26-10-2006

מבנים אלגבריים - תרגול מס' 1

המתרגל: עמי אייזנמן

amie@math.huji.ac.il

הגשת תרגילים חובה 70%.

מהציון הם התרגילים 10%.

כל אחד מהמבחנים (1 או 2) 5%.

הגדרה: קבוצה G היא **חבורה** אם קיימת פעולה דו-מקומית (כלומר לכל $a,b\in G$ מתאים איבר $a*b\in G$) $*$, כך שמתקיימים התנאים הבאים:

(א) אסוציאטיביות $\forall a,b,c\in G$ $(a*b)*c=a*(b*c)$

(ב) קיים איבר $e\in G$ המקיים: $\forall a\in G,\ e*a=a*e=a$

(ג) לכל $a\in G$ קיים איבר $b\in G$ המקיים: $a*b=b*a=e$

הערה: אפשר לכתוב את הפעולה כ: $\mu: G\times G\longrightarrow G$ כך ש: $\mu((a,b))=a*b$

הגדרה: אם $a*b=b*a$ $\forall a,b\in G$ אז G נקראת חבורה אבלית או קומוטטיבית.

(i) אם G חבורה אז קיים איבר יחיד e המקיים את תנאי (ב), נקרא לו איבר היחידה.

(ii) $\forall a\in G$ קיים איבר יחיד $b\in G$ המקיים את תנאי (ג) נקרא לו ההפכי ונסמנו a^{-1}.

לפעמים נסמן חבורה ע"י $(G,*)$

דוגמאות: (א) $(\mathbb{Z},+)$

(ב) אם V מרחב וקטורי מעל שדה כלשהו אז $(V,+)$ חבורה.

(ג) אם F שדה אזי $(F,+)$ חבורה.

(ד) $(F^*,\cdot)$ חבורה כאשר $F^*=F\setminus\{0\}$

(ה) $(\mathbb{Z}_n,+)$ $[a]\in\mathbb{Z}_n$ $[a]=\{b\in\mathbb{Z}\mid n|a-b\}$

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

(*) נסתכל ב- $\bar{2}\in\mathbb{Z}_4$ $\bar{2}\cdot\bar{2}=0$ $\bar{a}\cdot\bar{2}=\bar{1}$ a הופכי ל-2

נכפול משני הצדדים ונקבל $0=\bar{a}\cdot\bar{2}\cdot\bar{2}=\bar{1}\cdot\bar{2}=\bar{2}$ סתירה.

אם $a\in\mathbb{Z}_n$ וקיים $b\neq 0\in\mathbb{Z}_n$ כך ש: $a\cdot b=0$ אז אין ל-a הפכי

לכן מסתכלים על $(\mathbb{Z}_n^*,\cdot)$ שמוגדר: $\mathbb{Z}_n^*=\{a\in\mathbb{Z}_n \mid n \text{ זר ל} a\}$

הגדרה: (א) $a,b\in\mathbb{Z}$ נאמר ש- $a|b$ אם יש $c\in\mathbb{Z}$ כך ש- $a\cdot c=b$

(ב) יהיו $a,b\in\mathbb{Z}$ d' נקרא מחלק משותף של a ושל b אם $d'|a$ ו- $d'|b$

(ג) d יקרא מחלק משותף מקסימלי (מ.מ.מ) אם d מחלק משותף ולכל מחלק משותף d' מתקיים $d'|d$ $d=(a,b)$

טענה: לכל שני מספרים שלמים a,b ישנו מחלק משותף מקסימלי (a,b)

הגדרה: $a,b\in \mathbb{Z}$ נקראים זרים אם $(a,b)=1$.

טענה: יהיו $(a,b)\in \mathbb{Z}$ $(a,b)=1 \iff$ קיים $p,q\in\mathbb{Z}$ המקיימים $a\cdot p+b\cdot q=1$ זאת אומרת ש- $ap=1-bq$.

(הסבר ההוכחה:) מספר זה $n\in\mathbb{N}$ $(a,n)=1$ קיימים p,q שלמים כך ש- $ap=1-bq$. מודולו n מתקיים $\bar{a}\cdot\bar{p}=1$ וגם $(p,n)=1$

אם $(a,n)=d$ אז אין איבר הפכי.

אם $(a,n)=1$ + $(b,n)=1 \Rightarrow (ab,n)=1$ לכן מסתכלים על $\mathbb{Z}_n^*$

דוגמא: נמשיך בדוגמאות של חבורות:

1. יהי V מרחב וקטורי מעל שדה F $GL(V)=\{T:V\to V \mid T \text{ טרנספורמציה לינארית הפיכה}\}$ עם פעולת ההרכבה.

2. F שדה, $GL_n(F)=\{A\in M_n(F)\mid \det A\neq 0\}$ עם כפל מטריצות.

3. עבור הקבוצה X נגדיר $S_X=\{\text{תמורות על } X\}$ עם פעולת ההרכבה.

תמורות: העתקות חח"ע ועל $\sigma: X\to X$

אם $X=\{1,\dots,n\}$ אז נסמן $S_X=S_n$

איך נכתוב תמורות? $\sigma\in S_n$

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n)\end{pmatrix}$$

S_n $\forall n>2$ איננה קומוטטיבית!!!

26-10-2006 ②

הגדרה: נאמר שתמורה $\sigma \in S_X$ מזיזה את $x \in X$ אם $\sigma(x) \neq x$

יהיו $1 \le i_1, i_2, \dots, i_k \le n$ ונניח כי $\sigma \in S_n$ לא מזיזה את יתר המספרים (השונים מ- $i_1, \dots, i_k$) וכן $\sigma(i_1)=i_2,\ \sigma(i_2)=i_3, \dots\dots, \sigma(i_k)=i_1$

אז σ נקראית **מחזור** מאורך k.

נכתוב: $\sigma = (i_1, i_2, \dots, i_k)$. מחזור מאורך 1 הוא הזהות (תמורת הזהות)

מחזור מאורך 2 נקרא **חילוף**.

הגדרה: $\sigma, \tau \in S_X$ נקראות **זרות** אם לא קיים $x \in X$ כך ש- $\sigma(x) \neq x$ וגם $\tau(x) \neq x$

טענה: כל $\sigma \in S_n$ הוא מחזור או מכפלה של מחזורים זרים.

האם הפירוק יחיד?

