<u>אלגברה מופשטת 1 – הרצאה 2</u>

(עדכון 25.07.13)

נחדד כמה נושאים מהרצאה קודמת.

<u>דוגמה</u>: לפתור משוואה $6x \equiv 7mod35$ (כאשר x שלם).

פתרון: ניתן לרשום $[6]x = [7]$ במונואיד $(\mathbb{Z}_{35},\cdot)$. למדנו בשיעור קודם כי עבור ax=b (בכל מונואיד$(X,\cdot)$ ולכל הפיך $a \in Gr(X)$) קיים $x = a^{-1}b$. במקרה שלנו, $[6]_{35}^{-1} = [6]_{35}$.

לכן, קיבלנו שהפתרון למשוואה הוא: $x = [6]^{-1}[7] = [6][7] = [42]_{35} = [7] = \{35k + 7|k \in Z\}$.

מה קורה כשהמספרים גדולים? ננסה לפתור את $14x \equiv 10mod(29)$. מצאנו כי $[14]_{29}^{-1} = [-2] = [27]$. ומכאן ניתן לפתור בקלות.

תרגיל שיהיה יותר קשר לנחש את ההופכי: שוב, לפתור בשלמים את $365x \equiv 2mod1876$. בגלל שקשה לנו לנחש, היה עלינו לפתח שיטה. נשתמש בהמשך בשיטה המבוססת על אחד מהטריקים מתורת המספרים.

נסתכל על המשוואה שלנו באופן כללי: $ax = b\ mod(n)$. ואם (a,n)=1 נוכיח בהמשך את משפט אוילר שאומר סימון: $Gr(\mathbb{Z}_n,\cdot) = \{[a]|(a,n) = 1\} = U_n$ וזה ייקרא חבורת אוילר. ז״א, חבורת הפיכים של מונואיד Z_n. השאלה כעת הומרה למציאת $[a]_n^{-1}$ כאשר (a,n)=1.

משפט: שמבוסס על שיטת אוקלידס: (a,n)=1 אוי״א קיימים u,v מספרים שלמים כך שצירוף ״לינארי״ של ua+vn=1.

הוכחה: הכיוון שמאלה הוא טריוויאלי. על הכיוון השני, ימינה, נדבר בהמשך.

משפט: נניח ש(a,n)=1 אז [a] הפיך ב$\mathrm{Z_n}$ ו$[a]^{-1} = [u]$ כאשר ua+vn=1.

הוכחה: אנחנו מתבסס על ההנחה ש$vn = 0$. וקיבלנו ש$ua \equiv 1$. לכן $[a]^{-1} = [u]$.

סיכום: לגבי Z_n עבור n טבעי קיבלנו $\mathrm{Z}_n = \left\{\overbrace{[0]}^{nZ}, \overbrace{[1]}^{nZ+1}, \overbrace{[2]}^{nZ+2}, \dots, \overbrace{[n-1]}^{nZ+n-1}\right\}$. כדי שמחלקות שקילות יהיו שוות, $[k_1] = [k_2]$, צריך שההפרש יהיה אפס מודולו n. ז״א $n|k_1 - k_2$.

נוכיח כי אין תלות בנציגים בחיבור וכפל של מחלקות שקילות: $[x]\oplus[y] = [x + y], [x]\cdot[y] = [x\cdot y]$. כל זאת בגלל $x_1 \equiv y_1 modn, x_2 \equiv y_2 modn \to x_1 + x_2 \equiv (y_1 + y_2)modn, x_1x_2 \equiv y_1y_2 modn$

משפט: $(Z_n, \oplus\ )$ חבורה ציקלית.

<u>משפט</u>: כל חבורה ציקלית היא אבלית.

הוכחה: $G =< a >= \{a^k|k \in Z\}$ לכל x,y ששייכים לG מתקיים $xy = a^{k_1}a^{k_2} = a^{k_1+k_2} = a^{k_2}a^{k_1} = yx$ ולכן תמיד xy=yx ומכאן שמדובר בחבורה אבלית. מ.ש.ל. ■.

הערה: עוד נוסחה לחזקות $a^{k_1}a^{k_2} = a^{k_1+k_2}$: $(X,\cdot)$ באגודה $\forall k_1, k_2 \in N$.

