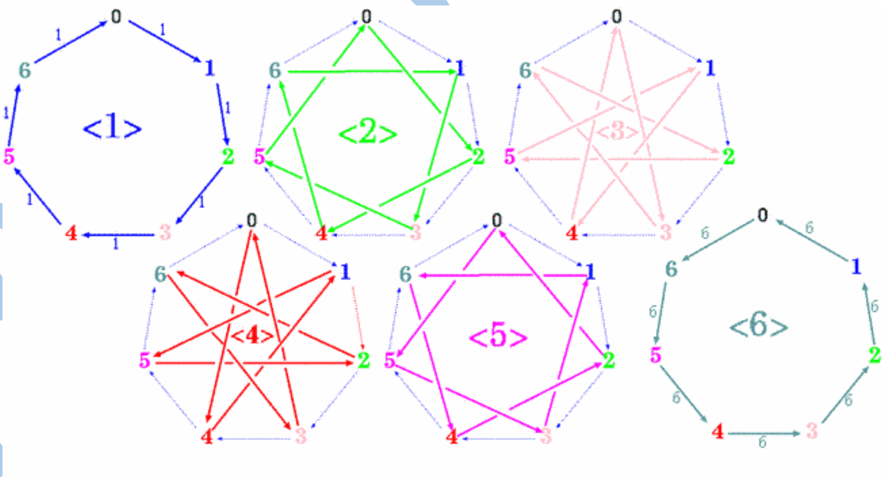
ב"ה

אלגברה מופשטת 1

כתב: בנימין לוין
מההרצאות של רוני ביתן
קיץ תשע"ג

מייל : levbinyamin@gmail.com



כל הזכויות שמורות לבנימין לוין ©

הרצאה 1

Rony.bitan@gmail.com

90% מבחן +10% בוחן

מבנים אלגברים עם פעולה אחת

<u>הגדרה:</u> 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

<u>הגדרה:</u> שתי מערכות אלגבריות S,T, עם פעולה אחת * תקראנה שקולות (איזומורפיזם) אם קיימת פונקציה חח"ע ועל $f: S \to T$ המשמרת את הפעולה של S, כלומר

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

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

<u>הערה:</u> באגודה מותר להשתמש בחוקי חזקות.

<u>הגדרה:</u> 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.

<u>טענה:</u> אם קיים איבר נטרלי מימין b וגם קיים נטרלי משמאל a אז a=b

<u>מסקנה:</u> אם קיים איבר נטרלי אזי הוא יחיד.

<u>הגדרה:</u> 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 $a = b^{-1}$

<u>טענה:</u> אם לאיבר a במונואיד קיים הופכי מימין b ומשמאל c אזי הם שווים

<u>הוכחה:</u> $c = c*e = c*(a*b) = (c*a)*b = e*b = b$

<u>הגדרה:</u> א)מונואיד שכל אבריו הפיכים נקרא חבורה group.

כל הזכויות שמורות לבנימין לוין ©

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

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

<u>טענה:</u> כל חבורה ציקלית היא בהכרח אבלית

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

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

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 <u>נסמן</u> $W_n = cis\left(\frac{2\pi}{n}\right)$

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

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 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:</u> <u>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.

תת חבורה:

<u>הגדרה:</u> תהא (G,*) חבורה, תת קבוצה $H \subseteq G$ נקראת תת-חבורה ונסמן $H \le G$, אם H היא חבורה, כלומר אם 1) $e \in H$

2)סגירות 3) <u>$\forall a \in H : a^{-1} \in H$</u>

<u>דוגמאות:(1</u> $(Z,+)$: $\forall n \in Z : nZ = \langle n \rangle \le Z$

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

כל הזכויות שמורות לבנימין לוין ©

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

חבורות קונגרואנציה

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

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

למשל $2 = 5mod3 = 8mod3$

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.

בנימין לוין

כל הזכויות שמורות לבנימין לוין ©

הרצאה 2- תכונת הצמצום ומחלקי אפס בחוג

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

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

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

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

נאמר שהוא ניתן לצמצום אם הוא ניתן לצמצום מימין וממשמאל.