(א) מחזורים זרים מתחלפים.

(ב) אפשר להוסיף או להוריד מחזורים מאורך 1.

הגדרה: נקרא לפירוק $\sigma \in S_n$ למכפלת מחזורים זרים **פירוק מלא** אם הוא מכיל את כל המחזורים מאורך 1.

טענה: תהי $\sigma \in S_n$ תמורה $\sigma = \alpha_1, \dots, \alpha_t$ פירוק מלא של σ למחזורים זרים; אז הפירוק הנ"ל יחיד עד כדי שינוי סדר.

טענה: כל תמורה $\sigma \in S_n$ ניתן לכתוב כמכפלה של חילופים.

הוכחה: מספיק להראות שכל מחזור היא מכפלת חילופים:

$$(1\,2 \dots r) = (1\ r)(1\ r-1)\dots(1\,3)(1\,2) \quad \dashv$$

תהי G חבורה, $G = \{a_1, \dots, a_n\}$ ניתן לכתוב לוח כפל לחבורה:

	a_1	a_2	......	a_n
a_1	a_1a_1	a_1a_2		
a_2	a_2a_1			
$\vdots$			a_ia_j	
a_n				

* אם $|G|=1$ אז לוח הכפל הוא:

$\cdot$	1
1	1

(החבורה הטריוויאלית)

* אם $|G|=2$ אז לוח הכפל הוא:

$\cdot$	1	a
1	1	a
a	a	1

דוגמא: $(\mathbb{Z}_2, +)$ $(G=\{\pm 1\}, \cdot)$

(*) $|G|=3$:אזי

+	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

$ab\neq b$ כי אם $ab=b$ אז

$a=a\cdot b\cdot b^{-1}=1$ וזה לא יכול להיות

כי $a\neq 1$

כנ"ל $ab\neq a$ מאותו ההסבר בדיוק.

ולכן נשאר $ba=ab=1$

$a^2\neq a$ (אחרת $a=1$) אם $a^2=1 \Leftarrow a=a\cdot a\cdot b=b$

והרי $a\neq b$ ולכן $a^2=b$ וכנ"ל $b^2=a$

<u>דוגמא:</u> $(\mathbb{Z}_3,+)$ $\{1,(1\,2\,3),(1\,3\,2)\}\overset{\text{הכלה}}{\subseteq} S_3$

(*) אם $|G|=4$

+	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	c	1	a	b

$ac\neq a$ $\quad ac\neq a$

(א) אם $ac=1$ אז גם $ca=1$

($b^2=1$ כי a ו-c לא הופכיים של b)

$ac\neq ab \Leftarrow ab=c$ כנ"ל $ca\neq ba$

$\Leftarrow ba=c$

$ab\neq 1\neq a\neq b$

$bc\neq ac \Leftarrow bc=a$ $\quad cb=a$

$a^2=b$ $\quad c^2=b$

ישנה גם אפשרות (ב): אם $ac=b$. אפשר להניח כי $ab\neq 1$ $\quad ac\neq 1$ ו- $bc\neq 1$

אז $ab=c$ $\quad ba=c$ $\quad cb=bc=a$ $\quad ac=ca=b$

נשאר: $a^2=b^2=c^2=1$

	1	a	b	c
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	c	b	a	1

<u>דוג:</u> $(\mathbb{Z}_8^*,\cdot)$

מבנים אלגבריים - תרגול מס' 2

הגדרה: יהיו $a,b \in \mathbb{Z}$. m' יקרא כפולה משותפת של a,b

אם $a|m'$ $b|m'$

m יקרא כפולה משותפת מינימלית

אם m כפולה משותפת. ולכל כפולה משותפת m' מתקיים $m|m'$

סימון: $m=[a,b]$

חימור $|G|=4$

אחד מלוחות הכפל שמצאנו

הוא לוח הכפל של $\mathbb{Z}_8^*$

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

הגדרה: יהיו H,G חבורות. $H\times G$ היא החבורה שאיבריה הם הזוגות

(h,g) $h\in H$, $g \in G$.

והמכפלה מוגדרת ע"י $(h_1,g_1)\cdot(h_2,g_2)=(h_1\cdot h_2, g_1\cdot g_2)$

תרגיל: זו חבורה

דוגמא: $G=\mathbb{Z}_2\times\mathbb{Z}_2$

לוח כפל:

$+\times+$	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

הגדרה: יהיו G,H חבורות. העתקה $\varphi: G \to H$ תיקרא **הומומורפיזם**

אם $\forall g_1,g_2 \in G \quad \varphi(g_1 \cdot g_2) = \varphi(g_1)\varphi(g_2)$

הומומורפיזם יקרא **איזומורפיזם** אם הוא חח"ע ועל.

אם $\varphi: G \to H$ איזומורפיזם אז נאמר ש- G ו- H איזומורפיות $H \cong G$

עתה נגדיר איזומורפיזם $\varphi: \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_8^*$ (בין שני לוחות הכפל שהיו לנו)

$$\varphi((0,0))=1, \quad \varphi((1,0))=3 \quad \varphi((0,1))=5 \quad \varphi((1,1))=7$$

ברור כי φ חח"ע ועל כי ממש רואים

וגם רואים כי הוא הומומורפיזם

מסקנה: $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_8^*$ ונמצא איזומורפיזם נוסף:

נגדיר עכשיו $\Psi: \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_8^*$

$$\Psi((0,0))=1, \quad \Psi((1,0))=5, \quad \Psi((0,1))=7$$

$$\Psi((1,1))=3$$

גם Ψ הוא איזומורפיזם וישנן נוספים.

נגדיר $f: \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ איזומורפיזם בין $\mathbb{Z}_2 \times \mathbb{Z}_2$ לעצמה

$$f((0,0))=(0,0) \qquad f((1,1))=((1,0))$$

$$f((1,0))=(0,1)$$

$$f((1,1))=(1,1)$$

הגדרה: איזומורפיזם $\varphi: G \to G$ נקרא **אוטומורפיזם**

מסמנים:

$Aut(G) = \{$ האוטומורפיזמים של $G\}$

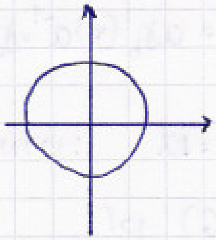
$Aut(G)$ עם פעולת ההרכבה היא חבורה.

