

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 ש S סופי אם נכפיל את a בעצמו מספיק פעמים נחזור על איבר שכבר היינו בו,

$$\text{כלומר } \exists i < \infty, k : 1 \leq k \leq i : a^k = a^i$$

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

(הפיך)

מונואיד כללי לצמצום ניתן

לצמצום ניתן לא

הגדרה: יהא $(R, *)$ מונואיד בו מוגדרת גם פעולת + (לאו החיבור הרגיל) אזי המבנה $(R, *, +)$ נקרא חוק 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: יהיה $a \in R$ ניתן לצמצום, ונניח בשלילה שהוא מחלק אפס משמאל, אזי
 סתירה $\exists 0 \neq b \in R : ab = 0 = a * 0 \Rightarrow b = 0$

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 $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$

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

משפט: באגודה X סופית יש לפחות אדמ' אחד.

הוכחה: כיוון ש- X סופית קיימת לה $K \leq X$ תת-אגודה מינימלית (כך ש: $\emptyset \neq k_1 \leq k \rightarrow k_1 = k$)

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

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 אדמ' אחד.

אם X היה אינסופי, לא בהכרח היתה תת-אגודה מינימלית, למשל $X = \mathbb{Z} - \{0\}$. $\{0\} \leq n\mathbb{Z}$ 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 $\exists q \in Z : aq = b$

(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 שניהם. 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 ששניהם 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 $a \in Z, b \neq 0$ קיימים באופן יחיד $\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$

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

הוכחה: אלגוריתם אוקלידס למציאת ממב"ג

יהיו $a, b \in \mathbb{Z}$

$$a = bq_1 + r_1 \quad \text{נחשב:}$$

$$b = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3$$

.....

gcd

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

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

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

כעת נותר להראות מקסימליות של r_k כמחלק של a, b

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

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

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

.....

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

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) .

$$\text{דוגמא: } (594, 420) = 6$$

$$594 = 420 * 1 + 174$$

$$420 = 174 * 2 + 72$$

$$174 = 72 * 2 + 30$$

$$72 = 30 * 2 + 12$$

$$30 = 12 * 2 + 6$$

$$12 = 6 * 2$$

החבורה הסמטרית

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

