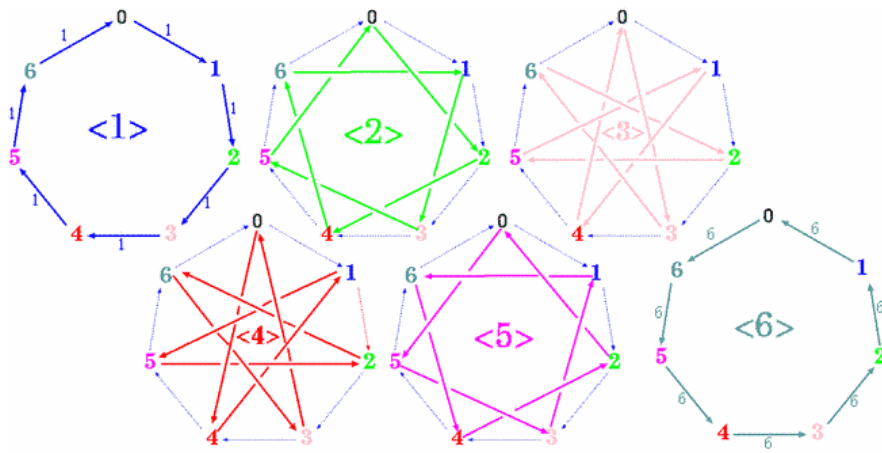




אלגברה מופשטת 1

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

מספר קורס 88-211



הקדמה ותודות

תודות

תודה לד"ר רוני ביתן על שעבר על כל ההרצאות ושיפר ותיקן אותם.
תודה לדביר חדד, לניר שורץ ולרועי גוטליב על שהשלימו לי הרצאות כשהחסרתי, ועל כתיבת רוב התרגולים המופיעים בסוף החוברת.

תודה למתרגלת לווי 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.

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 ב- S .

הגדרה: שתי מערכות אלגבריות (S, T) , עם פעולה אחת $*$ תקראנה שקולות (איזומורפיות) אם קיימת פונקציה חח"ע ועל $f: S \rightarrow T$ 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 נטרלי 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

$$c = c * e = c * (a * b) = (c * a) * b = e * b = b \quad \text{הוכחה:}$$

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

$$\exists g \in G : \langle g \rangle := \{g^i : i \in \mathbb{Z}\}$$

טענה: כל חבורה ציקלית היא בהכרח אבלית

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

$$a * b = g^i * g^j = g^{i+j} \stackrel{\text{חוקי}}{=} g^j g^i = b * a$$

חוקי
חזקות
באגודה

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

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

$$cis\theta_1 * cis\theta_2 = cis(\theta_1 + \theta_2)$$

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

$$\Omega_n = \langle W_n \rangle = \{1, W_n, W_n^2, \dots, W_n^{n-1}\}$$

(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 ציקלית.

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

סימון: עבור מונואיד $(M, *)$ נסמן ב $Gr(M, *)$ את קבוצת כל ההפיכים במונואיד **טענה:** $Gr(M, *)$ היא חבורה.

הוכחה: (1) תכונת האסוציאטיביות היא תורשתית מהמונואיד.

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

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

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

(4) כל האיברים הפיכים : ע"פ הגדרה.

תת חבורה:

הגדרה: תהא $(G, *)$ חבורה, תת קבוצה $H \subseteq G$ נקראת תת-חבורה ונסמן $H \leq G$, אם H היא חבורה, כלומר אם $e \in H$

$$\forall a \in H : a^{-1} \in H \quad (2) \text{ סגירות}$$

$$\forall n \in \mathbb{Z} : nZ = \langle n \rangle \leq \mathbb{Z} : (\mathbb{Z}, +) \quad (1) \text{ דוגמאות:}$$

$$\langle 3 \rangle = 3\mathbb{Z} = \{0, \pm 3, \pm 6, \dots\}$$

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

חבורות קונגרוואנציה

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

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

$$2 = 5 \text{ mod } 3 = 8 \text{ mod } 3 \text{ למשל}$$

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

הגדרה: המבנה $\mathbb{Z}_n = \{0, 1, \dots, n - 1\}$ הוא חבורה ונקראת חבורת קונגרוואנציה, או חבורת השאריות מודולו n .

הרצאה 2- תכונת הצמצום ומחלקי אפס בחוג

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

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

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

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

נאמר שהוא ניתן לצמצום אם הוא ניתן לצמצום מימין ומשמאל.

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

הוכחה: נראה רק עבור צמצום מימין

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

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

עוד דוגמא: במונואיד $(Z_6, * \text{ mod } 6)$ איברים שאינם ניתנים לצמצום: 0, 2, 3, 4 לדוגמא $3*2=0*2$ אבל 0 שונה מ-3.

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

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

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

$$a^{i-k} = e \rightarrow a^{-1} = a^{i-k-1} \in S \text{ פעמים ונקבל } k \text{ מימין } a \text{ פעמים ונקבל } k$$

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

$$(1) \text{ מתקיים חוק הפילוג } a(b + c) = ab + ac$$

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

(2) $(R, +)$ חבורה אבלית.

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

$(M_n, *, +)$ חוג, לגבי הכפל רק מונואיד.

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

הגדרה: אבר בחוג $(R, *, +)$ $a \neq 0$ 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) $(Z_6, *, \text{mod} 6, +, \text{mod} 6)$ $0=3*2$ ולכן 2,3 מחלקי אפס.

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

הוכחה: בכיוון ראשון: יהי $a \in R$ ניתן לצמצום, ונניח בשלילה שהוא מחלק אפס משמאל, אזי

$$\exists 0 \neq b \in R : ab = 0 = a * 0 \Rightarrow b = 0$$

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.

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

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 .

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

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

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

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: $\emptyset \neq K_1 \leq K \rightarrow K_1 = K$)

יהי $a \in K$ 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:

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

שוב מתוך המינימליות נסיק כי $A=K$, מכאן שיש לפחות אדם אחד.

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

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 $\pm 1, \pm p$

המשפט היסודי של הארתמיטקה:

כל מספר טבעי ניתן לייצוג יחיד עד כדי חילוף סדר הגורמים $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

הגדרה: (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 $\text{lcm}(a, b) = [a, b]$

לדוגמא $[8, 12] = 24$

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

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

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

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

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

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

הגדרה: חילוק עם שארית: לכל $a, b \in \mathbb{Z}$, $b \neq 0$ קיימים באופן יחיד

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

משפט: $(a, b) = d \rightarrow \exists k_1, k_2 \in \mathbb{Z} : k_1a + k_2b = d$

הוכחה: אלגוריתם אוקלידס למציאת מ"ב"
 $a, b \in \mathbb{Z}$ יהיו

נחשב: $a = bq_1 + r_1$
 $b = r_1q_2 + r_2$
 $r_1 = r_2q_3 + r_3$

.....

$$r_{k-2} = r_{k-1}q_k + \widehat{r}_k$$

$$r_{k-1} = r_kq_{k+1}$$

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 $t \leq r_k$

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

$$t | \overbrace{(b - r_1q_2)}^{r_2}$$

.....
 $.... t | r_k \rightarrow t \leq r_k$

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: $(594, 420) = 6$
 $594 = 420 * 1 + 174$
 $420 = 174 * 2 + 72$
 $174 = 72 * 2 + 30$
 $72 = 30 * 2 + 12$
 $30 = 12 * 2 + 6$
 $12 = 6 * 2$

החבורה הסמטרית

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

הרצאה 3

חבורת אוילר (Euler)

