מבנים אלגבריים – 83-218

מידע מקדים

מרצה

דר' קלר נתן

משרד: בניין 216 חדר 223

דואר אלקטרוני: nkeller@math.biu.ac.il
nathan.keller27@gmail.com

פקס: 03-7384057

מתרגלים

מר אחיה בר-און

שעות קבלה: יום רביעי, 18:00-19:00 בתיאום מראש.

דואר אלקטרוני: abo1000@gmail.com
Achiyabaron@gmail.com

חלוקת ציון

80% - מבחן מסכם.
20% - בחנים.

מבחן

בחירה של 4 שאלות 5 שאלות.
כל שאלה 2 סעיפים.
סעיף קל עם 10 נקודות.
סעיף קשה עם 15 נקודות.

בחנים

3 בחנים של 2 שעות, בוחרים 2 בחנים מתוך 3 עבור הציון.
בחירה של 3 מתוך 4 שאלות, 2 מהשאלות יהיו מתוך שיעורי בית.
07/12/2016 בין השעות 16:00-18:00 – תרגילי בית 0 עד 3 כולל.
04/01/2017 בין השעות 16:00-18:00 – תרגיל בית 4 עד 6 כולל.
25/01/2017 בין השעות 16:00-18:00 – תרגיל בית 6 עד 8 כולל.

אתר הקורס

http://www.math-wiki.com/index.php?title=83-218_מבנים_אלגבריים_להנדסה_סמסטר_א_תשעז

הפניות וספרות

קורס אלגברה מודרנית ח' – טכניון.
גולן, יונתן, "עיונים באלגברה מודרנית", הוצאת הספרים של אוניברסיטת חיפה, 1992.
"מתמטיקה דיסקרטית II: מבנים אלגבריים", האוניברסיטה הפתוחה.

שעות ומיקומים

קוד קורס	יום	שעה	בניין	חדר
01	א	12:00-14:00	1104	249
02	ב	14:00-15:00	1104	249

הערות מהמסכם

- עדכון אחרון: 04/03/2018, י"ז אדר תשע"ח.
- **אני כותב את ההרצאות תוך כדי שיעור**, לכן אין לי עותק בכתב יד, אבל אני בטוח שניתן למצוא עותקים כאלו אם תחפשו/תבקשו.
- להערכתי יש טעות הקלדה אחת או טעות סימן אחת לכל 5 עמודים בסיכום.
- ההרצאות משתנות משנה לשנה, לכן אני לא ממליץ להסתמך על הסיכומים באופן בלעדי.
- כל הזכויות לחומרים בסיכום שמורות למרצים ולמתרגלים שהעבירו את ההרצאות.

תוכן עניינים

מידע מקדים 1
שיעור 1 – הקדמה והגדרות 3
שיעור 2 – חבורה, חזקה, חבורה ציקלית 7
שיעור 3 – חבורה ציקלית, סדר של איבר, תת-חבורה 11
שיעור 4 – תת-חבורה, יוצר, איזומורפיזם 15
שיעור 5 – איזומורפיזם, הומומורפיזם, יחס ומחלקות שקילות, משפטי אוילר ולגרנז' 19
שיעור 6 – משפטי לגרנז', אוילר ופרמה, המחלקה השמאלית/ימנית, חבורה נורמלית 22
שיעור 7 – חוגים 26
שיעור 8 – חוג הפולינום ודרגתו 29
שיעור 9 – מחלק משותף מקסימלי (gcd), אלגוריתם אוקלידס, תת-חוג 32
שיעור 10 – חוג המנה, משפט ההומומורפיזם הראשון לחוגים 35
שיעור 11 – אידאלים בחוג הפולינומים, שדות סופיים 39
תרגול 1 – הגדרת החבורה 44
תרגול 2 – החבורה הסימטרית, מחזור 46
תרגול 3 – איברים מתחלפים, חבורה חילופית, תת-חבורה 50
תרגול 4 – המרכז, סדר של איבר, יוצר 55
תרגול 5 – תתי-חבורות 58
תרגול 6 – הומומורפיזם, איזומורפיזם 60
תרגול 7 – תת-חבורה נורמלית 64
תרגול 8 – חוגים 66
תרגול 9 – חוג הפולינומים, פולינום ראשוני, פולינום פריק ואי-פריק 69
תרגול 10 – שדות סופיים 72
תרגול 11 – משפט ההומומורפיזם הראשון לחוגים 75
תרגול 12 – תרגילים בנושא שדות ושדות סופיים 78

שיעור 1 – הקדמה והגדרות

6/11/2016

דוגמאות לשאלות שנראה במהלך הקורס

דוגמה 1

מהי השארית של המספר 2017^{5777} בחלוקה ל-103?
אנחנו נלמד לפתור שאלות כאלה ושאלות שדומות להן.

דוגמה 2

יהי $n = 2017^{5777}$ ו-$m = 103$.
למצוא k כך ש-$k \cdot m$ נותן שארית 1 בחלוקה ל-n.
נרצה למצוא דרך יעילה למצוא את k.
המחשב שלנו פותר בעיות דומות בתהליכי הצפנה ופענוח, ישנם 2 סוגים של הצפנה:

1. הצפנה במפתח פרטי – הצפנה קלאסית.
2. הצפנה במפתח ציבורי.

דוגמה 3

האם קיים שדה עם 256 איברים? או עם 5777 איברים?
ואם קיים, איך לבנות אותו?
התשובה היא שעבור 256 יש, ועבור 5777 אין, ובהמשך נלמד איך לבנות את השדה עבור 256.

מה זה בעצם מבנים אלגבריים?

אנחנו בעצם ניקח מבנים המוכרים לנו, נפשט ונחקור אותם.
זו בעצם דרך לתת כלים לפתרון לבעיות הדומות אחת לשנייה.

הגדרה – מאגמה

מאגמה (magma) היא קבוצה S שמוגדרת עליה פעולה שמקבלת כקלט זוג איברים ב-S ומחזיקה איבר ב-S.
פורמלית, הפעולה היא פונקציה:

$$*: \underbrace{S \times S}_{\text{זוגות סדורים של איברים ב-}S} \to S$$

בדרך כלל נסמן את הפעולה ב-$*$ ואת הפעלתה על הזוג (a,b) נסמן ב-$a * b$.

דוגמאות

א) $(\mathbb{R},+)$
ב) $(\mathbb{R},\cdot)$
ג) $(\mathbb{Z},-)$
ד) $(\mathbb{Z},\cdot)$
ה) (כפל מטריצות , מטריצות 3×3 מעל $\mathbb{R}$)
ו) (שרשור מחרוזות , מחרוזות סופיות מעל אלפבית Σ)

שאלה

האם $(\mathbb{N},-)$ מאגמה?
לא, כי $2 - 3 \notin \mathbb{N}$.

שאלה

האם $\left(\mathbb{R}, \underset{\text{חילוק}}{:}\right)$ מאגמה?

לא, כי אי אפשר להפעיל את הפעולה על הזוג $(x,0)$ [כי אי אפשר לחלק ב-0].

הגדרה – אגודה / חבורה למחצה

תהי $(S,*)$ מאגמה.

אם הפעולה $*$ מקיימת **אסוציאטיביות**, כלומר:

$$\forall a,b,c\in S,\quad (a*b)*c=a*(b*c)$$

אז S תיקרא **אגודה**, או **חבורה למחצה** (semi-group).

מתוך הדוגמאות שראינו:

א) $(\mathbb{R},+)$ – כן אגודה.

ב) $(\mathbb{R},\cdot)$ – כן אגודה.

ג) $(\mathbb{Z},-)$ – לא אגודה – חיסור הוא לא אסוציאטיבי:

$$(a-b)-c\neq a-(b-c)$$

ליתר דיוק, לא בהכרח מתקיים שוויון.

ד) $(\mathbb{Z},\cdot)$ – כן אגודה.

ה) (כפל מטריצות, מטריצות 3×3 מעל $\mathbb{R}$) – כן אגודה.

ו) (שרשור מחרוזות, מחרוזות מעל סופיות אלפבית Σ) – כן אגודה.

הגדרה – יחידה

תהי $(S,*)$ אגודה.

אם עבור $c\in S$ מסוים ועבור כל $x\in S$ מתקיים $x=c*x$ אז c תיקרא **יחידה ימנית** של S.

בדומה, אם עבור $d\in S$ מסוים ועבור כל $x\in S$ מתקיים $d*x=x$ אז d תיקרא **יחידה שמאלית** של S.

אם c הוא גם יחידה ימנית וגם יחידה שמאלית, אז הוא ייקרא **יחידה דו-צדדית** או סתם **יחידה** של S.

מתוך הדוגמאות שראינו:

א) $(\mathbb{R},+)$ – 0 הוא יחידה דו-צדדית.

ב) $(\mathbb{R},\cdot)$ – 1 הוא יחידה דו-צדדית.

ג) $(\mathbb{Z},-)$ – זו אמנם לא אגודה, ולכן פורמלית יחידה לא מוגדרת, אבל אם הייתה מוגדרת, 0 היה יחידה שמאלית ולא שמאלית, כי $x-0=x$ אבל $0-x\neq x$.

ד) $(\mathbb{Z},\cdot)$ – 1 הוא יחידה דו-צדדית.

ה) (כפל מטריצות, מטריצות 3×3 מעל $\mathbb{R}$) – I יחידה דו-צדדית (למרות שכפל מטריצות לא קומוטטיבי).

ו) (שרשור מחרוזות, מחרוזות מעל סופיות אלפבית Σ) – המחרוזת הריקה היא יחידה דו-צדדית.

ז) (בחירת ימני, $\mathbb{Z}$) – זו אגודה, כל איבר הוא יחידה שמאלית (כי $\forall c,\forall x, c*x=x$) ואין יחידה ימנית.

<u>טענה</u>
אם באגודה $(S,*)$ יש יחידה ימנית c ויחידה שמאלית d, אז בהכרח $c = d$.
<u>הוכחה</u>
נתבונן בביטוי $d * c$.
מצד אחד, c יחידה ימנית, ולכן $d * c = d$.
מצד שני, d יחידה שמאלית, ולכן $d * c = c$.
ולכן בסך הכל:

$$c = d * c = d \quad \Rightarrow \quad c = d$$

■

<u>הגדרה – מונואיד</u>
אגודה $(S,*)$ שיש בה יחידה דו-צדדית, תיקרא **מונואיד** (monoid).
<u>הערה</u>
יכולה להיות רק יחידה דו-צדדית אחת.

מתוך הדוגמאות שראינו:
א) $(\mathbb{R},+)$ – כן מונואיד.
ב) $(\mathbb{R},\cdot)$ – כן מונואיד.
ג) $(\mathbb{Z},-)$ – לא אגודה אז לא מונואיד.
ד) $(\mathbb{Z},\cdot)$ – כן מונואיד.
ה) (כפל מטריצות , מטריצות 3×3 מעל $\mathbb{R}$) – כן מונואיד.
ו) (שרשור מחרוזות , מחרוזות מעל סופיות אלפבית Σ) – כן מונואיד.
ז) (בחירת ימני , $\mathbb{Z}$) – לא מונואיד.
ח) (כפל , זוגיים) – זוהי אגודה אבל לא מונואיד כי אין איבר יחידה (1 לא קיים בה).

<u>הגדרה – הופכי</u>
יהי $(S,*)$ מונואיד, ויהי $a \in S$.
$b \in S$ יקרא **הופכי ימני** של a אם $a * b = e$ כאשר e איבר היחידה של S.
בדומה, אם $b * a = e$ אז b יקרא **הופכי שמאלי** של a.
ואם b גם הופכי ימני וגם הופכי שמאלי, אז הוא ייקרא **הופכי דו-צדדי** או סתם **הופכי** של a.

מתוך הדוגמאות שראינו:
א) $(\mathbb{R},+)$ – לכל $x \in \mathbb{R}$, $(-x)$ הוא הופכי דו-צדדי.
ב) $(\mathbb{R},\cdot)$ – לכל $x \neq 0$, $\frac{1}{x}$ הוא הופכי דו-צדדי, עבור $x = 0$ אין הופכי (לא ימני ולא שמאלי).
ג) $(\mathbb{Z},-)$ – לא מונואיד.
ד) $(\mathbb{Z},\cdot)$ – רק ל-(± 1) יש הופכי דו-צדדי, לשאר האיברים אין הופכי.
ה) (כפל מטריצות , מטריצות 3×3 מעל $\mathbb{R}$) – יש הופכי אם ורק אם הדטרמיננטה $\neq 0$, וכאשר יש הופכי הוא דו-צדדי (למרות שכפל מטריצות לא קומוטטיבי).

ו) $\left(\text{שרשור מחרוזות}, \text{מחרוזות מעל סופיות אלפבית } \Sigma\right)$ – רק למחרוזת הריקה יש הופכי דו-צדדי שזה היא עצמה, לשאר המחרוזות אין הופכי.

ז) $\left(\text{בחירת ימני}, \mathbb{Z}\right)$ – לא מונואיד.

ח) $\left(\text{כפל}, \text{זוגיים}\right)$ –לא מונואיד.

ט) $\left(\text{הרכבת פונקציות}, \text{פונקציות מקבוצה לעצמה}\right)$ – כאן יש הבדל בין הופכי ימני להופכי שמאלי, נסו לחשוב מתי לפונקציה יש הופכי מכל סוג.

<u>טענה</u>

יהי $(S,*)$ מונואיד, ויהי $a \in S$.

אם b הופכי משמאל של a, ו-c הופכי מימין של a אז $b = c$.

<u>הוכחה</u>

נתבונן בביטוי $(b*a)*c$.

$$c \underbrace{=}_{\text{איבר יחידה } e} e*c \underbrace{=}_{\text{כי } b \text{ הופכי משמאל של } a} (b*a)*c = b*(a*c) \underbrace{=}_{\text{כי } c \text{ הופכי מימין של } a} b*e \underbrace{=}_{\text{איבר יחידה } e} b$$

וקיבלנו $c = b$.

<u>הגדרה – חבורה</u>

מונואיד $(S,*)$ שבו לכל איבר יש הופכי דו-צדדי נקרא **חבורה** (group).

מתוך הדוגמאות שראינו רק דוגמה א' היא חבורה (כי לכל x קיים $(-x)$).

שיעור 2 – חבורה, חזקה, חבורה ציקלית

20/11/2016

תזכורת

הגדרה – חבורה

תהי S קבוצה.

S תקרא **חבורה** אם:

א. קיימת פעולה:

$$*: S \times S \to S$$

(מספיק בשביל להגדיר **מאגמה**)

ב. הפעולה היא אסוציאטיבית:

$$a * (b * c) = (a * b) * c$$

(א+ = מספיק בשביל להגדיר **אגודה**)

ג. קיים איבר יחידה (דו-צדדי) $e \in S$ כך ש:

$$\forall x \in S \quad e * x = x * e = x$$

(א+ ב+ = מספיק בשביל להגדיר **מונואיד**)

ד. לכל איבר $x \in S$ יש הופכי (דו-צדדי) $y \in S$ כך ש:

$$x * y = y * x = e$$

(**חבורה** → group)

דוגמה

תהי G קבוצת המטריצות $n \times n$ מעל $\mathbb{R}$ עם פעולת כפל מטריצות.

האם זו חבורה?

נבדוק את התנאים:

מאגמה – ✓ – אפשר להכפיל כל שתי מטריצות $n \times n$ ותתקבל מטריצה $n \times n$.

אגודה – ✓ – כפל מטריצות אסוציאטיבי.

מונואיד – ✓ – המטריצה I יחידה.

הופכי – ✗ – יש הופכי רק למטריצות שהדטרמיננטה שלהן $\neq 0$.

מסקנה

G לא חבורה.

אולי נוכל לצמצם את G כך שנקבל חבורה?

הגדרה – $GL_n(\mathbb{R})$

$GL_n(\mathbb{R})$ היא קבוצת המטריצות **ההפיכות** $n \times n$ מעל $\mathbb{R}$ עם פעולת כפל מטריצות.

$\Leftarrow$ $GL_n(\mathbb{R})$ היא אכן חבורה.

הגדרה – $SL_n(\mathbb{R})$

$SL_n(\mathbb{R})$ היא קבוצת המטריצות $n \times n$ מעל $\mathbb{R}$ עם דטרמיננטה 1 עם פעולת כפל מטריצות.

הגדרה – חבורה קומוטטיבית

חבורה $(G,*)$ תיקרא קומוטטיבית (או חילופית, או אָבֵלִית) אם:

$$\forall x, y \in G, \quad x * y = y * x$$

דוגמה א

$(\mathbb{R}, +)$, $(\mathbb{R}\backslash\{0\}, \cdot)$, $(\mathbb{C}, +)$, $(\mathbb{Z}, +)$ חבורות קומוטטיביות.

דוגמה ב

$S = \{x\}$ עם פעולה $x * x = x$ חבורה קומוטטיבית.

דוגמה ג

$GL_n(\mathbb{R})$ חבורה לא קומוטטיבית, למשל:

$$\begin{pmatrix}1 & 2\\3 & 4\end{pmatrix}\begin{pmatrix}2 & 3\\4 & 5\end{pmatrix}=\begin{pmatrix}10 & 13\\20 & 29\end{pmatrix}$$
$$\neq$$
$$\begin{pmatrix}2 & 3\\4 & 5\end{pmatrix}\begin{pmatrix}1 & 2\\3 & 4\end{pmatrix}=\begin{pmatrix}11 & 16\\19 & 28\end{pmatrix}$$

דוגמה ד

$Sym(x)$ פונקציות חד-חד ערכיות ועל מהקבוצה x לעצמה, עם פעולת הרכבה.
$Sym(x)$ חבורה. היא קומוטטיבית אם ורק אם $|x|\le 2$.
אם $x=\{a,b\}$ אז:

$$Sym(x)=\left\{\begin{pmatrix}a\to a\\b\to b\end{pmatrix},\begin{pmatrix}a\to b\\b\to a\end{pmatrix}\right\}$$

וקל לראות ש- $f\circ g=g\circ f$ לכל $f,g\in Sum(X)$.
כדי להראות ש- $Sym(x)$ לא קומוטטיבית לכל $|x|\ge 3$, מספיק להראות שהיא לא קומוטטיבית עבור $|x|=3$.
ניקח אם כן $x=\{1,2,3\}$ ואת הפונקציות:

$$f=\begin{pmatrix}1\to 2\\2\to 3\\3\to 1\end{pmatrix}\quad,\quad g=\begin{pmatrix}1\to 2\\2\to 1\\3\to 3\end{pmatrix}$$

לכן לא קומוטטיבית:

$$f\circ g=\begin{pmatrix}1\to 3\\2\to 2\\3\to 1\end{pmatrix}\quad\neq\quad g\circ f=\begin{pmatrix}1\to 1\\2\to 3\\3\to 2\end{pmatrix}$$

הגדרה – איברים מתחלפים, המרכז

תהי $(G,*)$ חבורה, ויהיו $x,y\in G$. נאמר ש-x,y **מתחלפים**, אם:

$$x*y=y*x$$

המֶרְכָּז $Z(G)$ הוא אוסף האיברים שמתחלפים עם **כל** האיברים:

$$\{x\in G:\quad \forall y\in G\quad x*y=y*x\}$$

דוגמה א

אם G קומוטטיבית אז $Z(G)=G$.

דוגמה ב

לכל חבורה G, $e\in Z(G)$.

דוגמה ג

מהו המרכז של $GL_n(\mathbb{R})$?

טענה

$$Z\big(GL_n(\mathbb{R})\big)=\{\alpha\cdot I:\alpha\in\mathbb{R}\}$$

הוכחה

מצד אחד, לכל $A\in GL_n(\mathbb{R})$ מתקיים:

$$A\cdot(\alpha I)=(\alpha I)\cdot A=\alpha\cdot A$$

ולכן $\alpha\cdot I\in Z\big(GL_n(\mathbb{R})\big)$ לכל α.
מצד שני, נניח $A\in Z\big(GL_n(\mathbb{R})\big)$.
בפרט, לכל i,j, A מתחלפת עם המטריצה:

$$E_{ij}=\begin{pmatrix}0&\cdots&\cdots&\cdots&\cdots&\cdots&0\\ \vdots&\ddots&\cdots&\cdots&\cdots&\iddots&\vdots\\ \vdots&\vdots&0&\cdots&0&\vdots&\vdots\\ \vdots&\vdots&\vdots&1_{ij}&\vdots&\vdots&\vdots\\ \vdots&\vdots&0&\cdots&0&\vdots&\vdots\\ \vdots&\iddots&\cdots&\cdots&\cdots&\ddots&\vdots\\ 0&\cdots&\cdots&\cdots&\cdots&\cdots&0\end{pmatrix}$$

[אמנם מובטח רק ש-A מתחלפת עם מטריצות הפיכות, ו-E_{ij} לא הפיכה. אבל $I+E_{ij}$ כן הפיכה ולכן מובטח שמתקיים:

$$A(I+E_{ij})=(I+E_{ij})A$$
$$A+A\cdot E_{ij}=A+E_{ij}\cdot A$$

ולכן $A\cdot E_{ij}=E_{ij}\cdot A$].
נסתכל על הכפל:

$$A\cdot E_{ij}=\left(\begin{array}{ccccc|c|ccccc}0&0&0&&&\overbrace{a_{1i}}^{j}&&&0&0&0\\0&\vdots&\vdots&&&a_{2i}&&&0&\vdots&\vdots\\0&\vdots&\vdots&&&\vdots&&&0&\vdots&\vdots\\ \vdots&\vdots&\vdots&\cdots&&\vdots&&\cdots&\vdots&\vdots&\vdots\\ \vdots&\vdots&\vdots&&&\vdots&&&\vdots&\vdots&\vdots\\ \vdots&\vdots&\vdots&&&\vdots&&&\vdots&\vdots&\vdots\\0&0&0&&&a_{ni}&&&0&0&0\end{array}\right)$$

כל העמודות חוץ מהעמודה ה-j הן 0 כי במטריצה E_{ij} כל העמודות חוץ מה-j הן 0.

$$E_{ij}\cdot A=\begin{pmatrix}0&0&0&\cdots&\cdots&0\\0&\cdots&\cdots&\cdots&\cdots&0\\0&\cdots&\cdots&\cdots&\cdots&0\\ &&\vdots&&&\\ \hline a_{j1}&a_{j2}&\cdots&\cdots&a_{jn}\}\,i\\ \hline &&\vdots&&&\\0&0&0&\cdots&\cdots&0\\0&\cdots&\cdots&\cdots&\cdots&0\\0&\cdots&\cdots&\cdots&\cdots&0\end{pmatrix}$$

כלומר:

$$\left(A\cdot E_{ij}\right)_{ij}=a_{ii}$$
$$\left(E_{ij}\cdot A\right)_{ij}=a_{jj}$$

על מנת שיתקיים $A\cdot E_{ij}=E_{ij}\cdot A$, חייבים:
א. $\forall k\neq i\ a_{ki}=0$.
ב. $\forall k\neq j\ a_{jk}=0$.
ג. $a_{ii}=a_{jj}$.

אם $A\in Z\big(GL_n(\mathbb{R})\big)$ אז תנאים א, ב, ג חייבים להתקיים **לכל** i,j. מתנאים א ו-ב נובע ש-A חייבת להיות **אלכסונית** ומתנאי ג נובע שכל איברי האלכסון של A שווים זה לזה, ולכן $A=\alpha\cdot I$.

■

<u>הגדרה – חזקה</u>

תהי $(G,*)$ חבורה, $g\in G$, $n\in\mathbb{N}$. **החזקה** ה-n של g היא:

$$g^n=\underbrace{g*g*\cdots*g}_{\text{פעמים } n}$$

נגדיר $g^0=e$ לכל $g\in G$, וכן נגדיר g^{-n} להיות $(g^{-1})^n$.

טענה
לכל $g \in G$ ולכל $m,n \in \mathbb{Z}$:
א. $g^{m+n} = g^m * g^n$.
ב. $g^{m \cdot n} = (g^m)^n$.
הוכחה
(נוכיח את א – הוכחת ב באופן דומה)
נחלק למקרים:
1. $m,n > 0$:

$$g^{m+n} = \underbrace{g * g * \cdots * g}_{m+n \text{ פעמים}} \underbrace{=}_{\text{אסוציאטיביות}} \underbrace{(g * g * \cdots * g)}_{m \text{ פעמים}} * \underbrace{(g * g * \cdots * g)}_{n \text{ פעמים}} = g^m * g^n$$

2. $m,n < 0$ – אותו הדבר עם g^{-1} במקום g.
3. $m = 0$:

$$g^{m+n} = g^n = \underbrace{g * g * \cdots * g}_{n \text{ פעמים}} = e * \underbrace{(g * g * \cdots * g)}_{n \text{ פעמים}} = g^0 * g^n$$

4. $\begin{cases} m > 0 \\ n < 0 \end{cases}$ נניח בלי הגבלת הכלליות (בה"כ) $|m| \geq |n|$:

$$g^m * g^n = \underbrace{(g * g * \cdots * g)}_{m \text{ פעמים}} * \underbrace{(g^{-1} * g^{-1} * \cdots * g^{-1})}_{(-n) \text{ פעמים}} =$$

$$\underbrace{=}_{\text{אסוציאטיביות}} \underbrace{(g * g * \cdots * g)}_{m-1 \text{ פעמים}} * \cancel{(g * g^{-1})} * \underbrace{(g * g * \cdots * g)}_{(-n)-1 \text{ פעמים}} =$$

$$\underbrace{=}_{\text{אסוציאטיביות}} \underbrace{(g * g * \cdots * g)}_{m-(-n) \text{ פעמים}} = g^{m-(-n)} = g^{m+n}$$

מסקנה
לכל $g \in G$ ולכל $m,n \in \mathbb{Z}$:

$$g^m * g^n = g^n * g^m$$

הגדרה – חבורה ציקלית
חבורה G תקרא **ציקלית** אם קיים $g_0 \in G$ כך שכל איברי G הם חזקות של g_0.

מסקנה
כל חבורה ציקלית היא קומוטטיבית.