בנוסף: $k_1a + k_2a = (k_1 + k_2)a$: בכל אגודה חיבורית $\forall k_1, k_2 \in Z$.

דוגמה: של חבורה אבלית ושאינה צקלית. ... $(R^n,+), (Q^n,+)$.

דוגמה טיפה יותר מיוחדת לחבורה שהיא אבלית ושאינה ציקלית היא למשל $Z_2^2 =$ $\{([0],[0]),([0],[1]),([1],[0]),([1],[1])\}$.

נגדיר את הפעולה שלנו (שהיא מין הרחבה של החיבור) בטבלה :

+	([0], [0])	([0], [1])	([1], [0])	([1], [1])
([0], [0])	([0], [0])	([0], [1])	([1], [0])	([1], [1])
([0], [1])	([0], [1])	([0], [0])	([1], [1])	([1], [0])
([1], [0])	([1], [0])	([1], [1])	([0], [0])	([0], [1])
([1], [1])	([1], [1])	([1], [0])	([0], [1])	([0], [0])

אז היא אינה ציקלית, בוודאות, ביחס לפעולה זו, אבל היא אבלית באופן וודאי.

יותר מזה, נקבל משפט :

משפט : לכל G_1, G_2 חבורות אבליות גם $G_1 x G_2$ אבלית (לגבי הפעולה הטבעית).

משפט : $(Z_n,\cdot)$ מונואיד קומוטטיבי.

הסבר : אסוציאטיביות נובעת מהאסוציאטיביות של כפל ב*Z*. נייטרלי הוא $[1]$.

משפט : $(Z_n, \oplus, \cdot)$ חוג קומוטטיבי.

הגדרה : מבנה $(X, +\cdot)$ עם 2 פעולות ייקרא חוג (*Ring*) אם מתקיים :

1. *(X,+)* חבורה אבלית
2. $(X,\cdot)$ מונואיד
3. דיסטריבוטיביות (וזה הקשר שבין 1 ו2!)

במשפט הקודם שימו לב ש$(Z, +, \cdot)$ חוג. ומכאן נובע בקלות ש$(Z_n, \oplus, \cdot)$ חוג.

הגדרה : חוג קומוטטיבי $(X, +, \cdot)$ שבו כל איבר $x \in X^* := X\backslash\{0\}$ הפיך וגם $|X| \geq 2$ נקרא שדה (*Field*).

דוגמה : *Q,R,C,* $\mathbb{Z}_2$.

משפט : $(Z_n, \oplus, \cdot)$ שדה או״א *n=prime* (ראשוני)

הוכחה : כיוון אחד , ימינה, הוא פשוט. הכיוון השני פחות טריוויאלי ונראה בהמשך.

משפט : לכל *n* טבעי $Z \overset{f_n}{\to} Z_n$ נגדיר $x \to [x]_n$. מתקיים כי $f_n(x+y) = f_n(x) \oplus f_n(y)$ וגם $f_n(xy) = f_n(x)f_n(y)$. ז״א אפימורפיזם של חבורות.

דוגמה : $f_{10}: Z \to Z_{10}$. במקרה שלנו, נחפש את הספרה האחרונה (ספרת היחידות) כי כל דבר אחר ניתן לחלוקה בעשר באופן שלם. נניח כעת שמדובר ב$x = 1959^{1999}$. נמצא את ערכו לאחר הפעלת הפונקציה, לכן : $f_n(x) =$ $f_{10}(1959^{1999}) = f_{10}(1959)^{1999} = 9^{1999} = f_{10}(-1)^{1999} = -1mod10 = 9$.

למצוא בבית את שתי הספרות האחרונות של $x = 1959^{1999}$. רמז : להשתמש בf_{100}.

תזכורת : $(X^X, \circ)$ מונואיד עם נייטרלי *id*. מספר האיברים (או העוצמה) של המונואיד הוא $|X^X| = |X|^{|X|}$. אם *|x|=n* אז $|X^X| = n^n$.

דוגמה (1) : כמה מבנים אלגברים בינאריים קיימים מעל קבוצה *X* בת *n* איברים?

תשובה : מבנה אלגברי הוא $|\{X \times X \to X\}| = \left|X^{X^2}\right| = n^{n^2}$

דוגמה (2) : כמה מבנים קומוטטיביים קיימים מעל קבוצה *X* בת *n* איברים?