הגדרה

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

משפט

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

הוכחה

הכיוון \Rightarrow נובע ממשפט כללי יותר שהוכחנו

בכיוון \Leftarrow נניח

$$\exists k_1, k_2 \in \mathbb{Z} : k_1 m + k_2 n = 1$$

ונניח $(m, n) = d$

אזי

$$d|m \wedge d|n \Rightarrow d|(k_1 m + k_2 n) \Rightarrow d|1 \Rightarrow d = 1$$

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

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

הגדרה

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

$$U_n := Gr(\mathbb{Z}, * \pmod n)$$

דוגמא

$$\langle 3 \rangle = \{1, 3, 9, 7\} \text{ - צקלית כי } U_{10} = (\{1, 3, 7, 9\}, * \pmod{10})$$

$$U_8 = \{1, 3, 5, 7\} \text{ לא צקלית}$$

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

טענה

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

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 המשוואה $3x = 55$ ב- \mathbb{Z}_{2000}

פתרון

$$3 * 667 = 2001 = 1 \text{ mod } 2000$$

$$\Rightarrow 3 * \underbrace{667 * 55}_x = 55 \text{ mod } 2000$$

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 $\{a_i \text{ mod } m_i\}$ קיימת שארית יחידה $x \text{ mod } m$

$$\begin{cases} x = a_1 \text{ mod } m_1 \\ x = a_2 \text{ mod } m_2 \\ \dots \\ x = a_k \text{ mod } m_k \end{cases}$$

המהווה פתרון למערכת המשוואות

דוגמא

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

מצא פתרון למערכת למערכת

הוכחת המשפט

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

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

ואז

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

הבנייה של $\{e_k\}$ תעשה בצורה הבאה:

לכל $1 \leq i \leq k$ נגזיר $n_i = \frac{m}{m_i}$. כיוון שכל ה- m_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 $e_i := s_i n_i$ ונקבל $e_i = 1 \pmod{m_i}$

כמו כן לכל $i \neq j$ $m_j | n_i$ ולכן $e_i = 0 \pmod{m_j}$, 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 $x = y \pmod{m}$

הגדרה

תהינה H, K חבורות עם איברים נטרליים e_H, e_K

המכפלה הישרה H -ו- K היא הקבוצה של הזוגות הסדורים

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

$$(h_1, k_1) * (h_2, k_2) = (h_1 h_2, k_1 k_2)$$

$H \times K$ היא חבורה.

דוגמא

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

הגדרה

העתקה בין מונואידים $\varphi: (G, *) \rightarrow (H, *)$ 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 מונומורפיזם.
- אם φ היא על אז היא נקראת אפימורפיזם.
- אם φ היא חח"ע ועל אז היא נקראת אזומורפיזם.

דוגמאות

1. $\varphi: \mathbb{Z} \rightarrow \mathbb{Z} \quad x \mapsto 2x$ – מונומורפיזם

2. $\varphi: U_{10} \rightarrow \langle 9 \rangle \quad x \mapsto x^2$ – אפימורפיזם

$$\text{Im}(\varphi) = \{1, 9\} = \langle 9 \rangle$$

3.

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

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

$$G \cong H$$

טענה

אם $f: G \rightarrow H$ ההומומורפיזם של חבורות אזי

$$f(1_G) = 1_H \quad (1)$$

$$f(x^{-1}) = f(x)^{-1} \quad \text{אם } x \text{ הפיך ב-} G \quad (2)$$

הוכחה

$$f(1_G) = f(1_G 1_G) = f(1_G) f(1_G) \Rightarrow f(1_G) = 1_H \quad (1)$$

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

מסקנה

בהינתן איזומורפיזם של מונואידים $G \cong H$ 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 $\varphi: \mathbb{Z}_{nm} \rightarrow \mathbb{Z}_n \times \mathbb{Z}_m$ ע"י:

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

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

וכנ"ל לגבי כפל.

תכונות החזקה 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 $\varphi(p) = p - 1$

מי הם המספרים $1 \leq m \leq p^k$ שאינם זרים ל- p ? $\varphi(p^k) = ?$

$$|\{p, 2p, \dots, p^2, 2p^2, \dots, p^k\}| = p^{k-1}$$

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

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

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

לדוגמא

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

הרצאה 4

סדר של איבר ושל חבורה

הגדרה

• סדר של חבורה הוא מס' האיברים בה.
 • סדר של איבר g בחבורה הוא

$$o(g) = \begin{cases} \min\{k \in \mathbb{N} : g^k = 0\} \\ \infty \text{ if there is no such } k \end{cases}$$

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

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

בכיוון הנגדי

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

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

$$e = a^k = (a^{o(a)})^q a^r \Rightarrow a^r = e$$

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

הערה

תמונה הומומורפית של חבורה צקלית היא חבורה צקלית.

$$f: \langle a \rangle \rightarrow H \Rightarrow H = \langle f(a) \rangle$$

הוכחה

$$\forall G \in G : g = a^i \rightarrow f(g) = f(a)^i \Rightarrow Im(f) = H = \langle f(a) \rangle$$

משפט

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

הוכחה

← הוכחנו באמצעות CRT.

⇒

$$\begin{aligned} \mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm} = \langle i \rangle &\Rightarrow \exists (a, b) \in \mathbb{Z}_n \times \mathbb{Z}_m : o(a, b) = nm \\ \Rightarrow (a, b)^{[n, m]} = ([n, m]a, [n, m]b) &= (ng_1a, mg_2b) = (0, 0) \\ o(a, b) = nm \leq [n, m] &\Rightarrow nm = [n, m] \Leftrightarrow (n, m) = 1 \end{aligned}$$

מיון חבורת ציקליות

משפט

תהא $G = \langle a \rangle$ 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 $f: \mathbb{Z} \rightarrow G : k \mapsto a^k$

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

לכן f הומו' (משמר פעולה).

כיוון שניתן להגיע לכל חזקה שלמה של a , $Im(f) = \langle a \rangle = G$, בנוסף אם $m \neq n$ אז בהכרח $a^m \neq a^n$ שכן אחרת G הייתה סופית (חזקות חוזרות על עצמן נכנסים ללולאה סופית) בסתירה לנתון, מכאן f מונו' ובסה"כ איזו'.

ב. שוב נגדיר את ההעתקה $f: \mathbb{Z}_n \rightarrow G : k \mapsto a^k$

שימור פעולה: $\forall k_1, k_2 \in \mathbb{Z}_n : k_1 \oplus k_2 = k_1 + k_2 - \alpha n$

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

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

דוגמא

$$\mathbb{Z} \cong \langle 1+i \rangle \leq \mathbb{C}$$

$$|1+i| \neq 1$$

חבורה צקלית אינסופית.

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

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

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 $G = \langle a \rangle$, צ"ל $H = \langle a^k \rangle$, $\exists k \in \mathbb{N}$

אם $H = \{e\}$ אזי $H = \langle e \rangle$

אחרת נגדיר $k := \min\{i \in \mathbb{N} : a^i \in H\}$ ונראה כי $H = \langle a^k \rangle$

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

טענה 1

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

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

דוגמא

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

הוכחה

$$1. \text{ התיכנות } (a^d)^{\frac{n}{(d, n)}} = (a^n)^{\frac{d}{(d, n)}} = e$$

2. מינימליות: נניח כי $(a^d)^t = e$ אזי $a^{dt} = e$. ידוע כי $o(a) = n$ ולכן $n | dt$ מכאן שגם:

$$t \geq \frac{n}{(d, n)} \left| \frac{d}{(d, n)} \right| \text{ אבל } \left(\frac{n}{(d, n)} \mid \frac{d}{(d, n)} \right) \text{ ולכן } \frac{n}{(d, n)} | t$$

תרגיל נחמד:

תהא $G = \langle a \rangle$, כמה איברים ב- G יוצרים את כל G (כל אחד בנפרד)?