הערה
חזקה של האיבר $a * b$ בדרך כלל אינה שווה ל-"מכפלת" החזקות המתאימות של a,b.
כלומר:

$$a^n * b^n \neq (a * b)^n$$

בפרט, אם $\forall a,b$ מתקיים $a^2 * b^2 = (a * b)^2$, אז החבורה **קומוטטיבית**, כי נקבל:

$$(a * a) * (b * b) = (a * b) * (a * b)$$

נכפיל משמאל ב-a^{-1} ומימין ב-b^{-1} ונקבל:

$$\cancel{a^{-1} * a} * a * b * \cancel{b * b^{-1}} = \cancel{a^{-1} * a} * b * a * \cancel{b * b^{-1}}$$

$$\Downarrow$$

$$\underline{a * b = b * a}$$

שיעור 3 – חבורה ציקלית, סדר של איבר, תת-חבורה

27/11/2016

הגדרה – חבורה ציקלית
חבורה $(G,*)$ תקרא **ציקלית** אם קיים $g_0 \in G$ כך שלכל $g \in G$ קיים $n \in \mathbb{Z}$, עבורו $g = g_0^n$.
במקרה כזה, g_0 ייקרא **יוצר** של החבורה.

הערה
יוצר של חבורה ציקלית לא חייב להיות יחיד.

הערה
נשים לב שאם $g_0 \in G$ אז מסגירות נובע:

$$g_0^2 = g_0 * g_0 \in G$$

ומכאן באינדוקציה:

$$\forall k \in \mathbb{N}: \quad g_0^k \in G$$

ובנוסף, $g_0^{-1} \in G$ (סגירות להופכי) ולכן:

$$g_0^{-2} = (g_0^{-1}) * (g_0^{-1}) \in G$$

ומכאן באינדוקציה:

$$\forall k \in \mathbb{N}: \quad g_0^{-k} \in G$$

לכן G **חייבת** להכיל את כל החזקות של g_0.
לפיכך, חבורה ציקלית ש-g_0 הוא יוצר שלה היא החבורה **המינימלית** שמכילה את האיבר g_0 (ביחס לפעולה $*$).

מסקנה (מהשיעור שעבר)
כל חבורה ציקלית היא קומוטטיבית.

דוגמאות
דוגמה 1
$(\mathbb{Z},+)$ – זו חבורה ציקלית. אכן, 1 יוצר שלה כי כל $n \in \mathbb{Z}$ נוכל לרשום בצורה $n = 1^n (= 1 + 1 + \cdots)$.
כמו כן, (-1) יוצר של $\mathbb{Z}$ כי כל $n \in \mathbb{Z}$ נוכל לרשום בצורה $n = (-1)^{-n}$.
תרגיל לבית
להראות שאין יוצרים נוספים.
פתרון
נניח בשלילה שיש לנו מספר $\mathbb{Z} \ni x \neq \pm 1,0$, שהוא יוצר, נשים לב שהוא חייב להיות גדול מ-1, ומכיוון שהוא גדול מ-1, אי אפשר להגיע ל-1 באמצעותו, ולכן הוא אינו יוצר.

דוגמה 2
$(\mathbb{Q},+)$ – החבורה אינה ציקלית.
נוכיח בשלילה – נניח ש-a יוצר של $\mathbb{Q}$. $a \neq 0$ (כי $0^n = 0$ לכל n). כעת נשים לב שלא ניתן להציג את $\frac{a}{2}$ כחזקה של a. לכן a לא יוצר .

דוגמה 3
$(\mathbb{Z}_6,+)$ – חבורה ציקלית, כי 1 יוצר שלה. כמו-כן, 5 יוצר שלה, אבל 2,3,4 לא יוצרים.

דוגמה 4
$(\mathbb{Z}_{10},+)$ – היוצרים הם 1,3,7,9.

באופן כללי, $(\mathbb{Z}_n,+)$ חבורה ציקלית, והיוצרים הם:

$$\left\{ a \middle| \begin{matrix} 1 \le a \le n-1 \\ (a,n)=1 \\ \uparrow \\ a \text{ זר ל } n \end{matrix} \right\}$$

<u>הגדרה – סדר של איבר</u>

תהי $(G,*)$ חבורה, $g \in G$.

הסדר של g הוא החזקה האי-שלילית המינימלית n, כך ש-$g^n = e$.

אם אין חזקה כזו, נאמר שהסדר של g הוא ∞.

<u>סימון</u>

הסדר מסומן $o(g)$.

<u>דוגמאות</u>

<u>דוגמה 1</u>

בכל חבורה, איבר היחידה הוא מסדר 1, והוא האיבר היחיד מסדר 1.

<u>דוגמה 2</u>

$(\mathbb{Z}_6,+)$ – מה הם הסדרים האפשריים של האיברים?

$$o(1)=6 \quad o(4)=3$$
$$o(2)=3 \quad o(5)=6$$
$$o(3)=2 \quad o(0)=1$$

<u>טענה</u>

בחבורה $(\mathbb{Z}_n,+)$, הסדר של k הוא:

$$\frac{n}{\underbrace{\gcd(k,n)}_{\text{מחלק משותף מינימלי}}}$$

הוכחה – בתור תרגיל בית.

<u>דוגמה 3</u>

$(\mathbb{Z},+)$ – מה הם הסדרים האפשריים של האיברים?

הסדר של 0 הוא 1, הסדר של כל איבר אחר הוא ∞, כי לכל k, לא קיים n כך ש- $k^n = k \cdot n$.

<u>טענה</u>

תהי $(G,*)$ חבורה, $g \in G$, $k,l \in \mathbb{N}$. אזי $g^k = g^l$ אם ורק אם:

$$o(g) | l-k$$

[כלומר, $(l-k)$ מתחלק בסדר של g].

<u>הוכחה</u>

נניח תחילה $o(g)|l-k$. נוכל לרשום $l-k = o(g)\cdot m$.

כעת מתקיים:

$$g^l \underbrace{=}_{\text{חוקי חזקות}} g^k * g^{l-k} = g^k * g^{o(g)\cdot m} \underbrace{=}_{\text{חוקי חזקות}} g^k * \left(g^{o(g)}\right)^m = g^k * e^m = g^k * e = g^k$$

בכיוון השני, נניח $g^l = g^k$, אזי מתקיים:

$$g^l * g^{-k} = g^k * g^{-k} = e$$

כלומר, $g^{l-k} = e$.

נחלק את $l-k$ ב-$o(g)$ עם שארית:

$$l = k = m\cdot o(g) + r$$

כאשר $0 \le r < o(g)$.

כעת:

$$e = g^{l-k} = g^{o(g)\cdot m+r} \underbrace{=}_{\text{חוקי חזקות}} \left(g^{o(g)}\right)^m * g^r = e^m * g^r = g^r$$

אבל $r < o(g)$, ולפי ההגדרה, $o(g)$ היא החזקה הטבעית **המינימלית** שאם מעלים בה את g מקבלים את e.
לכן בהכרח $r = 0 \Leftarrow (l-k)$ מתחלק ב-$o(g)$.

<u>מסקנה</u>
לכל $g \in G$, הסדרה $e, g, g^2, g^3, \dots$ מכילה בדיוק $o(g)$ איברים שווים.
<u>הוכחה</u>
ראשית, החזקות $e, g, g^2, \dots, g^{o(g)-1}$ שונות זו מזו [כי לפי הטענה הקודמת, עם $g^k = g^l$ עבור $l > k$ אז $(l-k)$ מתחלק ב-$o(g)$ ובפרט $l-k \geq o(g)$].
מצד שני, לכל $n \in \mathbb{N}$, נוכל לחלק את n ב-$o(g)$ עם שארית ונקבל $n = m \cdot o(g) + r$ עבור $0 \leq r < o(g)$ ואז מתקיים $g^n = g^r$ [כי $n - r = m \cdot o(g)$ מתחלק ב-$o(g)$] אז g^n שווה לאחד מהאיברים $e, g, g^2, \dots, g^{o(g)-1}$ שכבר ספרנו.

<u>מסקנה</u>
אם $(G,*)$ חבורה סופית, אז **הסדר** של כל $g \in G$ הוא **סופי**.
<u>הוכחה</u>
לפי המסקנה הקודמת, אילו היה $g \in G$ עם סדר אינסופי, החבורה G הייתה מכילה ∞ חזקות שונות שלו. וזה לא ייתכן כי היא סופית.

<u>מסקנה</u>
תהי $(G,*)$ חבורה סופית, ויהי $g \in G$. אזי קיים $m \in \mathbb{N}$ כך ש-$g^{-1} = g^m$.
<u>הוכחה</u>
לפי המסקנה הקודמת, $o(g)$ הוא סופי. כעת, נשים לב ש:

$$g * g^{o(g)-1} = g^{o(g)} = e$$

ולכן $g^{o(g)-1}$ הוא ההופכי של g.

בעקבות המסקנה האחרונה, נוכל לשנות במקצת את ההגדרה של חבורה ציקלית לתמורות סופיות.

<u>הגדרה – חבורה ציקלית</u>
חבורה סופית $(G,*)$ תיקרא **ציקלית** אם קיים $g_0 \in G$ כך שלכל $g \in G$, ניתן לרשום $g = g_0^n$ עבור $n \in \mathbb{N}\backslash\{0\}$.

<u>טענה</u>
תהי $(G,*)$ חבורה בת n איברים. אזי g הוא יוצר של G אם ורק אם $o(g) = n$.
<u>הוכחה</u>
לפי המסקנה לעיל, סדרת החזקות של g מכילה בדיוק $o(g)$ איברים שונים. לכן היא מכילה את כל איברי החבורה G אם ורק אם $o(g) = n$.

<u>הגדרה – תת-חבורה</u>
תהי $(G,*)$ חבורה, $H \subseteq G$. H תיקרא **תת-חבורה** של G אם H מהווה חבורה ביחס לפעולה של G.

<u>שאלה</u>
איזה תכונות צריך לבדוק כדי לוודא ש-H תת-חבורה של G?
1. **סגירות** – חייבים לבדוק! אמנם סגירות של G מבטיחה שאם $a, b \in H$ אז $a * b \in G$, אבל היא לא מבטיחה $a * b \in H$.
2. **אסוציאטיביות** – לא צריך לבדוק, מגיע בירושה מ-G.
3. **איבר יחידה** – מספיק לבדוק שאיבר היחידה של G נמצא ב-H, ואז הוא יהיה איבר היחידה של H.
שאלה: האם ייתכן שיש ל-H איבר יחידה e' שהוא שונה מאיבר היחידה של G?

תשובה: זה לא ייתכן. נשים לב ש-$e' \in G$.
יהי $h \in H$. מתקיים:

$$e' \underbrace{*}_{\text{יש יחידה של } H} h = h$$

ומצד שני "נכפיל" את שני הצדדים מימין ב-h^{-1} (בתור איברים ב-G) ונקבל:

$$e' = e' * h * h^{-1} = h * h^{-1} = e$$

4. **סגירות להופכי** – צריך לוודא שההופכי (ב-G) נמצא ב-H.

לסיכום, צריך לבדוק סגירות לפעולה ולהופכי ושאיבר היחידה של G נמצא ב-H. לא צריך לבדוק אסוציאטיביות.

<u>דוגמאות לתת-חבורה</u>
בכל חבורה, איבר היחידה לבדו הוא תת-חבורה.
מהן תתי-החבורות של $\mathbb{Z}, \mathbb{Z}_n$?

–

שיעור 4 – תת-חבורה, יוצר, איזומורפיזם

4/12/2016

הגדרה – תת-חבורה

תהי $(G,*)$ חבורה. תת-קבוצה $H \subseteq G$ תיקרא **תת-חבורה** אם היא מהווה חבורה ביחס לפעולה של G.
מה צריך לבדוק כדי לוודא ש-H תת-חבורה?
- סגירות לפעולה.
- איבר היחידה של G נמצא ב-H.
- סגירות להופכי – לכל $h \in H$, ההופכי שלו (כאיבר ב-G) נמצא ב-H.

דוגמאות

דוגמה 1
לכל חבורה G, תת-הקבוצה $\{e\}$ (איבר היחידה) היא תת-קבוצה.

דוגמה 2
$G = (\mathbb{Z}, +)$, מה הן תתי החבורות של G?
- זוגיים: $\{2n: n \in \mathbb{Z}\}$
- $\{kn: n \in \mathbb{Z}\} = k\mathbb{Z}$, נוודא:
  - אכן, אם $k|b$, $k|a$ אז $k|(a+b)$ ← סגירות.
  - $k|0$ ← יחידה.
  - $k|a \Rightarrow k|(-a)$ ← הופכי.

נראה בהמשך שאלו כל תתי החבורות של $(\mathbb{Z}, +)$.

דוגמה 3
האם $(\mathbb{Z}_n, +)$ תת-חבורה של $(\mathbb{Z}, +)$?
לא! כי הפעולה ב-$\mathbb{Z}_n$ היא לא אותה פעולה כמו ב-$\mathbb{Z}$.

דוגמה 4
תהי $(G,*)$ חבורה. אזי המרכז $C(G)$ הוא תת-חבורה של G.
(תזכורת: $C(G) = \{a \in G: \forall b \in G, a*b = b*a\}$).

הוכחה
סגירות לפעולה – יהיו $x, y \in C(G)$ ויהי $z \in G$. מתקיים:

$$(x*y)*z \underbrace{=}_{\text{אסוציאטיביות}} x*(y*z) \underbrace{=}_{y \in C(G)} x*(z*y) \underbrace{=}_{\text{אסוציאטיביות}} (x*z)*y =$$
$$\underbrace{=}_{x \in C(G)} (z*x)*y \underbrace{=}_{\text{אסוציאטיביות}} z*(x*y)$$

$\Leftarrow$ $x*y \in C(G)$.
יחידה – $e \in C(G)$ כי $\forall x, x*e = e*x$.
הופכי – יהי $x \in C(G)$ ויהי $z \in G$. מתקיים:

$$x^{-1}*z = (z^{-1}*x)^{-1} \underbrace{=}_{x \in C(G)} (x*z^{-1})^{-1} = z*x^{-1}$$

$\Leftarrow$ $x^{-1} \in C(G)$.
ולכן בסך הכל $C(G)$ תת-חבורה.

דוגמה 5
תהי $(G,*)$ חבורה, $x \in G$, אזי $H = \{x^n | n \in \mathbb{Z}\}$ תת-חבורה של G.
הוכחה
סגירות לפעולה – יהיו $y, z \in H$ אזי קיימים $m, n \in \mathbb{Z}$, כך ש- $y = x^m, z = x^n$. אזי:

$$y*z = x^m * x^n = x^{m+n} \in H$$

יחידה – $e = x^0$ ולכן $e \in H$.

הופכי – אם $z\in H$ אז קיים m כך ש-$z=x^m$, ואז $z^{-1}=x^{-m}\in H$.
ולכן בסך הכל H תת-חבורה.

__**טענה**__
אם $(G,*)$ חבורה סופית, H תת-קבוצה לא ריקה של G. על-מנת להוכיח ש-H תת-חבורה, מספיק לבדוק **סגירות לפעולה**.
__הוכחה__
נראה שאם H מקיימת סגירות לפעולה, אז "יחידה" ו-"סגירות להופכי" מובטחים.
יהי $x\in H$. **הסדר** של x הוא סופי ולכן קיים $n\in\mathbb{N}$ כך ש- $x^n=e$. ולכן מסגירות לפעולה נובע $e\in H$.
בדומה לגבי הופכי: ראינו בשיעור קודם, שבכל חבורה סופית G, אם $x\in G$ אז קיים $m\in\mathbb{N}$ כך ש-$x^{-1}=x^m$ ולכן מסגירות לפעולה נובע שאם $x\in H$ אז $x^{-1}\in H$.
__הערה__
אם G חבורה אינסופית, הטענה לעיל לא נכונה. למשל, $G=(\mathbb{Z},+)$, $H=(\mathbb{N},+)$. H תת-קבוצה של G הסגורה לפעולה, אבל לא תת-חבורה.

__**הגדרה – איזומורפיזם**__
תהיינה $(G,*),(H,\circ)$ חבורות.
פונקציה $f:G\to H$ תיקרא **איזומורפיזם** אם:
א. f חד-חד ערכית ועל.
ב. f שומרת פעולה:

$$\forall x,y\in G:$$
$$f(x)\circ f(y)=f(x*y)$$

אם קיימת f כזו, החבורות G,H יקראו **איזומורפיות**.
__תכונות__
1. אם $f:G\to H$ איזומורפיזם, אז $f(e_G)=e_H$, כלומר, הפונקציה מעבירה את איבר היחידה של G לאיבר היחידה של H.
__הוכחה__

$$f(e_G)=f(e_G*e_G)=f(e_G)\circ f(e_G)$$
$$\Downarrow$$
$$\xRightarrow{\circ\left[(f(e_G))^{-1}\right]} f(e_G)\circ\left[(f(e_G))^{-1}\right]=f(e_G)\circ f(e_G)\circ\left[(f(e_G))^{-1}\right]$$
$$\Downarrow$$
$$e_H=f(e_G)\circ e_H=f(e_G)$$

■

2. אם $f:G\to H$ איזומורפיזם, אז ההעתקה ההופכית $f^{-1}:H\to G$ גם היא איזומורפיזם.
__הוכחה__
לשם כך צריך להוכיח שלכל $z,w\in H$, מתקיים:

$$\underbrace{f^{-1}(z)*f^{-1}(w)}_{a}=\underbrace{f^{-1}(z\circ w)}_{b}$$

נשים לב שמתקיים:

$$f\left(\underbrace{f^{-1}(z)*f^{-1}(w)}_{\in G}\right)=\underbrace{f\left(f^{-1}(z)\right)\circ f\left(f^{-1}(w)\right)}_{\in H}=z\circ w=f\left(f^{-1}(z\circ w)\right)$$

הראינו ש-$f(a)=f(b)$, אבל f היא חד-חד ערכית ועל ולכן נובע מכאן ש-$a=b$.

■

3. אם $f:G\to H$ איזומורפיזם, אזי לכל $x\in G$ ולכל $n\in\mathbb{Z}$ מתקיים:

$$f(x^n)=\left(f(x)\right)^n$$

__הוכחה חלקית__
נוכיח עבור $n=-1$ (השאר – בבית).

מתקיים לכל $x \in G$:

$$e_H \underbrace{=}_{\text{תכונה 1}} f(e_G) = f(x * x^{-1}) = f(x) \circ f(x^{-1})$$

בדומה נוכל להראות:

$$e_H = f(x^{-1}) \circ f(x)$$

ולכן $f(x^{-1})$ הוא ההופכי של $f(x)$ ב-H.
בכדי להרחיב את ההוכחה לכל $n \in \mathbb{Z}$ ניתן להשתמש באינדוקציה.

<u>דוגמאות</u>

<u>דוגמה 1</u>

$G = (\mathbb{Z}_2, +)$, $H = (\{1, -1\}, \cdot)$, ננסה לבנות איזומורפיזם $f: G \to H$.
f חייב להעביר את e_G ל-e_H ולכן $f(0) = 1$.
f חד-חד ערכי ולכן בהכרח $f(1) = -1$.
זה מגדיר את f במלוכה, נותר לבדוק האם f איזומורפיזם.
f חד-חד ערכית ועל – ✓.
צריך לבדוק האם:

$$\forall x, y \in G: \quad f(x + y) = f(x) \cdot f(y)$$

יש 4 מקרים, אפשר לבדוק אחד-אחד ולראות ש-f אכן איזומורפיזם:

x	y	$f(x+y)$	$f(x) \cdot f(y)$
0	0	$f(0) = 1$	$f(0) \cdot f(0) = 1 \cdot 1 = 1$
0	1	$f(1) = -1$	$f(0) \cdot f(1) = 1 \cdot (-1) = -1$
1	0	$f(1) = -1$	$f(1) \cdot f(0) = (-1) \cdot 1 = -1$
1	1	$f(0) = 1$	$f(1) \cdot f(1) = (-1) \cdot (-1) = 1$

<u>דוגמה 2</u>

$G = (\mathbb{Z}_n, +)$, $H = \left(\underbrace{\left\{ e^{\frac{2\pi j}{n} i} \middle| 0 \leq j \leq n-1 \right\}}_{n \text{ שורשי היחידה מסדר}}, \cdot \right)$, ננסה לבנות איזומורפיזם $f: G \to H$.
ראשית, $f(0) = 1$.
ננסה להגדיר:

$$f(1) = e^{\frac{2\pi \cdot 1}{n} i}$$

נשים לב שלפי תכונה 3 לעיל, לכל $m \in \mathbb{Z}$ מתקיים:

$$f(1^m) = \left(f(1)\right)^m$$

מכיוון ש-1 יוצר של $\mathbb{Z}_n$, קביעת $f(1)$ קובעת את f באופן מוחלט:

$$f(m) = f(1^m) = \left(f(1)\right)^m = \left(e^{\frac{2\pi \cdot 1}{n} i}\right)^m = e^{\frac{2\pi \cdot m}{n} i}$$

ברור מההגדרה ש-f חד-חד ערכית ועל.
שמירת פעולה: רוצים להראות שלכל $k, m \in \mathbb{Z}_n$ מתקיים:

$$f\Big(k + m\big(mod(n)\big)\Big) = f(k) \cdot f(m)$$

או במילים אחרות:

$$e^{2\pi \cdot \frac{(k+m) \cdot mod(n)}{n} i} \stackrel{?}{=} e^{\frac{2\pi k}{n} i} \cdot e^{\frac{2\pi m}{n} i}$$

$$e^{\frac{2\pi}{n}((m+k) \cdot mod(n)) \cdot i} = e^{\frac{2\pi}{n}(m+k) \cdot i}$$

ואכן מתקיים שוויון כי $1 = e^{\frac{2\pi n}{1} i}$.

<u>דוגמה 3</u>

תהיינה $(G, *)$, $(H, \circ)$ חבורות ציקליות סופיות. אזי G, H איזומורפיות אם ורק אם $|G| = |H|$.

הוכחה
אם $|H| \neq |G|$ אז הן לא איזומורפיות כי לא קיימת פונקציה חד-חד ערכית ועל ביניהן.
נניח כעת $|G| = |H| = n$. יהיה g_0 יוצר של G ויהי h_0 יוצר של H.
נגדיר פונקציה $f: G \to H$ על-ידי $f(g_0) = h_0$, ובהתאם $\forall m: f(g_0^m) = h_0^m$.
זה מגדיר לחלוטין את f.
תרגיל – להראות ש-f חד-חד ערכית ועל.
נראה ש-f שומרת פעולה – צריך להראות שלכל $x, y \in G$ מתקיים:

$$f(x * y) = f(x) \circ f(y)$$

קיימים k, m כך ש:

$$\begin{cases} x = g_0^k \\ y = g_0^m \end{cases}$$

מתקיים:

$$f(x * y) = f\left(g_0^k * g_0^m\right) = f\left(g_0^{k+m}\right) = h_0^{k+m} = h_0^k \circ h_0^m = f(x) \circ f(y)$$

מסקנה
מכיוון שאיזומורפיזם שומר על כל התכונות של חבורה, כדי להבין את **כל** החבורות הציקליות הסופיות, מספיק להבין את החבורות $(\mathbb{Z}_n, +)$.

שיעור 5 – איזומורפיזם, הומומורפיזם, יחס ומחלקות שקילות, משפטי אוילר ולגרנז'

11/12/2016

הגדרה – איזומורפיזם

תהיינה $(H,\circ)$, $(G,*)$ חבורות.

פונקציה $f: G \to H$ תיקרא **איזומורפיזם** אם:

א. f חד-חד ערכית ועל.

ב. f שומרת פעולה:

$$\forall x,y \in G: \quad f(x*y)=f(x)\circ f(y)$$

אם ידוע רק שסעיף ב' מתקיים, f נקראת **הומומורפיזם**.

טענה

תהיינה G,H חבורות ציקליות סופיות. אזי G,H איזומורפיות אם ורק אם $|G|=|H|$.

דוגמה נוספת

ניקח את $G=(\mathbb{R},+), H=(\mathbb{R}_+,\cdot)$.

האם G,H איזומורפיות?

פתרון

תחילה בודקים האם סיבה פשוטה לכך שהן לא יהיו איזומורפיות (למשל, אחת ציקלית והשני לא). אם לא מוצאים סיבה, ננסה לבנות איזומורפיזם – מילת המפתח היא אומץ.

נניח f איזומורפיזם $f: G \to H$.

- $f(0)=1$ כי יחידה עוברת ליחידה.
- נסמן $f(1)=a$ ונראה מה נוכל להסיק מכך:

$$f(2)=f(1+1)=f(1)\cdot f(1)=a^2$$
$$f(3)=f(2+1)=f(2)\cdot f(1)=a^3$$

מכאן באינדוקציה:

$$\forall k \in \mathbb{N}: f(k)=a^k$$

- נוכל למצוא גם את $f\left(\frac{1}{2}\right)$:

$$a=f(1)=f\left(\frac{1}{2}+\frac{1}{2}\right)=f\left(\frac{1}{2}\right)\cdot f\left(\frac{1}{2}\right)$$

ולכן:

$$f\left(\frac{1}{2}\right)=\sqrt{a}$$

גם את $f\left(\frac{1}{3}\right)$:

$$f(1)=f\left(\frac{1}{3}+\frac{1}{3}+\frac{1}{3}\right)=f\left(\frac{1}{3}\right)\cdot f\left(\frac{1}{3}\right)\cdot f\left(\frac{1}{3}\right)\Rightarrow f\left(\frac{1}{3}\right)=a^{\frac{1}{3}}$$

ננסה להגדיר:

$$f(x)=a^x$$

בינתיים לא ראינו צורך לקבוע a מסוים, רק חייבים ש-a יהיה חיובי כדי ש-$\sqrt{a}$ יהיה מוגדר.

האם f חד-חד ערכי? כן, אם $a\neq 1$.

האם f על? כן, כי לכל $y\in\mathbb{R}_+$, ניקח $x=\log_a(y)$ ונקבל: $f(x)=a^x=a^{\log_a(y)}=y$.

האם f שומרת פעולה? נבדוק:

$$f(x_1*x_2)=f(x_1+x_2)=a^{x_1+x_2}=a^{x_1}\cdot a^{x_2}=f(x_1)\circ f(x_2)$$

ולכן בסך הכל f היא איזומורפיזם.

