בס"ד

תרגול מס' 3 במבנים אלגבריים 1

משפט השאריות הסיני

תהא $\{m_1,...,m_k\}$ קבוצת מספרים טבעיים הזרים זה לזה, כלומר כל זוג מספרים בקבוצה הם זרים.

נסמן את מכפלתם ב- m. בהינתן קבוצה כלשהי של שאריות $\{a_i \pmod{m_i} : 1 \le i \le k\}$,

קיימת שארית יחידה $x \pmod{m}$ המהווה פתרון למערכת המשוואות: $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ ..... \\ x \equiv a_k \pmod{m_k} \end{cases}$.

הוכחה:

נבנה בסיס של שאריות $\{e_1,...,e_k\}$ כך ש: $\forall i,j:\ e_i \equiv \delta_{ij} \pmod{m_j}$ (הדלתא של קרוניקר),

כלומר: $\forall i,j:\ e_i \pmod{(m_j)} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}$ ואז: $x = a_1 e_1 + ... + a_k e_k$ יהווה פתרון למערכת המשוואות.

הבנייה של $\{e_1,...,e_k\}$ תיעשה בצורה הבאה:

לכל $1 \le i \le k$ נגדיר: $n_i = m / m_i$. כיוון שכל ה-$\{m_i\}$ זרים אחד לשני, נקבל כי: $(n_i, m_i) = 1$.

מכאן ש: $\exists s_i, r_i \in \mathbb{Z}:\ s_i n_i + r_i m_i = 1$. נגדיר את: $e_i = s_i n_i$ ונקבל: $e_i \equiv 1 \pmod{m_i}$.

כמו כן, לכל $i \neq j$, $m_j \mid n_i$ לכן: $e_i \equiv 0 \pmod{m_j}$ כנדרש.

להוכחת היחידות, נניח כי קיים פתרון אחר y. אזי מתוך מערכת המשוואות נקבל: $\forall i : m_i \mid (x-y)$.

אבל כל ה-$\{m_i\}$ זרים אחד לשני ולכן גם: $m \mid (x-y)$. מכאן שבעצם: $y \equiv x \pmod{m}$. □

דוגמה: מצא פתרון למערכת המשוואות: $\left.\begin{matrix} x\equiv 1(\bmod 4) \\ x\equiv 2(\bmod 7) \\ x\equiv 3(\bmod 15) \end{matrix}\right\}$.

פתרון: ע"י אלגוריתם אוקלידס נקבל עבור הקבוצה $\{4,7,15\}$ את הבסיס: $\begin{matrix} e_1=105, \\ e_2=120, \\ e_3=196 \end{matrix}$ ומכאן: $x=93$.

תת-חבורות

ראינו בהרצאה שכדי להוכיח כי תת-קבוצה H בחבורה G היא תת-חבורה מספיק להראות ש:

1. $H\neq\varnothing$ או לחילופין: $e\in H$,
2. $\forall h_1,h_2\in H:\ h_1\cdot h_2^{-1}\in H$.

<u>דוגמה:</u> $H=\left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}: ad\neq 0\right\},\ G=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}: ad\neq bc\right\}$. נראה: $H\leq G$:

1. $I_2\in H$,
2. $\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}\cdot\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}^{-1}=\frac{1}{ad}\begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix}\cdot\begin{pmatrix} d & -b \\ 0 & a \end{pmatrix}=\begin{pmatrix} \alpha d & -\alpha b+\beta a \\ 0 & \gamma a \end{pmatrix}\in H$.

<u>תרגיל:</u> תהי G חבורה, ו- H,K שתי תתי-חבורות בה. הוכח: $HK=KH\ \Leftrightarrow\ HK\leq G$.

<u>פתרון:</u>

כיוון $(\Leftarrow)$: צ"ל: $HK=\{h\cdot k\mid h\in H,k\in K\}\leq G$. עפ"י קיצור הדרך:

א. $e\in H,K\rightarrow e\cdot e=e\in HK$

ב. צ"ל: $\forall x,y\in HK:\ x\cdot y^{-1}\in HK$. אכן: $x\cdot y^{-1}=(h_1k_1)\cdot(h_2k_2)^{-1}=h_1k_1k_2^{-1}h_2^{-1}=h_1\underbrace{k_3h_2^{-1}}_{\in KH}$

$k_3h_2^{-1}\in KH=HK\ \Rightarrow\ \exists h_3,k_4:\ k_3h_2^{-1}=h_3k_4\ \Rightarrow\ x\cdot y^{-1}=h_1h_3k_4=h_4k_4\in HK$

כיוון $(\Rightarrow)$: נסמן $X^{-1}=\{x^{-1}\mid x\in X\}$ ונקבל:

$H,K,HK\leq G\ \Rightarrow\ HK=(HK)^{-1}=K^{-1}H^{-1}=KH$.

חבורות דיהדרליות

<u>הגדרה</u>: לכל מספר טבעי n, הקבוצה D_n של סיבובים ושיקופים, המעתיקים מצולע משוכלל בן n צלעות על עצמו, היא חבורת **דיהדר**.

אם a הוא סיבוב ב-$\frac{2\pi}{n}$, ו-b הוא שקוף סביב ציר סימטריה כלשהוא של המצולע, אזי:

$$D_n = \left\{ 1, a, a^2, ..., a^{n-1}, b, ba, ba^2, ..., ba^{n-1} \right\} \quad \left(\left| D_n \right| = 2n \right)$$

החבורה נוצרת ע"י שני איברים, וניתן לרשום: $D_n = \left\langle a, b \mid a^n = e,\ b^2 = e,\ ab = ba^{n-1} \right\rangle$

(להראות בדוגמה של $n = 4$, כיצד $ab = ba^3$).

<u>תרגיל</u>: מצא חבורה סופית G ותתי-חבורות H, K כך ש-HK <u>אינה</u> תת-חבורה ב-G.

<u>פתרון</u>:

ראינו לעיל כי: $HK = KH \Leftrightarrow HK \le G$ ולכן נחפש מקרה בו $HK \neq KH$.

דוגמה: ב-$D_3 = \left\{ 1, a, a^2, b, ba, ba^2 \right\}$, $H = \{1, b\}$, $K = \{1, ba\}$

$HK = \{1,\ b,\ a,\ ba\} \neq KH = \left\{ 1,\ b,\ ba,\ bab = a^2 \right\}$ וברור שאף אחת מהן אינה תת-חבורה שכן לא מתקיימת סגירות: $a^2 \notin HK$ ו- $a^2 \cdot a^2 = a \notin KH$.