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

<u>הוכחה:</u>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 $(Z_6,* \ mod6)$ 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 : $\exists i < \infty, k$
$1 \leq k \leq i : a^k = a^i$

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

(הפיך)
מונואיד כללי   לצמצום ניתן
לצמצום ניתן לא

<u>הגדרה:</u> יהא (R,*) מונואיד בו מוגדרת גם פעולת + (לאו החיבור הרגיל) אזי המבנה (R,*,+) נקרא חוק 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.

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

כל הזכויות שמורות לבנימין לוין ©

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

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

<u>מחלק אפס שמאלי:</u> אם $\exists 0 \neq b \in R : ab = 0$

<u>מחלק אפס:</u> 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.

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

כלומר a ניתן לצמצום משמאל.

<u>מסקנה:</u> 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).

<u>הגדרה:</u> 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: $a^2 = a = ae \to a = e$

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

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

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

<u>משפט:</u> באגודה X סופית יש לפחות אדמ' אחד.

<u>הוכחה:</u> כיוון ש-X סופית קיימת לה $K \leq X$ תת-אגודה מינימלית (כך ש: $\emptyset \neq k_1 \leq k \to k_1 = k$

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.

כל הזכויות שמורות לבנימין לוין ©

נשים לב כי $A \le k$, נראה סגירות:

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

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}. $nZ - \{0\} \le x$ 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 הילוף 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 ©

<u>הגדרה:</u> חילוק עם שארית: לכל $0 \neq b, a \in Z$ 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: <u>אלגוריתם אוקלידס למציאת ממב"ג</u>

<u>יהיו</u> $a, b \in Z$

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 $t \leq r_k$

$$t | \overbrace{(a - bq_1)}^{r_1}$$
$$t | \overbrace{(b - r_1 q_2)}^{r_2}$$
$$\underline{\dots\dots\dots}$$
$$\dots\dots t | r_k \rightarrow t \leq r_k$$

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

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

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

$$(\mathrm{m}, \mathrm{n}) = 1 \Leftrightarrow \exists \mathrm{k}_1, k_2 \in \mathbb{Z} : k_1 m + k_2 n = 1 \Leftrightarrow \exists k_1 \in \mathbb{Z}\; k_1 m = 1 mod\; n$$

הגדרה

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

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

דוגמא

$\mathrm{U}_{10} = (\{1,3,7,9\}, *\; mod 10)$ - צקלית כי $< 3 >= \{1,3,9,7\}$

$\mathrm{U}_8 = \{1,3,5,7\}$ 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:

$$143 * 17 - 90 * 24 = 1$$

ולכן $90^{-1} = -27mod143 = 116mod143$

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

$$3 * 667 = 2001 = 1mod2000$$
$$\Rightarrow 3 * \underbrace{677 * 55}_{x} = 55mod2000$$

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
$$\begin{cases} x = 1mod4 \\ x = 2mod7 \\ x = 3mod15 \end{cases}$$

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 $e_i := s_i n_i$ 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. $x \mapsto 2x$ $\varphi: \mathbb{Z} \to \mathbb{Z}$ לגבי חיבור – מונומורפיזם
2. $x \mapsto x^2$ $\varphi: U_{10} \to < 9 >$ 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 $H \cong G$ נקבל איזומורפיזם של חבורות $Gr(G) \cong Gr(H)$

טענה

אם $(n,m) = 1$ אזי $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ 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?

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

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

טענה

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

כל הזכויות שמורות לבנימין לוין ©

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

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

בנימין לוין

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

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

בכיוון הנגדי

$$a^k = e \Rightarrow a(a) < k$$

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.

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

הוכחה

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

משפט

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

כל הזכויות שמורות לבנימין לוין ©

הוכחה

$\Leftarrow$ הוכחנו באמצעות CRT.