יחס שקילות ומחלקות שקילות

הגדרה – יחס שקילות

יחס שקילות R על קבוצה X הוא קבוצה של זוגות סדורים $R \subset X \times X$ כך שמתקיים:

רפלקסיביות – $\forall x \in X: \quad (x,x) \in R$.

סימטריות – $\forall x,y \in X \quad (x,y) \in R \Rightarrow (y,x) \in R$.

טרנזיטיביות – $\forall x,y,z \in X: \quad \begin{cases}(x,y) \in R \\ (y,z) \in R\end{cases} \Rightarrow (x,z) \in R$.

כל יחס שקילות מחלק את הקבוצה X לתתי קבוצות **זרות**. שנקראות **מחלקות שקילות**:

לכל $x_0 \in X$, נגדיר $[x] = \{x \in X: \quad (x_0,x) \in R\}$ ←מחלקת השקילות של x_0.

מתקיימת התכונה הבאה – כל שתי מחלקות שקילות הן או **שוות** או **זרות** (וכך נוצרת חלוקה של X למחלקות שקילות זרות).

משפט לגרנז'

תהי $(G,*)$ חבורה סופית, ותהי H תת-חבורה (לא ריקה) של G. אזי $|G||H|$, כלומר, מספר האיברים ב-G מתחלק במספר האיברים ב-H.

הוכחה

נגדיר יחס R על קבוצת איברי G:

$$x,y \in G, \quad (x,y) \in R \quad \Leftrightarrow \quad \exists h \in H, \quad x = h * y$$

טוענים שזה יחס שקילות.

רפלקסיביות – מתקיים $(x,x) \in R$ כי $x = e * x$ ו-$e \in H$.

סימטריות – נניח $(x,y) \in R$ אז קיים $h \in H$ כך ש-$x = h * y$.

כדי להראות ש-$(y,x) \in R$ צריך להראות שקיים $h' \in H$ כך ש-$y = h' * x$, ניקח $h' = h^{-1}$ – הוא נמצא ב-H בגלל סגירות להופכי, ומתקיים:

$$h^{-1} * x = h^{-1} * (h * y) = (h^{-1} * h) * y = y$$

טרנזיטיביות – אם $\begin{cases}(x,y) \in R \\ (y,z) \in R\end{cases}$ אז קיימים $h_1, h_2 \in H$ כך ש- $\begin{cases}y = h_1 * x \\ z = h_2 * y\end{cases}$ ואז:

$$z = h_2 * y = h_2 * (h_1 * x) = (h_2 * h_1) * x$$

אבל $h_2 * h_1 \in H$ (מסגירות) ולכן $(x,z) \in R$.

ולכן בסך הכל R יחס שקילות.

סימון

עבור $a \in G$, נסמן $[a] = Ha$.

טענה

עבור היחס שהגדרנו, כל שתי מחלקות שקילות **שוות בגודלן**.

הוכחה

תהי Ha מחלקת שקילות. נגדיר $f: H \to Ha$ בצורה הבאה: $f(x) = x * a$.

טוענים ש-f חד-חד ערכית ועל.

חד-חד ערכית – נניח $f(h_1) = f(h_2) \Leftarrow h_1 * a = h_2 * a$

$$\Downarrow$$

$$(h_1 * a) * a^{-1} = (h_2 * a) * a^{-1}$$

$$\Downarrow$$

$$h_1 = h_2$$

על – יהי $y \in Ha$. אזי קיים $h_0 \in H$ כך ש-$y = h_0 * a$. במקרה כזה, $y = f(h_0)$.

קיבלנו שלכל $a \in G$ מתקיים $|Ha| = |H|$.

ניזכר שיחס השקילות R מחלק את G למחלקות שקילות **זרות**. נניח שיש k מחלקות כאלה. הגודל של כל מחלקה הוא $|H|$ ולכן $|G| = k \cdot |H| \Leftarrow |G|$ מתחלק ב-$|H|$ כנדרש.

מסקנה 1
תהי $(G,*)$ חבורה סופית, ויהי $g \in G$.
אזי $o(g)||G|$.
הוכחה
נתבונן בקבוצה:
$$\{g, g^2, g^3, \dots, g^{o(g)} = e\}$$
קל לראות שזו תת-חבורה של G. יש בה $o(g)$ איברים ולכן לפי משפט לגרנז', $o(g)$ חייב לחלק את $|G|$.

מסקנה 2
תהי G חבורה שמספר איבריה **ראשוני**.
אזי G ציקלית וכל איבריה מלבד היחידה יוצרים שלה.
הוכחה
יהי $g \in G$. לפי המסקנה הקודמת, $o(g)||G|$. מכיוון ש- $|G|$ ראשוני, נובע מכאן ש-$o(g) = 1$ או $o(g) = |G|$, אבל $o(g) = 1$ רק עבור איבר היחידה ולכן לכל $g \neq e$, $o(g) = |G| \Leftarrow g$ יוצר של G.

מסקנה 3
יהי p ראשוני. אזי כל שתי חבורות עם p איברים הן איזומורפיות.
הוכחה
לפי מסקנה 2, כל חבורה עם p איברים היא **ציקלית** וראינו בשיעור הקודם שכל שתי חבורות ציקליות עם אותות מספר של איברים הן איזומורפיות.

הגדרה – פונקציית אוילר
יהי n מספר טבעי. **פונקציית אוילר** $\varphi(n)$ מוגדרת על-ידי:
$$\varphi(n) = \left|\{1 \le a \le n-1 \middle| n - \text{ל זר } a\}\right|$$
למשל:
$$\varphi(10) = \varphi(12) = 4$$

משפט אוילר
לכל $n \in \mathbb{N}$ ולכל a זר ל-n:
$a^{\varphi(n)} - 1$ מתחלק ב-n.
הוכחה
נתבונן בקבוצה:
$$Z_n^* = \{1 \le a \le n-1 | n - \text{ל זר } a\}$$
עם הפעולה:
$$a * b = a \cdot b(\mathrm{mod}(n))$$
מתברר שזו חבורה (תבדקו לבד).
מספר האיברים שלה הוא $\varphi(n)$.
לכן לפי מסקנה 1, לכל $a \in Z_n^*$, $o(a)|\varphi(n)$. יהי $a \in Z_n^*$, נסמן $k = \frac{\varphi(n)}{o(a)}$. נקבל:
$$a^{\varphi(n)} = a^{o(a)\cdot k} = \left(a^{o(a)}\right)^k = 1^k = 1$$
קיבלנו $a^{\varphi(n)} = 1$ במודולו $n \Leftarrow a^{\varphi(n)} - 1$ מתחלק ב-n.

שיעור 6 – משפטי לגרנז', אוילר ופרמה, המחלקה השמאלית/ימנית, חבורה נורמלית

18/12/2016

משפט לגרנז'

תהי G חבורה סופית, ותהי H תת-חבורה של G, אזי:

$$|H|\,\big|\,|G|$$

משפט אוילר

לכל n טבעי ולכל $1 \leq a \leq n-1$ שהוא **זר** ל-n, $a^{\varphi(n)}-1$ מתחלק ב-n, כאשר:

$$\varphi(n)=\left\{\begin{matrix}\text{כמות המספרים בין} \\ \text{1 ל-}(n-1)\text{ שהם} \\ \text{זרים ל-}n\end{matrix}\right\}$$

משפט פרמה

יהי p ראשוני, $1 \leq a \leq p-1$.

אזי $a^{p-1}-1$ מתחלק ב-p.

הוכחה

נשים לב שמתקיים $\varphi(p)=p-1$, לכן לפי משפט אוילר:

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

מתחלק ב-p.

תרגיל

לחשב:

$$8^{2000}\big(\mathrm{mod}(1997)\big)$$

פתרון

נשים לב ש-1997 הוא ראשוני (כדי לבדוק, מספיק לראות האם הוא מתחלק בכל ראשוני עד ל- $\sqrt{1997}\approx 44.5$ – בערך 14 בדיקות, (2,3,5,7,11,13,17,19,23,29,31,37,41,43), לכן לפי משפט פרמה:

$$8^{1997-1}=1\cdot \mathrm{mod}(1997)$$

$$8^{2000}=8^{1996+4}=\underbrace{8^{1996}}_{1\cdot \mathrm{mod}(1997)}\cdot 8^4=8^4\big(\mathrm{mod}(1997)\big)=4096\big(\mathrm{mod}(1997)\big)=102\big(\mathrm{mod}(1997)\big)$$

הגדרה – המחלקה השמאלית/הימנית

תהי G חבורה, H תת-חבורה.

עבור $a\in G$, הקבוצה $Ha=\{h*a:\quad h\in H\}$ תיקרא **המחלקה השמאלית** (left coset) של a ביחס ל-H.

בדומה, $aH=\{a*h:\quad h\in H\}$ תיקרא **המחלקה הימנית** של a ביחס ל-H.

האינדקס של תת-חבורה H של חבורה סופית G מסומן $[G:H]=\frac{|G|}{|H|}$.

מהוכחת משפט לגרנז' שראינו בשיעור הקודם נובע שאם G סופית, אז לכל $a\in G$, $|Ha|=|aH|=|H|$, ומספר המחלקות השמאליות השונות הוא $[G:H]$.

דוגמה

$G=S_3$, $H=\left\{id,\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\right\}$. ניקח $a=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$. נחשב את המחלקות של a ביחס ל-H:

$$Ha:\quad \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

ולכן:

$$Ha=\left\{\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$$

ומהצד השני:

$$aH:\quad \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$$

ולכן:

$$aH = \left\{\begin{pmatrix}1 & 2 & 3\\2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\2 & 1 & 3\end{pmatrix}\right\}$$

בדוגמה שלנו, $aH \neq Ha$.

הגדרה – גרעין ותמונה

תהיינה $(G,*), (H,\circ)$ חבורות, ויהי $f: G \to H$ הומומורפיזם.
כלומר, מתקיים $\forall x,y \in G: \quad f(x*y) = f(x) \circ f(y)$.
הגרעין של f (Kernel) הוא:

$$\ker(f) = \{x \in G: \quad f(x) = e_H\}$$

התמונה של f (Image) היא:

$$Im(f) = \{y \in H | \exists x \in G, f(x) = y\}$$

דוגמה א

$G = (\mathbb{Z}, +)$, $H = (\mathbb{Z}_k, +)$ ונגדיר $f(n) = n \cdot \mathrm{mod}(k)$.
f היא הומומורפיזם (תבדקו לבד).

$$\ker(f) = \{n \in \mathbb{Z} | k | n\} = k\mathbb{Z}$$
$$Im(f) = \mathbb{Z}_k$$

דוגמה ב

$G = (\mathbb{Z}_3, +)$, $H = (\mathbb{Z}_g, +)$, $f(x) = 3x$.
f היא הומומורפיזם.

$$\ker(f) = \{0\}$$
$$Im(f) = \{0,3,6\}$$

הגדרה – תת-חבורה נורמלית

תהי G חבורה, H תת-חבורה של G.
H תיקרא **נורמלית**, אם לכל $a \in G$:

$$Ha = aH$$

הגדרה שקולה – אם לכל $a \in G$ ולכל $h \in H$ מתקיים:

$$a * h * a^{-1} \in H$$

תרגיל לבית – להראות שההגדרות שקולות.

דוגמה א

אם G קומוטטיבית אז כל תת-חבורה H היא נורמלית.

דוגמה ב

כפי שראינו בדוגמה לעיל, אם $G = S_3$, $H = \left\{id, \begin{pmatrix}1 & 2 & 3\\1 & 3 & 2\end{pmatrix}\right\}$ אז H לא נורמלית.

דוגמה ג

אם G סופית, ו-$|H| = \frac{|G|}{2}$ אז H נורמלית.

הוכחה

נתבונן במחלקות שמאליות ביחס ל-H. ראינו שמחלקות שמאליות הן או שוות או זרות. H עצמה היא מחלקה שמאלית ולכן יש מחלקה נוספת יחידה שהיא $G \backslash H$.
יהי $a \in G$. מהי המחלקה השמאלית של a ביחס ל-H?
← אם $a \in H$ אז $Ha = H$.
← אם $a \notin H$ אז לא ייתכן $Ha = H$ כי $a \in Ha$ ולכן בהכרח $Ha = G \backslash H$.

אותם שיקולים נכונים גם ביחס למחלקות ימניות, ולכן בסך הכל נקבל:

$a \in H \quad \rightarrow \quad aH = H$

$a \notin H \quad \rightarrow \quad aH = G \backslash H$

לכן לכל a מתקיים $Ha = aH$.

ומכאן ש-H נורמלית.

<u>דוגמה ספציפית</u>

אם $G = S_3$, $H = \left\{ id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$ אזי H נורמלית ב-G.

<u>הגדרה – חבורת המנה</u>

תהי G חבורה ותהי H תת-חבורה נורמלית של G. **חבורת המנה** (Factor group) ${}^{G}/_{H}$ היא קבוצת המחלקות $\{Ha: \quad a \in G\}$ עם הפעולה $Ha \circ Hb \coloneqq H(a * b)$.

תרגיל (לא חובה) – לוודא שזו אכן חבורה.

<u>דוגמה</u>

$G = (\mathbb{Z}, +)$, $H = (k\mathbb{Z}, +)$. איך נראית ${}^{G}/_{H}$?

עבור $a \in \mathbb{Z}$:

$$Ha = \{h * a: \quad h \in H\} = \{h + a: \quad h \in k\mathbb{Z}\} = \left\{ b \in \mathbb{Z}: \begin{array}{c} \text{השארית של } b \text{ בחלוקה} \\ \text{ל-}k \text{ שווה לשארית} \\ \text{של } a \text{ בחלוקה ל-}k \end{array} \right\}$$

לכן יש בסך-הכל k מחלקות שקילות.

$$S_i = \left\{ \begin{array}{c} \text{כל השלמים שהשארית שלהם} \\ \text{בחלוקה ל-}k \text{ היא } i \end{array} \right\} \quad 0 \le i \le k - 1$$

$$Ha \circ Hb = H(a * b) = H(a + b) = \left\{ \begin{array}{c} \text{כל המספרים שהשארית שלהם} \\ \text{בחלוקה ל-}k \text{ שווה לזו של } a + b \end{array} \right\}$$

אם נשים לב, החבורה שקיבלנו בעצם "זהה" (כלומר, איזומורפית) לחבורה $\mathbb{Z}_k$.

כלומר קיבלנו ${}^{\mathbb{Z}}/_{k\mathbb{Z}} \cong \mathbb{Z}_k$ $\quad (*)$.

<u>תזכורת</u>

ראינו בתחילת השיעור את ההומומורפיזם הבא: $G = (\mathbb{Z}, +)$, $H = (\mathbb{Z}_k, +)$, $f(n) = n(\mathrm{mod}(k))$.

ראינו שמתקיים $Im(f) = \mathbb{Z}_k$, $\ker(f) = k\mathbb{Z}$.

אז $(*)$ אומר לנו שמתקיים ${}^{\mathbb{Z}}/_{\ker(f)} \cong Im(f)$.

<u>משפט ההומומורפיזם (הראשון)</u>

תהיינה G, H חבורות, ויהי $f: G \rightarrow H$ הומומורפיזם. אזי:

א. $\ker(f)$ היא תת-חבורה נורמלית G.

ב. $Im(f)$ היא תת-חבורה של H.

ג. מתקיים ${}^{G}/_{\ker(f)} \cong Im(f)$.

<u>הוכחת (חלק מ-) המשפט</u>

א. נשתמש בהגדרה השקולה של תת-חבורה נורמלי: צריך להראות שאם $a \in G$, $b \in \ker(f)$ אז מתקיים:

$$a * b * a^{-1} \in \ker(f)$$

כלומר, צריך להראות:

$$f(a * b * a^{-1}) = e_H$$

ואכן, f הומומורפיזם ולכן:

$$f(a*b*a^{-1}) = f(a)\circ f(b)\circ f(a^{-1}) = f(a)\circ e_H \circ \left(f(a)\right)^{-1} =$$
$$= f(a)\circ \left(f(a)\right)^{-1} = e_H$$

ולכן:

$$a*b*a^{-1} \in \ker(f)$$

ב. הוכחה סבירה.
ג. הוכחה סבירה.

שיעור 7 – חוגים

1/1/2017

הגדרה – חוג (ring)

חוג הוא קבוצה R עם שתי פעולות, שיסומנו $\cdot,+$, כך ש:

א) $(R,+)$ חבורה קומוטטיבית.

ב) $(R,\cdot)$ הוא אגודה.

ג) פילוג, דיסטריבוטיביות:

$$a\cdot(b+c)=a\cdot b+a\cdot c$$
$$(b+c)\cdot a=b\cdot a+c\cdot a$$

חוגים עם תכונות נוספות

נסמן $R^*=R\setminus\{0\}$ כאשר 0 איבר היחידה של $(R,+)$.

- אם $(R^*,\cdot)$ הוא **מונואיד** אז R ייקרא **חוג עם יחידה**.
- אם $(R^*,\cdot)$ הוא **חבורה** אז R ייקרא **חוג עם חילוק** (division ring).
- אם $(R^*,\cdot)$ **קומוטטיבי** אז R ייקרא **חוג קומוטטיבי**.
- חוג קומוטטיבי שהוא גם חוג עם חילוק נקרא **שדה** (field).

דוגמה א

$R=(\mathbb{N},+,\cdot)$ – לא חוג, כי אין איברים הופכיים לחיבור.

דוגמה ב

$R=(\mathbb{Z},+,\cdot)$ – זהו חוג קומוטטיבי עם יחידה, שאינו חוג עם חילוק.

דוגמה ג

$(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ – אלה שדות.

דוגמה ד

$(\mathbb{Z}_n,+,\cdot)=$ המספרים $\{0,1,\dots,n-1\}$ עם חיבור וכפל מודולו n.

לכל n, זה חוג קומוטטיבי עם יחידה.

אם n לא ראשוני – נגיד, $n=a\cdot b$ אז $\mathbb{Z}_n$ לא חוג עם חילוק, כי ל-a אין הופכי.

אם n ראשוני, נראה בהמשך שלכל איבר יש הופכי ולכן $\mathbb{Z}_n$ שדה.

דוגמה ה

$(\mathbb{Z}_p,+,\cdot)$ כאשר p ראשוני $\Leftarrow$ זהו שדה.

דוגמה ו

$(\mathbb{R}^{n\times n},+,\cdot)=$ מטריצות $n\times n$ עם פעולות חיבור וכפל מטריצות.

זהו חוג עם יחידה, שאינו קומוטטיבי ואינו חוג עם חילוק.

איבר היחידה החיבורי הוא מטריצת האפס, איבר היחידה הכפלי הוא מטריצת היחידה.

הערה – לא נוכל להפוך את החוג לחוג עם חילוק על-ידי צמצום למטריצות הפיכות בלבד, כי אז נאבד את הסגירות לחיבור.

דוגמה ז

$(\mathbb{F}[x],+,\cdot)=$ הפולינומים במשתנה אחד מעל שדה $\mathbb{F}$, עם פעילות חיבור וכפל פולינומים.

זהו חוג קומוטטיבי עם יחידה, אבל לא חוג עם חילוק, כי כמעט לכל פולינום אין הופכי כפלי.

דוגמה ח

$(\mathbb{H},+,\cdot)=$ קבוצת הקווטרניונים (quaternions):

$$\{a+bi+cj+dk|a,b,c,d\in\mathbb{R}\}$$

עם חיבור בכל קואורדינטה בנפרד, וכפל שמוגדר על-ידי:

$$\begin{cases} i^2 = j^2 = k^2 = -1 \\ ij = k, \quad ji = -k \\ jk = i, \quad kj = -i \\ ki = j, \quad ik = -j \end{cases}$$

ומורחב על-ידי דיסטריבוטיביות.
זהו חוג עם יחידה שאינו קומוטטיבי.
מתברר שזה כן חוג עם חילוק, מתקיים:

$$(a + bi + cj + dk) \cdot \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} = 1$$

הערה – הקווטרניונים הם חוג **אינסופי** שהוא עם חילוק ולא קומוטטיבי.
לא קיימת דוגמה כזו בחוגים סופיים – יש משפט של Wedderburn שאומר שכל חוג סופי עם חילוק הוא קומוטטיבי, כלומר שדה.

<u>טענה</u>
יהי $(R, +, \cdot)$ חוג. אזי לכל $x \in R$ מתקיים $x \cdot 0 = 0$.
<u>הוכחה</u>

$$\begin{aligned} x \cdot 0 = x \cdot (0 + 0) &= x \cdot 0 + x \cdot 0 \\ x \cdot 0 + \big(-(x \cdot 0)\big) &= x \cdot 0 + x \cdot 0 + \big(-(x \cdot 0)\big) \\ 0 &= x \cdot 0 \end{aligned}$$

<u>מסקנה</u>
איבר ה-0 (כלומר, היחידה החיבורית) בחוג, לעולם לא יהיה הפיך.

<u>הגדרה – מחלק אפס</u>
יהי $(R, +, \cdot)$ חוג. איבר $0 \neq a \in R$ ייקרא **מחלק אפס ימני** אם קיים $b \neq 0$ כך ש-$b \cdot a = 0$. בדומה, a ייקרא **מחלק אפס שמאלי** אם קיים $b \neq 0$ כך ש-$a \cdot b = 0$. a ייקרא **מחלק אפס דו-צדדי** (או סתם **מחלק אפס**) אם הוא מחלק אפס ימני וגם שמאלי.

<u>טענה</u>
מחלק אפס שמאלי (או ימני) אינו הפיך.
<u>הוכחה</u>
נניח שקיים b כך ש-$a \cdot b = 0$, ובכל זאת a הפיך, כלומר, קיים c כך ש-$a \cdot c = c \cdot a = 1$ (כאשר 1 מסמן את היחידה הכפלית). מתקיים:

$$b \underbrace{=}_{\text{יחידה 1 כפלית}} 1 \cdot b \underbrace{=}_{c \cdot a = 1} (c \cdot a) \cdot b \underbrace{=}_{\text{אסוציאטיביות}} c \cdot (a \cdot b) \underbrace{=}_{a \cdot b = 0} c \cdot 0 \underbrace{=}_{\text{טענה קודמת}} 0$$

וזו סתירה.
<u>מסקנה</u>
בחוג עם חילוק (ובפרט, בשדה) אין מחלקי אפס.

<u>דוגמה א</u>
ב- $\underbrace{\mathbb{H}}_{\text{קווטרניונים}}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ אין מחלקי אפס כי אלו חוגים עם חילוק.

<u>דוגמה ב</u>
ב-$\mathbb{Z}, \mathbb{F}[x]$ אין מחלקי אפס (למרות שאלה לא חוגים עם חילוק).

<u>דוגמה ג</u>
ב-$\mathbb{Z}_n$ עבור n לא ראשוני, כל מספר שאינו זר ל-n הוא מחלק אפס.
ב-$\mathbb{R}^{n \times n}$, כל מטריצה לא הפיכה היא מחלק אפס.

<u>הערה</u>
ראינו כעת שאם בחוג יש מחלק אפס, אז לא נוכל "להפוך אותו" לחוג עם חילוק על-ידי הוספה של איברים.
מתברר שאם אין מחלקי אפס, אז הרחבה כזו תמיד אפשרית. מוסיפים באופן מלאכותי איברים מהצורה $\frac{1}{r}$ לכל $r \in R$, ואז כדי לקבל סגירות לכפל, מוסיפים ביטויים מהצורה $\frac{r_1}{r_2} = r_1 \cdot \frac{1}{r_2}$ לכל $r_1, r_2 \in R$ כאשר $r_2 \neq 0$.
מתברר שהקבוצה המתקבלת (עם הפעולות מ-R) היא חוג עם חילוק, לקבוצה המתקבלת קוראים **שדה השברים של R**.
מתוך הדוגמאות שראינו לעיל, נוכל להפעיל את התהליך הזה על $\mathbb{Z}$ ועל $\mathbb{F}[x]$.
עבור $\mathbb{Z}$, נקבל:

$$\left\{\frac{m}{n} : \begin{matrix} m, n \in \mathbb{Z} \\ n \neq 0 \end{matrix}\right\}$$

כלומר, את השדה $\mathbb{Q}$!
עבור $\mathbb{F}[x]$, נקבל:

$$\left\{\frac{p(x)}{q(x)} : \begin{matrix} p(x), q(x) \in \mathbb{Z} \\ q(x) \not\equiv 0 \end{matrix}\right\}$$

זה נקרא $\mathbb{F}(x)$ שדה הפונקציות הרציונליות.

<u>**הגדרה – תחום שלמות**</u>
חוג קומוטטיבי עם יחידה וללא מחלקי אפס נקרא **תחום שלמות**.
לדוגמה – $\mathbb{Z}$, $\mathbb{F}[x]$.

שיעור 8 – חוג הפולינום ודרגתו

15/1/2017

ערך מחקר על דרך לבנות מערכת שפורצת לאימובילייזרים של רכבי יוקרה, מכרו את מסקנות המחקר לסוכנות ביון של אחת מהמדינות באיחוד האירופי.

הגדרה – חוג הפולינום

יהי $\mathbb{F}$ שדה, **חוג הפולינום** $\mathbb{F}[x]$ הוא אוסף הביטויים מהצורה:

$$\sum_{k=0}^{n} a_k x^k$$

כאשר $a_k \in \mathbb{F}$ ו-x משתנה, עם פעולות:

חיבור:

$$\left(\sum_{k=0}^{n} a_k x^k\right) + \left(\sum_{k=0}^{m} b_k x^k\right) = \sum_{k=0}^{\max(m,n)} (a_k + b_k) x^k$$

כפל:

$$\left(\sum_{k=0}^{n} a_k x^k\right) \cdot \left(\sum_{k=0}^{m} b_l x^l\right) = \sum_{k=0}^{m+n} \left(\sum_{l=0}^{k} a_l \cdot b_{k-l}\right) x^k$$

ראינו ש-$\mathbb{F}[x]$ מהווה חוג קומוטטיבי עם יחידה ביחס לפעולות אלה.

הגדרה - הדרגה

הדרגה (degree) של פולינום $p(x) = \sum a_k x^k$ היא החזקה המקסימלית k כך ש-$a_k \neq 0$.

