דביר חדד

<u>אלגברה מופשטת 1 – הרצאה 1</u>

אין ציוני תרגילים. יש חובת הגשה ובוחן אמצע. הקורס ינוהל דרך math-wiki.com ולשם יועלו התרגילי בית וסיכומים לסוגיהם. המטרה היא לא רק ללמוד את הקורס, אלא גם ללמוד דברים רלוונטיים אחרים. 90% מהקורס הוא תורת החבורות (English: Group Theory), ו10% זה נושאים שונים שקשורים לחבורות למחצה (English: Semigroups) וכו'.

המבחן הוא על כל החומר, אבל רמת התרגילים אינם קשים (לא בהתחייבות כמובן! ☺). 80% מהתרגילים יהיו מוכרים- תרגילים שנלקחו מההרצאות ומהתרגילי בית וכיתה. חשוב מאוד להכיר את ההרצאות.

נתחיל מההגדרות הראשוניות שקשורות למבנים הבסיסיים:

<u>הגדרה</u>: פעולה בינארית מעל קבוצה X שאינה הקבוצה הריקה היא פונקציה. ז"א $X \times X \overset{w}{\to} X$ או $(x,y) \mapsto w(x,y)$.
סימנו מוכרים אחרים לw הם $x\cdot y$, $x*y$, xy , $x+y$. אז הזוג (X,w) נקרה מבנה אלגברי (או מערכת אלגברית) (English: Algebraic Structure).

דוגמאות: ... $(\mathbb{N},+),(\mathbb{Z},+),(\mathbb{R},\cdot)$ כל אלה הם מבחנים אלגבריים. מה לא? לדוגמה; $(\mathbb{N},-)$ כי הוא לא מוגדר , אין סגירות.

<u>אקסיומות</u>:

1. אסוציאטיביות (חוק הקיבוץ הכללי) - $\forall x,y,z\in X:\ (\boldsymbol{x}\cdot\boldsymbol{y})\cdot z = x\cdot(y\cdot z)$.
ומכאן , אסוציאטיביות מוכללת- עבור כל n טבעי החל מ3 אין משמעות לסוגריים (כאשר מדובר באותה פעולה. אם מדובר בפעולה אחרת בוודאי ובוודאי שיש משמעות לסדר של הסוגריים). ז"א שעבור a,b,c,d מתקיים $(ab)(cd)=a(bc)d=a\big(b(cd)\big)$.
2. קומוטטיביות- $\forall x,y\in X: x\cdot y = y\cdot x$.

<u>הגדרה</u>: מבנה אלגברי $(X,\cdot)$ נקרא אגודה (או חבורה למחצה (*English: Semigroup*)) אם הפעולה היא אסוציאטיבית.

3. איבר ניטרלי משמאל- נניח $(X,\cdot)$ מבנה. אומרים ש$a\in X$ איבר נייטרלי משמאל (או "יחידה משמאלי") אם $\forall x\in X: ax=x$.
4. איבר נייטרלי מימין- באופן דומה למשמאל, $\forall x\in X: xa=x$.

טענה: אם קיימים נייטרלי משמאל e_1 ומימין e_2 אזי $e_1=e_2$.

הוכחה: נסתכל כל המכפלה של שתיהם פעם מימין ופעם משמאל (המכפלה מוגדרת כי זהו מבנה): $e_1e_2 = \begin{matrix}\nearrow e_1\\ \searrow e_2\end{matrix}$ ולכן $e_1=e_2$.

תרגיל: $X := \left\{\begin{pmatrix} x & y\\ 0 & 0\end{pmatrix} \mid x,y\in R\right\}$. מבנה לגבי כפל מטריצות. צריך להוכיח שיש אינסוף נייטרלים משמאל. ולכן אין נייטרלים מימין (חשוב לשים לב לטענה הקודמת!)

<u>הגדרה</u>: חזקה (וכפולה). $a^n=\underbrace{a\cdot a\cdots a}_{n}$. לכל $a\in X$ ולכל n טבעי כאשר $(X,\cdot)$ אגודה. והגדרה זו מוגדרת היטב בגלל אסוציאטיביות מוכללת.

דוגמה נגדית להגדרה (א), בהנחה ואין אסוציאטיביות. נביט ב$(\mathbb{Z},-)$ שם $(x-x)-x\neq x-(x-x)$ ולכן אין זה מתקיים. במקרה שלנו החזקה היא עבור הפעולה של החיסור. הנקודה "" של האגודה שלנו היא -.