דוגמאות: (א) $det: Gl_n(F) \longrightarrow F^*$ זהו אפימורפיזם:

$$Ker(det) = Sl_n(F) = \{A \in Gl_n(F) \mid |A| = 1\}$$

$Im(det) = F^*$ כלומר ההעתקה היא על.

(ב) $T = \{x \in \mathbb{C} \mid |x| = 1\}$ כל המספרים המרוכבים עם ערך מוחלט 1



T עם פעולת הכפל היא חבורה (תרגיל)

צורת כתיבה נוספת:

$$(T = \{e^{i\theta} \mid \theta \in \mathbb{R}\}$$

עתה נגדיר הומומורפיזם: יהי $y \in \mathbb{R}$

נגדיר $f_y: \mathbb{R} \longrightarrow T$ ע"י:

$$f_y(x) = e^{iyx}$$

$$f_y(x+x') = e^{iy(x+x')} = e^{iyx} \cdot e^{iyx'} = f_y(x) \cdot f_y(x')$$

אז רואים כי f_y הומומורפיזם.

אם $y=0$ $\quad Im f_y = \{1\}$

$Ker f_y = \mathbb{R}$

אם $y \neq 0$ $\quad Im f_y = T$

כי אם $e^{i\theta} \in T$ $\quad x = \frac{\theta}{y}$

ואז $f_y(x) = e^{i\theta}$

$$Ker f_y = \{\frac{2\pi k}{y} \mid k \in \mathbb{Z}\}$$

(ג) שורשי היחידה מסדר n (שורשים של $x^n=1$)

$$G = \{e^{i\frac{2\pi k}{n}}\}_{k=0}^{n-1}$$

עכשיו נגדיר: $\varphi: G \longrightarrow \mathbb{Z}_n,\ \varphi(e^{\frac{i2\pi k}{n}}) = k$

סגנה: φ הוא איזומורפיזם (תרגיל)

ⓐ תהי G חבורה ויהי $a\in G$

נגדיר $\gamma_a : G \longrightarrow G$

ע"י: $\gamma_a(x) = axa^{-1}$ (הצמדה ע"י a)

γ_a הומומורפיזם כי

$$\gamma_a(xy) = axya^{-1} = axa^{-1}aya^{-1} = \gamma_a(x)\gamma_a(y)$$

γ_a איזומורפיזם כי $\gamma_{a^{-1}}$ הופכית ל- γ_a

נשים לב ש- $\gamma_{ab} = \gamma_a \circ \gamma_b$

$$\gamma_{ab}(x) = ab\cdot x(ab)^{-1} = abxb^{-1}a^{-1} = a\gamma_b(x)a^{-1} = \gamma_a\gamma_b(x)$$

כמו כן: $\gamma_1 = id$ $\quad (\gamma_a)^{-1} = \gamma_{a^{-1}}$

ולכן $\{\gamma_a\}_{a\in G} = H \leq Aut(G)$

ⓑ $G = (\mathbb{R}^+, \cdot)$

$(\mathbb{R}^+ = \{x\in\mathbb{R} \mid x>0\})$

$$\log : G \longrightarrow (\mathbb{R}, +)$$

$\log(xy) = \log x + \log y \Longrightarrow \log$ הומו'

e^x ההפכי של $\log$ ולכן $\log$ איזומורפיזם.

① $\varphi : \mathbb{Z} \longrightarrow n\mathbb{Z}$

$\varphi(a) = n\cdot a$ $\quad \varphi$ איזומורפיזם (רואים פה חבורה אינסופית שאיזומורפית לתת-חבורה שלה, לא יתכן בחבורה סופית)

③ $\varphi: \mathbb{Z} \longrightarrow \mathbb{Z}_n$

$\varphi(a) = [a]$ המחלקה מודולו n של a

(דרך נוספת לראות $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$)

מהו הגרעין של ההעתקה $\ker\varphi = n\mathbb{Z}$ (הכפולות של n)

$\operatorname{Im}\varphi = \mathbb{Z}_n$

ח) S_n חבורת התמורות. נגדיר העתקה: $i: S_{n-1} \longrightarrow S_n$

אם $\sigma \in S_{n-1}$ נגדיר $i(\sigma) \in S_n$ באופן הבא:

$i(\sigma)(k) = \sigma(k)$ עבור $1 \le k \le n-1$

$i(\sigma)(n) = n$ (ישאר במקום)

לדוגמא: $i\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$

$i((1\,2)) = (1\,2) \in S_4$

ברור ש i הומומורפיזם

" מחט "

הגדרה: תהי G חבורה. $X \subset G$ קבוצה.

תת-החבורה הנוצרת ע"י X היא תת-החבורה המינימלית של G המכילה את X נסמנה $\langle X \rangle$

דוגמא: $x \in G$

$\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\} = H$

למה? ברור ש: $H \subseteq \langle x \rangle$

מאידך H תת-חבורה של G אז מההגדרה $\langle x \rangle \subseteq H$

לכן $H = \langle x \rangle$

הגדרה: חבורה הנוצרת ע"י איבר אחד נקראת ציקלית.

הגדרה: תהי G חבורה $X \subseteq G$ קבוצה

מילה ב X היא ביטוי מהצורה $x_1^{e_1} \cdot x_2^{e_2} \cdot x_3^{e_3} \cdot \ldots \cdot x_n^{e_n}$

כאשר $e_i \in \{\pm 1\}$ $\forall i \quad x_i \in X$

טענה: G חבורה $\emptyset \neq X \subseteq G$ קבוצה אז $\langle X \rangle$ שווה לכל המילים של איברי X.

הוכחה: נסמן ב-W את אוסף המילים של X.

W חבורה (תרגיל)

ברור ש- $W \subseteq \langle X \rangle$

מאידך מההגדרה $\langle X \rangle \subseteq W$

ולכן מתקיים שוויון.

נדבר עכשיו על S_n.

אמרנו בשיעור שעבר שאת S_n יוצרים כל החילופים

תזכורת: S_n נוצרת ע"י כל החילופים.

טענה א': S_n נוצרת ע"י החילופים $(12)(13)\dots\dots(1n)$

הוכחה: מספיק להראות שכל חילוף (a,b) נוצר ע"י חילופים אלה:

אכן: $(1a)(1b)(1a)=(ab)$

טענה ב': S_n נוצרת ע"י החילופים $(12)(23)\dots\dots(n-1\ n)$

הוכחה: נראה ש- $(1\ k)$ מתקבל ע"י איברים אלו לכל $n \geq k \geq 2$ ואז מטענה א' נקבל את ב'.