$\Rightarrow$

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong Z_{nm} =< i >\Rightarrow \exists (a,b) \in \mathbb{Z}_n \times \mathbb{Z}_m : o(a,b) = nm$$
$$\Rightarrow (a,b)^{[n,m]} = ([n,m]a,[n,m]b) = (nq_1 a, mg_2 b) = (0,0)$$

$$o(a,b) = nm \leq [n,m] \Rightarrow nm = [n,m] \Leftrightarrow (n,m) = 1$$

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 $f\colon \mathbb{Z} \to G : k \mapsto a^k$

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

לכן f הומו' (משמר פעולה).

כיוון שניתן להגיע לכל חזקה שלמה של a, $Im(f) =< a >= G$
כלומר f אפי' (על). בנוסף אם $m \neq n$ אז בהכרח $a^m \neq a^n$ 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 $f\colon \mathbb{Z}_n \to G : k \mapsto a^k$
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 $0 \leq k \leq n-1$ מתאפשרת בתמונה, כלומר כל G נפרשת, כלומר f על, ומתוך כך f הוא מונו' (כי $|\mathbb{Z}_n| = |G| = n$).

דוגמא

$$\mathbb{Z} \cong < 1+i > \leq \mathbb{C}$$

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

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 $H \le G$ 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 $0 \le r < k$. ע"פ הסגירות נקבל $a^r = a^{t-kq} = a^t(a^k)^{-q} \in H$
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 :

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

דוגמא

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

הוכחה

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

תרגיל נחמד:

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

פתרון

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

לדוגמא $\mathbb{Z}_6 =< 1 >$ 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 $g,h \in G$

1. $gh = hg$

כל הזכויות שמורות לבנימין לוין ©

2. $\big(o(g), o(h)\big) = 1$

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

$m = nk$

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

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.

הערה

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

כל הזכויות שמורות לבנימין לוין ©

הגדרה

הדרגה של חבורה G : rank(G) היא המס' המינימלי של פורשים יחד את כל G.

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, למשל $a^3a^4 = a^7, aa^{-1} = e$

הגדרה

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

⇐עבור $n = p$ ראשוני כלשהו, חבורת אויילר היא $U_p = \{1,2, \dots, p-1\}$.

כיוון שהחבורה אבלית, מכפלת כל האיברים היא $m = (p-1)!$, ומקיימת $m^2 = 1$ $(m^2 \equiv 1(mod\ p))$ ע"י הצבת כל איבר ליד ההופכי שלו הודות לקומוטטיביות.

כל איבר a ההפוך לעצמו: $(a-1)(a+1) = a^2 - 1 = 0$, כיוון שאין מחלקי אפס בU_p, האיברים ההופכיים לעצמם הם רק ± 1 (כי אחד הגורמים צריך להתאפס), מכאן שלכל איבר אחר יש איבר הופכי אחר, לכן במכפלת כל האיברים פעם אחת האיבר היחיד שלא מצטמצם הוא -1 ולכן $m \equiv (-1)(mod\ p)$ ■

⇒ נניח בשלילה כי n אינו ראשוני, אם n=4 קל לבדוק ש: $(4-1)! = 6 \equiv 2(mod 4)$

עבור $n > 4$ כיוון ש-n אינו ראשוני ב$\mathbb{Z}_n^*$ (לגבי כפל) יש בהכרח לפחות איבר אחד a מחלק אפס.
אם $a = \sqrt{n}$ אז $4 < n \Rightarrow 2 < a \Rightarrow 2a < a^2 = n$ ולכן a,2a נמצאים במכפלה $(n-1)!$ ולכן $2a^2$ מאפס אותה (מודולו n).

אחרת $(n \neq \sqrt{n})$ $ab \equiv (0 mod\ n)$ $\exists 1 < a, b < n$ ⇐ ab נמצא במכפלה ומאפס אותו. ■

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 $13 | 116! + 1 \Rightarrow 117 | 116!$ $9 *$.

קוסטים ומשפט לגרנז'

הגדרה

תהא חבורה G ות"ח H, שני איברים $x, y \in G$ יקראו קונגרוארטים 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 בH.