דוגמה נגדית נוספת (ב): נגדיר $(\mathbb{N},*)$ $a*b=a^b$ ואז $27^3=(3*3)*3\neq 3*(3*3)=3^{27}$.

$\cdot$	a	b
a	b	b
b	a	a

דוגמה (ג): נגדיר מבנה מעל קבוצה בת 2 איברים. $X = \{a, b\}$. נרשום את "לוח הכפל" של אותה פעולה משמאל. גם כן ניתן לראות כי $b = \underbrace{a \cdot \overbrace{(a \cdot a)}^{b}}_{ab} \neq \underbrace{\overbrace{(a \cdot a)}^{b} \cdot a}_{ba} = a$.

<u>תכונות חשובות של החזקה (באגודה):</u>

ב$(X,\cdot)$ מתקיים $(x^n)^m = x^{mn}$ ובאופן אנלוגי לחזקה וכפל נקבל את הכפולה לחיבור. ז"א $na \coloneqq \underbrace{a + a + \cdots + a}_{n}$ וב$(X,+)$ מתקיים $m(nx) = (mn)x$.

<u>הגדרה</u>: איבר נקרא נייטרלי או יחידה אם הוא נייטרלי משמאל וגם מימין. ז"א (נסמן e) $\forall x \in X:\ ex = xe = x$ (ב$(x,\cdot)$). וב$(x,+)$ 0 תופס את מקומו של 1, הם אנלוגיים. אותו יצור רק מתורגם. וקיבלנו 0+x=x+0=x (הסימון בד"כ הוא אכן 0).

טענה: אם קיים נייטרלי, אז הוא יחיד.

הסבר: נובע מהטענה הקודמת.

<u>הגדרה</u>: אגודה עם נייטרלי נקרא גם מונויד (English: Monoid) או יחידון ☺.

<u>הגדרה</u>: נניח $(x,\cdot)$ מונויד עם e נייטרלי.

- איבר a$\in X$ נקרא הפיך משמאל אם קיים $b \in X$ כך ש$b \cdot a = e$.
- במצב זה ניתן גם לומר שb הפיך מימין.
- a נקרא הפיך אם הוא הפיך משמאל וגם מימין.

טענה: נניח a הפיך מימין. $\exists b': a \cdot b' = e$ וגם הפיך משמאל $\exists b'': b'' \cdot a = e$ אזי b''=b'.

הוכחה: $ab' = e \rightarrow b''(ab') = b''e \rightarrow (b''a)b' = b'' \rightarrow eb' = b'' \rightarrow b' = b''$ ■ מ.ש.ל.

מסקנה: אם a הפיך משמאל וימין, אז הפכי מימין שווה להפכי משמאל. נקרא לאיבר זה האיבר ההפכי.

<u>הגדרה</u>: חבורה (Group).

מבנה $(X,\cdot)$ נקרא חבורה אם הוא מונויד שכל האיברים הפיכים. הגדרה זו שקולה לתנאים הבאים:

א. אסוציאטיביות
ב. קיום איבר נייטרלי
ג. קיום איבר הופכי. $\forall x \in X\ \exists y: xy = e$ נסמן $y \coloneqq x^{-1}$. יש יחידות להפיכות ולכן הוא מוגדר באופן חד משמעי.

<u>הגדרה</u>: אם חבורה היא קומוטטיבית אומרים שהיא חבורה אבלית (על שם Abel).

<u>הגדרה</u>: נניח $(X,\cdot)$ $(Y,*)$ חבורות. פונקציה $f: X \rightarrow Y$.

הומומורפיזם $\forall a, b \in X: f(ab) = f(a) * f(b)$.

אפימורפיזם $Im(f) = Y$, $f(x) = Y$

מונומופריזם זה הומומורפיזם חח"ע.

איזומורפיזם = הומומורפיזים (חח"ע ועל). אם קיים איזו' אז מסמנים $(x,\cdot) \cong (Y,*)$ יש להן אותן תכונות אלגבריות.

<u>לבדוק</u>:

1. הרכבה של הומומורפיזם (מונו, אפי, איזו) גם הומ(...) בהתאמה
2. איזומורפיזם מקיים רפלקסיביות סימטריות וטרנזיטיביות.

<u>תכונות של הפיכים במונויד</u>:

נניח $(X,\cdot)$ מונויד עם נייטרלי e. נסמן: $Gr(X,\cdot):=\{$הפיכים של X$\}\subseteq X$.