פתרון

$$G = \langle a^k \rangle \Leftrightarrow o(a^k) = n = \frac{n}{(n, k)} \Leftrightarrow (n, k) = 1$$

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

תרגיל

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

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

טענה 2:

נניח שבחבורה G מתקיים עבור $g, h \in G$

$$\begin{aligned} 1. & gh = hg \\ 2. & (o(g), o(h)) = 1 \end{aligned}$$

אזי $o(gh) = o(g) o(h)$

הוכחה

$$o(gh) = m, o(g) = n, o(h) = k$$

צ"ל $m = nk$

$$(gh)^{nk} = (g^n)^k (h^k)^n = ee = e$$

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

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

$$m = nk$$

טענה

יהיו 2 איברים a, b בחבורה כך ש:

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

אזי

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

הוכחה

$$o(a^{(n,m)}) = \frac{n}{(n,m)} : 1$$

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

$$o((ab)^{(n,m)}) = o(a^{(n,m)} b^{(n,m)}) = \frac{nm}{(n,m)^2} = \frac{[n,m]}{(n,m)} : 2$$

קבוצת יוצרים של חבורה

הגדרה

בהינתן חבורה G , תת קבוצה $A \subset G$ נקראת קבוצת יוצרים של G אם $G = \langle A \rangle$.
אם A סופית אז נאמר כי G נוצרת סופית.

$$\mathbb{Z}^2 = \langle (1,0), (0,1) \rangle$$

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.

הערה

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

הגדרה

הדרגה של חבורה G : $\text{rank}(G)$ 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).

$$\text{rank}(\mathbb{Z}^n) = n \text{ למשל}$$

חבורה חופשית

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

$$C_n = \langle a : a^n = e \rangle \text{ לדוגמא}$$

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

הגדרה

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

הגדרה

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

$$G = F(X) \text{ סימון}$$

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

הגדרה

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

$$G = A(X) \text{ מסמנים חבורה אבלית חופשית מעל } X \text{ היא}$$

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

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

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

וקטור של חזקות בגודל n .

הרצאה 5

משפט ווילסון – Wilson

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

הוכחה

בכיוון האחד: עבור $n = p > 1$ ראשוני חבורת אוילר היא: $U_p = 1, 2, \dots, p-1$. כל איבר $a \in U_p$ ההפוך לעצמו מקיים:

ממנו. לכן כיוון שהחבורה אבלית, במכפלת האיברים $m = (p-1)!$ האיבר היחיד שאינו מצטמצם (ע"י סידור כל איבר ליד ההופכי שלו) הוא: $m = p-1 \equiv (-1) \pmod{p}$.

בכיוון ההפוך: נניח בשלילה כי n אינו ראשוני. אם $n = 4$ קל לבדוק כי: $(4-1)! = 6 \equiv 2 \pmod{4}$. 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: $2 < a \Leftrightarrow 4 < n \Leftrightarrow 2a < a^2 = n \Leftrightarrow 2a < a^2 = n$ כלומר $a, 2a$ מופיעים כ"א במכפלה $(n-1)!$ ומכפלתם מאפסת אותה בסתירה לנתון.

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

תרגיל (מועד א 2007)

הוכח או הפרך:

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

$1 + 116! \mid 117$ לא נכון כי $117 = 9 * 3$ ולכן $117 \mid 116! \Rightarrow 1 + 116! \not\equiv 1 \pmod{117}$.

קוסטים ומשפט לגרנז'

הגדרה

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

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

(x הוא הזזה של y ע"י איבר מ- H)

טענה

היחס $x \sim^L y$ הוא יחס שקילות

הוכחה

רפלקסיביות: $x \sim^L x : x = xe$

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

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

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

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

$$a \in H \Leftrightarrow aH = H$$

אכן \Rightarrow נובע מתוך סגירות

$$\Leftarrow \text{אם } a \notin H \text{ אזי } a^{-1} \notin aH \text{ אין } e$$

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.

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

$$0 + H = H, 1 + H = \{1, 4\}, 2 + H = \{2, 5\}$$

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

באותו אופן מגדירים קוסט ימני ב- H .

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: $G \setminus H = \{Ha : a \in G\}$

טענה

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

הוכחה

נגדיר את ההעתקה $\varphi: G/H \rightarrow G \setminus H$

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

$$Hg_1^{-1} = Hg_2^{-1} \Rightarrow H \underbrace{g_1^{-1}g_2}_{\in H} = H \Rightarrow g_2H = g_1H : \text{חח"ע}$$

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

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

$$[G:H] = |G/H|$$

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 $\varphi_a: H \rightarrow Ha$ ע"י $\varphi_a(h) = ha$.

$$h_1a = h_2a \Rightarrow h_1 = h_2$$

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

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

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

$$(1) \quad [G:H], |H| \mid |G|$$

$$(2) \quad \forall a \in G: o(a) = |\langle a \rangle| \mid |G|$$

$$(3) \quad \forall a \in G: a^{|G|} = e$$

משפט (מיון של ת"ח של חבורה ציקליות).

תהא $G = \langle a \rangle$ חבורה ציקלית, אם G מסדר n אזי:

$$(1) \quad H \leq G \Rightarrow |H| \mid n$$

$$(2) \quad \text{לכל } k \text{ טבעי, } k \mid n, \text{ קיימת ת"ח יחידה } H \leq G \text{ כך } |H| = k$$

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

הוכחה

$$(1) \quad \text{משפט לגראנז'}$$

$$(2) \quad \text{כל ת"ח של חבורה ציקלית היא ציקלית, כמו כן לכל } k \mid n:$$

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

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

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

משפט אויילר

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

הוכחה

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

תרגיל

חשב את $9^{121} \pmod{100}$

$$(9, 100) \Rightarrow 9^{\varphi(100)} = 1 \pmod{100}$$

$$\varphi(100) = \varphi(4)\varphi(25) = 2 * 20 = 40$$

$$9^{40} = 1 \pmod{100} \Rightarrow 9^{121} = (9^{40})^3 9 = 9 \pmod{100}$$

מקרה פרטי של משפט אויילר:

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

אלגוריתם ההצפנה RSA (ריבסט-שמיר-אדלמן) 1977

אליס מעוניינת שבוטב ישלח לה הודעה חסויה באמצעות תקשורת פומבית.

אלגוריתם:

- (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 $e \equiv d^{-1} \pmod{\varphi(n)}$ באמצעות אלגוריתם אוקלידס.
- (3) אליס שולחת לבוב את המפתח הציבורי (n, e) .
- (4) בוב מצפין הודעה M המקיימת $(M, n) = 1$ ע"י $E = m^e \pmod{n}$ ושולח לאליס.
- (5) אליס משחזרת את M : $E^d = M^{ed} = M^{1+\varphi(n)k} = M(M^{\varphi(n)})^k = M$

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.

תת-חבורה נורמלית וחבורת המנה

הגדרה:

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

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

אם $H \triangleleft G$ אזי קבוצת המנה $G \setminus H$ היא חבורה עם פעולת הכפל המוגדרת ע"י $Hx * Hy = Hxy$.
 אכן, אם $H \triangleleft G$ אזי $Hx = xH$ ובהתאם לכך $(Hx)^{-1} = Hx^{-1} = Hx^{-1}$ שכן $HH = H$ שכן $HxHx^{-1} = HHxx^{-1} = HH = H$ הוא איבר היחידה.