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

כל הזכויות שמורות לבנימין לוין ©

טענה

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

הוכחה

נגדיר את ההעתקה $\varphi: \frac{G}{H} \to H\backslash_G$

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

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

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 לגרנז'

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 $\varphi_a = H \to Ha$

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) $\forall a \in G: o(a) = |<a>| \mid |G|$
3) $\forall a \in G : a^{|G|=o(a)q} = e$

כל הזכויות שמורות לבנימין לוין ©

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 $\left(d, \varphi(n)\right) = 1$ 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 $H \Delta G$ אזי קבוצת המנה $H\backslash_G$ היא חבורה עם פעולת הכפל המוגדרת ע"י $Hx * Hy = Hxy$

אכן, אם $H \lhd G$ 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 $H \leq G$ מתקיים $HxHy = Hxy$

דוגמא

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

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

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

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

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

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

נשים לב כי $a < b >=< b > a$

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

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

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

H ⊲ G 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 $H \le G$ היא $H \lhd \mathrm{G}$

לדוגמא

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

$$3\mathbb{Z} \le \mathbb{Z}$$

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

הגדרה:

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

טענה:

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

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 $K \coloneqq \ker(f)$, 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 $Ker(f) \lhd \mathrm{G}$

טענה

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

א. $1_H = f(1_G) \Rightarrow 1_H \in Im(f)$

ב. $h_1, h_2 \in Im(f) \Rightarrow h_1 = f(g_1), h_2 = f(g_2) \Rightarrow f(g_1 g_2) = h_1 h_2 \Rightarrow h_1 h_2 \in Im(f)$

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

כל הזכויות שמורות לבנימין לוין ©

תוצאה

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

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

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 $v: G \to G/H$ ע"י $v(a) = aH$, אזי v הוא הומורפיזם ומתקיים $\ker(v) = H$.
v נקרא ההומומורפיזם הטבעי.

הוכחה

$$\forall a, b \in G : v(ab) = abH = abHH = aHbH = v(a)v(b)$$
$$\ker(v) = \{a \in G : aH = H\} = H$$

משפט האיזומורפיזם הראשון:

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

דוגמא

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

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 $K \lhd G$:

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

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 בD_3 : $\{id, < b >, D_3\}$

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

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

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

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

$$|kar| \mid_{|G_1|} \quad |Im| \mid_{|G_2|}$$

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

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

$$|Im(\varphi)| \mid_{|G_1|}$$

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

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$A \le G, H \lhd G$ שתי חבורות, אזי מתקיים:

1) $\{ah: a \in A, h \in H\} = AH \le G$
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 $\forall a_1 a_2, h_1, h_2: (a_1h_1) * (h_2^{-1}a_2^{-1}) \in AH$

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

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

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

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 $G \triangleleft N, G \triangleleft H$ 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

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

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

יהיו G חבורה $G \triangleleft H, A \le G$, 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 ©

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 מומורפית של חבורה צקלית היא צקלית, אם נרצה שהתמונה גם על (באשר חבורת השווה צקלית) נצטרך ש $f(\text{יוצר}) = \text{יוצר}$

כיוון שבZ ישנם שני יוצרים, $< \pm 1 >$, נוצרים שני איזומורפיזם אפשריים:

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

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

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 $\ker(f) = \{0\} \Leftrightarrow (a,n) = 1$

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

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

דוגמאות

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

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

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

ולכן הומו'. נבדוק חח"ע:

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

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

כל הזכויות שמורות לבנימין לוין ©

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) $z_{1,2} \in Z(G): z_1z_2g = z_1gz_2 = gz_1z_2 \Rightarrow z_1z_2 \in Z(G)$

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) $c_{1,2} \in C(x): c_1c_2x = xc_1c_2 \Rightarrow c_1c_2 \in C(x)$

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 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

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

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

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.

הוכחה

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

כל הזכויות שמורות לבנימין לוין ©

אלגוריתם לקביעת זוגיות של תמורה

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

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

כל הזכויות שמורות לבנימין לוין ©

דוגמא

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

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

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

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

הגדרות:

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

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

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:

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

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.