תשובה: להשלים בבית. רמז: בטבלה של הפעולה, צריכה להיות סימטריות לגבי האלכסון.

דוגמה (3): $\left(\mathrm{N}^{\mathrm{N}},\circ\right)$ מונואיד. יש איברים שלא הפיכים אבל הפיכים רק מצד אחד. ניקח כדוגמה את הפונקציה *f(n)=n+1* ונגדיר $g_t(n)=\begin{Bmatrix} n-1 & ,n>1 \\ t & ,n=1\end{Bmatrix}$.

$$g_{t^{\circ}f=id} \qquad f^{\circ}g_t{\neq}id$$

בעצם לא קיים הופכי, כי יש אינסוף אפשרויות לצד השני.

<u>תזכורת</u>: $S_x \coloneqq Gr(X^X,\circ)$ (*Symmetric Group*).

בהמשך נוכיח שכל חבורה סופית *G* עם *n* איברים איזומורפית לתת חבורה של $S_n = S_{\{1,2,\dots,n\}}$ "חבורת התמורות".

n=1: $S_1=\left\{\begin{pmatrix}1\\1\end{pmatrix}=e\right\}$ חבורה טריויאלית עם איבר 1.

n=2: $S_2=\left\{\begin{pmatrix}1,2\\1,2\end{pmatrix}=e,\begin{pmatrix}1,2\\2,1\end{pmatrix}=\sigma\right\}$ עם 2 איברים.

<u>הגדרה</u>: תהי $(G,\cdot)$ חבורה ו-$a\in G$. נגדיר $\mathrm{l_a}:\mathrm{G}\to G\ ,x\to ax\quad ,\quad r_a:G\to G\ ,x\to xa$.

משפט: לכל *a* שייך ל-*G* ולכל חבורה *G* l_a,r_a חח"ע ועל.

הוכחה: במקרה של $\mathrm{l_a}$. לכל *b* שייך ל-*G* יש פתרון למשוואה *ax=b*. ומכאן נובע ש-$\mathrm{l_a}(x)=b$ ז"א הוכחנו ש-$\mathrm{l_a}$ היא על.

קל לבדוק שהיא גם חח"ע. נניח ש-$\mathrm{x_1}\neq x_2$. לכן $ax_1\neq ax_2\to l_a(x_1)\neq l_a(x_2)$ ומ.ש.ל. ■. עבור r_a ההוכחה דומה.

תוצאה: בשורה של a שמתאימה לa בטבלת Cayley מקבלים איברים $\{ax\}_{x\in G}$. לכן נקבל אותם איברים (אולי בסדר אחר פשוט). אותה תוצאה לגבי הטור שמתאים לa.

<u>תרגיל</u>: הוכח שכל חבורה מ2/3 איברים היא ציקלית. נוכיח זאת בתרגול

נביט בתמורות שוב. *n=3*. $S_3=\left\{\begin{pmatrix}1,2,3\\1,2,3\end{pmatrix}=e\ ,\begin{pmatrix}1,2,3\\2,1,3\end{pmatrix}=\sigma,\begin{pmatrix}1,2,3\\2,3,1\end{pmatrix}=a\ ,a^2\ ,\sigma\circ a,\sigma\circ a^2\right\}$ אבל היא לא אבלית כי $a\circ\sigma\neq\sigma\circ a$.

הערה: בהמשך נלמד חבורת סימטריות של $\mathrm{D_3}$ של משולש שווה צלעות וגם שם יש 6 איברים. בעצם $D_3\cong S_3$.

הערה: נוכיח שחבורה ציקלית אינסופית $\simeq(Z,+)$. וכל חבורה ציקלית סופית עם *n* איברים $\simeq(Z_n,\oplus)\simeq(\Omega_n,\cdot)$.

<u>הגדרה</u>: נניח $(\mathrm{G},\cdot)$ חבורה ו-*a* שייך ל-*G*. $O(a)=Ord(a)=|a|\coloneqq\begin{Bmatrix}\min\{k\in N|\ a^k=e\} \\ \infty\ ;\text{אם אין } k \text{ כזה}\end{Bmatrix}$.

דוגמה: $O(7)=\infty$ ב-$(R^*,\cdot)$

$O(cis30^\circ)=12$ ב-$(C^*,\cdot)$.