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

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

דוגמא

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

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

$$GL_2(\mathbb{Z}_2) = \langle a, b \rangle \text{ rank}(GL_2\mathbb{Z}_2) = 2$$

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

$$G \setminus \langle b \rangle = \left\{ \overbrace{\langle b \rangle}^{\{1, b, b^2\}}, \overbrace{\langle a \rangle}^{\{a, ab, ab^2\}} \right\}$$

$$G / \langle b \rangle = \left\{ \overbrace{\langle b \rangle}^{\{1, b, b^2\}}, \overbrace{\langle a \rangle}^{\{a, ba, b^2a=ab\}} \right\}$$

נשים לב כי $a \langle b \rangle = \langle b \rangle a$

$$G / \langle a \rangle = \left\{ \overbrace{\langle a \rangle}^{\{1, a\}}, \overbrace{\langle b \rangle}^{\{b, ba\}}, \overbrace{\langle b^2 \rangle}^{\{b^2, b^2a\}} \right\}$$

$$G \setminus \langle a \rangle = \left\{ \overbrace{\langle a \rangle}^{\{1, a\}}, \overbrace{\langle a \rangle b}^{\{b, ab\}}, \overbrace{\langle a \rangle b^2}^{\{b^2, ab^2\}} \right\}$$

שלא שווים!

$G / \langle b \rangle \cong \mathbb{Z}_2$ חבורת המנה.

$G / \langle a \rangle$ קבוצת מנה!

הרצאה 6 – גרעין ותמונה של הומומורפיזם

$$\begin{aligned} \forall g \in G : gH = Hg & \text{ ת"ח נורמלית אם } H \triangleleft G \\ \Leftrightarrow \forall g \in G : gHg^{-1} &= H \\ \Leftrightarrow \forall g \in G, h \in H : ghg^{-1} &\in H \end{aligned}$$

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

לדוגמא

$$G = \mathbb{Z}, H = n\mathbb{Z} = \langle n \rangle$$

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

$$\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\} = \mathbb{Z}_3$$

הגדרה:

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

טענה:

$$\ker(f) \triangleleft G$$

הוכחה

$$f(1_G) = 1_H \Rightarrow 1_G \in \ker(f)$$

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

ולכן תת חבורה.

לגבי נורמליות:

נסמן $K := \ker(f)$, 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 $\ker(f) \triangleleft G$

טענה

בהינתן $f: G \rightarrow H$ הומו, $\text{Im}(f) \leq H$.

$$1_H = f(1_G) \Rightarrow 1_H \in \text{Im}(f) \quad \text{א.}$$

$$h_1, h_2 \in \text{Im}(f) \Rightarrow h_1 = f(g_1), h_2 = f(g_2) \Rightarrow f(g_1g_2) = h_1h_2 \Rightarrow h_1h_2 \in \text{Im}(f) \quad \text{ב.}$$

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

תוצאה

אם G סופית, H סופית, $f: G \rightarrow H$, 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} .

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

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

טענה

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

הוכחה

$$\ker(f) = \{1_G\} \Leftrightarrow (\forall x, y \in G: xy^{-1} \in \ker(f) \Rightarrow x = y)$$

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

משפט האיזומורפיזם (!!!) Emmy Nother

טענה

תהא G חבורה ו $H < G$, נגדיר העתקה $\nu: G \rightarrow G/H$ 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 $\varphi: G \rightarrow H$ אפימורפיזם אז קיים איזומורפיזם $\psi: G/\ker(\varphi) \cong H$ כך ש $\varphi = \psi \circ \nu$ כאשר $\nu: G \rightarrow G/\ker(\varphi)$ הוא ההומומורפיזם הטבעי.

דוגמא

$$\begin{aligned} \varphi: \mathbb{Z} &\rightarrow \mathbb{Z}_n \\ x &\mapsto x \pmod{n} \\ \ker(\varphi) &= n\mathbb{Z} \\ \mathbb{Z}/n\mathbb{Z} &\cong \mathbb{Z}_n \end{aligned}$$

הוכחה:

נסמן $K = \ker(\varphi)$ ונגדיר את ההעתקה $\psi: G/K \rightarrow H$ 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 ש ψ הומומורפיזם, נעזר בעובדה כי $K < G$:

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

כעת נבדוק כי ψ חז"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 $f: G \rightarrow H$ כך ש: $K = \ker(f)$

דוגמא:

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

שלוש תתי חבורות נורמליות ב- D_3 : $\{id, \langle b \rangle, D_3\}$

איזה איזומורפיזם φ מ- D_3 מתאים ל- $\ker(\varphi) = \{id\}$?

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

$Im(\varphi)$	φ	$\ker(\varphi)$
6	$x \mapsto x$	$\{id\}$
2	$x \mapsto x^3$	$\langle b \rangle$
1	$x \mapsto id$	D_3

תרגיל

תהיינה שתי חבורות G_1, G_2 מסדרים זרים, כמה הומומורפיזם שונים קיימים מ- G_1 ל- G_2 ?

פתרון

$$\varphi: G_1 \rightarrow G_2$$

אזי

$$|kar|_{|G_1|} |Im|_{|G_2|}$$

$$G_1/\ker(\varphi) \cong Im(\varphi)$$

$$\frac{|G_1|}{|\ker(\varphi)|} = |Im(\varphi)|_{|G_2|}$$

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

דוגמאות נוספות

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

הומו' לפי תכונות הדטרמיננטה.

נבדוק על: לכל מספר ממשי שונה מאפס r .

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

$$SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$$

$$|GL_n(\mathbb{R})|/|SL_n(\mathbb{R})| \cong (\mathbb{R}^*, *) : I \text{ לפי משפט איזור 1}$$

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

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

פתרון

נגדיר אפימורפיזם $\varphi: \mathbb{R} \rightarrow \mathbb{C}$ 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 $G/H \cong \mathbb{R}$

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

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

$$\mathbb{R}^2/H \cong \mathbb{R} : I \text{ ע"פ איזור 1}$$

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

הרצאה 7

משפט האיזומורפיזם השני

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

$$\{ah: a \in A, h \in H\} = AH \leq G \quad (1)$$

$$AH/H \cong A/A \cap H \quad (2)$$

הוכחה

סעיף 1:

$$1 \in AH \quad (1)$$

$$\forall a_1 a_2, h_1, h_2: (a_1 h_1) * (h_2^{-1} a_2^{-1}) \in AH \quad (2)$$

נרצה להראות כי $(AH)(AH)^{-1} \subseteq AH$ (זה בקבוצות, כלומר $(a_1 h_1) * (h_2^{-1} a_2^{-1}) = a_1 h_3 a_2^{-1} = a_1 \underbrace{a_2 h_4}_{H \triangleleft G} \in AH$)

סעיף 2:

(א) נתון $H \triangleleft AH$ ולכן $g = ah \in AH$ ובפרט עבור $H \triangleleft G \Rightarrow \forall g \in G: gH = Hg$

(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 $H \triangleleft G$). 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 $\varphi: A \rightarrow AH/H$ כך $\ker(\varphi) = A \cap H$

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

נראה הומו:

$$\varphi(ab) = abH = a \widetilde{b}H = aHbH = \varphi(a)\varphi(b)$$

φ היא על שכן המקור לכל $aH = ahH$ 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 איזול' הראשון.