נסכים שהדרגה של פולינום האפס היא $-\infty$.

טענה

יהיו $p(x), q(x)$ פולינומים. אזי:

א) $\deg(p+q) \leq \max\{deg(p), deg(q)\}$ ואם הדרגות של p, q לא שוות, אז מתקיים שוויון.

ב) $\deg(p \cdot q) = \deg(p) + \deg(q)$.

הוכחה

א) נניח בלי הגבלת הכלליות (without loss of generality): $n = \deg(p) \geq \deg(q) = m$, אזי:

$$\sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{m} b_k x^k = \sum_{k=0}^{m} (a_k + b_k) x^k + \sum_{k=m+1}^{n} a_k x^k$$

לכן $\deg(p+q) \leq n = \max\begin{Bmatrix}\deg(q)\\ \deg(p)\end{Bmatrix}$ וכן אם $n \neq m$ אז $\deg(p+q) = n = \max\begin{Bmatrix}\deg(q)\\ \deg(p)\end{Bmatrix}$ כי המקדם של x^n בפולינום הוא $a_n \neq 0$.

ב) מצד אחד, המקדם של x^{n+m} בפולינום $p \cdot q$ הוא $a_n \cdot b_m \neq 0$ ולכן $\deg(p \cdot q) \geq n + m$.

מצד שני, לכל $k > n + m$, המקדם של x^k ב-$p \cdot q$ הוא 0 (כי אפילו אם ניקח את החזקה הכי גדולה מכל אחד מהפולינומים p, q, עדיין נגיע רק ל-$n + m$ ולא יותר מזה) ולכן בסך הכל:

$$\deg(p \cdot q) = n + m = \deg(p) + \deg(q)$$

מסקנה

$p(x) \in \mathbb{F}[x]$ הוא **הפיך** אם ורק אם הוא מהצורה $p(x) = c$ עבור $c \neq 0$.

הוכחה

מצד אחד, אם $p(x)$ מהצורה הנ"ל, אז הוא הפיך - $q(x) = c^{-1}$ הפכי שלו.

מצד שני, נניח ש-p הפיך, אזי קיים q, כך ש:

$$p(x)\cdot q(x)=1$$

במקרה כזה, אנו יודעים:

$$0=\deg(1)=\deg(p\cdot q)=\underbrace{\deg(p)}_{\geq 0}+\underbrace{\deg(q)}_{\geq 0}$$

מכיוון שהדרגות של p,q אי-שליליות* והסכום שלהן הוא 0, חייב להתקיים $\deg(p)=\deg(q)=0$, כלומר, $p(x)=c$.

[יש לציין שיתכן גם $\deg(p)<0$ או $\deg(q)<0$ אם אחד מהם הוא פולינום האפס, אבל אנחנו יודעים שפולינום האפס אינו הפיך].

<u>טענה</u>

יהיו $a,b\in\mathbb{F}[x]$. אזי קיים זוג יחיד p,r של פולינומים, כך ש:

א) $a=b\cdot p+r$.

ב) $\deg(r)<\deg(b)$, או $r=0$.

<u>הוכחה</u>

נוכיח תחילה שקיימים p,r כאלה. נקבע b מסוים (אבל לא נדרוש עליו כלום, כך שאותו שיקול יעבוד לכל b).

נוכיח באינדוקציה על $\deg(a)$.

אם $\deg(a)<\deg(b)$, ניקח $p=0,r=a$. אכן מתקיים:

$$p\cdot b+r=a\Rightarrow 0\cdot b+a=a$$

וכן:

$$\deg(r)<\deg(b)\Rightarrow\deg(a)<\deg(b)$$

כעת, יהי $k\geq\deg(b)$ ונניח שהוכחנו את הטענה לכל $\deg(a)<k$. נוכיח עבור $\deg(a)=k$.

נסמן:

$$a=\sum_{i=0}^{k}a_ix^i\quad,\quad b=\sum_{j=0}^{l}b_jx^j$$

כאשר $l=\deg(b)$, ונגדיר:

$$c=\frac{a_k}{b_l}x^{k-l}$$

(זה אכן פולינום כי הנחנו $k\geq l$). כעת נתבונן בפולינום $a-b\cdot c$. זהו פולינום מדרגה k לכל היותר (לפי הטענה לעיל), והמקדם של x^k בו הוא:

$$a_k-b_l\cdot\frac{a_k}{b_l}=0$$

לכן הוא פולינום ממעלה קטנה מ-k. לכן לפי הנחת האינדוקציה, קיימים פולינומים p',r' כך ש:

א) $a-b\cdot c=p'\cdot b+r'$.

ב) $\deg(r')<\deg(b)$.

נעביר אגפים ונקבל:

$$a=b\cdot c+p'\cdot b+r'=b(c+p')+r'$$

ולכן נוכל לקחת $\begin{cases}p=c+p'\\ r=r'\end{cases}$ ומתקיים:

א) $a=b\cdot p+r$.

ב) $\deg(r)<\deg(b)$.

זה משלים את ההוכחה באינדוקציה.

כעת, נוכיח ש-p,r **יחידים**.

נניח שמתקיים:

$$a=p_1\cdot b+r_1=p_2\cdot b+r_2$$

כאשר:

$$\begin{matrix}\deg(r_1)\\ \deg(r_2)\end{matrix}<\deg(b)$$

נעביר אגפים ונקבל:

$$p_1 \cdot b + r_1 = p_2 \cdot b + r_2$$
$$\Downarrow$$
$$b(p_1 - p_2) = r_2 - r_1$$

נתבונן בדרגות של שני האגפים.
אגף ימין – הדרגה **קטנה** מ-$\deg(b)$.
אגף שמאל – הדרגה היא סכום של $\deg(b)$ עם $\deg(p_1 - p_2)$, לכן, אם $p_1 \neq p_2$ נקבל סתירה, כי דרגת אגף ימין קטנה מ-$\deg(b)$, ודרגת אגף שמאל לפחות $\deg(b)$.
קיבלנו שחייב להתקיים $p_1 = p_2$ ולכן אגף שמאל הוא פולינום האפס ⇐ גם אכף ימין חייב להיות פולינום האפס, כלומר $r_1 = r_2$.

■

<u>הגדרה – המחלק המשותף המקסימלי – gcd</u>

יהיו a, b פולינומים. **המחלק המשותף המקסימלי (gcd)** של a, b הוא הפולינום d בעל התכונות הבאות:
א) $d|b$, $d|a$, כלומר **השארית** r בחילוק של a ב-d היא 0 (וכן בחילוק של b ב-d).
ב) אם $d'|a$, $d'|b$ אז $\deg(d') \leq \deg(d)$.
ג) המקדם המוביל (כלומר המקדם של החזקה הגבוהה ביותר) של d הוא 1.

שיעור 9 – מחלק משותף מקסימלי (gcd), אלגוריתם אוקלידס, תת-חוג
22/1/2017

תזכורת
טענה
יהיו $a(x),b(x)\in\mathbb{F}[x]$. אזי קיימים $p(x),r(x)$ יחידים כך ש:
א) $a(x)=b(x)\cdot p(x)+r(x)$.
ב) $\deg\big(r(x)\big)<\deg\big(b(x)\big)$.

הגדרה – מחלק משותף מקסימלי – gcd
יהיו $a(x),b(x)\in\mathbb{F}[x]$. **המחלק המשותף המקסימלי (gcd)** של a,b הוא הפולינום היחיד d כך שמתקיים.
א) $d|a,b|b$, כלומר **השארית** r בחילוק של a ב-d היא 0 (וכן בחילוק של b ב-d).
ב) אם d' מקיים $d'|a$, $d'|b$, אז $\deg(d')\le\deg(d)$.
ג) המקדם המוביל (כלומר המקדם של החזקה הגבוהה ביותר) של d הוא 1.

טענה
עבור פולינומים $a(x),b(x)$, נגדיר:
$$S_{a,b}=\{c\cdot a+c'\cdot b|c,c'\in\mathbb{F}[x]\}$$
יהי $d\in S_{a,b}$ בעל דרגה מינימלית (מלבד פולינום האפס) ועם מקדם מוביל = 1, אזי:
$$d=\gcd(a,b)$$
הוכחה
נסמן את האיבר העומד בדרישות ב-d'. נחלק את a ב-d' עם שארית.
נקבל:
$$a=p\cdot d'+r$$
כאשר $\deg(r)<\deg(d')$.
הנחנו $d'\in S_{a,b}$ ולכן קיימים c,c' כך ש- $d'=c\cdot a+c'\cdot b$. כעת:
$$r=a-p\cdot d'=a-p\cdot(c\cdot a+c'\cdot b)=a-p\cdot c\cdot a-p\cdot c'\cdot b=\underbrace{a\cdot(1-p\cdot c)-b\cdot p\cdot c'}_{\in S_{a,b}}$$
קיבלנו $r\in S_{a,b}$ וכן $\deg(r)<\deg(d')$. אבל d' הוא האיבר בעל דרגה מינימלית ב-$S_{a,b}$ מלבד פולינום האפס, ולכן $r=0$.
קיבלנו $d'|a$ וכן בדומה $d'|b$. לכן אם $d=\gcd(a,b)$ אז מהגדרת gcd נובע $\boxed{\deg(d')\le\deg(d)}$.
מצד שני, $d|a$ וגם $d|b$ ולכן לכל $c,c'\in\mathbb{F}[x]$, $d|c\cdot a+c'\cdot b$ ובפרט $\boxed{d|d'}$.
אבל ראינו קודם ש- $\deg(d')\le\deg(d)$ ולכן בהכרח קיים **קבוע** α כך ש- $d=\alpha\cdot d'$. לסיום, בהכרח $\alpha=1$ כי המקדם המוביל של d שווה ל-1 וכך גם המקדם המוביל של d'.
ולכן $d'=d$, כנדרש.

■

משפט – אלגוריתם אוקלידס
יהיו $a,b\in\mathbb{F}[x]$ כך ש- $\deg(a)\ge\deg(b)>-\infty$. אזי ניתן לחשב את $\gcd(a,b)$ ביעילות בעזרת האלגוריתם הבא:
א) נקבע $r_{-1}=a,r_0=b$.
ב) נגדיר באופן רקורסיבי סדרה בצורה הבאה:
a. בהינתן r_{i-2},r_{i-1}.
b. נחלק את r_{i-2} ב-r_{i-1} עם שארית.
c. נקבל $r_{i-2}=q_i\cdot r_{i-1}+r_i$, וכך נגדיר את r_i.
ג) נעצור כאשר $r_j=0$ ואז מתקיים:
$$\gcd(a,b)=r_{j-1}$$
למעשה, זה לא בדיוק נכון, כדי לקבל gcd צריך להכפיל בקבוע כדי שהמקדם המוביל יהיה 1.
בנוסף, האלגוריתם מאפשר למצוא פולינומים $c,c'\in\mathbb{F}[x]$ כך ש- $\gcd(a,b)=c\cdot a+c'\cdot b$.

<u>הוכחה</u>
יהיה לנו נוח יותר להראות תחילה למה "בנוסף..." מתקיים.
נשים לב, שלכל אורך התהליך, נוכל להציג את r_i כצירוף של a,b. זה ברור עבור שני האיברים הראשונים.
כעת, נניח:

$$\begin{cases} r_{i-2} = c_1 \cdot a + c_2 \cdot b \\ r_{i-1} = c_3 \cdot a + c_4 \cdot b \end{cases}$$

אזי מתקיים:

$$r_i = r_{i-2} - q_i \cdot r_{i-1} = (c_1 \cdot a + c_2 \cdot d) - q_i \cdot (c_3 \cdot a + c_4 \cdot b) = \\ = a \cdot (c_1 - q_i \cdot c_3) + b \cdot (c_2 - q_i \cdot c_4)$$

בפרט, גם את $r_{j-1} \overset{?}{=} \gcd(a,b)$ נוכל לרשום כצירוף של a,b (ואנחנו רואים בדיוק כיצד לעשות את זה).
למה האלגוריתם מסתיים?
נשים לב שלכל i מתקיים $\deg(r_i) < \deg(r_{i-1})$, וכן נתון $\deg(r_0) = \deg(b)$ ולכן לאחר $(\deg(b)+1)$ צעדים לכל היותר נגיע לפולינום האפס.
לסיום, נניח $r_j = 0$. למה $r_{j-1} = \gcd(a,b)$ עד כדי הכפלה בקבוע?
נשים לב שכפי שאמרנו קודם, נוכל להציג את r_{j-1} כצירוף של a,b ולכן $r_{j-1} \in S_{a,b}$. לכן לפי הטענה הקודמת, מספיק להראות ש-r_{j-1} בעל דרגה מינימלית ב-$S_{a,b}$ פרט לפולינום האפס.
נראה ש-r_{j-1} מחלק את a ואת b, לשם כך, נראה ש-r_{j-1} מחלק את r_{j-2}, את r_{j-3} וכן הלאה עד a,b.
מתקיים $r_{j-2} = q_j \cdot r_{j-1} + r_j$. אבל $r_j = 0$, לכן $r_{j-1} | r_{j-2}$.
כעת, מתקיים:

$$r_{j-3} = \underbrace{q_{j-1} \cdot r_{j-2}}_{r_{j-1}\text{מתחלק ב}} + \underbrace{r_{j-1}}_{r_{j-1}\text{מתחלק ב}}$$

לכן גם $r_{j-1} | r_{j-3}$. נמשיך באותה צורה באינדוקציה, ונקבל ש- $r_{j-1} | r_i$ לכל $i \le j-1$, ובפרט $r_{j-1} | a$, $r_{j-1} | b$.
נותר להראות ש-r_{j-1} בעל דרגה מקסימלית בין הפולינומים שמחלקים את a,b.
ראינו ש-$r_{j-1} \in S_{a,b}$ וכן ראינו ש-$\gcd(a,b)$ בעל דרגה **מינימלית** בין כל איברי $S_{a,b}$.
לכן $\deg(r_{j-1}) \ge \deg(gcd(a,b))$ ולכן $r_{j-1} = \gcd(a,b)$ עד כדי כפל בקבוע.

<u>תרגיל</u>
לחשב $\gcd(x^3-1, x^2-1)$ ולהציג אותו כצירוף שלהם.
<u>פתרון</u>
נפעיל את אלגוריתם אוקלידס.
א) נקבע $r_{-1} = x^3 - 1, r_0 = x^2 - 1$.
ב) נחלק את r_{-1} ב-r_0 עם שארית.

$$\begin{array}{l} x \\ \overline{x^3 - 1} \big| \, x^2 - 1 \\ - \\ \underline{x^3 - x} \\ \qquad x - 1 \end{array}$$

קיבלנו:

$$x^3 - 1 = x(x^2 - 1) + (x - 1)$$

ולכן:

$$r_1 = x - 1$$
$$r_1 = 1(x^2 - 1) - x(x^2 - 1)$$

נמשיך לשלב הבא ונחלק את r_0 ב-r_1 עם שארית:

$$\begin{array}{l} x + 1 \\ \overline{x^2 - 1} \big| \, x - 1 \\ - \end{array}$$

$$\begin{array}{r} \underline{x^2 - x} \\ x - 1 \\ - \\ \underline{\underline{x - 1}} \end{array}$$

קיבלנו:

$$x^2 - 1 = (x + 1)(x - 1) + 0$$

ולכן:

$$r_2 = 0 \Rightarrow \boxed{\gcd(x^3 - 1, x^2 - 1) = r_1 = x - 1}$$

שימוש מעשי של אלגוריתם אוקלידס

נוכל להשתמש באלגוריתם אוקלידס כדי לחשב הופכי בחוג $\mathbb{Z}_n$.
כלומר, בהינתן $a \in \mathbb{Z}_n$, רוצים למצוא b כך ש-$a \cdot b = 1\big(mod(n)\big)$.
נעשה זאת כך, נפעיל את אלגוריתם אוקלידס, כדי לחשב $\gcd(a, n) = 1$ (חייב להיות 1 כי אחרת a לא הפיך).
ולהציגו כצירוף לינארי:

$$1 = c \cdot a + c' \cdot n$$

נפעיל $mod(n)$ על שני האגפים ונקבל $1 = c \cdot a\big(mod(n)\big)$, כלומר c הוא ההופכי של a במודולו n. [יש לציין ש-c אינו בין 0 ל-$n - 1$, ואז ההופכי אינו c אלא $c\big(mod(n)\big)$].

<u>הערה</u>

ניתן לחשב ולהראות שזמן הריצה של האלגוריתם הוא $O(\log(n))$ צעדים, כאשר כל צעד שקול לחילוק עם שארית מודולו n, שזה בערך $O(\log(n))$ פעולות אלמנטריות, ולכן בסך הכל זמן הריצה הוא $O(\log^2(n))$ פעולות. אלגוריתם זה משמש באופן קבוע ברוב מערכות ההצפנה מסוג public key שנמצאות בשימוש כיום.

הגדרה – תת-חוג

יהי R חוג. $S \subset R$ ייקרא תת-חוג של R אם S מהווה חוג ביחס לפעולות של R.

<u>דוגמה</u>

יהי $R = (\mathbb{Z}, +, \cdot)$. מה הם תתי החוגים של R?

<u>תשובה</u>

כל הקבוצות מסוג $k\mathbb{Z} = \{n \cdot k | n \in \mathbb{Z}\}$. מצד אחד, כל קבוצה כזו היא תת-חוג. אנחנו כבר יודעים שהיא תת-חבורה לפעולת החיבור, נותר לבדוק סגירות לכפל, ואכן אם $k|a$, $k|b$ אז $k|a \cdot b$. מצד שני, אין תתי-חוגים נוספים כי תת-חוג הוא בפרט תת-חבורה ביחס לחיבור ואנחנו יודעים שתת-החבורות היחידות ביחס לחיבור הן $k\mathbb{Z}$.

מה צריך לבדוק כדי לראות ש-S הוא תת-חוג?

1. S תת-חבורה ביחס לחיבור.
2. S סגורה ביחס לכפל (אין צורך לבדוק אסוציאטיביות ודיסטריבוטיביות כי מקבלים אותו בירושה מהחוג הגדול, אין צורך לבדוק יחידה, קומוטטיביות והופכי כי קיומם לא מובטח בחוג).

שיעור 10 – חוג המנה, משפט ההומומורפיזם הראשון לחוגים

29/1/2017

תזכורת

הגדרה – תת-חוג

יהי $(R,+,\cdot)$ חוג. תת-קבוצה $S\subseteq R$ תיקרא **תת-חוג** אם היא מהווה חוג ביחס לפעולות של R.

טענה

על מנת להראות ש-S הוא תת-חוג של R, מספיק להראות:

א) S תת-חבורה של R ביחס ל- $+$

ב) S סגורה ביחס ל- $\cdot$

שאלה

מה הם תתי החוגים של $(\mathbb{Z},+,\cdot)$?

תשובה

כל הקבוצות מהצורה:

$$k\mathbb{Z}=\{kn:\quad n\in\mathbb{Z}\}$$

הגדרה – אידאל

יהי R חוג קומוטטיבי. תת-קבוצה I תיקרא **אידאל** של R אם:

א) I תת-חבורה ביחס ל- $+$

ב) ביחס לכפל, מתקיימת תכונת שנקראת **בליעה**:

$$\forall i\in I,r\in R\quad\Rightarrow\quad i\cdot r\in I$$

הערה

אפשר להגדיר אידאל גם בחוג לא קומוטטיבי, אבל אז צריך להבדיל בין אידאל שמאלי, אידאל ימני, ואידאל דו-צדדי.

הגדרה – חוג המנה

יהי $(R,+,\cdot)$ חוג קומוטטיבי, ויהי I אידיאל של R. **חוג המנה** $R/_I$ הוא אוסף מחלקות השקילות, המתאימות ליחס:

$$a\sim b\quad\Leftrightarrow\quad a-b\in I$$

(שקל לראות שהוא יחס שקילות), עם הפעולות:

$$[a]+[b]=[a+b]$$
$$[a]\cdot[b]=[a\cdot b]$$

דוגמה

האידיאלים של $(\mathbb{Z},+,\cdot)$ הם כל הקבוצות מהצורה $k\mathbb{Z}=\{kn:\quad n\in\mathbb{Z}\}$.

כיצד נראה חוג המנה $\mathbb{Z}/_{k\mathbb{Z}}$?

יחס השקילות כאן הוא $a-b\in k\mathbb{Z}\quad\Leftrightarrow\quad a\sim b$, כלומר, $a-b$ מתחלק ב-k.

כלומר, $a\sim b$ אם ורק אם ל-a,b אותה שארית בחלוקה ל-k. לכן יש k מחלקות שקילות:

$$[0],[1],\dots,[k-1]$$

כאשר:

$$[i]=\left\{\begin{array}{c}\text{כל השלמים}\\\text{שהשארית שלהם}\\\text{בחלוקה ל- }k\text{ היא }i\end{array}\right\}$$

פעולות

$$[a]+[b]=[a+b]$$

כלומר, אם $[a]$ הם כל המספרים שהשארית שלהם בחלוקה ל-k היא a, $[b]$ הם כל המספרים שהשארית שלהם בחלוקה ל-k היא b, אז $[a+b]$ היא קבוצת המספרים שהשארית שלהם בחלוקה ל-k שווה לשארית של $a+b$.
בדומה:

$$[a]\cdot[b]=[a\cdot b]$$

בחוג שקיבלנו "איזומורפי" (="נראה אותו דבר כמו") החוג $\left(\underbrace{\mathbb{Z}_k}_{k \text{ מודולו}}, \underbrace{+}_{\text{חיבור}}, \underbrace{\cdot}_{\text{כפל}}\right)$.

<u>הגדרה – הומומורפיזם ואיזומורפיזם של חוגים</u>

יהיו $(R_1,+_1,\cdot_1)$, $(R_2,+_2,\cdot_2)$ חוגים. פונקציה $f:R_1\to R_2$ תיקרא **הומומורפיזם של חוגים** אם לכל $x,y\in R_1$ מתקיים:

א) $f(x+_1y)=f(x)+_2f(y)$.

ב) $f(x\cdot_1 y)=f(x)\cdot_2 f(y)$.

אם בנוסף f חד-חד ערכית ועל, אז f תיקרא **איזומורפיזם** של חוגים. אם קיים איזומורפיזם $f:R_1\to R_2$ נאמר שהחוגים R_1,R_2 איזומורפיזם.

<u>הגדרה – גרעין ותמונה של חוגים</u>

יהי $f:R_1\to R_2$ הומומורפיזם של חוגים אזי:

$$\ker(f)=\{x\in R_1:\quad f(x)=0\}$$
$$Im(f)=\{y\in R_2:\quad \exists x\in R_1,\quad y=f(x)\}$$

<u>משפט ההומומורפיזם הראשון לחוגים</u>

יהיו $(R_1,+_1,\cdot_1)$, $(R_2,+_2,\cdot_2)$ חוגים. ויהי $f:R_1\to R_2$ הומומורפיזם של חוגים. אזי:

א) $\ker(f)$ אידאל של R_1.

ב) $Im(f)$ תת-חוג של R_2.

ג) מתקיים $R_1/\ker(f)\cong Im(f)$.

כאשר $R_1/\ker(f)$ הוא חוג המנה עם הפעולות:

$$[x]+_3[y]=[x+_1y]$$
$$[x]\cdot_3[y]=[x\cdot_1 y]$$

<u>הוכחה חלקית</u>

א) $\ker(f)$ תת-חבורה ביחס לחיבור:
זה נובע ממשפט ההומומורפיזם הראשון לחבורות – נשים לב ש-f הוא הומומורפיזם בין החבורות $(R_1,+_1,\cdot_1)$, $(R_2,+_2,\cdot_2)$ ולכן $\ker(f)$ תת-חבורה נורמלית של $(R_1,+_1,\cdot_1)$.
נותר להוכיח בליעה לכפל. כלומר:

$$\forall x\in R,\forall y\in\ker(f),\quad x\cdot y\overset{?}{\in}\ker(f)$$

זה אכן מתקיים:

$$f(x\cdot_1 y)=f(x)\cdot_2 f(y)=f(x)\cdot_2 0=0$$

ולכן $x\cdot_1 y\in\ker(f)$.

ב) צריך להראות ש- $Im(f)$ תת-חבורה ביחס לחיבור, וסגורה ביחס לכפל.
תת-חבורה לחיבור:
כמו בסעיף א', מקבל זאת בחינם מכיוון ש-f הומומורפיזם של החבורות $(R_1,+_1,\cdot_1)$, $(R_2,+_2,\cdot_2)$.
סגירות לכפל:
אם $y_1,y_2\in Im(f)$ אז קיימים $x_1,x_2\in R_1$ כך ש- $\begin{cases}y_1=f(x_1)\\y_2=f(x_2)\end{cases}$ ואז $y_1\cdot_2 y_2=f(x_1\cdot_1 x_2)$ ולכן $y_1\cdot_2 y_2\in Im(f)$.

ג) נרצה להגדיר איזומורפיזם מ- ${}^{R_1}\!/_{\ker(f)}$ ל- $Im(f)$. נשים לב שאם $x_1, x_2 \in R_1$ ומתקיים $x_1 \sim x_2$ (כלומר $x_1 - x_2 \in \ker(f)$) אז $f(x_1) = f(x_2)$. אכן, אם נסמן $z = x_1 - x_2$ אז:

$$\underline{\underline{f(x_1)}} = f\left(x_2 +_1 \underbrace{z}_{x_1 - x_2}\right) = f(x_2) +_2 f(z) \underbrace{=}_{z \in \ker(f)} f(x_2) +_2 0 = \underline{\underline{f(x_2)}}$$

לפיכך, נגדיר את הפונקציה $g: {}^{R_1}\!/_{\ker(f)} \to Im(f)$ על-ידי:

$$g([x]) = f(x)$$

(ההגדרה אכן חוקית, כי f מעתיקה את כל איברי המחלקה לאותו מקום).

למה g חד-חד ערכית?

נניח $g([x]) = g([z])$, זה אומר שאם ניקח $x_0 \in [x]$, $z_0 \in [z]$ אז יתקיים $f(z_0) = f(x_0)$. אבל מכאן נקבל:

$$f(z_0 -_1 x_0) = f(z_0) - f(x_0) = 0$$

ולכן $z_0 -_1 x_0 \in \ker(f) \Leftarrow z_0, x_0$ באותה מחלקת שקילות, סתירה.