באינדוקציה על k:

$k=2$ ברור

נניח ש: $(1,k)$ מתקבל ע"י האיברים הנ"ל

אז: $(1\ k)(k\ k+1)(1\ k)=(1\ k+1)$

טענה ג: S_n נוצר ע"י $(12),(12\dots n)$

הוכחה: נוכיח באינדוקציה על n.

עבור $n=2$ ברור.

נסמן $H=\langle (12),(12\dots n)\rangle$

$H \ni [(12\dots n)]^{-1}=(n\ n-1\dots 1)$

לכן $H \ni (n\ n-1\dots 1)(12)(12\dots n)=(1n)$

2-11-2006

4

ולכן $H \ni (1\ n)(1\ 2\ 3 \ldots\ldots n)$

$= (1\ 2\ 3 \ldots\ldots n-1)$

מהנחת האינדוקציה $(1\ 2)$ ו- $(1\ 2 \ldots\ldots n-1)$ יוצר את S_{n-1}

ובפרט את המחזורים $(1\ 2), (1\ 3) \ldots\ldots (1\ n-1)$

ולכן $H \ni (1\ 2) \ldots\ldots (1\ n)$

$\Leftarrow$ $H = S_n$.

מבנים אלגבריים - תרגול מס' 3

סימון: G חבורה, $H \leq G$ תת-חבורה. אז $[G:H]$ נקרא האינדקס של H ב-G וזהו מס' המחלקות (השמאליות/ימניות) של H ב-G.

משפט לגרנג': $|G| = |H| \cdot [G:H]$ (G סופית, H תת-חבורה)

הגדרה: G חבורה. $H \leq G$. H נורמלית ב-G אם $gHg^{-1} = H$ $\forall g \in G$.

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\}$$

מספיק להניח $g^{-1}Hg \subseteq H$ $(\forall g \in G)$

סימון: $H \lhd G$

מה שקול לדבר הזה:

$$H \lhd G \iff gH = Hg \quad \forall g \in G$$

כי:
$$Hg = (gHg^{-1})g = gH(g^{-1}g) = gH$$

דוגמא עקרונית לתת-חבורה נורמלית:

כל גרעין של הומומורפיזם $\varphi : G \to H$ הוא תת-חבורה נורמלית

כי: אם $k \in Ker\varphi$,

$$\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(gg^{-1}) = 1$$

דוגמא חשובה: בחבורה אבלית, כל תת-חבורה היא נורמלית.

(ההפך אינו נכון, יכולה להיות חבורה שכל תת-החבורות שלה נורמליות אך היא אינה אבלית)

דוגמאות: $GL_n(F) \rhd SL_n(F)$

כי $SL_n(F) = Ker(det)$

* $A_n \lhd S_n$ = התמורות הזוגיות על $\{1, \dots, n\}$ כי $A_n = Ker(sgn)$

* דוגמא לתת-חבורה שאינה נורמלית:

$H = \langle(12)\rangle \qquad G = S_3$

נראה כי $H \ntriangleleft G$ (כי תת-החבורה אינה נורמלית):

דרך אחת: נבחר $\sigma \in S_3$ ונראה ש $\sigma(12)\sigma^{-1} \notin H$

בדרך אחרת, מפורשת יותר:

נסתכל על מחלקות ימניות ושמאליות של H ב- G:

מחלקות שמאליות: $H = \{e, (12)\}, (13)H = \{(13), (123)\}, (23)H = \{(23), (132)\}$

מחלקות ימניות:

$H(13) = \{(13), (132)\}, H(23) = \{(23), (123)\}$

רואים כי המחלקות הימניות והשמאליות אינן שוות ולכן תת-החבורה אינה נורמלית.

מצב שני: $K = \langle(123)\rangle$ אז $K \triangleleft S_3$

$K = \{e, (123), (132)\}$

$(12)K = \{(12), (23), (13)\}$

$K(12) = \{(12), (23), (13)\}$

$K = A_3$

מעבר הטכניקה שראינו פה, אנחנו יכולים להוכיח טענה פשוטה:

טענה: תהי G חבורה. $H \leq G$ תת-חבורה. $[G:H] = 2$, אז $H \triangleleft G$

הוכחה: ישנן שתי מחלקות ימניות/שמאליות H ! $G \setminus H$.

לכן ברור שמחלקות שמאליות שוות לימניות $gH = Hg$ $\forall g \in G$.

עבור $N \triangleleft G$ ניתן להגדיר מבנה של חבורה על המחלקות של N ב- G ע"י:

* $(a, b \in G)\ (aN) * (bN) = aNbN = \{an_1bn_2 \mid n_1, n_2 \in N\}$

$aNbN = a(bNb^{-1})bN = abN(b^{-1}b)N = abNN = abN$ (כי נורמליות / סגירות)

* N איבר היחידה ועבור aN $(aN)^{-1} = a^{-1}N$

9-11-2006 ②

סימון:

נסמן את החבורה של המחלקות G/N. היא נקראית חבורת המנה.

ישנה העתקה טבעית $\nu : G \to G/N$

$$g \mapsto gN$$

ברור שזהו הומומורפיזם והוא על

$\ker \nu = N$ - לכן כל תת-חבורה נורמלית היא גרעין של הומומורפיזם.

דוגמא: $G=\mathbb{Z}$ $H=n\mathbb{Z}$

$H \triangleleft G$ (אבליות)

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$$

למשל: $\mathbb{Z}$, $5\mathbb{Z}$:

המחלקות של $5\mathbb{Z}$ ב-$\mathbb{Z}$ הן:

$$5\mathbb{Z} = \{\dots -5, 0, 5, 10, \dots\}$$

$$5\mathbb{Z}+1 = \{\dots -4, 1, 6, 11, \dots\}$$

$$5\mathbb{Z}+2 = \{\dots -3, 7, 12, \dots\}$$

וכו'....

איך מתבצע החיבור? דוגמא: $(5\mathbb{Z}+3)+(5\mathbb{Z}+4) = 5\mathbb{Z}+7 = 5\mathbb{Z}+2$

דוגמא: S_4, $V = \{e, (12)(34), (13)(24), (14)(23)\}$. מתרגיל מראים כי $V \triangleleft S_4$ ולכן

מוגדרת חבורת המנה.