הערה

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

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 $G, N \triangleleft H \triangleleft G, N \triangleleft G$ אזי

$$G/N / H/N \cong G/H$$

הוכחה

נגדיר את ההעתקה $\varphi: G/N \rightarrow G/H$ ע"י $\varphi(gN) = gH$

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 $\mathbb{Z}/6\mathbb{Z}$

$$\mathbb{Z}/6\mathbb{Z} / 2\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}_2$$

תרגיל נחמד

יהיו G חבורה $G, H \triangleleft G, A \leq G$, הוכח:

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

$$A/A \cap H \cong AH/H \leq G/H$$

$$[A : A \cap H] = [AH : H] \leq [G : H]$$

$$G/A \cap H / A/A \cap H \cong G/A \Rightarrow [G : A \cap H] = [A : A \cap H][G : A] \Rightarrow [G : A \cap H] \leq [G : A][G : H]$$

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

אנדומורפיזם

הגדרה:

בהינתן מונואיד M , הומומורפיזם $f: M \rightarrow M$ 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) $f(\text{יוצר}) =$

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

$$\begin{aligned} \text{א) } f = id \quad 1 \mapsto 1 \Rightarrow k \mapsto k \\ \text{ב) } f = -id \quad 1 \mapsto -1 \Rightarrow k \mapsto -k \end{aligned} \quad (2) \quad Aut(\mathbb{Z}_n)$$

טענה:

$$\mathbb{Z}_n = \langle a \rangle \Leftrightarrow (a, n) = 1$$

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

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

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

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

דוגמאות

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

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

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

ולכן הומו'. נבדוק חח"ע:

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

כיוון שהראינו $|Aut(\mathbb{Z}_n)| = |U_n|$, 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':

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

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

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

ולכן אוטו'.

סימון

קבוצת כל האוטומורפיזמים הפנימיים

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

טענה

$$\text{Inn}(G) \triangleleft \text{Aut}(G)$$

הוכחה

תחילה נראה כי היא תת חבורה

$$I_e = id \in \text{Inn}(G) \quad (1)$$

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

$$I_{b^{-1}} \circ I_b(x) = b^{-1}bxb^{-1}b = x \Rightarrow (I_b)^{-1} = I_{b^{-1}}$$

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

כעת נראה נורמליות:

$$\forall f \in \text{Aut}(G), I_a \in \text{Inn}(G), x \in G$$

$$(f \circ I_a \circ f^{-1})(x) = f(I_a(f^{-1}(x))) = f(af^{-1}(x)a^{-1}) = f(a)xf(a^{-1}) = I_{f(a)}(x) \in \text{Inn}(G)$$

הגדרה

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

דוגמאות

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

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

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

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

טענה

$$Z(G) \triangleleft G$$

הוכחה

$$\begin{aligned} \forall g \in G: 1g = g1 &\Rightarrow 1 \in Z(G) & (1) \\ \forall z \in Z(G), g \in G: z^{-1}g &= (g^{-1}z)^{-1} = gz^{-1} \Rightarrow z \in Z(G) & (2) \\ z_{1,2} \in Z(G): z_1z_2g &= z_1gz_2 = gz_1z_2 \Rightarrow z_1z_2 \in Z(G) & (3) \end{aligned}$$

נורמליות:

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

טענה

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

הוכחה

$$\varphi: G \rightarrow \text{Inn}(G), g \mapsto I_g$$

נגדיר העתקה I_g 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

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

$$\begin{aligned} 1x = x1 &\Rightarrow 1 \in C(x) & (1) \\ \forall c \in C(x): c^{-1}x &= (x^{-1}c)^{-1} = (cx^{-1})^{-1} = xc^{-1} \Rightarrow c^{-1} \in C(x) & (2) \\ c_{1,2} \in C(x): c_1c_2x &= xc_1c_2 \Rightarrow c_1c_2 \in C(x) & (3) \end{aligned}$$

הערה

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

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 $a_1 \mapsto a_2 \mapsto \dots \mapsto a_k \mapsto a_1$ ומסומנת ע"י $(a_1 a_2 \dots a_k)$ למשל $(1 3 5)$.

ניתן לכתוב כל תמורה ב S_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

$$\sigma^m = \sigma_1^m \dots \sigma_k^m \text{ זרים שהעגילים זרים}$$

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

m 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 לכתובה כמכפלה של מס' זוגי של חילופים.

אחרת, התמורה נקראת אי זוגית.

טענה

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

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 . $A_n \triangleleft S_n$

הוכחה

- (א) $id = (1 \ 2)(1 \ 2) \in A_n$
- (ב) אם σ 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 $\sigma \mapsto \sigma(1 \ 2) \in A_n^c$, $A_n \rightarrow S_n - A_n$. 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 $[S_n : A_n] = 2$ ולכן $A_n \triangleleft S_n$

עוד דרך לראות זאת:

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

זהו הומומורפיזם $have\ to\ same\ parity$ otherwise $sign(\sigma\tau) = \begin{cases} 0 \\ 1 \end{cases}$ ולכן

$$\ker(sign) = A_n \triangleleft S_n$$

דוגמא

$$\begin{aligned} & \text{אורתוגונליות} \\ \varphi: \overline{O_n(\mathbb{R})} & \rightarrow \{\pm 1\} \\ A & \mapsto \det(A) \\ \ker(\varphi) & = SO_n(\mathbb{R}) \\ [O_n(\mathbb{R}):SO_n(\mathbb{R})] & = 2 \end{aligned}$$

הגדרות:

$$\begin{aligned} \text{the orthogonal group} & = O_n(F) = \{A \in M_n(F): AA^T = I_n\} \\ \text{special orthogonal group} & = SO_n(F) = \{A \in O_n(F): \det(A) = 1\} \end{aligned}$$

דוגמא

$$\begin{aligned} A_4 & = \left\{ \begin{array}{l} id, (1\ 2\ 3), (1\ 3\ 2), (2\ 3\ 4), (2\ 4\ 3), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 5), (1\ 4\ 3) \\ (1,2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3) \end{array} \right\} \\ |A_4| & = 12 = \frac{4!}{2} \end{aligned}$$

החבורה הזיהדרלית (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:

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

כל איבר ב- D_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.

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

טיפוס (מבנה) של תמורה

תהא σ תמורה ב- S_n . נפרק אותה למכפלה של מספרים זרים $(a_{11} \dots a_{1r_1}) \dots, (a_{k1} \dots a_{kr_k})$ כד ש $r_1 \geq r_2 \geq \dots \geq r_k$. 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

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

דוגמא

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

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

$$1 \rightarrow 1 \rightarrow 2 \rightarrow 4$$

$$2 \rightarrow 3 \rightarrow 3 \rightarrow 2$$

$$3 \rightarrow 4 \rightarrow 1 \rightarrow 1$$

$$4 \rightarrow 2 \rightarrow 5 \rightarrow 5$$

$$5 \rightarrow 5 \rightarrow 4 \rightarrow 3$$

הוכחה

נוכיח טענה שקולה:

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

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

טענה

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

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

דוגמא

הראה כי $V_4 \triangleleft A_4$

פתרון

 V_4 מכיל את כל התמורות מטיפוס $(2,2)$ ב- A_4 . מכאן ש:

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

משפט

$$\forall n \geq 2 : S_n = \langle (1\ 2), (1\ 2 \dots n) \rangle$$

$$\text{rank}(S_n) = 2$$

הוכחה

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

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

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

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

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

.....