למה g על?

אם $y \in Im(f)$ אז קיים $x \in R_1$ כך ש- $f(x) = y$, ואז $g([x]) = y$.

כעת, נראה שמירת פעולת "חיבור", צריך להראות:

$$\forall x, z \in R_1, \quad g([x] +_3 [z]) \overset{?}{=} g([x]) +_2 g([z])$$

אגף ימין שווה ל- $f(x) + f(z)$.

עבור אגף שמאל מתקיים $[x] +_3 [z] = [x +_1 z]$ ולכן:

$$g([x] +_3 [z]) = g([x +_1 z]) = f(x +_1 z)$$

אז בעצם צריך להוכיח $f(x) +_2 f(z) = f(x +_1 z)$ וזה נכון כי f הומומורפיזם.

שמירת פעולה ב"כפל" – מוכיחים בדומה.

לכן g איזומורפיזם, כנדרש.

<u>דוגמה</u>

ניקח:

$$R_1 = (\mathbb{Z}, +, \cdot)$$

$$R_2 = \left(\underbrace{\mathbb{Z}_k}_{\text{מודולו } k}, \underbrace{+}_{\text{חיבור}}, \underbrace{\cdot}_{\text{כפל}}\right)$$

נגדיר $f: R_1 \to R_2$ על-ידי $f(n) = n\big(mod(k)\big)$.

קל לראות ש- f הומומורפיזם.

$$\ker(f) = \begin{Bmatrix} \text{כל הכפולות} \\ \text{של } k \end{Bmatrix} = k\mathbb{Z}$$

$$Im(f) = \mathbb{Z}_k$$

לכן לפי משפט ההומומורפיזם הראשון לחוגים, מתקיים:

$$\mathbb{Z}/_{k\mathbb{Z}} \cong \mathbb{Z}_k$$

כפי שראינו קודם.

<u>**שאלה**</u>

איך נראים אידאלים בחוג הפולינומים $\mathbb{F}[x]$?

ניסיונות לפתרון:

$\begin{Bmatrix} \text{אוסף הפולינומים} \\ \text{הקבועים} \end{Bmatrix}$ אמנם זה תת-חוג אבל לא אידאל כי זה לא בהכרח פולינום קבוע.

$\begin{Bmatrix} \text{אוסף הפולינומים שכל המקדמים} \\ \text{שלהם שלמים שמתחלקים ב- } k \end{Bmatrix}$ גם כן תת-חוג ולא אידאל.

תשובה (חלקית)
יהי $p(x)$ פולינום כלשהו.
אזי:

$$I = \left\{ p(x) \cdot q(x) : \begin{matrix} q(x) \\ \text{פולינום} \end{matrix} \right\}$$

[כלומר, כל הפולינומים שמתחלקים ב-$p(x)$] מהווה אידיאל של $\mathbb{F}[x]$.
הערה
נשים לב שאם $I \ni p(x)$ עבור אידיאל I כלשהו, אז בגלל בליעה, כל פולינום מהצורה $p(x) \cdot q(x)$ גם הוא נמצא ב-I. לכן I_0 הוא האידיאל **המינימלי** שמכיל את $p(x)$ והוא נקרא **האידיאל הנוצר על-ידי $\boldsymbol{p(x)}$** ומסומן $\langle p(x) \rangle$.
בתרגיל הבית נראה **שכל** אידיאל של $\mathbb{F}[x]$ הוא מהצורה $\langle p(x) \rangle$ עבור p מסויים.

שיעור 11 – אידאלים בחוג הפולינומים, שדות סופיים

5/2/2017

שאלה
אין נראים אידאלים בחוג הפולינומים $\mathbb{F}[x]$?

טענה
אם $p \in \mathbb{F}[x]$ פולינום, אז הקבוצה:
$$I(p) = \{p(x) \cdot g(x) | g(x) \in \mathbb{F}[x]\}$$
היא אידיאל בחוג $\mathbb{F}[x]$.
הוכחת הטענה – ראינו בשיעור שעבר.

טענה
כל אידיאל של $\mathbb{F}[x]$ הוא מהצורה $I(p)$ עבור איזשהו פולינום p.

יהי $p \in \mathbb{F}[x]$ פולינום. נתבונן בחוג המנה $\mathbb{F}[x]/I(p)$.
האיברים הם מחלקות שקילות של היחס:
$$q_1 \sim q_2 \quad \Leftrightarrow \quad p | (q_1 - q_2)$$
לכן מחלקות השקילות מתאימות **לשאריות האפשריות** בחלוקה בפולינום $p(x)$. כל מחלקה תהיה מהצורה:
$$[r] = \left\{ q: \begin{matrix} \text{השארית בחלוקה של} \\ q \text{ ב-} p \text{ היא } r \end{matrix} \right\}$$
אנחנו יודעים ששארית בחלוקה ל-p היא פולינום מדרגה קטנה מ-$\deg(p)$, מצד שני, כל פולינום מדרגה קטנה מ-$\deg(p)$ יכול להתקבל כשארית בחלוקה ל-p.
לכן, אם $\deg(p) = d$, אז:
$$\mathbb{F}[x]/I(p) \cong \left\{ \begin{matrix} \text{אוסף הפולינומים מדרגה} \\ \text{קטנה או שווה } d-1 \end{matrix} \right\}$$
עם פעולות חיבור **רגיל** של פולינומים וכפל פולינומים מודולו p (כלומר, כופלים ואז עושים שארית בחלוקה ל-p).

שאלה
האם בחוג $\mathbb{F}[x]/I(p)$ יש מחלקי אפס?
תשובה
תלוי האם p פריק, כלומר האם ניתן לרשום $p = p_1 \cdot p_2$ עבור פולינומים p_1, p_2 מדרגה קטנה מ-$\deg(p)$.
אם p פריק, אז בחוג $\mathbb{F}[x]/I(p)$ יש מחלקי אפס, כי $[p_1] \cdot [p_2] = [p_1 \cdot p_2] = [p] = [0]$.

טענה
אם p אי-פריק, אז כל איבר בחוג $\mathbb{F}[x]/I(p)$ הוא **הפיך**.
הוכחה
נשים לב שלכל $p_1 \neq 0$ מדרגה קטנה מ-$\deg(p)$ מתקיים:
$$\gcd(p_1, p) = 1$$
[אכן, אם $\gcd(p_1, p) = p_2$ אז נוכל לרשום $p = \frac{p}{p_2} \cdot p_2$ ואז p פריק].
לכן לפי אלגוריתם אוקלידס, קיימים פולינומים c_1, c_2 כך ש- $c_1 p_1 + c_2 p = 1$. נתבונן בשני האגפים מודולו p, ונקבל $c_1 p_1 = 1$ ולכן ההופכי של $[p_1]$ בחוג $\mathbb{F}[x]/I(p)$ הוא $[c_1]$.

מסקנה

אם p אי-פריק, אז $\mathbb{F}[x]/I(p)$ הוא **שדה**.

בינתיים, יצרנו מתכון לבניית שדות. נשתמש בו בהמשך לבנות שדות סופיים.

שדות סופיים

יהי $\mathbb{F}$ שדה. נתבונן באיבר היחידה הכפלי 1, ונסתכל על הסדרה:

$$1, \quad 1+1, \quad 1+1+1, \quad 1+1+1+1, \quad \ldots$$

נשים לב שאם האיבר 0 לא מופיע בסדרה, אז כל איבריה הם **שונים**, ולכן השדה $\mathbb{F}$ אינסופי.

לכן בשדה סופי, קיים n כך ש:

$$n \cdot 1 := \underbrace{1+1+\cdots+1}_{\text{פעמים } n} = 0$$

טענה

n המינימלי כך ש- $\underbrace{1+1+\cdots+1}_{\text{פעמים } n} = 0$ הוא **ראשוני**.

הוכחה

אם $\underbrace{1+1+\cdots+1}_{\text{פעמים } p\cdot q} = 0$ אז מפילוג אנחנו יודעים:

$$\underbrace{(1+1+\cdots+1)}_{\text{פעמים } p}\underbrace{(1+1+\cdots+1)}_{\text{פעמים } q} = 0$$

ומכיוון שאין מחלקי אפס, אחד מאלה חייב להיות 0.

הגדרה – המציין

המספר המינימלי p כך ש- $\underbrace{1+1+\cdots+1}_{\text{פעמים } p} = 0$ נקרא **המציין** של השדה $\mathbb{F}$ ומסומן $char(\mathbb{F})$. אם לא קיים מספר כזה, מסמנים $char(\mathbb{F}) = 0$.

טענה

יהי $\mathbb{F}$ שדה עם מציין p, אזי $\mathbb{F}$ מהווה מרחב וקטורי מעל השדה $\mathbb{Z}_p$.

תקציר הוכחה

פעולת החיבור היא פעולת החיבור הרגילה של $\mathbb{F}$. צריך להגדיר כפל בסקלר מתוך $\mathbb{Z}_p$. נגדיר:

$$\underbrace{k}_{0\le k\le p-1} \cdot \underbrace{x}_{\text{איבר בשדה}} = \underbrace{x+x+\cdots+x}_{\text{פעמים } k}$$

ואפשר להראות בקלות שהדרישות של מרחב וקטורי מתקיימות בזכות העובדה שלכל $x \in \mathbb{F}$ מתקיים $\underbrace{x+x+\cdots+x}_{\text{פעמים } p} = 0$.

מסקנה

אם $char(\mathbb{F}) = p$ אז קיים n כך ש- $|\mathbb{F}| = p^n$.

הוכחה

לפי הטענה הקודמת, $\mathbb{F}$ מרחב וקטורי מעל $\mathbb{Z}_p$. נסמן את מימד המרחב הזה ב-n ויהי $y_1, y_2, \ldots, y_n$ בסיס שלו. אז איברי $\mathbb{F}$ הם כל הביטויים מהצורה $c_1y_1 + c_2y_2 + \cdots + c_ny_n$ עבור $c_1, c_2, \ldots, c_n \in \mathbb{Z}_p$. יש p אפשרויות לכל מקדם ולכן בסך הכל יש p^n אפשרויות $\Leftarrow$ יש p^n איברים ב-$\mathbb{F}$.

מסקנה

אם $\mathbb{F}$ שדה סופי אז מספר האיברים ב-$\mathbb{F}$ הוא p^n עבור p ראשוני.

בנוסף, אם $|\mathbb{F}| = p^n$ אז **הסדר** של כל איבר ב-$\mathbb{F}$ הוא p (כלומר, לכל $x \in \mathbb{F}$ מתקיים $\underbrace{x + x + \cdots + x}_{p \text{ פעמים}} = 0$).

כיצד נבנה שדה עם p^n איברים?
נשתמש ב-"מתכון" שהצגנו לעיל, עם השדה $\mathbb{Z}_p$.
כלומר, מתבוננים בחוג הפולינומים $\mathbb{Z}_p[x]$.

נניח שקיים פולינום אי-פריק f מדרגה n ב-$\mathbb{Z}_p[x]$. נתבונן בשדה $\mathbb{Z}_p[x]/I(f)$. כמה איברים יש בו?
איברי השדה מתאימים לכל השאריות בחלוקה ל-f, כלומר כל הפולינומים מדרגה קטנה מ-n:
$$q(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}$$
כאשר $c_0, c_1, \dots, c_{n-1} \in \mathbb{Z}_p$.
לכל מקדם יש p אפשרויות, ולכן בסך הכל יש p^n איברים.

<u>משפט (שלא נוכיח)</u>
לכל p ולכל n, קיים פולינום אי-פריק מדרגה n מעל $\mathbb{Z}_p$.

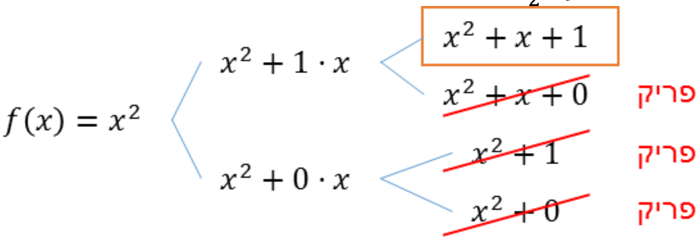
<u>מסקנה</u>
לכל n, $\underbrace{p}_{\text{ראשוני}}$ נוכל לבנות שדה סופי עם p^n איברים.

<u>משפט (שלא נוכיח)</u>
לכל n, $\underbrace{p}_{\text{ראשוני}}$ קיים שדה **יחיד** עם p^n איברים, עד כדי איזומורפיזם.

<u>דוגמה</u>
נבנה שדה עם 4 איברים.
<u>פתרון</u>
לפי המתכון שראינו, נצטרך להתבונן בשדה $\mathbb{F} = \mathbb{Z}_2$ ובפולינום אי-פריק מדרגה 2 מעל $\mathbb{Z}_2$.

הערה – נשים לב שאם פולינום מדרגה 2 או 3 הוא **פריק**, אז בהכרח יש לו שורש. לכן כדי למצוא פולינום אי-פריק מדרגה 2 או 3, נוכל לנסות כמה פולינומים, עד שנמצא אחד שאין לו שורש.

נחפש פולינום אי-פריק מדרגה 2 מעל $\mathbb{Z}_2$:



לכן אנחנו יודעים ש-$\mathbb{Z}_2[x]/I(x^2 + x + 1)$ שדה עם 4 איברים.
את האידיאל $I(x^2 + x + 1)$ לפעמים מסמנים $\langle x^2 + x + 1 \rangle$

מה הם איברי השדה?
האיברים הם $[0],[1],[x],[x+1]$.
טבלת חיבור:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

טבלת כפל:

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

כאשר:
$$x \cdot x = x^2 mod(x^2+x+1) = x+1$$

-לא בחומר-
בעיות יווניות עתיקות
1) הכפלת קובייה – לבנות קובייה שנפחה פי 2 מהנפח של קובייה נתונה.
2) ריבוע העיגול – לבנות עיגול בעל שטח כשטחו של ריבוע נתון.
3) לחלק זווית לשלושה חלקים שווים.

כל הבעיות האלו נפתרו באמצעות החומר שלמדנו.

הרחבה של שדות
יהי $\mathbb{F}$ שדה. אם $\mathbb{K}$ שדה שמכיל את $\mathbb{F}$ אז $\mathbb{K}$ ייקרא **הרחבה** של $\mathbb{F}$.
(דוגמה – השדה עם p^n איברים הוא הרחבה של השדה $\mathbb{Z}_p$ שמשוכן בו).

טענה
אם $\mathbb{K}$ הרחבה של $\mathbb{F}$ אז $\mathbb{K}$ מרחב וקטורי מעל $\mathbb{F}$.

הגדרה – מימד ההרחבה
מימד ההרחבה המסומן $[\mathbb{K}:\mathbb{F}]$ הוא המימד של $\mathbb{K}$ כמרחב וקטורי מעל $\mathbb{F}$.

משפט
אם $\mathbb{K}$ הרחבה של $\mathbb{F}$ ו-$\mathbb{F}$ הרחבה של $\mathbb{E}$, אז:
$$[\mathbb{K}:\mathbb{E}] = [\mathbb{K}:\mathbb{F}] \cdot [\mathbb{F}:\mathbb{E}]$$

הרחבה של שדה על-ידי הוספת איבר
נתון שדה $\mathbb{K}$ ואיבר $\alpha \notin \mathbb{K}$. נגדיר את $\mathbb{K}(\alpha)$ להיות השדה המינימלי שמכיל את $\mathbb{K}$ ואת α.
הרחבות כאלה מתחלקות לשני סוגי:
- הרחבה אלגברית.
- הרחבה טרנסנדנטית.

ההרחבה נקראת **אלגברית** אם קיים פולינום $p(x)$ עם מקדמים ב-$\mathbb{K}$ ש-α שורש שלו.

<u>טענה</u>
אם $\mathbb{K}(\alpha)$ הרחבה אלגברית, אז מימד ההרחבה $[\mathbb{K}(\alpha):\mathbb{K}]$ הוא הדרגה המינימלית של פולינום עם מקדמים ב-$\mathbb{K}$ ש-α שורש שלו.
אם אין פולינום כזה אז $[\mathbb{K}(\alpha):\mathbb{K}]=\infty$.

גלואה היה גאון אבל יום אחרי שהוא כתב את כל הגאונות שלו הוא מת בדו-דו-דו-דו-קרב.

מה נדרש עבור הבעיות היווניות?
1) הכפלת קובייה – לבנות את $\sqrt[3]{2}$ – בלתי אפשרי עם סרגל ומחוגה.
2) ריבוע העיגול – לבנות את π – אי אפשר לבנות.
3) לחלק זווית לשלושה חלקים שווים – $\cos(20°)$ פתרון של פולינום ממעלה 3 – אי אפשר לבנות.

בלוג שנקרא "לא מדויק".

תרגול 1 – הגדרת החבורה

6/11/2016

הגדרות

הגדרה – חבורה

הזוג הסדור $(G,*)$, כאשר G היא קבוצה ו-$*$ פעולה בינארית על G, יקרא חבורה אם מתקיימים התנאים הבאים:

1. סגירות:
$$\forall a,b \in G: \quad a*b \in G$$
2. קיבוציות:
$$\forall g_1,g_2,g_3: \quad (g_1*g_2)*g_3 = g_1*(g_2*g_3)$$
3. איבר יחידה (ניטרלי):
$$\exists e \in G: \quad \forall g \in G: \quad g*e = e*g = g$$
4. הופכי:
$$\forall g \in G, \exists h: \quad gh = hg = e$$

מונואיד הוא חבורה בלתי תנאי ההופכי.
אגודה (חבורה למחצה) היא מונואיד ללא תנאי איבר יחידה.

הגדרה – איבר הפיך, הופכי

יהא $(G,*)$ מונואיד. ו-$g,h \in G$. אם $gh = e$ אז g יקרא הפיך מימין ו-h יקרא הפיך משמאל.
אם g הוא הפיך מימין ומשמאל הוא יקרא הפיך דו-צדדי (בחבורה כל האיברים הם הפיכים דו-צדדיים). ההופכי לו יסומן g^{-1}.

הגדרה – יחידה

תהא $(G,*)$ אגודה.
אם קיים $e \in G$ כך ש- $\forall g \in G: g*e = g$ הוא יקרא יחידה משמאל. באותו אופן מגדירים יחידה מימין ודו-צדדית.

הערה

יחידה דו-צדדית היא יחידה. ההופכי הדו-צדדי הוא יחיד.

דוגמאות

1. מרחב וקטורי $(V,+)$ הוא חבורה עם יחידה 0, ההופכי ל-v הוא $(-v)$.
   א) מטריצות $\mathbb{F}^{m\times n}$ עם חיבור.
   ב) פולינומים $(\mathbb{F}_n[x], \mathbb{F}[x])$ עם חיבור.
   ג) $\mathbb{Z}_2$ עם חיבור מודולו 2.
   ד) $\mathbb{Z}_2^n$.
2. $(\mathbb{C}/\mathbb{R}/\mathbb{Q}/\mathbb{Z},+)$ הן חבורות חיבוריות עם יחידה 0. ההופכי ל-x הוא $(-x)$.
3. $(\mathbb{C}^*/\mathbb{R}^*/\mathbb{Q}^*/\mathbb{Z}^*,\cdot)$ הן חבורות כפליות עם יחידה 1. ההופכי ל-x הוא $\frac{1}{x}$.
4. $(\mathbb{N},\cdot)$ מונואיד כפלי עם יחידה 1.
5. מטריצות $\mathbb{F}^{m\times n}$ עם חיבור הן חבורה חיבורית עם יחידה מטריצת האפס. ההופכי של A היא $(-A)$.
6. מטריצות הפיכות $GL_n(\mathbb{F})$ עם כפל הן חבורה כפלית עם מטריצת היחידה. ההופכי של A היא A^{-1}.
7. הקבוצה $\mathbb{Z}_n = \{0,1,\dots,n-1\}$ עם פעולת חיבור מודולו n היא חבורה חיבורית עם יחידה 0. ההופכי של m הוא $n-m$.
   הערה – הקבוצה $\{1,\dots,n-1\}$ עם פעולת כפל מודולו n אינה בהכרח אגודה!
   למשל $\{1,2,3,4\}$ אבל $2\cdot 2 = 0$.
8. המטריצות $\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}\right\}$ עם כפל היא מונואיד כפלי עם יחידה $\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}$.
   יחידה שמאלית נוספות הן $\left\{\begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}\right\}$. אין עוד יחידות ימניות.

9. הפולינומים $(\mathbb{R}[x],\cdot)$ הן מונואיד. אין הפיך לפולינום מדרגה גדולה מאפס.
10. סדרות בינאריות עם מספר סופי של אחדים

$$X = \{(a_n)_{n\in\mathbb{N}} | \#\{n | a_n = 1\} < \infty\}$$

עם פעולת and היא אגודה בלי יחידה (אם הייתה יחידה היא הייתה צריכה להיות $(1)_{n\in\mathbb{N}}$ שלא שייכת ל-X.

11. תמורות:

$$S_3 = \{f: \{1,2,3\} \to \{1,2,3\} | f \text{ bijection}\}$$

היא חבורה עם יחידה פונקציית הזהות.

ההופכי של f היא f^{-1}. הצגות תמורות כמחזורים זרים וייצוג $\begin{pmatrix} 1 & 2 & 3 \\ * & * & * \end{pmatrix}$.

תרגול 2 – החבורה הסימטרית, מחזור

13/11/2016

הקדמה

תהא X, אזי $M = X^X = \left\{f: X \to X \middle| \underset{\text{פונקציה}}{f}\right\}$ היא מונואיד ביחס לפעולה – הרכבת פונקציות.
עם יחידה שהיא פונקציית הזהות.
עבור שתי פונקציות $f, g \in X^X$ מוגדרת ההרכבה $g \circ f \in X^X$ כך:

$$f, g \in M \Rightarrow (g \circ f)(x) = g\big(f(x)\big)$$

דוגמה

עבור $X = \{1,2,3\}$ נסתכל על הפונקציות:

$$f: 1 \to 1{,}2 \rightleftarrows 3$$
$$g: 1 \rightleftarrows 2{,}3 \to 3$$

אזי:

$$f \circ g: (1,3,2) \quad , \quad g \circ f: (1,2,3)$$

בפרט, קיבלנו ש: $g \circ f \neq f \circ g$.

דוגמה נוספת

$X = \mathbb{N}$ הטבעיים, למשל:

$$f(n) = n + 1 \quad (f \in M)$$

$$\begin{array}{ccccc} 1 \mapsto 2 & & 1 & \searrow & 1 \\ 2 \mapsto 3 & & 2 & \searrow & 2 \\ 3 \mapsto 4 & & 3 & \searrow & 3 \\ \vdots & & \vdots & \vdots & \vdots \end{array}$$

נגדיר גם את $g(n) = n^2$, ואז ההרכבה היא:

$$(g \circ f)(n) = g\big(f(n)\big) = g(n+1) = (n+1)^2$$
$$(f \circ g)(n) = g\big(g(n)\big) = f(n^2) = n^2 + 1$$

שימו לב שקיבלנו $g \circ f \neq f \circ g$, למשל:

$$(g \circ f)(2) = 9 \neq 5 = (f \circ g)(2)$$

הערה

$(M,*)$ מונואיד, אזי $M^X = \left\{a \in M \middle| \underset{\text{הפיך}}{a}\right\}$ חבורה ביחס ל-$*$ במונואיד $M = \left\{f: X \to X \middle| \underset{\text{פונקציה}}{f}\right\}$.

משפטים:

1. f חד-חד ערכית $\Leftrightarrow$ $\exists g: g \circ f = id$.
2. f על $\Leftrightarrow$ $\exists g: f \circ g = id$
3. f חד-חד ערכית + על $\Leftrightarrow$ f הפיכה.

משפט

תהא X **סופית**,
אזי $f: X \to X$ הפיכה (כלומר, חד-חד ערכית + על):
$\Leftrightarrow$ f חד-חד ערכית.
או
$\Leftrightarrow$ f על.

הערה

$id: X \to X$ המוגדרת $id(x) = x$ נקראת הזהות והיא מקיימת $id \circ f = f \circ id = f$.

הגדרה – חבורה

הזוג הסדור $(G,*)$, כאשר G היא קבוצה ו-$*$ פעולה בינארית על G, יקרא **חבורה** אם מתקיימים התנאים הבאים:

1. סגירות:

$$\forall a,b \in G: \quad a*b \in G$$

2. קיבוציות:

$$\forall g_1,g_2,g_3: \quad (g_1*g_2)*g_3 = g_1*(g_2*g_3)$$

3. איבר יחידה:

$$\exists e \in G: \forall g \in G: \quad g*e = e*g = g$$

4. הופכי:

$$\forall g \in G\ \exists h: \quad gh = hg = e$$

מונואיד הוא חבורה בלי תנאי ההופכי.

החבורה הסימטרית S_n

עבור $X=\{1,2,\dots,n\}$, הקבוצה $\{f: X \to X | f \text{ bijection}\}$ עם הרכבה, היא חבורה המסומנת כ-S_n ונקראת החבורה הסימטרית (או חבורת התמורות). היחידה בחבורה היא פונקציית הזהות.

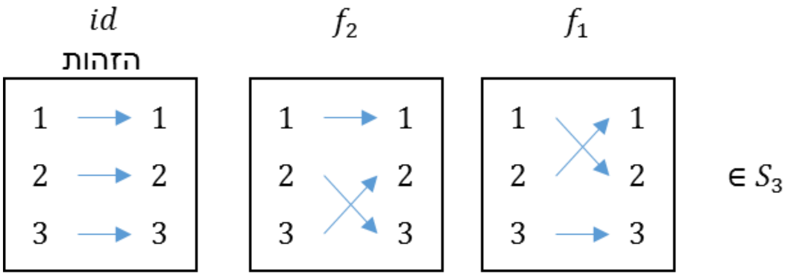
הגדרה נוספת

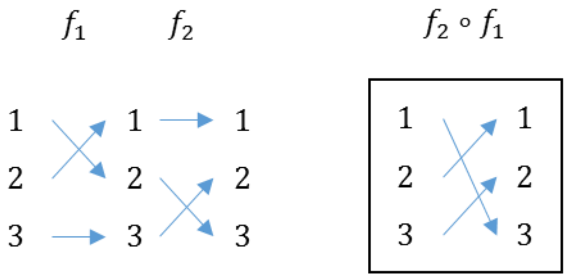
יהיא $n \in \mathbb{N}$ טבעי.