מחלקות: V, $\{(123), (243), (142), (134)\}$

$\{(234), (124), (132), (143)\}$

$\{(12), (34), (1423), (1324)\}$

ועוד שתי מחלקות

למשל: $(123)V \cdot (12)V = (123)\cdot(12)V = (13)V =$

$= \{(13), (24), (1432), (1324)\}$

הערה: אם G חבורה; $H \le G$ תת-חבורה $K \le H$ תת-חבורה של H אז $K \le G$

אבל אם $H \triangleleft G$, $K \triangleleft H$ אז לא בהכרח $K \triangleleft G$ חשוב!

דוגמא: עבור V לעיל $V \triangleleft S_4$ (תרגיל) אבל $K = \langle (12)(34) \rangle$! $K \triangleleft V$ כי $[V:K]=2$ (אינדקס 2)

תרגיל $K \ntrianglelefteq S_4$. (לבדוק לבד)

חבורות ציקליות

ראינו בתרגיל כי כל תת-החבורות של $\mathbb{Z}_{30}$ הן ציקליות

וכי לכל מספר שמחלק את 30 יש תת-חבורה ציקלית יחידה מסדר זה.

משפט: תהי G חבורה ציקלית, אזי כל תת-חבורה של G היא ציקלית.

הוכחה: תהי $H \leq G$ תת-חבורה. $G = \langle a \rangle$, $a \in G$

איברי G הם מהצורה a^m ו- $m \in \mathbb{Z}$

נבחר $k>0$ מינימלי כך ש: $a^k \in H$.

ברור ש- $\langle a^k \rangle \subseteq H$.

נניח $a^m \in H$. נכתוב $m = b \cdot k + r$, $0 \leq r < k$

$H \ni a^m \cdot a^{-bk} = a^r$ אם $r \neq 0$ נקבל סתירה למינימליות.

לכן $a^m = a^{bk}$

$\Leftarrow$ $H \subseteq \langle a^k \rangle$ $\Leftarrow$ הראינו הכלה בכיוון השני ולכן $H = \langle a^k \rangle$

משפט: H, G חבורות ציקליות איזומורפיות $\Longleftrightarrow$ $|H| = |G|$

הוכחה: נראה שאם $|H| = |G|$ אז $|H| \cong |G|$:

נניח $G = \langle a \rangle$, $H = \langle b \rangle$. $|H| = |G| = n$

נגדיר הומומורפיזם $\varphi: G \longrightarrow H$ ע"י $\varphi(a^i) = b^i$ כאשר $0 \leq i < n$

ברור כי φ חח"ע ועל.

φ הומומורפיזם: $\varphi(a^i b^j) = \varphi(a^{i+j})$

אם $i+j < n$

$$= \begin{cases} b^{i+j} = b^i \cdot b^j = \varphi(a^i)\varphi(a^j) \\ \varphi(a^{i+j-n}) = b^{i+j-n} = b^{i+j} = b^i \cdot b^j = \varphi(a^i)\varphi(a^j) \end{cases}$$

2 **טענה:** תהי $G=\langle a\rangle$ ציקלית $|G|=n$.

אז a^k יוצרת את G $\iff$ $(k,1)=1$

הוכחה: נניח $(k,n)=1$ ונאמר $o(a^k)=m$

אז $a^{km}=(a^k)^m=1$

$\Leftarrow$ $n|km$ (כי כל חזקה של a מתאפסת)

אבל $(k,n)=1 \Leftarrow n|m$. מצד שני $m\le n$. לכן $n=m$.

ולכן $\langle a^k\rangle=\langle a\rangle$

בכיוון השני: נניח כי $(k,n)=d>1$. אז $k=c\cdot d$ $n=b\cdot d$ $(c,b\in\mathbb{Z})$

נתבונן ב: $(a^k)^b=(a^{c\cdot d})^b=a^{c\cdot d\cdot b}=(a^{bd})^c=$

$=(a^n)^c=1$

אבל $b<n$ ולכן a^k <u>לא</u> יוצר את $\langle a\rangle$.
(כלומר הראינו כי אם הם לא זרים אז לא יוצר)

סימון: פונקציית φ של אוילר מוגדרת ע״י $\varphi(1)=1$

ו- $\varphi(n)=|\{k: 1\le k<n,\ (k,n)=1\}|$ (מס׳ המספרים שקטנים מ-n וזרים לו)

במילים אחרות: אם G ציקלית מסדר n אז יש לה $\varphi(n)$ יוצרים.

3 **טענה:**

תהי G חבורה ציקלית ו-$n=|G|$. לכל $d|n$ יש תת-חבורה ציקלית <u>יחידה</u> מסדר d.

הוכחה: אם $d|n$ ו- $G=\langle a\rangle$ אז $\langle a^{\frac{n}{d}}\rangle$ היא מסדר d

נניח ש- $\langle b\rangle$ תת-חבורה מסדר d (ברור שהיא ציקלית)

נכתוב $b=a^m$. אז $(a^m)^d=a^{md}=1 \Rightarrow n|md$

כלומר $pn=md$ $(p\in\mathbb{N})$ לכן $a^m=a^{\frac{pn}{d}}=(a^{\frac{n}{d}})^p$

לכן $b\in\langle a^{\frac{n}{d}}\rangle$

$\Leftarrow$ $\langle b\rangle\subseteq\langle a^{\frac{n}{d}}\rangle$ אבל $d=|\langle a^{\frac{n}{d}}\rangle|=|\langle b\rangle|$

לכן $\langle b\rangle=\langle a^{\frac{n}{d}}\rangle$

הערה: בכיתה ראינו שאם G חבורה אבלית $|G|=n$ ו- $d|n$ אז יש תת-חבורה מסדר d אבל לא בהכרח יחידה.

דוגמא: $G=\mathbb{Z}_2\times\mathbb{Z}_2$ $\quad H=\{(0,0),(1,0)\}$ $\quad H''=\{(0,0),(1,1)\}$ $\quad H'=\{(0,0),(0,1)\}$

כולם תת-חבורות מסדר 2.

ה) **טענה:** תהי $n\in\mathbb{N}$. אזי $n=\sum_{d|n}\varphi(d)$

הוכחה: ניתן תחילה מעט סימון:

תהי C חבורה ציקלית. נסמן ב- $gen(C)$ את קבוצת היוצרים של C.