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

כל הזכויות שמורות לבנימין לוין ©

טיפוס (מבנה) של תמורה

תהא σ תמורה ב-S_n. נפרק אותה למכפלה של מספרים זרים $\sigma=\left(a_{11}\dots a_{1r_1}\right)\dots,\left(a_{k1}\dots a_k r_k\right)$ כך ש $r_1\ge r_2\ge\dots\ge r_k$. 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

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

דוגמא

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

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

$1\to1\to2\to4$
$2\to3\to3\to2$
$3\to4\to1\to1$
$4\to2\to5\to5$
$5\to5\to4\to3$

הוכחה

נוכיח טענה שקולה:

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

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.

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

דוגמא

הראה כי $V_4\lhd A_4$

פתרון

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

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

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

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

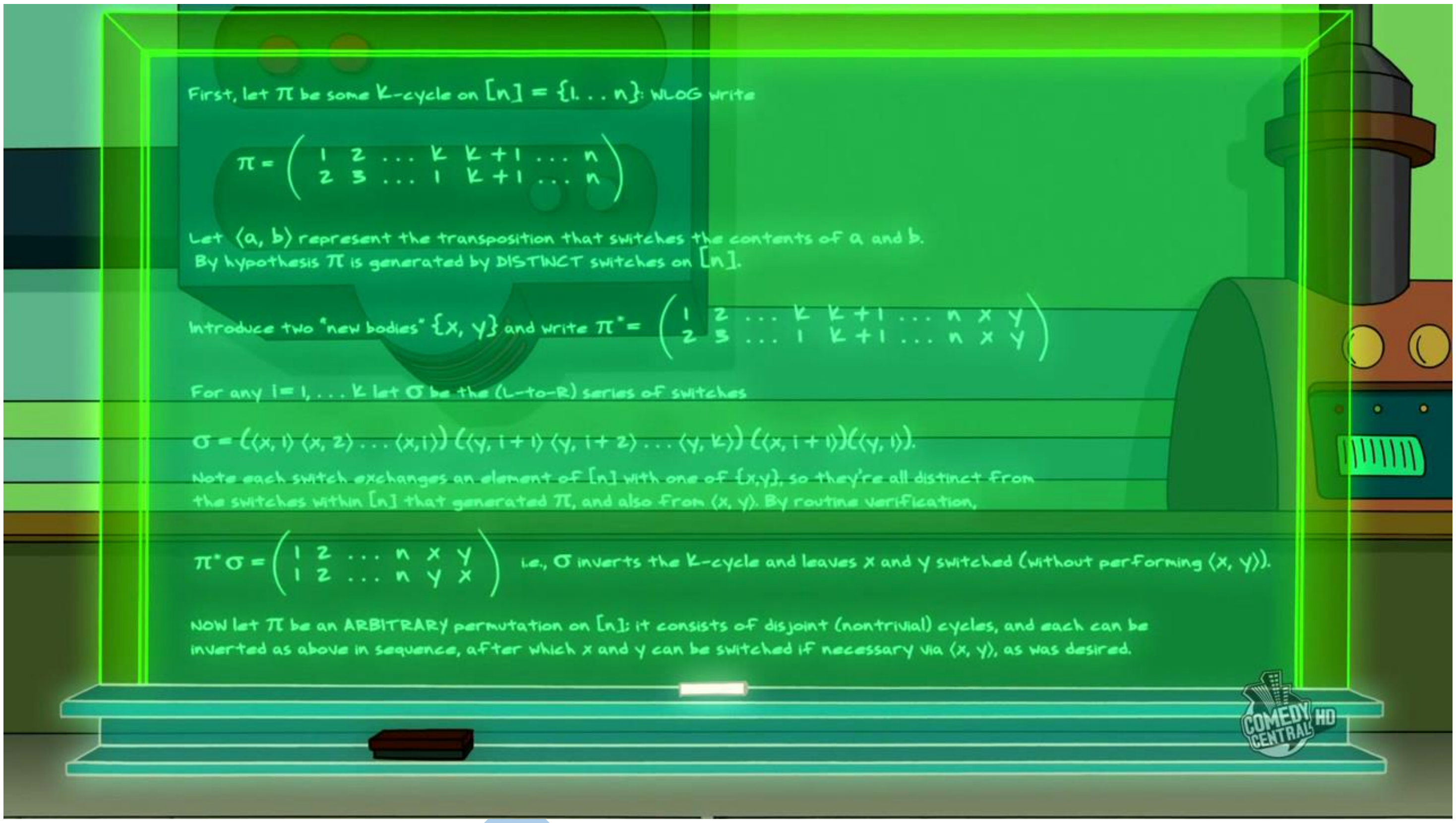
$$\tau\sigma\tau^{-1} = (2\ 3)$$
$$\tau^2\sigma\tau^{-2} = (3\ 4)$$
$$\dots \dots \dots \dots \dots \dots \dots$$
$$\tau^{n-2}\sigma\tau^2 = (n-1\ n)$$