אזי $S_n = \left\{ f:\{1,\dots,n\} \to \{1,\dots,n\} \middle| \underset{\text{הפיכה}}{f} \right\}$ היא חבורה ביחס להרכבת פונקציות עם יחידה = הזהות, והיא נקראת **החבורה הסימטרית** או **חבורת התמורות**.

למשל:

$$S_3 = \left\{ f:\{1,2,3\} \to \{1,2,3\} \middle| \underset{\text{חד-חד ערכית}}{f} \right\}$$





דרכי הצגה

דרך סטנדרטית להציג תמורה היא בצורה $\begin{pmatrix} 1 & 2 & \cdots & n \\ G(1) & G(2) & \cdots & G(n) \end{pmatrix}$. דרך נוספת היא בעזרת מחזורי זרים.

נדגים זאת בעזרת S_6:

$$(12534)(6) \quad \leftrightarrow \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 1 & 3 & 6 \end{pmatrix} \in S_6$$

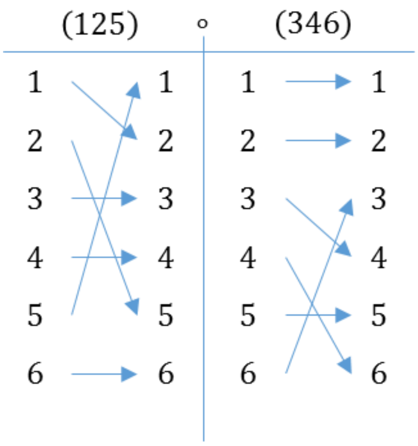
$$(125)(346) = (251)(634) \quad \leftrightarrow \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 6 & 3 & 1 \end{pmatrix} \in S_6$$

<u>הגדרה – מחזור</u>

מחזור $(i_1, i_2, \dots, i_m) \in S_n$ (כאשר $i_1, \dots, i_m$ שונים) הוא התמורה:

$$G(i_1) = i_2$$
$$G(i_2) = i_3$$
$$\vdots$$
$$G(i_{m-1}) = i_m$$
$$G(i_m) = i_1$$
$$\forall x \neq i_1, \dots, i_m: \quad G(x) = x$$

למשל:



ומתקבל:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 6 & 1 & 3 \end{pmatrix}$$

מחזורים יקראו **זרים** אם "אין להם מספר משותף".

כלומר $\begin{matrix}(i_1, \dots, i_m) \\ (i'_1, \dots, i'_m)\end{matrix}$ זרים אם $i_1, \dots, i_m, i'_1, \dots, i'_m$ מספרים שונים.

למשל:

(123) זר ל-(45) אבל (123) אינו זר ל-(24).

<u>הערה</u>

כל תמורה $\sigma \in S_n$ ניתנת להצגה כמכפלה (הרכבה) של מחזורים זרים.

<u>**משפט**</u>

מחזורים זרים מתחלפים.

כלומר, אם $\sigma_1, \sigma_2 \in S_n$ מחזורים זרים, אזי:

$$\sigma_1\sigma_2 = \sigma_2\sigma_1$$

למשל:

$$(125)(346) = (346)(125)$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 4 & 6 & 1 & 3 \end{pmatrix}$$

<u>הערות</u>

1. ההופכי של $(i_1, i_2, \dots, i_m)$ הוא $(i_m, i_{m-1}, \dots, i_1)$.
   למשל:
   $$(1,3,4)^{-1} = (4,3,1)$$
2. חישוב חזקה של מחזור:

$$S_{10} \ni (13527)^3 = (12375)$$

הערה

$$(i_1, i_2, \dots, i_m)^m = id$$

כי משלימים סיבוב מלא.

3. המחזור $(i_1, i_2, \dots, i_m)$ הוא מאורך m.
למשל, $(1,2,5)$ הוא מאורך 3. שימו לב ש $(1,2,3)^3 = id$.
4. מחזורים מאורך 1 נוהגים להשמיט בכתיב המחזורים.
למשל עבור S_6:

$$(123) = (123)(4)(5)(6)$$

5. מחזור מאורך 2 נקרא **חילוף**.
6. $(i_1, i_2, \dots, i_m) = (i_m, i_1, \dots, i_{m-1})$
למשל:

$$(1,2,3,4) = (2,3,4,1) = (3,4,1,2) = (4,1,2,3)$$

7. מתקיים כי $(i_1, i_2, \dots, i_m) = (i_1, i_2)(i_2, i_3) \dots (i_{m-1}, i_m)$ ולכן כל תמורה ניתן להציג כמכפלה של חילופים.
למשל:

$$(1,3,5,6) = (1,3)(3,5)(5,6)$$

8. אם $\sigma_1, \sigma_2, \dots, \sigma_k$ זרים, אזי:

$$(\sigma_1, \sigma_2, \dots, \sigma_k)^t = \sigma_1^t, \dots, \sigma_k^t = \underbrace{(\sigma_1, \sigma_2, \dots, \sigma_k)(\sigma_1, \sigma_2, \dots, \sigma_k) \dots (\sigma_1, \sigma_2, \dots, \sigma_k)}_{t \text{ פעמים}}$$

תרגול 3 – איברים מתחלפים, חבורה חילופית, תת-חבורה

20/11/2016

הגדרה – איברים מתחלפים

תהא $(G,\cdot)$ חבורה, $a,b\in G$ יקראו **מתחלפים** אם $a\cdot b=b\cdot a$.

למשל – מחזורים זרים ב-S_n או כל שני איברים ב-$\mathbb{Z}$.

$G=\mathbb{Z}$ אז $a=2, b=-3$ מתחלפים.

$G=S_5$ אז $\sigma_1=(1,2), \sigma_2=(4,5)$ מתחלפים.

הגדרה – חבורה חילופית

$(G,\cdot)$ תקרא **חבורה חילופית** (קומוטטיבית/אבלית) אם כל שני $a,b\in G$ איברים מתחלפים.

למשל – $\mathbb{Z},\mathbb{R}$ חילופיות.

לדוגמה S_3 אינה חילופית כי ראינו ש- $(1,2)(2,3)\neq(2,3)(1,2)$ (ולכן גם S_n עבור $n>3$ אינה חילופית).

הגדרה – תת-חבורה

תהא G חבורה, תת קבוצה $H\subseteq G$ תקרא **תת-חבורה** אם H חבורה ביחס לפעולה של G.

למשל – עבור $(G=\mathbb{Z},+)$ אז $H=3\cdot\mathbb{Z}=\{3z|z\in\mathbb{Z}\}$ היא תת-חבורה.

גם $n\cdot\mathbb{Z}=\{nz|z\in\mathbb{Z}\}$ תת-חבורה.

תזכורת

ראינו את החבורה $\mathbb{Z}_n=\{0,1,\dots,n-1\}$ עם חיבור מודולו n.

נראה הצגה שלה כ:

$$\mathbb{Z}/_{n\,\mathbb{Z}}=\{[0],[1],\dots,[n-1]\}$$

הגדרה – יחס

תהא A קבוצה, **יחס** R על A הוא תת קבוצה:

$$R\subseteq A\times A$$

סימון – $(a,a')\in R$, נסמן גם aRa'.

הגדרה – יחס שקילות

$\sim$ יחס על A יקרא **יחס שקילות** אם מתקיים:

1. $\sim$ רפלקסיבי:
$$\forall a\in A:\quad a\sim a$$
2. $\sim$ סימטרי:
$$\forall a,a'\in A:\quad a\sim a'\Rightarrow a'\sim a$$
3. $\sim$ טרנזיטיבי:
$$\forall a,a',a''\in A:\quad \left.\begin{matrix}a\sim a'\\ a'\sim a''\end{matrix}\right\}\Rightarrow a\sim a''$$

דוגמה

$A=\mathbb{Z}$ ונגדיר יחס עליה כך:

$$\forall x,y\in A:\quad x\equiv y\Leftrightarrow 3|x-y\ (\Leftrightarrow x-y\in 3\mathbb{Z})$$

הסימון $3|x-y$ אומר ש-3 "מחלק את" $x-y$, כלומר הביטוי $\frac{x-y}{3}$ הוא שלם.

הוכחה

1. רפלקסיביות:
יהא $a\in\mathbb{Z}$, צריך להוכיח $a\equiv a$, וזה אכן מתקיים:
$$3|a-a=0$$
2. סימטריות:
יהיו $x,y\in\mathbb{Z}$ כך ש-$x\equiv y$, צריך להוכיח $y\equiv x$, ואכן אם:
$$x\equiv y$$

$$\Rightarrow 3|x-y$$
$$\Rightarrow 3|y-x$$
$$\Rightarrow y \equiv x$$

<u>הגדרה – מחלקת השקילות</u>
תהא A קבוצה, N יחס שקילות עליה, ויהא $x \in A$.
נגדיר את $[x]_\sim$ – מחלקת השקילות של x ביחס ל-N:
$$[x]_\sim = \{y \in A | x \sim y\}$$

<u>דוגמה</u>
$A = \mathbb{Z}$, $\equiv$ מדוגמה קודמת, נסתכל על מספר מחלקות שקילות:
$$[0]_\equiv = \{y \in \mathbb{Z} | 0 \equiv y\} = \{0, \pm 3, \pm 6, \pm 9, \dots\} = [3]_\equiv = [6]_\equiv = \cdots$$
$$[1]_\equiv = \begin{Bmatrix} 1,4,7,10,\dots \\ -2,-5,-8,\dots \end{Bmatrix} = [4]_\equiv = [7]_\equiv = \cdots$$
$$[2]_\equiv = \begin{Bmatrix} 2,5,8,11,\dots \\ -1,-4,-7,\dots \end{Bmatrix} = [5]_\equiv = [8]_\equiv = \cdots$$
קיבלנו שיש 3 מחלקות שקילות בלבד.

<u>משפט</u>
תהא A קבוצה, ו- $\sim$ יחס שקילות (יח"ש) עליה.
אזי:
1. לכל $x, y \in A$:
$$x \sim y \Leftrightarrow [x]_\sim = [y]_\sim$$
$\Downarrow$
2. לכל שתי מחלקות שקילות $[x], [y]$ מתקיים כי:
$$[x] = [y] \quad \text{או} \quad [x] \cap [y] = \emptyset$$

<u>הגדרה – קבוצת המנה</u>
תהא A קבוצה, ו- $\sim$ יחס שקילות (יח"ש) עליה.
אזי **קבוצת המנה** היא:
$$A/_\sim = \{[x]_\sim | x \in A\}$$
והיא אוסף מחלקות השקילות.

<u>משפט</u>
קבוצת המנה $A/_\sim$ היא חלוקה של A.
כלומר:
$$A = \dot{\bigcup_x} [x]_\sim$$
(איחוד זר)

<u>דוגמה</u>
בהמשך לדוגמאות הקודמות, $A = \mathbb{Z}$ עם יחס שקילות $\equiv$ שהוגדר:
$$\mathbb{Z}/_\equiv = \{[0],[1],[2],\cancel{[3],[4]},\dots\} = \{[0],[1],[2]\}$$
$$\Downarrow$$
$$\mathbb{Z} = [0] \dot\cup [1] \dot\cup [2]$$

<u>בניה</u>
נרצה להגדיר את $\mathbb{Z}_3$ להיות:
$$\mathbb{Z}/_{3\mathbb{Z}} = \{[0]_\equiv, [1]_\equiv, [2]_\equiv\}$$
מה חסר? **פעולה**.

נרצה להגדיר:

$$[a]+[b]=[a+b]$$

האם זה מוגדר?
כלומר, האם בהינתן:

$$[a']=[a] \quad , \quad [b']=[b]$$

מתקיים:

$$[a+b]=[a'+b']$$

תשובה – כן.
<u>הוכחה</u>

$$a'\equiv a \Rightarrow 3|a'-a$$
$$b'\equiv b \Rightarrow 3|b'-b$$

נותר לשאול האם מתקיים:

$$3|a+b-(a'+b') \Leftrightarrow a+b\equiv a'+b'$$

מתוך הנתון שכתבנו נקבל:

$$3|a'-a+b'-b$$
$$\Downarrow$$
$$3|(a'+b')-(a+b)$$

ואכן מתקיים.

<u>הערה</u>
3 לא מיוחד. מגדירים באופן כללי:

$$\mathbb{Z}/_{n}\mathbb{Z}=\{[0],[1],\dots,[n-1]\} \quad , \quad (x\equiv y \Leftrightarrow n|x-y)$$
$$[a]+[b]=[a+b]$$

<u>תזכורת</u>
תהא A קבוצה. תת קבוצה $R\subseteq A\times A$ נקראת יחס על A.
<u>סימון</u>

$$(a,b)\in R \quad , \quad aRb$$

יחס יקרא:
1. רפלקסיבי, אם:

$$\forall a\in A: \quad (a,a)\in R$$

2. סימטרי, אם:

$$aRb\Rightarrow bRa$$

3. טרנזיטיבי, אם:

$$(aRb)R(bRc)\Rightarrow aRc$$

יחס המקיים את שלושת התכונות האלו נקרא **יחס שקילות**.
למשל, נגדיר יחס על $\mathbb{Z}$ בצורה הבאה:

$$x\sim y \quad \Leftrightarrow \quad 3|(x-y)$$

<u>טענה/עובדה</u>
$\sim$ הוא יחס שקילות.
למשל:

$$0\sim 3\sim 6\sim 9\sim 12$$

<u>הגדרה</u>
תהא A קבוצה, $\sim$ יחס שקילות, ו-$x\in A$.
מחלקת השקילות של x מוגדרת:

$$[x]_{\sim}=\{y\in A: x\sim y\}$$

כלומר, כל האיברים המתייחסים ל-x.
למשל, עבור היחס הקודם:

$$[0]_\sim = \{0, \pm 3, \pm 6, \dots\}$$
$$[1]_\sim = \begin{Bmatrix} 1,4,7,\dots \\ -2,-5,\dots \end{Bmatrix}$$
$$[2]_\sim = \begin{Bmatrix} 2,5,8,\dots \\ -1,-4,\dots \end{Bmatrix}$$

<u>משפט</u>

תהא A קבוצה, $\sim$ יחס שקילות עליה, ו-$x, y \in A$, אזי:

1. $x \sim y \Leftrightarrow [x] = [y]$
2. $x \nsim y \Leftrightarrow [x] \cap [y] = \emptyset$
3. $x \in [x]$

למשל, מחלקות השקילות בדוגמה הקודמת הן מחלקות השקילות היחידות, כל מספר שלם x שקול ל-0 או 1 או 2 ואז מחלקת השקילות $[x]$ היא אחת מהשלוש שצוינו.

<u>הגדרה</u>

קבוצת המנה מוגדרת:

$$A/_\sim = \{[x]_\sim : \quad x \in A\}$$

כלומר, קבוצת מחלקות השקילות.

בדוגמה הקודמת:

$$\mathbb{Z}_3 = \mathbb{Z}/_\sim = \{[0], [1], [2]\}$$

<u>משפט</u>

A היא איחוד זר של מחלקות השקילות, כלומר:

$$A = \bigcup [x]$$

(ניתן לראות בדוגמה הקודמת בדיוק זאת).

<u>הערה</u>

באופן דומה, לכל n טבעי ניתן להגדיר יחס שקילות על השלמים על-ידי:

$$x \sim y \Leftrightarrow n|(x - y)$$

ולהגדיר את קבוצת המנה כ:

$$\mathbb{Z}_n = \{0,1,2, \dots, n-1\}$$

לפעמים נרצה להפוך קבוצת מנה לחבורה, לשם כך צריך לבדוק שהפעולה שהוגדרה היא "מוגדרת היטב".

<u>דוגמה</u>

נגדיר פעולה ב-$\mathbb{Z}_n$ כך:

$$[a] + [b] = [a + b]$$

צריך לבדוק שהפעולה מוגדרת, כלומר, אם:

$$[a] = [a'], [b] = [b']$$

אזי:

$$[a + b] = [a' + b']$$

ואכן:

$$a \sim a', b \sim b' \Rightarrow n|a - a', n|b - b'$$

ואז:

$$n|(a - a') + (b - b') = (a + b) - (a' + b')$$

כלומר קיבלנו:

$$a + b \sim a' + b'$$

שזה אומר:

$$[a+b]=[a'+b']$$

כעת אחרי שיודעים שהפעולה מוגדרת, שאר האקסיומות פשוטות יותר:

1. קיבוציות נובע מקיבוציות של חיבור בשלמים.
2. $[0]$ הוא הניטרלי.
3. וההופכי גם כן מוגדר $-[a]=[-a]$.

תרגול 4 – המרכז, סדר של איבר, יוצר

27/11/2016

הגדרה – המרכז

תהא G חבורה, אזי **המרכז** שלה מוגדר:

$$C(G) = Z(G) = \{g \in G | \forall x \in G: gx = xg\}$$

למשל – $Z(\mathbb{R}) = \mathbb{R}$.

טענה

$Z(S_n) = \{id\}$ אם $n > 2$.

הוכחה

יהא $f \in Z(S_n)$, נראה כי $f(j) = j$ (כלומר id) לכל j. נניח בשלילה כי קיים j כך ש- $f(j) = i \neq j$.
מהגדרת המרכז נובע כי $fg = gf$ לכל $g \in S_n$, בפרט עבור החילוף $(i,j) - g$. נחשב:

$$fg(i) = f(j) = i$$

מצד שני:

$$g(f(i)) = \begin{cases} f(i) & f(i) \neq i,j \\ i & f(i) = j \\ j & f(i) = i \end{cases}$$

כיוון שהם שווים נקבל כי $f(i) = j$. נבחר כעת $k \neq i,j$ (אפשר כי $n > 2$) ונסתכל כעת על $h = (i,j,k)$.
נחשב:

$$fh(i) = f(j) = i$$

מצד שני:

$$hf(i) = h(j) = k$$

וקיבלנו סתירה.

דוגמה

מצאו את המרכז של $(1,2,3) \in S_n$.

פתרון

צריכים למצוא את כל $\sigma \in S_n$ המקיימות $(1,2,3)\sigma = \sigma(1,2,3)$ או באופן שקול:

$$\sigma(1,2,3)\sigma^{-1} = (1,2,3)$$

מתוך תרגילי הבית:

$$\sigma(1,2,3)\sigma^{-1} = (\sigma(1), \sigma(2), \sigma(3))$$

ולכן מהשוויון נובע:

$$(1,2,3) = (\sigma(1), \sigma(2), \sigma(3))$$

נקבל כי אם $\sigma \neq id, (1,2,3), (1,3,2) = (1,2,3)^i$ אזי בפירוק למחזורים זרים $\sigma = (1,2,3)^i\tau$ כאשר τ זר ל- $(1,2,3)$.

בניה

יהיו $(G_1,*)(G_2,\cdot)$ שתי חבורות.
אזי ניתן להגדיר את חבורת המכפלה:

$$G_1 \times G_2 = \{(g_1, g_2) | \forall i \; g_i \in G_i\}$$

עם פעולה:

$$(g_1, g_2)(g_1', g_2') = (g_1 * g_1', g_2 \cdot g_2')$$

למשל, החבורה $(\mathbb{R}^2)$:

$$\mathbb{R} \times \mathbb{R} = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \middle| x, y \in \mathbb{R} \right\}$$

$$(x, y) + (x', y') = (x + x', y + y')$$

גם לדוגמה:

$$\mathbb{R}_2 \times \mathbb{R}_3 = \{(x, y) | x \in \mathbb{R}_2, y \in \mathbb{R}_3\}$$

עם פעולה:

$$(x,y) ☯ (x',y') = \left(\underbrace{x ☯ x'}_{mod2}, \underbrace{y ☯ y'}_{mod3}\right)$$

<u>הגדרות</u>

תהא G חבורה.

1. **הסדר של G** הוא גודל הקבוצה G.
   למשל: $|S_n| = n!$.
2. לכל $g \in G$ **הסדר של g** הוא:
   $$o(g) = \min\{k \in \mathbb{N} | g^k = e\}$$
   עם המוסכמה שאם לכל $k \in \mathbb{N}$: $g^k \neq e$ אזי נסמן $o(g) = \infty$.
   למשל:
   $$A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \underbrace{GL_2(\mathbb{R})}_{\substack{\text{המטריצות ההפיכות} \\ \text{מגודל 2}}}$$
   המטריצה A מקיימת:
   $$A \neq I$$
   $$A^2 = I \Rightarrow o(A) = 2$$
   עוד דוגמה:
   $$\sigma = (i_1, \dots, i_m) \in S_n$$
   הסדר שלו הוא m כי $\sigma^m = id$, ובנוסף לכל $1 \leq k < m$ $\sigma^k \neq id$.
   דוגמה נוספת:
   $0 \in \mathbb{Z}$ הוא מסדר 1.
   $1 \in \mathbb{Z}$ הוא מסדר ∞.
3. לכל $g \in G$ נגדיר:
   $$\underbrace{\langle g \rangle}_{\substack{\text{תת החבורה הנוצרת} \\ \text{על ידי } g}} = \{g^k | k \in \mathbb{Z}\}$$
   ובנוסף, G תיקרא **ציקלית**, אם:
   $$\exists g \in G: \quad \langle g \rangle = G$$
   מינוח: אם $\langle g \rangle = G$, אזי g יקרא **יוצר**.
   למשל, $1 \in \mathbb{Z}$:
   $$\langle 1 \rangle = \left\{ \begin{matrix} 1, 1+1, 1+1+1, \dots \\ -1, -1-1, -1-1-1, \dots \end{matrix} \right\} = \mathbb{Z}$$
   $\Leftarrow$ 1 יוצר של $\mathbb{Z}$ ו-$\mathbb{Z}$ ציקלית.
   דוגמה נוספת, עבור $G = \mathbb{Z}_2 \times \mathbb{Z}_3$:

g	$o(g)$
$(0,0)$	1
$(0,1)$	3 $\big((0,1), (0,1)+(0,1), (0,1)+(0,1)+(0,1), \dots\big)$
$(0,2)$	3
$(1,0)$	2
$(1,1)$	6
$(1,2)$	6

החבורה G ציקלית כי:

$$\langle (1,1) \rangle = G$$
$$\langle (1,2) \rangle = G$$

והם שניהם יוצרים.

הערות

1. $|\langle g\rangle| = o(g)$.
2. אם G בעלת n איברים, אזי, G ציקלית $\Leftrightarrow \exists g: o(g) = n \ (= |\langle g\rangle|)$.
3. משפט
   סדר של איבר מחלק את סדר החבורה.

תרגיל

הוכיחו כי $\mathbb{Z}_n \times \mathbb{Z}_n$ $(n > 1)$ **אינה** ציקלית.

הוכחה

יהי $g = (a,b) \in \mathbb{Z}_n \times \mathbb{Z}_n$, נקבל:

$$g^n \underbrace{=}_{\text{כביכול}} \underbrace{(a,b) + (a,b) + \cdots + (a,b)}_{n \text{ פעמים}} = (na, nb) = (0,0)$$

$$\Rightarrow \forall g: o(g) \le n \neq n^2 = |\mathbb{Z}_n \times \mathbb{Z}_n|$$

תרגיל

הוכיחו כי S_n $(n \ge 3)$ אינה ציקלית.

הוכחה

לפי משפט: G ציקלית $\Leftarrow$ G חילופית.

אבל S_n אינה חילופית ולכן אינה ציקלית.

הגדרה

עבור $a, b \in \mathbb{N}$ מגדירים:

$$\gcd(a,b) = \text{המחלק המשותף המקסימלי}$$

למשל:

$$\gcd(2{,}1001) = 1$$
$$\gcd(3{,}15) = 3$$
$$\gcd(10{,}15) = 5$$
$$\underset{p \text{ ראשוני}}{\gcd}(p, 1000) = \begin{cases} p & p|1000 \\ 1 & \text{אחרת} \end{cases}$$

תרגול 5 – תתי-חבורות

4/12/2016

הגדרה – תת-חבורה

תהא G חבורה.

$G \subseteq H$ תקרא **תת-חבורה** אם H היא חבורה ביחס לפעולה של G.

למשל – עבור $G = (\mathbb{Z}, +)$:

$H = 2\mathbb{Z} = \{2 \cdot z | z \in \mathbb{Z}\}$

$H = 3\mathbb{Z} = \{2 \cdot z | z \in \mathbb{Z}\}$

$H = m\mathbb{Z} = \{m \cdot z | z \in \mathbb{Z}\}$

קריטריונים

תהא $(G,*)$ חבורה. $H \subseteq G$ תת-קבוצה, אזי H תת-חבורה:

אם ורק אם $\Leftrightarrow$:

1. $H \neq \emptyset$.
2. $\forall h_1, h_2 \in H: h_1 * h_2 \in H$.
3. $\forall h \in H: h^{-1} \in H$.

או, אם ורק אם $\Leftrightarrow$:

1. $e \in H$.
2. $\forall h_1, h_2 \in H: h_1 * h_2 \in H$.
3. $\forall h \in H: h^{-1} \in H$.

או, אם ורק אם $\Leftrightarrow$:

1. $e \in H$ (או $H \neq \emptyset$).
2. $\forall h_1, h_2 \in H: h_1 * h_2^{-1} \in H$.

הערה

אם G סופית אזי H תת-חבורה $\Leftrightarrow$:

1. $H \neq \emptyset$ (או $e \in H$).
2. $\forall h_1, h_2 \in H: h_1 * h_2 \in H$.

דוגמאות

דוגמה 1

תהא G חבורה, אזי G ו-$\{e\}$ תתי-חבורות ונקראות תתי-החבורות הטריוויאליות.

דוגמה 2

עבור מרחב וקטורי V (ההוא חבורה $(V, +)$), W שהוא תת-מרחב, הוא גם תת-חבורה.