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

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

$$(1\ 4) = (1\ 3)(3\ 4)(1\ 3)$$

$$(1\ 5) = (1\ 4)(4\ 5)(1\ 4)$$

.....

$$(1\ n) = (1\ n-1)(n-1\ n)(1\ n-1)$$

כלומר $S_n = \langle \sigma, \tau \rangle$

הרצאה 9

משפט קיילי | הצגה של חבורות

משפט Cayley

כל חבורה סופית G איזומורפית לתת חבורה של S_G

הוכחה

נגדיר את ההעתקה $\varphi: G \rightarrow S_G$ 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 $G \rightarrow G$.

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

ומתוך סופיות זוהי גם על.

נבדוק שימור פעולה של φ , כלומר נראה כי:

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

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

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 טרנזיטיבית:

$$A \triangleleft B \triangleleft C \not\Rightarrow A \triangleleft C$$

דוגמא

$$K = \{e, ba\} \triangleleft \underbrace{V_4}_{\{e, ba, a^2, ba^3\}} \triangleleft D_4 = \langle a, b \rangle$$

$$K \not\triangleleft D_4$$

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 כע"כ $g = xy$ כאשר $x \in X, y \in Y$ (ב) $\forall x \in X, y \in Y: xy = yx$.

משפט

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

הוכחה

⊆

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

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

והיא חח"ע ועל שכן:

קיים
יחיד

$$\forall g \in G: \exists! x \in X, y \in Y: xy = g$$

⊇

אם $G \cong X \times Y$ נגדיר $\varphi: G \rightarrow X \times Y$ כע"כ $\varphi^{-1}(X \times \{1_Y\}), \varphi^{-1}(\{1_X\} \times Y)$

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

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

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

דוגמא

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

$$U_8 = \langle 3, 5 \rangle = \langle 5 \rangle \times \langle 3 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

משפט פיצול חבורות

תהא G חבורה עם תתי חבורת X, Y כך ש:

$$X, Y \triangleleft G \quad (\alpha)$$

$$X \cap Y = \{e\} \quad (\beta)$$

$$G = XY \quad (\gamma)$$

אזי:

$$G \cong X \times Y$$

הוכחה

מתוך $X \triangleleft G$ נובע בפרט:

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

ולכן גם $xyx^{-1} \in X$

מתוך $Y \triangleleft G$ נובע בפרט:

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

ולכן גם $xyx^{-1} \in Y$

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

זה נכון לכל x, y .

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

הגדרה

תהא חבורה G עם ת"ח X, Y כך ש:

$$X \triangleleft G, Y \leq G \quad (\alpha)$$

$$X \cap Y = \{e\} \quad (\beta)$$

$$G = XY \quad (\gamma)$$

אזי נאמר כי G היא מכפלה חצי ישרה של X ו Y ונסמן

$$X \rtimes Y$$

דוגמא

$$D_3 \cong \langle a \rangle \rtimes \langle b \rangle \quad (1)$$

$$H = \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \right\} \text{ חבורת Heitenberg} \quad (2)$$

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

הראו בבית כי $H = X \rtimes Y$

בחבורה אבלית נהוגה כתיבה חיבורית: במקום x^m כותבים mx .
 $\forall x \in A : x = \sum_{i=1}^k m_i x_i \quad m_i \in \mathbb{Z}$ הכוונה $A = \langle x_1, \dots, x_k \rangle$ אם
 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 $\gcd(c_1, \dots, c_k) = 1$ קיימת קבוצה יוצרת $\{y_i\}_{i=1}^k$ כך ש $y_1 = c_1 x_1 + \dots + c_k x_k$.

הוכחה

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

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 $\{x_1, x_1 + x_2, x_3, \dots, x_k\}$.

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

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

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

$$y_1 = (c_1 - c_2)x_1 + c_2(x_1 + x_2) + \dots + c_k x_k = c_1 x_1 + c_2 x_2 + \dots + c_k x_k$$

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 ש x_1 הוא בעל סדר מינימלי. נרצה להראות ש:

$$A = \langle x_1 \rangle \oplus \langle x_2, \dots, x_k \rangle$$

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

$$m_1 x_1 + \dots + m_k x_k = 0 \quad \text{עם } m_1 x_1 \neq 0. \text{ כלומר } m_1 < o(x_1)$$

ניתן להניח כי כל ה m_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 $y_1 = c_1 x_1 + \dots + c_k x_k$

$$d y_1 = m_1 x_1 + \dots + m_k x_k = 0$$

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

מסקנה

A אבליית נוצרת סופית.

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

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

הגדרה

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

למשל \mathbb{Z}_8 היא חבורת-2.

לפי משפט שהראינו כל חבורה אבליית 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 $\sum_{i=1}^k r_i = r$

מסקנה

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

דוגמא

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

אקספוננט של חבורה

הגדרה

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

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

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

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

$$\sigma^m = ()^m \dots ()^m$$

הרצאה 10

מיון חבורות אבליות

טענה

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

$$G = mG \oplus nG$$

הוכחה

- א. $mG, nG \triangleleft G$
- 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 $G = 1G = (n, m)G = nG + mG$

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

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

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 $1 \leq i \leq k$ בהכרח קיימת ל- G ת"ח מסדר $p_i^{\alpha_i}$. 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.

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

פעולות של חבורות על קבוצות

הגדרה

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

כאשר הפעולה * מקיימת את התכונות הבאות:

$$\forall x \in X : 1 * x = x \quad (1)$$

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

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 ההצמדה, היא פעולה של החבורה על עצמה $G \times G \rightarrow G : (g_1, g_2) \mapsto g_1 g_2 g^{-1}$

נבדוק שהפעולה מוגדרת היטב

$$\forall g \in G : 1 * g = 1 g 1^{-1} = g \quad (1)$$

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

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

משפט

הן מאותו טיפוס $\sigma, \tau \in S_n \Leftrightarrow$ 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: $\tau = \gamma \sigma \gamma^{-1}$.

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

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

דוגמא

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

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 ?

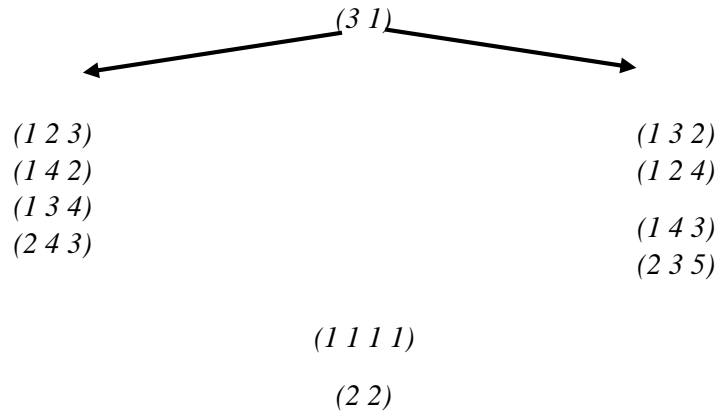
פתרון

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 $(1\ 2\ 3) \sim (1\ 3\ 2)$ אבל ב A_4 $(1\ 2\ 3) \not\sim (1\ 3\ 2)$ שכן המצמיד A_4 אינו מכיל $(2,3)$

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



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 , המייצב (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) $g \in Stb(G) \Rightarrow g * x = x \Rightarrow g^{-1} * x = g^{-1} * (g * x) = (g^{-1}g) * x = 1 * x = x \Rightarrow g^{-1} \in Stb(x)$
- (ג) $\forall g_1, g_2 \in Stb(X) : (g_1g_2) * x = g_1 * (g_2 * x) = g_1 * x = x \Rightarrow g_1g_2 \in Stb(x)$

משפט

תהא G חבורה הפועלת על X , אזי

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

הוכחה

$$\forall x \in X : \varphi : G * x \rightarrow G / Stb(x), \quad g * x \mapsto gStb(x)$$

