<u>הערה:</u> אם $H\le G$ אזי $H\prime\le G\prime$.

<u>משפט:</u> $G\prime\triangleleft G$.

<u>מסקנה:</u> אם G חבורה פשוטה ואינה אבלית אזי $G\prime=G$. למשל $A_n'=A_n$עבור $n\ge 5$.

<u>הסבר:</u> מתקיים $G\prime\triangleleft G$ וכן G פשוטה ולכן $G\prime=\{e\}$ או $G\prime=G$. אבל G לא אבלית ולכן $G\prime=G \Leftarrow G\prime\neq\{e\}$.

<u>משפט:</u> $G/_{G\prime}$ הוא המנה האבלית המקסימלית של G, כלומר:
1. לכל חבורה G, המנה $G/_{G\prime}$ היא אבלית.
2. לכל N◁G, $G/_N$אבלית $\Leftrightarrow G\prime\le N$.

<u>דוגמה:</u>
1. $D_4=\langle\sigma,\tau\rangle$. ראינו כי $Z(D_4)=\{id,\sigma^2\}\triangleleft D_4$ וכמו כן $|D_4/_{Z(D_4)}|=4$ ולכן $D_4'\le Z(D_4)$ לכן האפשרויות הן: $D_4'=\{id\},\{id,\sigma^2\}$. D_4 איננה אבלית ולכן $D_4'=\{id,\sigma^2\}$.
2. $(S_n)\prime=A_n$ עבור $n\ge 5$. $S_n/_{A_n}\cong\mathbb{Z}_2$ אבלי $\Leftarrow (S_n)\prime\triangleleft S_n \Leftarrow (S_n)\prime\triangleleft A_n$
$\Leftarrow (S_n)\prime\le A_n$ לכן $(S_n)\prime=\{id\}$או $(S_n)\prime=A_n$.
מכיוון ש־S_n איננה אבלית, $(S_n)\prime=\{id\}$ ולכן $(S_n)\prime\neq A_n$.

<u>הערה:</u> גם $(S_4)\prime=A_4$, וכן $(S_3)\prime=A_3$ (בדקו).

<u>הגדרה:</u> סדרת הקוממוטטורים/סדרת הנגזרת של החבורה G היא הסדרה
$G\le G^{(1)}\le G^{(2)}\le G^{(3)}\le\ldots\le G^{(n)}\le\ldots$ המוגדרת באינדקוציה ע"י
$G^{(0)}=G$, $G^{(1)}=G\prime$, $G^{(i+1)}=(G^{(i)})'$. (באופן כללי $G^{(n+1)}=[G^{(n)},G^{(n)}]$).

הערה: לכל $k \in \mathbb{N}$ מתקיים $G^{(k-1)} \triangleleft G^{(k)}$.
משפט: G היא חבורה פתירה $\Leftrightarrow$ קיים t סופי כך ש$G^{(t)} = \{e\}$.
לדוגמה: $G = D_3 \Leftarrow G\prime = \langle\sigma\rangle \Leftarrow G^2 = \{id\}$ ולכן D_3פתירה.
הערה: כך אפשר לראות ש-S_nאיננה פתירה עבור $n \geq 5$ שכן החל מ$i = 1$ מתקיים $(S_n)^{(i)} = A_n \neq \{id\}$.
תרגיל: תהא G חבורה מסדר 28. הוכיחו:
א. קיימת תת חבורה 7- סילו נורמלית.
ב. אם G לא אבלית אזי $|G\prime| = 7$.
ג.אם G לא אבלית ויש לה ת"ח נורמלית מסדר 2 אזי $|\ G/_{Z(G)}\ | = 14$.
פתרון:
א.$|G| = 28 = 2^2 \cdot 7 \Leftarrow n_7 \mid 4 \wedge n \equiv 1(\mod 7)$ ולכן $n_7 \in \{1,2,4\} \Leftarrow n_7 = 1$.
ולכן יש תת חבורה 7-סילו יחידה, נסמנה P_7 ולכן היא נורמלית (כי היא יחידה) כדרוש.

ב. $|\ G/P_7\ | = 4$ ולכן $G\prime \leq P_7 \Leftarrow$ $G\prime = \begin{cases} \{e\} \\ P_7 \end{cases}$ אבל G לא אבלית ולכן $G\prime \neq \{e\}$
ולכן $G\prime = P_7$ ולכן $|G\prime| = 7$ כדרוש.
ג. $Z(G) \in \{1,2,4,7,14,28\}$
ונפסול אותם לאט-לאט:

- 28 לא יתכן כיוון וG לא אבלית
- 14 ו4 לא יתכנו כי אזי $G/Z(G)$ ציקלית

ונותרנו סה"כ עם $Z(G) \in \{1,2,7\}$. נבדוק: תהי $N \triangleleft G$ ת"ח נורמלית מסדר 2.
$N = \{e,a\}$ אבל לכל $b \in G$

$$bab^{-1} \in N \Rightarrow bab^{-1} = \begin{cases} e & (\rightarrow impossible) \\ a \end{cases} \Rightarrow bab^{-1} = a \Rightarrow bab^{-1} = ab \Rightarrow ba = ab \Rightarrow a \in Z(G)$$

ולכן $Z(G)$ לא טריוויאלי. $Z(G)$ לא שווה ל-7 כי $a \in Z(G)$, $o(a) = 2$ וידוע $o(a) \mid |Z(G)| \Leftarrow 2 \mid |Z(G)| \Leftarrow Z(G) \neq 7$ ולכן $|Z(G)| = 2$ ולכן $|\ G/Z(G)\ | =$ 14כדרוש. מ.ש.ל $\square$

בהצלחה לכולם במבחן. ⍨