למשל:

$$H = \left\{\begin{matrix}\text{מטריצות} \\ \text{משולשיות} \\ \text{עליוניות}\end{matrix}\right\} \underset{\substack{\text{תת} \\ \text{חבורה}}}{\leq} G = (\mathbb{F}^{n\times n}, +)$$

דוגמה 3

$G = (\mathbb{Z}_n, +)$ חבורה סופית, $H = m\mathbb{Z}_n = \{m \cdot z | z \in \mathbb{Z}_n\}$, כאשר $m \in \mathbb{Z}$.

הוכחה

1. $0 \in H$ כי $m \cdot 0 \in H$.
2. $mz_1, mz_2 \in H$ אזי $mz_1 + mz_2 = m\underbrace{(z_1 + z_2)}_{\in G} \in H$.

■

דוגמה 4

$\{e^{i\pi x} | x \in \mathbb{R}\}$ תת-חבורה של $\mathbb{R} \setminus \{0\}$ (עם כפל).

הוכחה

1. $1 \in H$ כי $1 = e^{i\pi 0} \in H$.
2. לכל $e^{i\pi x_1} \cdot e^{i\pi x_2} \in H$:

$$e^{i\pi x_1} \cdot e^{i\pi x_2} = e^{i\pi x_1 + i\pi x_2} = e^{i\pi(x_1+x_2)} \in H$$

3. לכל $e^{i\pi x} \in H$ (ההופכי הוא $e^{i\pi(-x)}$ כי $e^{i\pi x} \cdot e^{i\pi(-x)} = 1$), מתקיים:

$$\left(e^{i\pi x}\right)^{-1} = e^{i\pi(-x)} \in H$$

דוגמה 5

$\{e^{i\pi x} | x \in \mathbb{Q}\}$ גם היא תת-חבורה של $\mathbb{R} \setminus \{0\}$ (היא גם תת-חבורה של $\{e^{i\pi x} | x \in \mathbb{R}\}$).

דוגמה 6

$$\underbrace{\mathbb{Z} \leq}_{\text{תת חבורה}} \underbrace{\mathbb{Q} \leq}_{\text{תת חבורה}} \underbrace{\mathbb{R} \leq}_{\text{תת חבורה}} \mathbb{C}$$

דוגמה 7

$G = S_n$, $\left\{ \sigma \in S_n \middle| \begin{array}{c}\text{ניתן להציג את}\\ \sigma\ \text{כמכפלה של}\\ \text{מספר זוגי של}\\ \text{חילופים}\end{array} \right\} = \left\{\begin{array}{c}\text{התמורות}\\ \text{הזוגיות}\end{array}\right\} = \{\sigma \in S_n | sign(\sigma) = 1\} = H = A_n$.

דוגמה 8

יהיו G_1, G_2 חבורות.

$G = G_1 \times G_2$ חבורת המכפלה, אזי $\underbrace{H_1 \times H_2 \leq}_{\text{תת חבורה}} G_1 \times G_2$ לכל $\underbrace{H_1 \leq}_{\text{תת חבורה}} G_2$ ו- $\underbrace{H_2 \leq}_{\text{תת חבורה}} G_2$.

למשל:

$\mathbb{Z}_2 \times \mathbb{Z}_2$, מהם תתי-החבורות של $\mathbb{Z}_2$?

$$\{0\}, \{0,1\}$$

ולכן:

$$\left.\begin{array}{c}\{0\} \times \{0\}\\ \{0\} \times \mathbb{Z}_2\\ \mathbb{Z}_2 \times \{0\}\\ \mathbb{Z}_2 \times \mathbb{Z}_2\end{array}\right. \underbrace{\leq}_{\text{תת חבורה}} \mathbb{Z}_2 \times \mathbb{Z}_2$$

האם כל $H \leq G_1 \times G_2$ מהצורה $H_1 \times H_2$?

לא.

תרגול 6 – הומומורפיזם, איזומורפיזם

11/12/2016

הגדרה – הומומורפיזם, איזומורפיזם

יהיו $(G_1,*),(G_2,\circ)$ שתי חבורות.
אזי פונקציה $\phi: G_1 \to G_2$ תקרא **הומומורפיזם** אם:

$$\forall x,y \in G_1: \phi(x*y) = \phi(x)\circ\phi(y)$$

אם ϕ הפיכה ($\Leftrightarrow$ חד-חד ערכית ועל) אזי ϕ תיקרא **איזומורפיזם**.

דוגמה

$\{\pm 1\}$

0	1	-1
1	1	-1
-1	-1	1

$\mathbb{Z}_2$

$+$	0	1
0	0	1
1	1	0

וניתן לראות ש:

$$\mathbb{Z}_2 \underbrace{\cong}_{\text{איזומורפי}} \{\pm 1\}$$

והאיזומורפיזם הוא:

$$\phi: \mathbb{Z}_2 \to \{\pm 1\}$$
$$0 \to 1$$
$$1 \to -1$$

הערה

אם $\phi: G_1 \to G_2$ איזומורפיזם, אזי:

1. $\phi(e_1) = e_2$ $\left(\begin{matrix} G_1 \text{ יחידה של } e_1 \\ G_2 \text{ יחידה של } e_2 \end{matrix}\right)$.
2. לכל $x \in G_1$ מתקיים:

$$o(x) = o(\phi(x))$$

טענה

תהא $\phi: G_1 \to G_2$ איזומורפיזם של חבורות.
אם G_1 חילופית, אז גם G_2 חילופית.

הוכחה

יהיו $a,b \in G_2$, צריך להוכיח $ab = ba$.
כיוון ש-ϕ על אז:

$$\exists x,y \in G_1: \begin{matrix}\phi(x) = a \\ \phi(y) = b\end{matrix}$$
$$\Downarrow$$
$$ab = \phi(x)\phi(y) \underbrace{=}_{\text{הומומורפיזם}} \phi(xy) \underbrace{=}_{\substack{G_1 \\ \text{חילופית}}} \phi(yx) = \phi(yx) \underbrace{=}_{\text{הומומורפיזם}} \phi(y)\phi(x) = ba$$

תרגיל 1
הוכיחו כי $S_n \ncong S_m$ עבור $m \neq n$.
פתרון

$$|S_m| = m!$$
$$|S_n| = n!$$

אם $m \neq n$ אז $m! \neq n!$, בפרט לא קיימת פונקציה הפיכה מ-S_n ל-S_m.

תרגיל 2
הוכיחו כי $S_3 \ncong \mathbb{Z}_6$.
פתרון
$\mathbb{Z}_6$ חילופית.
S_3 לא חילופית.
ולכן לא איזומורפיות.

תרגיל 3
הוכיחו כי $\mathbb{Z}_4 \times \mathbb{Z}_2 \ncong (\mathbb{Z}_2)^3$.
פתרון
לכל:

$$g = (x_1, x_2, x_3, x_4) \in (\mathbb{Z}_2)^3$$

מתקיים כי:

$$o(g) \leq 2$$

אבל $(1,0) \in \mathbb{Z}_4 \times \mathbb{Z}_2$ מסדר 4.
ולכן לא איזומורפיות.

תרגיל 4
הוכיחו כי $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$.
פתרון
ראינו כי:

$$\langle 1 \rangle = \mathbb{Z}_6$$
$$\langle (1,1) \rangle = \mathbb{Z}_2 \times \mathbb{Z}_3$$

נגדיר:

$$\phi: \quad \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$$
$$\phi(1) = (1,1)$$

במפורש:

$$\phi(1) = \phi\underbrace{(1 + \cdots + 1)}_{\text{פעמים } a} = \underbrace{\phi(1) + \cdots + \phi(1)}_{\text{פעמים } a} = \underbrace{(1,1) + \cdots + (1,1)}_{\text{פעמים } a} = a(1,1) = (a,a)$$

תרגיל 5
כמה איזומורפיזמים קיימים בין $\mathbb{Z}_6$ ל-$\mathbb{Z}_2 \times \mathbb{Z}_3$?
פתרון
בדומה לתרגיל הקודם, איזומורפיזם:

$$\phi: \quad \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$$

נקבע על-ידי $\phi(1) = ?$.
ϕ איזומורפיזם $\Leftrightarrow$ $\phi(1)$ יוצר של $\mathbb{Z}_2 \times \mathbb{Z}_3$ ומספר היוצרים = 2 $\big((1,1), (1,2)\big)$.

משפט

תהא G חבורה ו-$H \le G$ תת-חבורה.

אזי $|H|\,|\,|G|$.

מסקנות

1) לכל $g \in G$ מתקיים: $o(g)\,|\,|G|$.

2) $g^{|G|} = e$.

תרגיל 6

כמה הומומורפיזמים קיימים בין $\mathbb{Z}_6$ ל-G כאשר G היא חבורה עם 6 איברים (למשל S_3)?

פתרון

כמו מקודם, אם $\phi: \mathbb{Z}_6 \to G$ הומומורפיזם, אזי הוא נקבע על-ידי $\phi(1)$.

מה שצריך לבדוק זה שהיחסים שמתקיים ב-$\mathbb{Z}_6$ מתקיימים ב-G. כלומר, אם $\phi(1) = g$ אזי צריך לבדוק:

$$\phi(a) = g^a$$

$$6 \cdot 1 = 0 \quad \overset{?}{\Rightarrow} \quad g^6 = e$$

זה מתקיים כי לכל $g \in G$:

$$e = g^{|G|} = g^6$$

$\Leftarrow$ לכל $g \in G$ נקבע $\phi(1) = g$ וזה יגדיר הומומורפיזם שונים $\Leftarrow$ קיימים 6 הומומורפיזם.

למשל, עבור $\phi: \mathbb{Z}_6 \to \mathbb{Z}_3$:

$$1 \longrightarrow (1,2) \in S_3$$
$$2 \longrightarrow (1,2)^2 = id$$
$$3 \longrightarrow (1,2)^3 = (1,2)$$
$$4 \longrightarrow (1,2)^4 = id$$
$$5 \longrightarrow (1,2)^5 = (1,2)$$
$$6 \longrightarrow (1,2)^6 = id$$
$$\|$$
$$0 \longrightarrow (1,2)^0 = id$$

תרגיל 7

כמה הומומורפיזם קיימים עבור $\phi: \mathbb{Z}_n \to \mathbb{Z}$.

פתרון

כמו קודם, $\phi(1) = a$ קובע את ϕ.

$$\Downarrow$$
$$\phi(2) = 29$$
$$\phi(3) = 39$$
$$\vdots$$
$$0 = \phi(0) = \phi(n) = n \cdot a$$
$$\Downarrow$$
$$\phi(1) = 0$$
$$\Downarrow$$
$$\phi(2) = 0$$
$$\phi(3) = 0$$
$$\vdots$$

תרגיל 8
תהא G חבורה סופית.
$H_1 \leq G$ תת-חבורה $|H_1| = n_1$.
$H_2 \leq G$ תת-חבורה $|H_2| = n_2$.
אם n_1, n_2 זרים, אזי $H_1 \cap H_2 = \{e\}$.
פתרון
$H_1 \cap H_2 \leq H_1$ תת-חבורה.
$H_1 \cap H_2 \leq H_2$ תת-חבורה.
מתוך משפט לגרנז' נקבל:

$$|H_1 \cap H_2| \big| n_1$$
$$|H_1 \cap H_2| \big| n_2$$

כיוון ש-n_1, n_2 זרים, נקבל כי:

$$|H_1 \cap H_2| = 1$$

כיוון ש-$e \in H_1 \cap H_2$ נקבל ש- $H_1 \cap H_2 = \{e\}$.

תרגול 7 – תת-חבורה נורמלית

18/12/2016

הגדרה – תת-חבורה נורמלית

תהא G חבורה.
$H \subseteq G$ תת-חבורה, תקרא **תת-חבורה נורמלית** (תח"נ) אם:
$$\forall g \in G: \quad gH = Hg$$

הערה

H תת-חבורה נורמלית
$\Leftrightarrow \forall g \in G: \quad gHg^{-1} = H$
$\Leftrightarrow \forall g \in G: \quad gHg^{-1} \subseteq H$
$\Leftrightarrow \forall g \in G, h \in H: \quad ghg^{-1} = H$

דוגמאות

1. $G \leq G$, $\{e\}$ תת-חבורה נורמלית.
2. $G = S_4$ תת-חבורה נורמלית של G שהן:
א. S_4.
ב. $\{e\}$.
ג. $A_4 = \{\sigma \in S_4 | sign(\sigma) = 1\}$ – התמורות הזוגיות.
ד. $k = \{(i_1, i_2)(i_3, i_4) | \{i_1, i_2, i_3, i_4\} = \{1,2,3,4\}\} \cup \{id\}$, כלומר:
$$k = \{(1,2)(3,4), (1,3)(2,4), (1,4)(2,3), id\}$$

נוכיח נורמליות של תת-חבורות אלו:
א. $\forall \sigma \in S_4: \quad \sigma \cdot S_4 = S_4$.
$\subseteq$:
יהא $\sigma\tau \in \sigma S_4$, אז $\sigma\tau \in S_4$ כי הרכבה של תמורות היא תמורה.
$\supseteq$:
תהא $\tau \in S_4$ אז $\sigma^{-1}\tau \in S_4 \Leftarrow$ $\underbrace{\sigma \cdot (\sigma^{-1}\tau)}_{\tau} \in \sigma S_4$.
באותו אופן $S_4 \cdot \sigma = S_4$ ולכן $\sigma S_4 = S_4 \sigma$ ולכן S_4 תת-חבורה נורמלית.
ב. $\forall \sigma \in S_4: \quad \sigma \cdot \{e\} = \{\sigma\} = \{e\} \cdot \sigma \Leftarrow$ $\{e\}$ תת-חבורה נורמלית.
ג. $|S_4| = 4! = 24$, $|A_4| = \frac{4!}{2} = 12$ $\Leftarrow$ $\frac{|S_4|}{|A_4|} = 2$ $\Leftarrow$ A_4 תת-חבורה נורמלית.
ד. יהא $\sigma \in S_4$, $\tau \in k$, ונראה כי $\sigma\tau\sigma^{-1} \in k$.
אם $\tau = id$ אזי $\sigma\tau\sigma^{-1} \in k$.
אם $\tau = (1,2)(3,4)$ אזי:
$$\sigma\tau\sigma^{-1} = \sigma(1,2)(3,4)\sigma^{-1} = \sigma(1,2)\sigma^{-1}\sigma(3,4)\sigma^{-1} =$$
$$= \big(\sigma(1), \sigma(2)\big)\big(\sigma(3), \sigma(4)\big) \in k$$
וזאת כי:
$$\{\sigma(1), \sigma(2), \sigma(3), \sigma(4)\} = \{1,2,3,4\}$$
כי σ תמורה.

תרגיל

מצאו חבורה G כך ש:
1. $\forall g \in G: \quad o(g) < \infty$.
2. $\nexists n \in \mathbb{N}: \quad \forall g \in G: \quad g^n = e$.

פתרון

הקדמה – אם G חבורה, $H \leq G$ תת-חבורה נורמלית, אז:
$$G/_H = \{gH | g \in G\}$$

היא חבורה ביחס לפעולה:

$$(g_1H)(g_2H) = (g_1g_2)H$$

והיא נקראת חבורה המנה.

למשל, $\mathbb{Q}$ חבורה, $\mathbb{Z} \leq \mathbb{Q}$ תת-חבורה נורמלית, כי $\mathbb{Q}$ חילופית $\Leftarrow$

$$\forall q \in \mathbb{Q}: \quad q + \mathbb{Z} = \{q + x | x \in \mathbb{Z}\} = \{x + q | x \in \mathbb{Z}\} = \mathbb{Z} + q$$

נגדיר $G = {}^{\mathbb{Q}}/_{\mathbb{Z}}$.

<u>טענה</u>

לכל $q + \mathbb{Z} \in G$ הסדר סופי.

<u>הוכחה</u>

יהא $q + \mathbb{Z} \in G$, אזי:

$$\exists a, b \in \mathbb{Z}: \quad q = \frac{a}{b}$$

$$\underbrace{(q + \mathbb{Z}) + (q + \mathbb{Z}) + \cdots + (q + \mathbb{Z})}_{b \text{ פעמים}} =$$

$$= \underbrace{(q + q + \cdots + q)}_{b \text{ פעמים}} + \mathbb{Z} = a + \mathbb{Z} = 0 + \mathbb{Z} = e$$

$$a + \mathbb{Z} = \begin{Bmatrix} a + 0, a + 1, a + 2, \dots \\ a - 1, a - 2, a - 3, \dots \end{Bmatrix} = \mathbb{Z}$$

<u>טענה</u>

לא קיים $n \in \mathbb{N}$ כך ש- $\forall g \in G: \quad g^n = e$.

<u>הוכחה</u>

נניח בשלילה כי קיים $n \in \mathbb{N}$ כך ש:

$$\forall g \in G: \quad g^n = e$$

בפרט, עבור $\frac{1}{n+1} + \mathbb{Z}$:

$$\mathbb{Z} = \underbrace{\left(\frac{1}{n+1} + \mathbb{Z}\right) + \cdots + \left(\frac{1}{n+1} + \mathbb{Z}\right)}_{n \text{ פעמים}} = \frac{n}{n+1} + \mathbb{Z}$$

וזה גורר ש:

$$\frac{n}{n+1} \in \mathbb{Z}$$

וזו סתירה↯.

תרגול 8 – חוגים

1/1/2017

הגדרה

חוג הוא שלישיה $\Big(\underbrace{R}_{\text{קבוצה}}\ ,\ \underbrace{+,\cdot}_{\text{פעולות}}\Big)$ המקיימת:

1) $(R,+)$ חבורה חילופית:
   א) $r_1+r_2\in R$.
   ב) $(r_1+r_2)+r_3=r_1+(r_2+r_3)$.
   ג) $\exists 0\in E$.
   ד) $\forall r\in R: \exists(-r)\in R$.
   ה) $r_1+r_2=r_2+r_1$.
2) $(R,\cdot)$ אגודה:
   א) $r_1\cdot r_2\in R$.
   ב) $(r_1\cdot r_2)\cdot r_3=r_1\cdot(r_2\cdot r_3)$.
3) פילוג:

$$r_1\cdot(r_2+r_3)=r_1\cdot r_2+r_1\cdot r_3$$
$$(r_1+r_2)\cdot r_3=r_1\cdot r_3+r_2\cdot r_3$$

דוגמאות

1. $\mathbb{Z}$ – השלמים.
2. $\mathbb{Z}_n$ – שלמים מודולו n.

הערה

בכל חוג R מתקיים כי:

$$\forall r\in R:\quad \begin{matrix}0\cdot r=0\\ r\cdot 0=0\end{matrix}$$

חוגים מיוחדים

חוג חילופי

הוא חוג $(R,+,\cdot)$ המקיים:

$$\forall r_1,r_2\in R:\quad r_1\cdot r_2=r_2\cdot r_1$$

דוגמאות

1. $\mathbb{Z}$ חוג חילופי.
2. $\mathbb{R}^{n\times n}$ חוג שאינו חילופי.

חוג עם יחידה

הוא חוג $(R,+,\cdot)$ המקיים:

$$\exists 1\in R:\quad \forall r\in R:\quad r\cdot 1=1\cdot r=r$$

דוגמאות

1. $\mathbb{Z}$ חוג עם יחידה.
2. $2\mathbb{Z}$ חוג ללא יחידה.
3. $\left\{\begin{pmatrix}0 & a\\ 0 & 0\end{pmatrix}\middle| a\in\mathbb{R}\right\}$ חוג ללא יחידה.
4. $\left\{\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}\middle| a\in\mathbb{R}\right\}$ חוג עם יחידה (היחידה היא $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$).

חוג עם חילוק

הוא חוג עם יחידה $(R,+,\cdot)$ המקיים:

$$\forall r\in R:\quad \exists s\in R:\quad \begin{matrix}r\cdot s=1\\ s\cdot r=1\end{matrix}$$

סימון $s = r^{-1}$.

<u>דוגמאות</u>

1. $\mathbb{Z}$ חוג שאינו חוג עם חילוק.
2. $\mathbb{Q}$ הוא חוג עם חילוק.

<u>שדה</u>

הוא חוג עם חילוק שהוא גם חוג חילופי.

<u>דוגמאות</u>

1. $\mathbb{R}$ הוא שדה.
2. $\mathbb{Q}$ הוא שדה.
3. $\mathbb{Z}$ אינו שדה.
4. $\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in \mathbb{R}\right\}$ הוא שדה.
5. $\{a \cdot I | a \in \mathbb{R}\}$ הוא שדה.

<u>בניה</u>

יהא R חוג חילופי, אז $R[x]$ – חוג הפולינומים מעל R הוא חוג חילופי.
למשל – $R = \mathbb{Z}_4$ הוא חוג חילופי, לכן $\mathbb{Z}_4[x]$ הוא חוג חילופי.

<u>תרגיל 1</u>

הראו כי ב-$\mathbb{Z}_4[x]$ מתקיים כי:

1. $1 + 2x$ הפיך.
2. $2x$ אינו הפיך.

<u>פתרון</u>

סעיף 1:

$$(1 + 2x)^2 = (1 + 2x)(1 + 2x) = 1 + 2x + 2x + 4x^2 =$$
$$= 1 + \underbrace{4}_{\equiv 0} x + \underbrace{4}_{\equiv 0} x^2 = 1$$

סעיף 2:

נראה כי ל-$2x$ אין הפיך, נניח בשלילה כי קיים לו הפיך:

$$\exists p(x) \in \mathbb{Z}_4[x]: \quad 2x \cdot p(x) = 1$$

נכפיל ב-2 משני צדדי המשוואה:

$$0 = \underbrace{2 \cdot 2}_{=4 \equiv 0} x \cdot p(x) = 2 \cdot 1 = 2$$

וזו סתירה↯.

<u>תרגיל 2</u>

יהא R חוג המקיים:

$$\forall x \in R: \quad x^2 = x$$

הוכיחו כי R חילופי, כלומר:

$$\forall a, b \in R: \quad a \cdot b = b \cdot a$$

<u>פתרון</u>

יהיו $a, b \in R$, צריך להוכיח $a \cdot b = b \cdot a$:

$$a + b \underbrace{=}_{\text{נתון}} (a + b)^2 = a^2 + a \cdot b + b \cdot a + b^2 \underbrace{=}_{\text{נתון}} a + a \cdot b + b \cdot a + b$$

נחבר $(-a), (-b)$ לשני האגפים ונקבל:

$$0 = a \cdot b + b \cdot a$$
$$\Rightarrow a \cdot b = -(b \cdot a)$$

$$\Rightarrow a\cdot b \underbrace{=}_{\text{נתון}} (a\cdot b)^2 = [-(b\cdot a)]^2 \underbrace{=}_{\text{נתון}} (b\cdot a)^2 \underbrace{=}_{\text{נתון}} b\cdot a$$

■

ניתן מספר דוגמאות ל-R המקיים:

$$\forall x\in R:\quad x^2=x$$

1. $\mathbb{Z}_2$:

$$1^2=1$$
$$0^2=0$$

2. $\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2=(\mathbb{Z}_2)^3$, למשל:

$$(1,0,1)^2=(1^2,0^2,1^2)=(1,0,1)$$

3. $(\mathbb{Z}_2)^n$ לכל n טבעי:

$$(a_1,\dots,a_n)^2=(a_1^2,\dots,a_n^2)=(a_1,\dots,a_n)$$

תרגול 9 – חוג הפולינומים, פולינום ראשוני, פולינום פריק ואי-פריק

15/1/2017

תזכורת

שבוע הבא – בוחן.

משפט

יהא $\mathbb{F}$ שדה, $\mathbb{F}[x]$ חוג הפולינומים מעליו.
לכל $a(x), b(x) \in \mathbb{F}[x]$ (עם $b(x) \neq 0$) קיימים $q(x), r(x)$ יחידים, כך ש:
1. $a = q \cdot b + r$.
2. $\deg(r) < \deg(b)$ או $r = 0$.

הגדרה

עבור $a(x), b(x) \in \mathbb{F}[x]$ נסמן $d(x) = \gcd\big(a(x), b(x)\big)$, פולינום מתוקן המקיים:
1. $d|a, b$.
2. לכל d' המקיים $d'|a, b$ אזי $\deg(d') \leq \deg(d)$.

לגבי מתוקן הכוונה היא שהמקדם של החזקה הגבוהה הוא 1, למשל:
$x^5 + 2x + 5$ מתוקן.
$2x^5 + 2x + 5$ לא מתוקן.

הערה/משפט

$\gcd\big(a(x), b(x)\big)$ קיים והוא יחיד.
בנוסף קיימים $m(x), n(x)$ כך ש:

$$\gcd\big(a(x), b(x)\big) = a(x) \cdot m(x) + b(x) \cdot n(x)$$

תרגיל 1

ב-$\mathbb{R}[x]$:

$$a(x) = 1 + x^2 + x^4 + x^5 + x^6$$
$$b(x) = 1 + x + x^3$$

חלקו את $a(x)$ ב-$b(x)$.
מצאו $\gcd\big(a(x), b(x)\big)$ והציגו אותו כצירוף ליניארי שלהם.

פתרון

$$\begin{array}{l} \underline{x^3 + x^2 - 2 \qquad\qquad} \\ x^6 + x^5 + x^4 + x^2 + 1 \,|\, x^3 + x + 1 \\ - \\ \underline{x^6 + x^4 + x^3} \\ \qquad x^5 - x^3 + x^2 + 1 \\ \qquad - \\ \qquad \underline{x^5 + x^3 + x^2} \\ \qquad\quad -2x^3 + 1 \\ \qquad\quad - \\ \qquad\quad \underline{-2x^3 - 2x - 2} \\ \qquad\qquad\quad 2x + 3 \end{array}$$

כאשר $2x + 3$ היא השארית, שדרגתה קטנה ממש מדרגת $b(x)$.
נמשיך ל-$\gcd(a(x), b(x)$:

$$\underbrace{x^6+x^5+x^4+x^2+1}_{a(x)}=\underbrace{(x^3+x^2-2)}_{q_1(x)}\underbrace{(x^3+x+1)}_{b(x)}+\underbrace{(2x+3)}_{r_1(x)}$$

$$\underbrace{x^3+x+1}_{b(x)}=\underbrace{\left(\frac{1}{2}x^2-\frac{3}{4}x+\frac{13}{8}\right)}_{q_2(x)}\underbrace{(2x+3)}_{r_1(x)}+\underbrace{\left(-\frac{31}{8}\right)}_{r_2(x)}$$

$$2x+3=\left(-\frac{16}{31}x-\frac{24}{31}\right)\left(-\frac{31}{8}\right)+(0)$$

כאשר gcd = השארית שלפני שארית 0 + לתקן אותו $(r_2(x))$.