נראה שההעתקה מוגדרת היטב

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

נראה ש φ 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 $G = \langle \sigma \rangle$ על X המוגדרת ע"י $\sigma^i * x = \sigma^i(x)$

פתרון

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

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

$$Stb(1) = \{1, \sigma^3\} = Stb(3) = Stb(5)$$

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

הרצאה 11

נוסחת המחלקה

תהא G חבורה סופית, אזי:

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

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

$$|G| = \sum_{x \text{ rep}} |G * x| = \sum_{x \text{ rep}} \frac{|G|}{|C(x)|} \stackrel{\substack{\text{במרכז} \\ \text{כל} \\ \text{איבר} \\ \text{הוא} \\ \text{מחלקת צמידות} \\ \text{של עצמו} \\ \text{כלומר באורך 1}}}{=} |Z(G)| + \sum_{\substack{x \text{ rep} \\ \neq Z(G)}} \frac{|G|}{|C(x)|}$$

תוצאה

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

הוכחה

ע"י נוסחת המחלקה:

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

כלומר $|Z(G)|$ קולכן 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':

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

נניח בשלילה $|Z(G)| = p$. אזי בהכרח $|G/Z(G)| = p$ וזה לא יתכן, מכיוון:

$$e \neq a \in Z(G) \Rightarrow \langle a \rangle = Z(G)$$

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

אם $o(b) = p^2$ אזי G ציקלית בסתירה להנחה, לכן נניח $o(b) = p$ ואז $\langle a, b \rangle$ ציקלית.

$\langle a, b \rangle$ אבלית שכן $a \in Z(G)$ ולכן בפרט $ab = ba$. $\langle a, b \rangle = Z(G)$ ולכן $\langle a, b \rangle = G$ 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 G 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:

$G \setminus X$	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.

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

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:

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

החבורה $G = \langle \sigma \rangle$ 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 .

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 $|G| = p^r m$, 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 $H_i \cong \mathbb{Z}_{p^{r_i}} \leq P$ ונקבל

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

משפט סילו 1:

נראה באינדוקציה על |G|.

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

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

צ"ל: נכונה עבור $|G| = p^n m$

ישנם שני מקרים בלבד:

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

כלומר כל ת"ח היא מסדר $p^{n_1} m_1 < p^n m$ באופן כללי יתכן גם: $m_1 \leq m$

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

מכאן ע"פ נוסחת המחלקה:

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

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

$$(a \in Z(G)) \quad H = \langle a \rangle \triangleleft G$$

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

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

$$H \triangleleft G \Rightarrow \text{קיים אפי } \nu: G \rightarrow G/H, \quad g \mapsto gH$$

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

$$\nu_0: A^* \rightarrow A$$

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

לפי משפט איזול' 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 קמסדר p^n , יש ת"ח מסדר p^k לכל $1 \leq k \leq n$.

הוכחה

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

צ"ל עבור $|G| = p^n$ (ההתחלה ברורה).

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

ולכן בתוך $Z(G)$ חבורה אבלית יש איבר a מסדר p , נתייחס ל $a \geq H \triangleleft G$ ולהעתקה $\nu: G \rightarrow G/H$.

ע"פ הנחת האינדוקציה יש ב G/H (מסדר p^{k-1}) כל ת"ח מסדר p^k , נניח $|A| = p^k$ ונסמן $A^* = \nu^{-1}(A) \leq G$. ונמצא את $\nu: A^* \rightarrow A$ ומכאן ע"י איזול' 1.

תוצאה – משפט קושי

תהא G כך ש: $p \mid |G|$ 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 $p^{1 \leq k \leq n}$ בפרט עבור $k = 1$.

הרצאה 12

משפטי סילו'

הבהרה לגבי מה שלמדנו בפעם שעברה

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

אמרנו שזה למעשה מקרה פרטי של טענה כללית יותר שאם $|G| = p^k$ 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 קיש ת"ח מסדר p^k לכל $1 \leq k \leq n$.

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

כשמדובר ב- p^1 זה כן שקול כי \mathbb{Z}_p צקלית בהכרח.

משפט

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

הוכחה

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

נסיק ע"פ טענה קודמת כי:

$$P_1 = \{g \in G : o(g) = p_1^{\alpha_1}\}$$

$$G = \widehat{G_{p_1^{\alpha_1}}} \oplus \dots \oplus G_{p_k^{\alpha_k}}$$

ע"פ משפט סילו 1 לכל P_i קיימת ת"ח p_i -סילו וזו מקיימת $P_i \leq G_{p_i^{\alpha_i}}$. מכאן שהחיתוך של כל שני ת"ח p_i -סילו הוא טריוויאלי,

יחד עם האבליות נסיק (תנאי משפט פיצול חבורות) כי:

$$\bigoplus_i P_i \leq G$$

אבל $|G| = |\bigoplus_i P_i|$ 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 התיכוניםטים).



הסבר

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

בתוך 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 $x \in X$ ש $\forall g \in G: g * x = x$
- קבוצת נקודות השבת היא

$$\underbrace{F}_{Fixed} = \left\{ x \in X : \underbrace{G * x = x}_1 \right\}$$

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

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

X אחוד זר של מסלולים (המרכזו 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 שבדקים לאן סיטואציות חיצוניות בחיים לוקחות אותם. מתמטיקה \equiv חיים.

הגדרה

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

דוגמא

$$S_n \text{ פועלת על } \{1, \dots, n\}$$

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

$$\text{למשל } 1 \in X \text{ יכול להגיע ל-} s \in X \text{ ע"י } s = (1,5) * 1$$

משפט סילו 2:

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

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

הוכחה

תהא $H \leq G$ עם $|H| = p^k$.

קבוצת ת"ח p -סילו $Syl_p =$

ע"פ משפט סילו 1:

$$Syl_p \neq \emptyset$$

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

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

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

אבל $(m, p) = 1$ 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.

$$P_1 = xP_2x^{-1} \text{ ולכן } |xP_2x^{-1}| = |P_2| = p^n = |P_1|$$

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

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

הוכחה

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

דוגמא

$$|Syl_p(G)| := n_p$$

$$|D_3| = 6 = 2 * 3 : D_3 \text{ ב}$$

$$n_2 = 3(3 \text{ סילו}), n_3 = 1$$

$$\langle a \rangle \triangleleft D_3$$

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

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

הבהרה (משאלה של סטודנט)

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

הגדרה

תהא G חבורה ו $H \leq G$. הנורמליטור של H ב-G הוא:

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

טענה

$$N_G(H) \leq G$$

הוכחה

$$e \in N_G(H) \quad .1$$

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

משפט סילו 3

עבור חבורה G נסמן $n_p = |Syl_p(G)|$

$$n_p = [G : N_G(P)] \quad (\text{א})$$

$$n_p \equiv 1 \pmod{p} \quad (\text{ב})$$

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

הוכחה

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

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

$$n_p = |G * P| = [G : Stb(P)] = [G : N_G(P)] \text{ לכן}$$

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

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

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

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

ומכאן ע"פ נוסחת המחלקה הכללית:

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

$$|F| \equiv n_p \pmod{p} \text{ ונקבל כי}$$

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

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

מצד שני, יהי $Q \in Syl_p(G)$ כך ש $Q \in F$, אזי $P \leq N_G(Q)$ שכן Q היא נקודת שבת תחת הצמדה של

אברי P : $Q = pQp^{-1} \forall p \in P$ ולכן $P \leq N_G(Q)$.