תהי G חבורה.

$$G=\dot{\bigcup_{\substack{C\le G\\ \text{תת-חבורה ציקלית}}}} gen(C)$$ (איחוד זר) האיחוד הוא על כל תת-החבורות הציקליות של G.

כעת, נניח כי G חבורה ציקלית מסדר n (למשל $\mathbb{Z}_n$)

נקבל ש: $$n=|G|=\sum_{\substack{C\le G\\ \text{ציקלית}}}|gen(C)|=\sum_{d|n}|gen(C_d)|=\sum_{d|n}\varphi(d)$$

$C_d=$ תת-חבורה ציקלית מסדר d

$\boxtimes$

16-11-2006 (1)

מבנים אלגבריים - תרגול מס' 4

<u>תזכורת:</u> תהי G חבורה ציקלית מסדר n.

לכל d|n יש ל-G תת-חבורה מסדר d (ציקלית).

הראנו שמספר היוצרים של G הוא: $\varphi(n)=|\{k \mid 1<k<n, (k,n)=1\}|$

הגדרנו עבור חבורה ציקלית C את $gen(C)$ = קבוצת היוצרים של החבורה C. (דוגמא: $gen(\mathbb{Z}_6)=\{1,5\}$)

לכל חבורה G מתקיים: $G=\dot{\bigcup}_{\underset{\text{ציקלית}}{C\le G}} gen(C)$

כלומר G הוא איחוד זר של כל תתי החבורות הציקליות מ-G

(דוגמא: $\mathbb{Z}_6=\underset{C=\mathbb{Z}_6}{\{1,5\}}\cup\underset{C=\mathbb{Z}_2}{\{3\}}\cup\underset{C=\mathbb{Z}_3}{\{2,4\}}\cup\underset{C=e}{\{0\}}$)

תת חבורה איזומורפית ל-$\mathbb{Z}_2$ ב-$\mathbb{Z}_6$

מכאן עבור G ציקלית מסדר n:

$$n=|G|=\sum_{\underset{\text{ציקלית}}{C\le G}}|gen(C)|=$$

$$=\sum_{d|c}|gen(C_d)|=\sum_{d|n}\varphi(d)$$

C_d תת-חבורה ציקלית מסדר d

<u>טענה:</u> תהי G חבורה מסדר n ונניח שלכל d|n יש לכל היותר תת-חבורה ציקלית אחת מסדר d. אז G ציקלית.

<u>הוכחה:</u> $n=|G|=\sum_{\underset{\text{ציקליות}}{C\le G}}|gen(C)|\le\sum_{d|n}|gen(C_d)|=\sum_{d|n}\varphi(d)=n$ (טענה מהשבוע קודם)

$\Longleftarrow$ שיש שוויון מכאן לכל d|n יש תת-חבורה ציקלית מסדר d.

בפרט יש תת-חבורה ציקלית מסדר n ולכן G ציקלית.

<u>מסקנה:</u> (א) יהי F שדה ו-G תת-חבורה של F^* ($=F\setminus\{0\}$ עם כפל) סופית אז G ציקלית.

(ב) יהי F שדה סופי אז F^* ציקלית.

הוכחה: א' גורר את ב' ולכן נוכיח את א'.

אם $g\in G$, $g^{d}=1$ אז g שורש של הפולינום של הפונקציה x^d-1.

ל- x^d-1 יש לכל היותר d שורשים.

אם היו שתי תת-חבורות ציקליות מסדר d היו בהן יותר מ-d איברים, וכל איבר שורש של x^d-1 (כי הוא איבר בחבורה מסדר d) וזו סתירה.

לכן, לכל $d|n$ יש לכל היותר תת-חבורה ציקלית אחת מסדר d

$\Longrightarrow$ G ציקלית $\boxtimes$

בתרגיל, הגדרנו עבור חבורה G, $x\in G$ את מחלקת הצמידות של x:

$$x^G=\{gxg^{-1}\mid g\in G\}$$

והראינו כי:

תהי X קבוצה עם יחס שקילות כלשהו, $\equiv$, ואם עבור $x\in X$ מחלקת השקילות של x = $[x]=\{y\in X\mid x\equiv y\}$ אז $[x]\cap[y]=\emptyset$ או $[x]=[y]$

ולכן: $X=\biguplus_{x\in X}[x]$.

במקרה שלנו על G הגדרנו היחס $x\equiv y$ אם $y=gxg^{-1}$

* דוגמא נוספת ליחס שקילות על החבורה G:

תהי G חבורה. $H\leq G$ תת-חבורה. ונגדיר על G יחס שקילות: $y\equiv x$ אם $x^{-1}y\in H$

מחלקות השקילות הן מחלקות שמאליות של H. (תרגיל)

דוגמא: עבור $e\in G$ $e^G=\{e\}$

נניח כי $x=x^G \Longleftrightarrow gxg^{-1}=x$ לכל $g\in G \Longleftarrow gx=xg$

לכל $g\in G$ כלומר אם x מתחלף עם כל איברי החבורה.

הגדרה: G חבורה. המרכז של G הוא:

$$Z(G)=\{x\in G\mid gx=xg,\ \forall g\in G\}$$

כל האיברים ב-G אשר מתחלפים עם כל איבר ב-G $Z(G)\lhd G$.

נדבר עתה על מחלקות הצמידות ב-S_n.

מחלקות צמידות ב-S_n

הגדרה: יהיו $\tau,\sigma\in S_n$ ל- τ,σ אותו מבנה מחזורים אם בפירוק שלהם למכפלת מחזורים זרים, יש להם אותו מס' של מחזורים באורך r לכל r

דוגמא:

$$\sigma=(12)(345)(67)(8\,9\,10)$$

$$\tau=(34)(5\,9\,10)(18)(267)$$

טענה:

יהיו $\sigma,\tau\in S_n$ $\pi=\sigma\tau\sigma^{-1}$ אז ל- π ול- τ אותו מבנה מחזורים.