1. $e\in Gr(X,\cdot)$ וגם $e^{-1}=e$ ולכן e הפיך.
2. אם $a\in Gr(X,\cdot)$ אזי $a^{-1}\in Gr(X,\cdot)$. ההסבר הוא תכונת הסימטריות שהמונויד מקיים.
מ1,2 נובע כי $(a^{-1})^{-1}=a$
3. אם $a,b\in Gr(X,\cdot)$ אזי $ab\in Gr(X,\cdot)$. ומתקיים $(ab)^{-1}=b^{-1}a^{-1}$. בדיקה: $(ab)(b^{-1}a^{-1})=$ $a(bb^{-1})a^{-1}=a(ea^{-1})=aa^{-1}=e$.

כתוצאה מ1,2,3 נקבל:

משפט: לכל מונויד X הקבוצה Gr(X) יחד עם פעולת הצמצום מגדיר חבורה שנקראת חבורת הפיכים של מונויד X.

דוגמה (1): $Mat_{nxn}(R)=\{$מטריצות ריבועיות ממשיות$\}$ לגבי הכפל מונויד.

מתקבל $Gr\big(Mat_{nxn}(R)\big)=\{$מטריצות הפיכות$\}=\{A|\det(A)\neq 0\}$.

דוגמה (2): $(P(X),\cup)$ מונויד. כאשר $P(X)=\{A|A\subseteq X\}$ (קבוצת החזקה). סגירות, אסוציאטיביות ונייטרלי מתקיים ע"פ ההגדרה. האיבר הנייטרלי לפי הפעולה (איחוד) הוא הקבוצה הריקה, שגם כן שייך לP(X). כעת, מהו Gr(x) במקרה זה? יש לנו איבר נייטרלי אחד ויחיד, ולכן $Gr(P(X),\cup)=\{\phi\}$.

דוגמה (3): $X=(N\cup\{0\},+)$ ולכן Gr(x)={0}.

הערה: אם (X,+) מבנה נתון, אזי במקום הפיך אומרים נגדי ומסמנים בa- ולא בa^{-1}.

דוגמה (4): $X=(Mat_{nxn}(R),+)$ (חבורה אבלית) ואז Gr(X)=X.

באופן כללי, Gr(X)=X ⟺ X חבורה.

למדנו את התכונות הבאות:

א. $e^{-1}=e$
ב. $(a^{-1})^{-1}=a$
ג. $(ab)^{-1}=b^{-1}a^{-1}$ בהנחה וקיימים הופכיים לa,b.
ד. לכל a הפיך במונויד $(X,\cdot)$ מוגדרת $a^k=\overbrace{a\cdot a\cdots a}^{k}$ לכל $k\in\mathbb{Z}$. וגם $a^0=e$.
אם $-n=k<0$ (n טבעי) אז $a^k=(a^{-1})^{-k}=(a^{-1})^n$.

משפט: ניתן לצמצם בהפיך.

אם a הפיך במונויד $(X,\cdot)$ אז $ax=ay\to x=y$ וגם $xa=ya\to x=y$.

הוכחה: $ax=ay\to a^{-1}(ax)=a^{-1}(ay)\to(a^{-1}a)x=(a^{-1}a)y\to ex=ey\to x=y$■.

משפט: בכל מונויד X ולכל הפיך $a\in X$ המשוואה האלמנטרית (ax=b) פתירה עם פתרון יחיד כאשר $x=a^{-1}b$. ובאופן דומה $xa=b$ בעל פתרון שהוא $x=a^{-1}b$.

הוכחה: $ax=b\to a^{-1}(ax)=a^{-1}b\to(a^{-1}a)x=a^{-1}b\to ex=a^{-1}b\to x=a^{-1}b$■

הגדרה: תת חבורה. נניח $(X,\cdot)$ חבורה וY מוכל בX. אומרים Y תת חבורה של X ונסמן $Y \leq X$ אם פעולת הצמצום מעל Y מגדיר חבורה.

אפשרויות לבדיקה:

א. Y לא ריקה. בד״כ בודקים שהאיבר הנייטרלי של X שייך לY.
ב. סגירות. $y_1, y_2 \in Y \to y_1 \cdot y_2 \in Y$
ג. סגירות לגבי הפכיות. ז״א שאם $y_1 \in Y \to y_1^{-1} \in Y$.