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

כלומר $S_n < \sigma, \tau >$

בנימין לוין

כל הזכויות שמורות לבנימין לוין ©



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 $G \cong \varphi(G) \le S_G$

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: $X,Y\le G$ 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

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

והיא חח"ע ועל שכן:

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

$\boxed{\Rightarrow}$

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

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

אכן, כיוון ש-φ^{-1} איזו', 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

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

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

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 G חבורה 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$y_1 = c_1 x_1 + \dots + c_k x_k$.

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 במשפט)

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

$m_1 x_1 + \dots + m_k x_k = 0$ עם $m_1 x_1 \neq 0$. 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 $y_1 = c_1 x_1 + \dots c_k x_k$

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

כל הזכויות שמורות לבנימין לוין ©

כלומר $o(x_1) \leq m_1 \leq d \leq o(y_1)$ 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

ראינו $G = mG \oplus nG = G_n \oplus G_m = P_2 \oplus P_1$

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..

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

פעולות של חבורות על קבוצות

הגדרה

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

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 ההצמדה, 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

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

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- A_4, S_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 3 2)*
(1 4 2)	*(1 2 4)*
(1 3 4)	*(1 4 3)*
(2 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) $\forall g_1, g_2 \in Stb(X): (g_1 g_2) * x = g_1 * (g_2 * x) = g_1 * x = x \Rightarrow g_1 g_2 \in Stb(x)$

בנימין לוין

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

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

נראה ש-φ חח"ע:

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

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

$$|G| = \sum_{x\ rep} |G * x| = \sum_{x\ rep} \frac{|G|}{|C(x)|} \underset{ש}{=} |Z(G)| + \sum_{\substack{x\ rep \\ \neq Z(G)}} \frac{|G|}{|C(x)|}$$

(ש: במרכז כל איבר הוא מחלקת צמידות של עצמו כלומר באורך1)

תוצאה

תהא G חבורה 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 $ab = ba$. $< a, b > \subset Z(G)$ 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:

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

$\boldsymbol{g\backslash X_G}$	$\boldsymbol{\lvert X_g\rvert}$
$\boldsymbol{id}$	3^9
$\boldsymbol{\sigma,\sigma^3}$	3^3
$\boldsymbol{\sigma^2}$	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 $G=P_1P_2$ אבלית כאשר $(|P_1|,|P_2|)=1$ אזי

$$G=G_{|P_1|}\oplus G_{|P_2|}$$

$$P_1\oplus P_2\le G, |P_1\oplus P_2|=|P_1||P_2|=nm$$

$$G=P_1\oplus P_2$$

משפט סילו (Sylow)

טענה

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

הוכחה

נכתוב $|G|=p^rm$ 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 $\mathrm{H}_i\cong\mathbb{Z}_{p^{r_i}}\le P$ 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:

תהא G חבורה מסדר p^nm כאשר p ראשוני, $n,m\in\mathbb{N}$. אזי קיימת ת"ח p-סילו, הינו ת"ח מסדר p^n.