יתרה מזאת אם $\tau=\tau_1\cdot\tau_2\cdots\tau_k$ (τ_i מחזורים זרים)

ונניח $\tau_i=(i_1,i_2,\dots,i_r)$

אז $\tau_i'=(\sigma(i_1),\sigma(i_2),\dots,\sigma(i_r))$ ומתקיים $\pi=\sigma\tau\sigma^{-1}=\tau_1'\cdots\tau_k'$

(במילים אחרות, כל מחזור $(i_1,\dots,i_r)$ נהפך ל- $(\sigma(i_1)\dots\sigma(i_r))$)

דוגמא:

$$\tau=(12)(345)\qquad \sigma=(1234)\in S_5$$

$$\Longrightarrow\quad \sigma\tau\sigma^{-1}=(23)(415)$$

הוכחת הטענה:

מסימונים לעיל נסמן $\pi'=\tau_1'\cdots\tau_k'$

נראה ש- $\sigma\tau\sigma^{-1}=\pi=\pi'$

אם $\tau(i)=j$ אז $\pi'(\sigma(i))=\sigma(j)$ (נובע על-פי ההגדרה)

אולם $\pi(\sigma(i))=\sigma\pi\sigma^{-1}(\sigma(i))$

$=\sigma\tau(i)=\sigma(j)$

$\tau:\quad \tau_1\dots\ (i\ j)\ \dots\ \tau_k$

$\pi':\quad \tau_1'\dots\ (\sigma(i)\sigma(j))\ \dots\ \tau_k'$

לכן על כל האיברים מהצורה $\sigma(i)$ $1\le i\le n$ $\pi=\pi'$ (נקודתית)

אך ידוע כי σ היא תמורה ולכן היא על ולכן $\pi(k)=\pi'(k)$ $\forall\, 1\le k\le n$

$\Longleftarrow\ \pi=\pi'$

טענה: $\tau, \sigma \in S_n$ שייכים לאותה מחלקת צמידות $\iff$ ל-τ, ול-σ אותו מבנה מחזורים.

הוכחה: "$\Leftarrow$" הראינו.

"$\Rightarrow$": נניח של- τ, σ אותו מבנה מחזורים !

$\sigma=\sigma_1\cdots\sigma_k$

$\tau=\tau_1\cdots\tau_k$

ונסדר המחזורים כך ש- τ_i, σ_i מאותו אורך לכל i.

נאמר:
$$\sigma_i=(i_1 i_2 \cdots i_r)$$
$$\tau_i=(j_1 j_2 \dots j_r)$$

נגדיר $\gamma(i_1)=j_1 \quad \dots\dots \quad \gamma(i_r)=j_r$

ברור כי γ היא תמורה ומהטענה הקודמת $\tau=\gamma\sigma\gamma^{-1}$.

דוגמה:
$$\sigma=(12)(345)$$
$$\tau=(34)(125)$$
$$\gamma=\begin{pmatrix}1&2&3&4&5\\3&4&1&2&5\end{pmatrix}=(13)(24)$$
$$\gamma\sigma\gamma^{-1}=\tau$$

אם נכתוב $\sigma=(21)(453)$

$\tau=(34)(125)$

ונגדיר γ'
$$\gamma'=\begin{pmatrix}1&2&3&4&5\\4&3&5&1&2\end{pmatrix}=(14)(235)$$

גם $\gamma'\sigma(\gamma')^{-1}=\tau$

מסקנה: תהי $H\le S_n$.

$H\trianglelefteq S_n \iff \sigma\in H \Rightarrow$ כל התמורות עם אותו מבנה מחזורים נמצא ב-H.

לסיכום: תת-החבורות (הנורמליות) הלא טריוויאליות היחידות של S_4 הן V ו-A_4.

16-11-2006

דוגמא: S_3

$$S_3 = \left\{ \begin{matrix} id \\ (12),(23),(13) \\ (123)\ (132) \end{matrix} \right\}$$

אם $H \triangleleft S_3$, נוסף H תת-חבורה ולכן: $1 \in H$, $|H| \mid \underset{=|S_3|}{6}$

ו-H איחוד של מחלקות צמידות.

$\{id\} = e \triangleleft S_3$ (החבורה הטריוויאלית)

החבורה עצמה גם היא תמיד נורמלית $S_3 \triangleleft S_3$

אלו הם מקרים מנוונים

$A_3 \triangleleft S_3$ ואלה הן תת החבורות הנורמליות היחידות ב-S_3.

$A_3 = \{id,(123),(132)\}$

דוגמא ב': $|S_4|=24$

ב-S_4 יש: ⊛ מחזור 1 ע 1: id

$\frac{4\cdot3}{2}=6$ ⊛ מחזורים מאורך 2: 6 חילופים

$\frac{4\cdot3\cdot2}{3}$ ⊛ מחזורים מאורך 3: 8 מחזורים מאורך 3

⊛ מחזורים מאורך 4: 6 מחזורים מאורך 4

⊛ 3 תמורות מהצורה $(ab),(cd)$

ולכן, הגדלים של מחלקות הצמידות הם: $1, 6, 8, 6, 3$

נחפש תת-חבורות נורמליות ב-S_4: $H \triangleleft S_4$

$e \triangleleft S_4$ $S_4 \triangleleft S_4$

המחלקים של $|S_4|=24$ הם $1, \cancel{2}, \cancel{3}, 4, \cancel{6}, \cancel{8}, 12, 24$ ואלו הם הגדלים של ה תתי החבורה מכן.

אין תת-חבורות נורמליות מסדר 2,3

עבור 4 יש את V מהתרגיל. (היא נורמלית כי היא איחוד של מחלקות צמידות)

והיא היחידה הנורמלית מסדר 4.

אין תת-חבורות נורמליות מסדר 6, 8.

A_4 תת-חבורה נורמלית מסדר 12. (יחידה מסדר 12)

הגדרה: חבורה אבלית פשוטה היא חבורה אבלית, שתת-החבורות הנורמליות היחידות שלה הן $\{e\}$ והחבורה עצמה.

דוגמא: G אבלית פשוטה $\iff$ G ציקלית מסדר p ראשוני

הוכחה:

($\Leftarrow$) חבורה ציקלית, היא אבלית. ולחבורה מסדר p ראשוני, אין תת-חבורות לא טריוויאליות (לגרנג').

($\Rightarrow$) נניח כי G אבלית ופשוטה.

נבחר $e\neq x\in G$ $\quad \langle x\rangle = G$ (ציקלית)

אם $n=|\langle x\rangle|$ לא ראשוני אז $1<d\mid n$ אז יש תת-חבורה מסדר d ולכן n חייב להיות ראשוני. ▨

משפט: עבור $n\geq 5$ A_n חבורה פשוטה.