דוגמה נגדית: נניח $X = (\mathbb{Z}, +)$ חבורה. ו$Y := \mathbb{N} \cup \{0\}$. א,ב, מתקיימים, אבל ג לא.

אפשרות אחרת לבדיקה היא:

א. Y לא ריקה
ב. $y_1, y_2 \in Y \to y_1 \cdot y_2^{-1} \in Y$. לבדוק בבית איך שתי האפשרויות להגדרת תת חבורה שקולות.

דוגמה: ניקח $(\mathbb{Q},\cdot) \leq (\mathbb{R}^*,\cdot) \leq (\mathbb{C}^*,\cdot) = (\mathbb{C}\backslash\{0\},\cdot)$ חבורות אבליות.

באופן כללי, לכל שדה $(F,+,\cdot)$ ה$(F^*,\cdot)$ היא חבורה אבלית.

דוגמה: $\Omega_\infty := \{z \in C \mid \exists n \in Z : z^n = 1\} = \{\text{שורשי יחידה}\}$. נבדוק ש$\Omega_\infty \leq \left(\mathbb{C}^*,\cdot\right)$. נעשה זאת ע״פ המקוצרת.
התנאי הראשון מתקיים כי 1 שייך לΩ_∞. עבור התנאי השני ניקח $z_1, z_2 \in \Omega_\infty$ וצריך להוכיח כי $z_1 \cdot z_2^{-1} \in \Omega_\infty$. קיימים $n_1, n_2 \in Z$ס כך ש$z_1^{n_1} = z_2^{n_2} = 1$ ואז $(z_1 z_2^{-1})^{n_1 n_2} = \left(z_1^{n_1}\right)^{n_2}\left(z_2^{n_2}\right)^{-n_1} = 1$.

להוכיח בבית כי $\Omega_\infty \geq \Omega_n = \{\text{שורשי יחידה מסדר } n\}$ לכל n טבעי גם כן תת חבורה.

הגדרה: חבורה $(X,\cdot)$ נקראת ציקלית אם קיים איבר $a \in X$ כך ש$x =< a >:= \{a^k \mid k \in Z\}$ בעצם החזקות של a. A נקרא היוצא של X.

דוגמה (1): $\Omega_n =< w >$ כאשר $w := cis\frac{2\pi}{n}$. (יש עוד יוצרים למשועממים שבינינו...אופק?)

דוגמה (2): $(\mathbb{Z},+)$ כאשר $\{k1 \mid k \in \mathbb{Z}\} \geq 1 >= \mathbb{Z}$ (כפולות).

דוגמה (3) חשובה: X לא ריקה. נגדיר $\{f: X \to X\}_{\text{פונקציות}} =: Map(X,X) = X^X$. $\left(X^X, \circ_{\text{הרכבה}}\right)$ מונויד עם נייטרל id_X שהוא פונקציית הזהות. בעצם מדובר בהגדרת הרכבות של פונקציות.

- $(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$
- $e = id_x$

ואז נסמן $\{\text{פונקציות חחע ועל } f: X \to X\} = \{\text{הפיכים ב} x^x\} = S_X := Gr(X^x)$. $(S_x, \circ)$ נקראת חבורה סימטרית.

תרגיל: לבנות טבלה של S_3.

דוגמה גם חשובה מאוד: שאריות מודולו n.

הגדרה: מעל קבוצת השלמים מגדירים את יחס שקילות $a \equiv b \ mod(n) \overset{defined}{\Leftrightarrow} n|(a-b)$ ז״א שקיים מספר שלם q כך שab=nq. שקול ל: יש אותה שארית לa,b מודולו n.

מגדירים פעולות מעל $Z_n := \{[0],[1],\dots,[n-1]\}$ כך שכפל הוא $[a]\cdot[b] := [a \cdot b]$ וחיבור $[a] \oplus [b] := [a+b]$.
צריך לבדוק שההגדרה לא תלויה בנציגים. ז״א, לבחור $a_1 \equiv a_2 modn, b_1 \equiv b_2 modn$

ולהראות שנגרר $a_1b_1 \equiv a_2b_2 \ and \ a_1+b_1 \equiv a_2+b_2$.

משפט 1 : $(\mathbb{Z}_n, \oplus)$ חבורה ציקלית ולכן קומוטטיבית יוצר למשל [1] (יש עוד..)

משפט 2 : $(\mathbb{Z}_n, \cdot)$ מונויד קומוטטיבי.

לפתור בבית : $6x \equiv 7mod35$