הוכחה

נראה באינדוקציה על $|G|$.

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

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

צ"ל: נכונה עבור $|G|=p^nm$

ישנם שני ממקרים בלבד:

א) קיימת ת"ח $H\le G$ כך ש: $|H|=p^nm_1$, $m_1<m$. לפי הנחת האינדוקציה יש בתוך H ת"ח p-סילו ב-G.

ב) לא קיימת ת"ח $G\ge$H מסדר p^nm_1, $m_1<m$.
כלומר כל ת"ח היא מסדר $p^{n_1<n}m$

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

מכאן ע"פ נוסחת המחלקה:

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

 כל הזכויות שמורות לבנימין לוין ©

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: $|A| = p^{n-1}$

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

נסמן: $A^* = \nu^{-1}(A) \leq G$. 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 מסדר 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 $Z(G)$ כחבורה אבלית יש איבר a מסדר p , נתייחס ל$< a \geq H \lhd G$ 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 $G \geq A^* = \nu^{-1}(A)$. ונצמצם את ν: $\nu_0: A^* \to A$ ומכאן ע"י איזו' 1.

תוצאה – משפט קושי

תהא G כך ש: $|G| \,|p$ 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 $\mathrm{p^n}$ ולכן יש בה ת"ח מסדר $p^{1\leq k\leq n}$ 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 p-יש ת"ח מסדר p^k לכל $1 \le k \le n$.

<u>**אבל זה לא אומר שיש איבר מסדר p^k**</u> 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 ה-p-סילו שלה.

הוכחה

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

נסיק ע"פ טענה קודמת כי:

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

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 $|\oplus_i P_i| = |G|$ ולכן $G = \oplus_i P_i$

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.

כל הזכויות שמורות לבנימין לוין ©

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?

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

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

הידעתם?

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

הגדרה

תהא G חבורה הפועלת על חבורה X

- נקודת שבת היא איבר $x \in X$ כך 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!).

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

מליצה

אנלוגיה לחיים: אתם לא מכירים אנשים שאף אחד לא יוציא אותם מהבית?

מקרה כללי: מתמטיקה≡חיים.

משפט סילו 2:

תחת התנאים של משפט סילו 1 $((p,m)=0, |G|=p^n m)$:

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:

$$SyL_{lp} \neq \phi$$

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) ולכן בהכרח לפחות $r_x=0$ לפחות x אחד, כלומר קיימת לפחות נקודת שבת אחת, כלומר קיים xP כך שלכל $h \in H$

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

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

ב)

ע"פ בפרט $\mathrm{P}_1 \in SyL_p(G)$ (מסדר p^{n}) קיימת $P_2 \in SyL_p(G)$ כך ש: $P_1 \subseteq xP_2x^{-1}$ עבור x כלשהו.

אבל $|P_1| = p^n = |P_2| = |XP_2x^{-1}|$ ולכן $P_1 = xP_2x^{-1}$.

ההצמדה לא משנה את גודל הקבוצה!.

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

$\mathrm{H} \times G/_P$ 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

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

ב D_3 : $|D_3| = 6 = 2 * 3$

$$n_2 = 3(3 \text{ סילו}),\ \ n_3 = 1$$

$$< a > \lhd D_3$$

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

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$H \leq G$. הנורמילטור של H ב-G הוא:

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

טענה

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

הוכחה

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

כל הזכויות שמורות לבנימין לוין ©

משפט סילו 3

עבור חבורה G נסמן $n_p = \left|Syl_p(G)\right|$

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

ומכאן ע"פ נוסחת המחלקה הכללית:

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

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 $P \leq N_G(Q)$ שכן Q היא נקודת שבת תחת הצמדה של P: $\forall p \in P : pQp^{-1} = Q$ ולכן $P, Q \leq N_G(Q)$.