במקרה שלנו gcd = תיקון של $\frac{31}{8}$ = 1.

נמצא צירוף ליניארי = gcd באמצעות "קילוף אחורה":

$$-\frac{31}{8}=b(x)-q_2(x)\cdot r_1(x)=$$
$$=b(x)-q_2(x)\cdot\big(a(x)-q_1(x)\cdot b(x)\big)=$$
$$=-q_2(x)\cdot a(x)+\big(1+q_2(x)\cdot q_1(x)\big)\cdot b(x)$$
$$\Downarrow$$
$$1=\gcd=\frac{8}{-31}\cdot\frac{-31}{8}=\frac{8}{31}q_2(x)\cdot a(x)+\frac{8}{-31}\big(1+q_1(x)\cdot q_2(x)\big)\cdot b(x)$$

הגדרה – פולינום ראשוני

פולינום $p(x)\in\mathbb{F}[x]$ מדרגה גדולה מ-0, יקרא **ראשוני**, אם:

$$\forall a(x),b(x):\quad p|a\cdot b\quad\Rightarrow\quad[p|a\quad\vee\quad p|b]$$

הגדרה – פולינום פריק / אי-פריק

פולינום $p(x)\in\mathbb{F}[x]$ מדרגה גדולה מ-0 יקרא **פריק** אם קיימים $a(x),b(x)$ מדרגה קטנה **ממש** מ-$p(x)$ כך ש:

$$p(x)=a(x)\cdot b(x)$$

בנוסף, $p(x)$ יקרא **אי-פריק** אם הוא לא פריק.

תרגיל 2

הוכיחו/הפריכו:

יהא $p(x)\in\mathbb{F}[x]$ פולינום מדרגה גדולה מ-0. אזי:

p ראשוני $\Leftrightarrow$ p אי-פריק

הוכחה

$(\Rightarrow)$ – בשיעורי בית.

$(\Leftarrow)$ נתון p ראשוני. צריך להראות p אי-פריק.

נניח $p(x)=a(x)\cdot b(x)$, צריך להראות:

$$\deg(a)=\deg(p)\quad\text{או}\quad\deg(b)=\deg(p)$$

מתוך ההנחה שלנו:

$$p|a\cdot b$$
$$\Downarrow$$
$$p|a\quad\text{או}\quad p|b$$

מתוך צד ימין:

$$p|a\Rightarrow\exists g:a=gp\Rightarrow\deg(p)\le\deg(a)$$

אבל מתוך ההנחה ראינו ש- $\deg(p) \geq \deg(a)$, ולכן:

$$\deg(p) = \deg(a)$$

ובדומה נקבל עבור צד ימין ש:

$$\deg(p) = \deg(b)$$

והוכחנו.

$$\blacksquare$$

טענה

ב-$\mathbb{F}[x]$ נסמן:

$$X = \begin{Bmatrix} \text{הפולינומים} \\ \text{הראשוניים} \end{Bmatrix}$$

אזי לכל $0 \neq f(x) \in \mathbb{F}[x]$ קיים $S \subseteq X$, $c \in \mathbb{F}$, כך ש:

$$f(x) = c \cdot \prod_{p(x) \in D} p(x)$$

הוכחה

באינדוקציה על $\deg(f) = n$:

$n = 0$:

$f(x) = c \in \mathbb{F}$ ואז $S = \emptyset$, ו-$f(x) = c$.

נניח נכונות עד n לא כולל ונוכיח נכונות עבור n.

יהא $f(x)$ מדרגה n.

עבור $f(x)$ ראשוני:

$$S = \{f(x)\}, c = 1$$

וסיימנו.

עבור $f(x)$ לא ראשוני $\Leftarrow$ f פריק:

$$\exists a, b: \quad f = a \cdot b$$

כאשר a, b מדרגה קטנה מ-n.

לפי הנחת האינדוקציה קיימים $S_1, S_2 \subseteq X$ ו-$c_1, c_2 \in \mathbb{F}$ כך ש:

$$a(x) = c_1 \cdot \prod_{p \in S_1} p$$

$$b(x) = c_2 \cdot \prod_{p \in S_2} p$$

$$\Downarrow$$

$$p(x) = a(x) \cdot b(x) = c_1 \cdot c_2 \cdot \prod_{p \in S_1} p \cdot \prod_{p \in S_2} p$$

ונגדיר:

$$S = S_1 \cup S_2, \quad c = c_1 \cdot c_2$$

וסיימנו.

תרגול 10 – שדות סופיים

22/1/2017

משפט
יהא $\mathbb{F}$ שדה סופי.
אזי $|\mathbb{F}| = p^n$ כאשר p ראשוני ו-n טבעי.

משפט
יהא p ראשוני ו-n טבעי.
אזי קיים שדה סופי $\mathbb{F}$ עם p^n איברים.

איך הם נראים?
עבור p ראשוני, אזי $\mathbb{Z}_p$ הוא שדה עם p איברים.

מה עם שאר המקרים?
נתחיל לעבוד על זה...
הגדרה
יהא $\mathbb{F}$ שדה.
יהא $\mathbb{F}[x]$ חוג הפולינומים מעליו.
תת-קבוצה $I \subseteq \mathbb{F}[x]$ תיקרא **אידיאל** אם:
1. I חבורה ביחס לחיבור פולינומים.
2. בליעה:

$$\forall \begin{matrix} y(x) \in \mathbb{F}[x] \\ i(x) \in I \end{matrix}: \quad y(x) \cdot i(x) \in I$$

דוגמה
$\mathbb{F}$ שדה, $\mathbb{F}[x]$ חוג הפולינומים מעליו, $f(x) \in \mathbb{F}[x]$ אזי:

$$\langle f \rangle = \{f(x) \cdot g(x) | g(x) \in \mathbb{F}[x]\} \subseteq \mathbb{F}[x]$$

היא אידיאל.
הוכחה
1. צריך להראות את תכונות החבורה.

סגירות
יהיו $g_1, g_2 \in \mathbb{F}[x]$, $fg_1, fg_2 \in \langle f \rangle$, אזי:

$$fg_1 + fg_2 = f \underbrace{(g_1 + g_2)}_{\in \mathbb{F}[x]} \in \langle f \rangle$$

קיבוציות
נובע מקיבוציות של $\mathbb{F}[x]$.
ניטרלי
$0(x) \in \mathbb{F}[x] \Leftarrow 0(x) = f(x) \cdot 0(x) \in \langle f \rangle$.
נגדי
יהא $fg \in \langle f \rangle$ (כאשר $g \in \mathbb{F}[x]$), אזי:

$$-(fg) = f \underbrace{(-g)}_{\in \mathbb{F}[x]} \in \langle f \rangle$$

2. בליעה
יהא $fg \in \langle f \rangle$, ($g \in \mathbb{F}[x]$).
יהא $y \in \mathbb{F}[x]$, אזי:

$$(fg) \cdot y = f \underbrace{(gy)}_{\in \mathbb{F}[x]} \in \langle f \rangle$$

■

תרגיל
יהא $\mathbb{F}[x]$ חוג הפולינומים מעל $\mathbb{F}$ שדה.
יהא $I \subseteq \mathbb{F}[x]$ אידיאל.
אזי $I = \langle f \rangle$ עבור $f \in \mathbb{F}[x]$ כלשהו.
הוכחה
נסמן $f(x)$ את הפולינום המתוקן עם דרגה מינימלית ב-I ששונה מאפס.
טענה
$$I = \langle f \rangle$$
הוכחה
$\boxed{\supseteq}$:
יהא $fg \in \langle f \rangle$ $(g \in \mathbb{F}[x])$.
אזי $\underbrace{f}_{\in I} \underbrace{g}_{\in \mathbb{F}[x]} = fg \in I$ בגלל תכונת הבליעה.
$\boxed{\subseteq}$:
יהא $a(x) \in I$.
נחלק את $a(x)$ ב-$f(x)$:
$$a(x) = g(x) \cdot f(x) + r(x)$$
כאשר $\deg(r) < \deg(f)$ או $r(x) = 0$.
$$\Rightarrow r(x) = \underbrace{a(x)}_{\substack{\in I \\ \text{בגלל נתון}}} - \underbrace{\underbrace{g(x)}_{\in \mathbb{F}[x]} \cdot \underbrace{f(x)}_{\in I}}_{\substack{\in I \\ \text{בגלל בליעה}}} \in I$$
זאת כי I חבורה חיבורית, לכן $r(x) = 0$ כי אחרת $r(x) \in I$ עם דרגה קטנה מ-$f(x)$ $\lightning$.
ולכן:
$$a(x) = g(x) \cdot f(x) = f(x) \cdot g(x) \in \langle f \rangle$$
■

בניה
יהא $\mathbb{F}[x]$ חוג הפולינומים מעל $\mathbb{F}$ שדה.
יהא $f(x) \in \mathbb{F}[x]$, $I = \langle f \rangle$ אידיאל.
נגדיר יחס שקילות (צריך להוכיח זאת):
$$\forall g_1, g_2 \in \mathbb{F}[x]: \quad g_1 \equiv_f g_2 \quad \Leftrightarrow \quad \begin{matrix} g_1 - g_2 \in I \\ \Updownarrow \\ g_1 - g_2 = f \cdot \underbrace{g}_{\in \mathbb{F}[x]} \end{matrix}$$
נסמן את קבוצת המנה
$$\mathbb{F}[x] \big/ \langle f \rangle = \left\{ [g]_{\equiv_f} \middle| f \in \mathbb{F}[x] \right\}$$
הוא חוג – נקרא חוג המנה, ביחס לפעולות:
1. חיבור:
$$[g_1]_{\equiv_f} + [g_2]_{\equiv_f} = [g_1 + g_2]_{\equiv_f}$$
2. כפל:
$$[g_1]_{\equiv_f} \cdot [g_2]_{\equiv_f} = [g_1 \cdot g_2]_{\equiv_f}$$
קיימת יחידה $[1(x)]_{\equiv_f}$ ואיבר אפס שהוא $[0(x)]_{\equiv_f}$.

טענה

$$\mathbb{F}[x]\Big/\langle f\rangle = \left\{[g]_{\equiv_f} \middle| \deg(g) < \deg(f)\right\}$$

הוכחה

$\boxed{\supseteq}$:

פשוט.

$\boxed{\subseteq}$:

יהא $g \in \mathbb{F}[x]$ ו- $[g]_{\equiv_f} \in \mathbb{F}[x]\Big/\langle f\rangle$.

נרצה למצוא פולינום g' עם דרגה קטנה מדרגת f כך ש-$[g]_{\equiv_f} = [g']_{\equiv_f}$.

נבצע חילוק פולינומים:

$$g(x) = a(x)\cdot f(x) + r(x)$$

כאשר $\deg(r) < \deg(f)$ או $r(x) = 0$.

$$\Rightarrow g(x) - r(x) = a(x)\cdot f(x) \in I$$
$$\Rightarrow g(x) \equiv_f r(x)$$
$$\Rightarrow [g(x)]_{\equiv_f} = [r(x)]_{\equiv_f}$$

דוגמה

$\mathbb{R}[x]$ ו-$f(x) = x^2 + 1$. נקבל:

$$\mathbb{R}[x]\Big/\langle x^2+1\rangle = \left\{[a+bx]_{\equiv_f} \middle| a,b \in \mathbb{R}\right\}$$

מתקיים:

$$[x]\cdot[x] \underbrace{=}_{\text{הגדרה}} [x^2] \underbrace{=}_{x^2-(-1)\in\langle f\rangle} [-1]$$

דוגמה נוספת

$$\mathbb{Z}_2[x]\Big/\langle x^2+1\rangle = \left\{[a+bx]_{\equiv_f} \middle| a,b \in \mathbb{Z}_2\right\}$$

מתקיים:

$$[x+1]\cdot[x] = [x^2+x] = [-1+x] = [1+x]$$

מכך נובע ש-$[1+x]$ אינו הפיך, כי אחרת נכפול בהופכי שלו ונקבל $[x] = [1]$ ↯.

תרגול 11 – משפט ההומומורפיזם הראשון לחוגים

29/1/2017

ראינו כי ב-$\mathbb{R}[x]$ הפולינום x^2+1 אי-פריק, ולכן $R[x]/\langle x^2+1\rangle = \{[a+bx] \mid a,b\in\mathbb{R}\}$ שדה.

טענה

$$R[x]/\langle x^2+1\rangle \cong \mathbb{C}$$

הוכחה

בעזרת משפט האיזומורפיזם הראשון (של חוגים), נגדיר:

$$\phi: \mathbb{R}[x] \to \mathbb{C}$$
$$f(x) \longmapsto f(i)$$

למשל:

$$\phi(x^3+3x^2+x) = i^3+3i^2+i$$

נראה ש-ϕ הומומורפיזם, שומר חיבור:

$$\phi\big(f_1(x)+f_2(x)\big) = f_1(i)+f_2(i) = \phi\big(f_1(x)\big)+\phi\big(f_2(x)\big)$$

שומר כפל:

$$\phi\big(f_1(x)\cdot f_2(x)\big) = f_1(i)\cdot f_2(i) = \phi\big(f_1(x)\big)\cdot\phi\big(f_2(x)\big)$$

נראה ש-ϕ על, יהא $z\in\mathbb{C}$, צריך למצוא לו מקור:

$$\exists a,b\in\mathbb{R} \quad z = a+bi$$

נגדיר $f(x) = a+bx \in \mathbb{R}[x]$ והוא ישמש כמקור:

$$\phi\big(f(x)\big) = z$$

נציג את $\ker(\phi)$:

$$\ker(\phi) = \big\{f(x)\in\mathbb{R}[x] \,\big|\, \phi\big(f(x)\big) = 0\big\}$$

טענה:

$$\ker(\phi) = \langle x^2+1\rangle$$

הוכחה:

$\boxed{\supseteq}$ הצבה של i ב- x^2+1 שווה 0 ולכן $x^2+1\in\ker(\phi)$ ולכן $\langle x^2+1\rangle \subseteq \ker(\phi)$.

$\boxed{\subseteq}$ יהא $f(x)\in\ker(\phi) \Leftarrow f(i)=0$, נחלק $f(x)$ ב- x^2+1:

$$f(x) = q(x)\cdot(x^2+1)+r(x)$$

כאשר $\deg(r)<2$, ונקבל:

$$r(i) = f(i)-q(i)\cdot(i^2+1) = 0-0 = 0$$

כלומר $r(x)=0$ כי אין פולינום מדרגה 0 או 1, שכשמציבים i מקבלים 0.

$$\Rightarrow f(x) = g(x)\cdot(x^2+1)\in\langle x^2+1\rangle$$

תזכורת

יהא $\mathbb{F}[x]$ חוג הפולינומים מעל השדה $\mathbb{F}$, יהא $p(x)\in\mathbb{F}[x]$ פולינום, ויהא $I=\langle p(x)\rangle$ האידיאל שנוצר על-ידו.

ראינו כי $\mathbb{F}[x]/\langle p(x)\rangle = \left\{[y(x)]_{\equiv_p} \,\middle|\, \deg(y)<\deg(p)\right\}$ חוג (חוג המנה).

(הגדרנו יחס על $\mathbb{F}[x]$: $f_1\equiv_p f_2 \Leftrightarrow f_1-f_2\in\langle p(x)\rangle$).

בנוסף – אם $p(x)$ ראשוני/אי-פריק אז $\mathbb{F}[x]/\langle p(x)\rangle$ שדה.

תרגיל 1

$\mathbb{Z}_5[x]$ ($\mathbb{F}=\mathbb{Z}_5$). הוכיחו כי $1+x+x^3$ אי-פריק, ולכן $\mathbb{Z}_5[x]/\langle 1+x+x^3\rangle$ שדה.
ומצאו את ההופכי של:

$$[1+x+x^2]\in \mathbb{Z}_5[x]/\langle 1+x+x^3\rangle$$

<u>פתרון</u>

$1+x+x^3$ פולינום מדרגה 3, ולכן אי-פריק $\Leftrightarrow$ אין לו שורש.
נסמן $f(x)=1+x+x^3$, נראה שלכל $a\in\mathbb{Z}_5$: $f(a)\neq 0$

$$f(0)=1$$
$$f(1)=1+1+1=3$$
$$f(2)=1+2+8=11=1$$
$$f(3)=1+3+27=31=1$$
$$f(4)=1+4+64=69=4$$

נמצא הופכי ל-$[1+x+x^2]$ על-ידי שימוש ב-gcd:

$$\gcd(1+x+x^2,1+x+x^3)=1$$

$1+x+x^3$ אי-פריק וראשוני, ולכן אם $f(x)\neq 0$ מדרגה קטנה מ- $\deg(1+x+x^3)$ אזי $\gcd=1$.

$$\begin{array}{l} x-1 \\ \hline x^3+x+1 \mid x^2+x+1 \\ - \\ \underline{x^3+x^2+x} \\ \quad -x^2+1 \\ \quad - \\ \quad \underline{-x^2-x-1} \\ \qquad\qquad x+2 \end{array}$$

כלומר:

$$x^3+x+1=(x^2+x+1)(x-1)+(x+2)$$
$$\Rightarrow x^2+x+1=(x+2)(x-1)+3$$
$$\Rightarrow 3=x^2+x+1-(x+2)(x-1)=$$
$$=(x^2+x+1)-(x-1)\big((x^3+x+1)-(x^2+x+1)(x-1)\big)=$$
$$=(x^2+x+1)(1+(x-1)^2)-(x-1)(x^3+x+1)$$

עבור $\mathbb{Z}_4$: $3^{-1}=2$ ונקבל:

$$1=2\cdot(x^2+x+1)(1+(x-1)^2)-2(x^3+x+1)(x-1)$$
$$\Downarrow$$
$$[1]_{\equiv_f}=[x^2+x+1]_{\equiv_f}\cdot[2(1+(x-1)^2)]_{\equiv_f}$$
$$\Downarrow$$
$$[x^2+x+1]^{-1}=[2(1+(x-1)^2)]$$

■

<u>הערות</u>

1. שימו לב כי:

$$\mathbb{Z}_5[x]/\langle 1+x+x^3\rangle=\{[a_0+a_1x+a_2x^2]\mid a_0,a_1,a_2\in\mathbb{Z}_5\}$$

ויש בו 5^3 איברים.

2. $\mathbb{Z}_5[x]/\langle 1+x+x^3\rangle \supseteq \mathbb{Z}_5$ על-ידי הזיהוי:

$$\mathbb{Z}_5\cong\{[0],[1],[2],[3],[4]\}$$

<u>תרגיל 2</u>

מצאו שדה עם 8 איברים בו יש פתרון למשוואה:

$$x^3+x+1=0$$

<u>פתרון</u>

$f(x)=x^3+x+1\in\mathbb{Z}_2[x]$ אי-פריק מעל $\mathbb{Z}_2$ $\begin{pmatrix} f(0)=1 \\ f(1)=1 \end{pmatrix}$.

$\Leftarrow$ $\mathbb{Z}_2[x]\big/\langle f(x)\rangle=\{[a_0+a_1x+a_2x^2]|a_0,a_1,a_2\in\mathbb{Z}_2\}$ שדה עם 2^3 איברים כאשר 3= דרגת $f(x)$, $2=$ $|\mathbb{Z}_2|$.

$\Leftarrow$ $[x]$ פתרון ל- $x^3+x+1=0$, כי:

$$[x]^3+[x]+[1]=[x^3]+[x]+[1]=[x^3+x+1]=[0]$$

■

תרגול 12 – תרגילים בנושא שדות ושדות סופיים

5/2/2017

תרגיל

יהי $0 \neq p(x) \in \mathbb{F}[x]$ מדרגה n.
אזי קיימים לו לכל היותר n שורשים.
הוכיחו.

פתרון

באינדוקציה על n:
עבור $n = 0$, $f(x) \equiv c$ פולינום קבוע, ואכן יש לו 0 שורשים.
נניח נכונות עד n (לא כולל). ונוכיח עבור n.
יהי $p(x) \neq 0$ מדרגה n, אם אין לו שורשים, סיימנו.
אחרת, $\alpha \in \mathbb{F}$ שורש שלו, כלומר $p(\alpha) = 0$.

$$\Downarrow$$

$$\underbrace{\exists q(x) \in \mathbb{F}[x]}_{n-1\ \text{מדרגה}}: \quad p(x) = (x - \alpha) \cdot q(x)$$

לפי הנחת האינדוקציה ל-$q(x)$ לכל היותר $n - 1$ שורשים.

$$\Downarrow$$

$$\begin{Bmatrix} \text{שורשים} \\ p(x)\ \text{של} \end{Bmatrix} = \{\alpha\} \cup \begin{Bmatrix} \text{שורשים} \\ q(x)\ \text{של} \end{Bmatrix}$$

$$\#\begin{Bmatrix} \text{שורשים} \\ p(x)\ \text{של} \end{Bmatrix} \leq 1 + n - 1 = n$$

תרגיל

יהי $\mathbb{F}$ שדה עם p^n איברים (p ראשוני, $n \in \mathbb{N}$).
הוכיחו כי:

$$\forall a \in \mathbb{F}: \quad a^{p^n} = a$$

הוכחה

$\mathbb{F}^* = \mathbb{F} \setminus \{0\}$ הוא חבורה ביחס לכפל של השדה.
ל-$\mathbb{F}^*$ יש $p^n - 1$ איברים, כאשר $1 \in \mathbb{F}^*$ היחידה בחבורה זו.
לפי לגרנז':

$$\forall a \in \mathbb{F}^*: \quad a^{p^n - 1} = 1$$

נכפיל ב-a ונקבל:

$$\forall \underbrace{a}_{\neq 0} \in \mathbb{F}^*: \quad a^{p^n} = a$$

שוויון זה מתקיים גם עבור $a = 0$ ולכן לכל $a \in \mathbb{F}$.

תרגיל

יהי $\mathbb{F}$ שדה עם p^n איברים (p ראשוני, $n \in \mathbb{N}$).
אזי:

$$x^{p^n} - x = \prod_{a \in \mathbb{F}} (x - a)$$

הוכחה

לפולינום $x^{p^n} - x \in \mathbb{F}[x]$ יש לכל היותר p^n שורשים.
בנוסף כל $a \in \mathbb{F}$ הוא שורש שלו (כי $a^{p^n} = a$) ולכן אלו בדיוק p^n שורשיו.
למשל, $\mathbb{F} = \mathbb{Z}_2$ עם $p = 2$ איברים:

$$x^2 - x = \prod_{a \in \mathbb{Z}_2} (x - a) = (x - 0)(x - 1) = x(x - 1)$$

למשל, $\mathbb{F}=\mathbb{Z}_5$ עם $p^n=5^1$ איברים:

$$x^5-x=\prod_{a\in\mathbb{Z}_5}(x-a)=(x-0)(x-1)(x-2)(x-3)(x-4)$$

הגדרה

יהי $\mathbb{F}$ שדה. תת קבוצה $\mathbb{F}'\subseteq\mathbb{F}$ תקרא תת-שדה אם $\mathbb{F}'$ שדה ביחס לפעולות של $\mathbb{F}$.

למשל:

1. $\mathbb{Q}\subseteq\mathbb{R}\subseteq\mathbb{C}$.
2. $\{[0],[1]\}=\mathbb{Z}_2\subseteq\underbrace{\mathbb{Z}_2[x]/\langle x^2+x+1\rangle}_{\text{שדה עם 4 איברים}}=\{[a+bx]|a,b\in\mathbb{Z}_2\}$.

תרגיל

יהי $\mathbb{F}$ שדה עם p^n איברים (p ראשוני, $n\in\mathbb{N}$).

יהי $\mathbb{F}'$ תת-שדה שלו, אזי $|\mathbb{F}'|=p^t$ כאשר $t|n$.

למשל, לשדה עם 2^n איברים יכולים להיות תתי שדות מהגדלים $2,2^2,2^4$.

למשל, לשדה $\mathbb{F}$ עם p^{31} איברים יש רק תת-שדות טריוויאליים $\mathbb{Z}_p,\mathbb{F}$.

הוכחה

נגדיר $K=\{1,1+1,1+1+1,\dots\}$, $K\cong\mathbb{Z}_p$, $|K|=p$.

$$\Downarrow$$
$$K\subseteq\mathbb{F}'$$

אז $|\mathbb{F}'|=p^t$ עבור $t\in\mathbb{N}$ כלשהו.

נשים לב כי $\mathbb{F}$ הוא מרחב וקטורי מעל $\mathbb{F}'$.

תזכורת

V מרחב וקטור מעל $\mathbb{F}$, מאפשר:

$$\forall v_1,v_2\in V:\quad v_1+v_2$$
$$\forall{\alpha\in F \atop v\in V}:\quad \alpha\cdot v$$

+ אקסיומות.

אז מכיוון ש-$\mathbb{F}$ הוא מרחב וקטורי זה אומר שקיים בסיס:

$$B=\{v_1,\dots,v_d\}\subseteq\mathbb{F}$$

כשיש לנו בסיס למרחב וקטורי, כל $v\in\mathbb{F}$ ניתן להצגה יחידה כצירוף ליניארי של איברי B. כלומר, קיימים $\alpha_1,\dots,\alpha_d\in\mathbb{F}'$ **יחידים** כך ש:

$$v=\sum_{i=1}^d\alpha_iv_i$$

מכאן ש:

$$\mathbb{F}=\left\{\sum_{i=1}^d\alpha_iv_i\,\middle|\,\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_d\end{pmatrix}\in(\mathbb{F}')^d\right\}\Rightarrow|\mathbb{F}|=\left|\mathbb{F}'^d\right|$$

ולכן:

$$p^n=|\mathbb{F}|=|\mathbb{F}'|^d=(p^t)^d=p^{t\cdot d}$$
$$\Downarrow$$
$$n=t\cdot d$$
$$\Downarrow$$
$$t|n$$