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

מסקנה:

$$|F| = 1 \Rightarrow n_p \equiv |F| \pmod{p} = 1$$

(ג) ע"פ לגראנז':

$$[G : P] = \frac{|G|}{|P|} = \frac{|G|}{|N_G(P)|} \frac{|N_G(P)|}{|P|} = [G : N_G(P)][N_G(P) : P] \\ \Rightarrow n_p \mid \frac{|G|}{|P|} = m$$

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

הגדרה

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

דוגמאות:

\mathbb{Z}_p עבור p טבעי

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

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

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

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.

הרצאה 13: חבורות פתירות solvable

הגדרה

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

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = \{e\}$$
 כך שלכל k חבורת המנה G_k/G_{k+1} אבליה.
- סדרה נורמלית אחת היא עידון של סדרה נורמלית אחרת אם היא תוצאה של הוספת ת"ח לסדרה.
- סדרה נורמלית נקראת סדרת הרכב אם לא ניתן לעדן אותה, כלומר שכל גורמיה פשוטים.

דוגמאות

- (1) כל חבורה אבליה היא פתירה. $G \triangleright \{e\}$.
- (2) $D_n \triangleright \langle a \rangle \triangleright \{e\}$ (הגורמים צקליים ולכן אבליים). $D_n / \langle a \rangle \cong \mathbb{Z}_2, \langle a \rangle / \{e\} \cong \langle a \rangle$
- (3) סדרת ההרכב היא $D_4 \triangleright \langle a \rangle \triangleright \langle a^2 \rangle \triangleright \{e\}$
 $S_4 \triangleright A_4 \triangleright V_4 \triangleright \{e\}$ פתירה: $S_4 \triangleright A_4 \triangleright V_4 \triangleright \{e\}$
 סדרת ההרכב $S_4 \triangleright A_4 \triangleright V_4 \triangleright \langle (1\ 2)(3\ 4) \rangle \triangleright \{e\}$
 $V_4 = \{ (1\ 2)(3\ 4), (1\ 3)(2\ 4) \}$

משפט

כל חבורת p פתירה

טענת עזר

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

הוכחת טענת העזר

באינדוקציה על $|G| = p^n$
 התחלה: אם $|G| = p$ אז ניקח את G עצמה.
 הנחה: נניח שהטענה נכונה לכל G כך ש- $|G| < p^n$, צ"ל עבור $|G| = p^n$.
 בחבורת p המרכז $Z(G)$ לא טריוויאלי.
 כחבורה אבליה ב- $Z(G)$ יש איבר a מסדר p .
 נסמן $H = \langle a \rangle$, כיוון ש- $H \leq Z(G), H \triangleleft G$. נתבונן באפימורפיזם הטבעי $v: G \rightarrow G/H, g \mapsto gH$.
 ע"פ לגראנז' $|G/H| = p^{n-1}$ ולכן עפ"י ההנחה לכל $1 \leq k \leq n$ קיימת ת"ח נורמלית $A \triangleleft G/H$, $|A| = p^{k-1}$.
 נתבונן ב- $\tilde{A} = v^{-1}(A)$. כיוון ש- v הומו, $\tilde{A} \triangleleft G$. ע"פ משפט איז'ר $\tilde{A}/H = \ker v \cong A$ (גם בצמצום של v ל- \tilde{A} הגרעין נשאר H).
 ולכן $|\tilde{A}| = |H||A| = pp^{k-1} = p^k$ ■

הוכחת המשפט

ע"פ טענת העזר נוכל לבנות סדרה נורמלית

$$G \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright \{e\}$$

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 אבליה.

טענה

A_5 אינה פתירה.

טענה

מספיק להראות כי A_5 פשוטה.

נתאר את מחלקות הצמידות של A_5 . ראשית נכתוב את הטיפוסים ב- S_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 $H \leq A_5$ תהיה נורמלית ב- A_5 היא צריכה להכיל מחלקות צמידות בשלמותם שכן הן מהוות את המסלולים של פעולת ההצמדה, ולכן אם H מכילה חלקית מסלול קיימת הצמדה $ghg^{-1} \notin H$ (חייבת להכיל את id)

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

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

מסקנה: A_5 אינה פתירה.

משפט (מיון של ת"ח של חבורה ציקלית).

תהא $G = \langle a \rangle$ חבורה ציקלית, אם G מסדר n אזי:

$$H \leq G \Rightarrow |H| \mid n \quad (3)$$

$$|H| = k \quad \text{לכל } k \text{ טבעי, } k \mid n, \text{ קיימת ת"ח יחידה } H \leq G \text{ כך } |H| = k \quad (4)$$

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

הוכחה

(3) משפט לגראנז'

(4) כל ת"ח של חבורה ציקלית היא ציקלית, כמו כן לכל $k \mid n$:

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

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

באופן כללי יותר, אם $j = \frac{n}{t}$ אז במילא $\langle a^j \rangle \leq \langle a^{\frac{n}{k}} \rangle$ ומכאן היחידות

דוגמא

תאר את כל ת"ח של \mathbb{Z}_{70} .

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

$$\langle 1 \rangle, \langle 2 \rangle, \langle 5 \rangle, \langle 7 \rangle, \langle 10 \rangle, \langle 14 \rangle, \langle 35 \rangle, \langle 70 \rangle$$

נגזרת של חבורה

הגדרה

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

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

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

הגדרה

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

$$G' = \langle \{[a, b] : a, b \in G\} \rangle$$

קוראים לזה נגזרת של G

משפט

לכל חבורה G מתקיים:

$$G' \triangleleft G \quad (\text{א})$$

$$G/G' \text{ אבלי} \quad (\text{ב})$$

הוכחה

(א)

$\forall g, a, b \in G$:

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

$$\forall x, y \in G: xG'yG' = yG'xG' \quad (\text{ב}) \text{ צ"ל:}$$

מתוך הנורמליות

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

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

למעשה G' היא ת"ח נורמלית הקטנה ביותר כך ש: G/G' אבלי.

מסקנה

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

דוגמאות:

$$[a, b] = aba^{-1}b^{-1} = a(ab^{-1})b = aab^{-1}b = a^2 = a^{-1} \text{ שכן } (D_3)' = \langle a \rangle \geq \langle a^2 \rangle \quad (1)$$

$$(D_4)' = \langle a^2 \rangle \quad (2)$$

תרגיל

הנגזרת של חבורת Heisenberg (מעל שדה F , יכול להיות גם סופי כמו \mathbb{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 אבלי, ולכן H פתירה!

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:

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

כלומר יתכנו 6 מסלולים באורך 2 כ"א ומסלול אחד באורך 7 ואז אין נקודות שבת: $F = \emptyset$.

למשל בצורה מפורשת: נגדיר את הפעולה של $D_7 = \langle a, b : a^7 = e, b^2 = e, ab = ba^6 \rangle$ על: $X = \{1, 2, \dots, 19\}$ ע"י:

b מזיז רק את המספרים $1 \leq i \leq 12$ בהתאם למסלולים:

$$(12), (34), (56), (78), (9 \ 10), (11 \ 12)$$

לעומתו a מזיז רק את המספרים $13 \leq i \leq 19$ בהתאם למסלול: $(13 \ 14 \ 15 \ 16 \ 17 \ 18 \ 19)$.

קל לבדוק שההגדרה הזו מקיימת את האקסיומות של פעולה, כלומר ש:

$$1. \quad \forall i: e * i = i$$

$$2. \quad \forall i, g_1, g_2 \in D_7: g_1 * (g_2 * i) = (g_1 \cdot g_2) * i$$