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>

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

ג) ע"פ לגראנז':

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

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

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

$$30 = 2 * 3 * 5$$

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

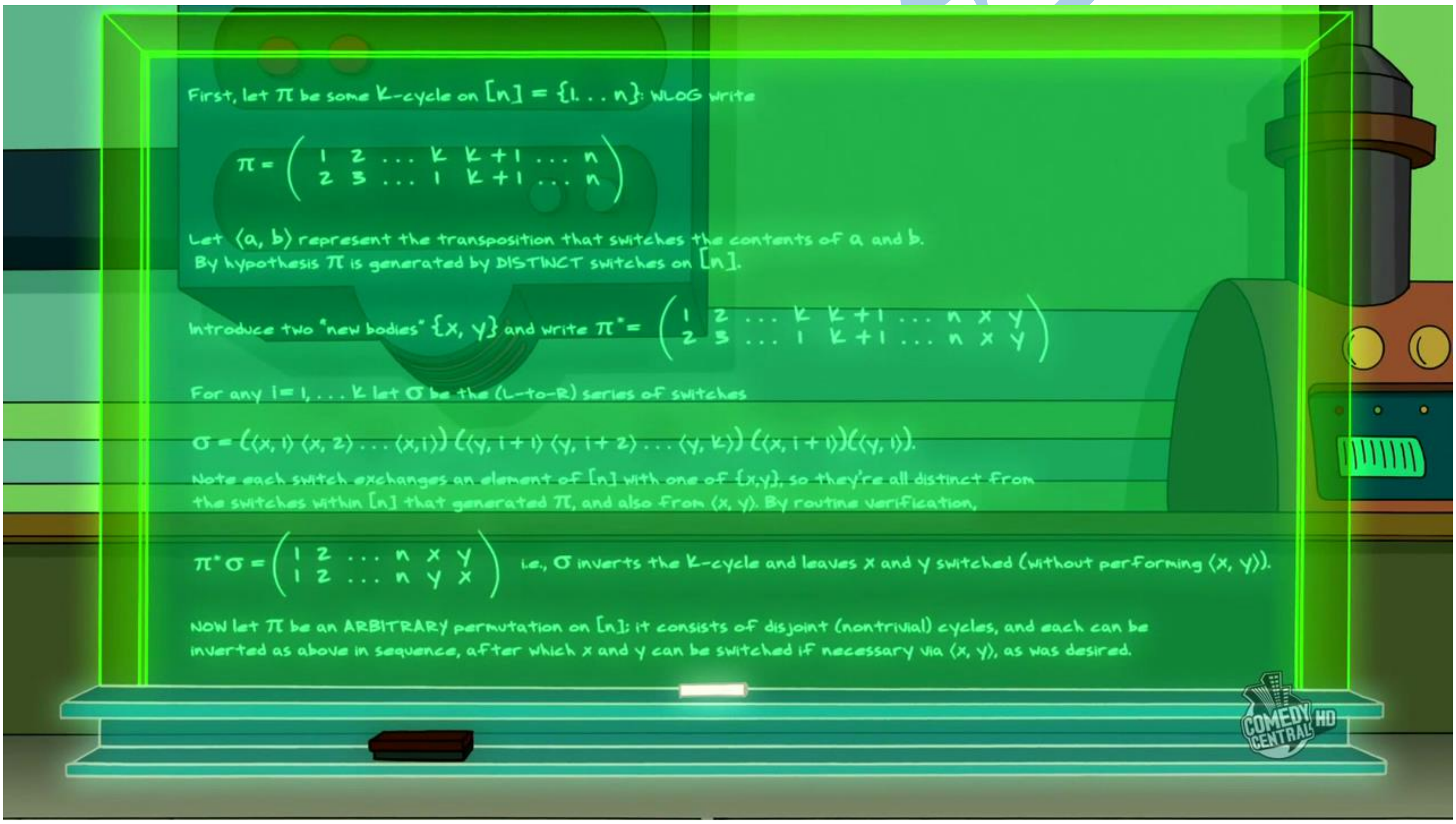
$$n_5 = 1 + 5k|6 = 1,6$$

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.

בנימין לוין

כל הזכויות שמורות לבנימין לוין ©