הגדרה: תהי G חבורה. $x\in G$ $\quad C_G(x)=\{g\in G\mid gx=gx\}$

$C_G(x)$ נקרא המרכז של x (כל האיברים שמתחלפים עם x)

דרך נוספת $\quad gx=xg \iff gxg^{-1}=x$

כלומר, כל האיברים שאם מצמידים בהם את x, נשארים במקום.

טענה: G חבורה. $x\in G$

מתקיים $\quad |x^G|=[G:C_G(x)]$

מחלקת הצמידות של x

בפרט, עבור $|G|<\infty$ $\quad |x^G|=|G|/|C_G(x)|$

הערה: $C_G(x)$ היא תת-חבורה.

הוכחת הטענה: נגדיר העתקה $f: x^G \longrightarrow G/C$ (נסמן $C=C_G(x)$)

נגדיר: $\quad f(gxg^{-1})=gC$

נבדוק כי f מוגדרת היטב:

אם $gxg^{-1}=hxh^{-1} \iff h^{-1}gx=xh^{-1}g$ אז $h^{-1}g\in C \xLeftrightarrow{\text{הגדרה}} hC=gC$

ובעצם קיבלנו גם כי f חח"ע.

ברור כי f על. לכל g נפעיל את f על gxg^{-1} ונקבל את gC

סוף הוכחת הטענה. ▨

הוכחת המשפט:

למה א': A_5 פשוטה.

תזכורת: ראינו ש- $\theta,\tau\in S_n$ צמודים אם ורק אם יש להם את אותו מבנה מחזורים.

הערה: $H<G$ תת-חבורה, $x,y\in H$ אז אם x,y צמודים ב-H אז הם צמודים ב-G אבל לא בהכרח להיפך.

הוכחת למה א': A_5 מכילה את id, מחזורים מאורך 3, כמה? $\frac{5\cdot4\cdot3}{3}=20$

מכפלות של חילופים זרים, כמה כאלו יש? $\frac{1}{2}\left(\frac{5\cdot4}{2}\cdot\frac{3\cdot2}{2}\right)$ מחזורים מאורך 5: $\frac{5!}{5}=4!=24$

(א) מחזורים מאורך 3 צמודים ב-A_5:

נניח, בלי הגבלת הכלליות כי $\theta=(123)$ נניח τ מחזור אחר מאורך 3.

קיים $\rho\in S_5$ כך ש- $\rho\theta\rho^{-1}=\tau$ אם ρ זוגית סיימנו.

אם לא, נגדיר $\rho'=\rho(45)$ ואז:

$$\rho'\theta\rho'^{-1}=\rho(45)(123)(45)\rho^{-1}=\rho(123)\rho^{-1}=\tau$$

אבל ρ' זוגית ולכן סיימנו.

(ב) כל התמורות שהן מכפלות של שני חילופים זרים צמודות ב-A_5.

שוב, נניח $\theta=(12)(34)$, τ תמורה כנ"ל ונניח $\rho\in S_5$

ו- $\rho\theta\rho^{-1}=\tau$

אם ρ זוגית סיימנו. אם ρ אי-זוגית נגדיר $\rho'=\rho(12)$ (זוגית)

$=\rho(12)(34)\rho^{-1}=\tau$

(ג) ב-A_5 יש שתי מחלקות צמידות של מחזורים מאורך 5, כל אחת מכילה 12 איברים.

הוכחה בעמ' הבא ⟵

הוכחה: נניח כי $\alpha=(12345)$. הראנו ש-

$|\alpha^{S_5}| = |S_5| / |C_{S_5}(\alpha)|$ ונקבל: $|C_{S_5}(\alpha)| = \frac{120}{24} = 5$

מאידך, נשתכנע ש $\langle\alpha\rangle \subseteq C_{S_5}(\alpha)$ אבל $|\langle\alpha\rangle|=5 \Longrightarrow C_{S_5}(\alpha)=\langle\alpha\rangle$

בתרגיל נראה טענה: עבור $H\le G$ תת-חבורה ו $x\in H$ אז

$$C_H(x)=C_G(x)\cap H$$

ולכן נקבל כי $C_{A_5}(\alpha)=C_{S_5}(\alpha)\cap A_5=\langle\alpha\rangle$

שוב, מהטענה שהוכחנו

$$|\alpha^{A_5}| = \frac{|A_5|}{|C_{A_5}(\alpha)|} = \frac{60}{5} = 12$$

לסיכום: גדלי מחלקות הצמידות ב-A_5 הם: 1,20,15,12,12

תת-חבורה נורמלית היא איחוד של מחלקות צמידות (כולל 1) והסכום שלה מחלק את 60 נובע כי אין תת-חבורה נורמלית לא טריוויאלית.

למה ב: עבור $n\ge 5$ אם $N\lhd A_n$ ו-N מכילה מחזור מאורך 3 אז $N=A_n$

הוכחה: נראה שאם N מכילה מחזור אחד מאורך 3 אז היא מכילה את כל המחזורים מאורך שלוש ומתרגיל 4, 3,5, $N=A_n$.

בתרגול ראינו כבר כי שתי תמורות מאורך 3 צמודות ב-A_n אם $n\ge 5$.

שוב דרך: נניח $\theta=(123)$ $\tau=(i,j,k)$ אם θ ו-τ לא זרות

אז (למשל $k\in\{1,2,3\}$) אז θ ו-τ מזיזות רק את האיברים $\{1,2,3,i,j\}$

נגדיר:

$A^*=\{\theta\in A_n \mid$ לא מזיזה איברים חוץ מ- $\{1,2,3,i,j\}$ $\theta\}$

$A^*\cong A_5$ ולכן מהלמה א θ ו-τ צמודות.

אם הן זרות אז: $\theta=(1,2,3)$ צמודה ל-$(12k)$ ו- $(12k)$ צמודה ל-(ijk)

ולכן θ צמודה ל-τ.

למה ג: A_6 פשוטה.

הוכחה: נניח כי $\{1\}\ne H\lhd A_6$

נניח כי $\theta\in H$ ו $\theta(i)=i$

נגדיר: $F=\{\tau\in A_6 \mid \tau(i)=i\}\cong A_5$

נשתכנע ש $\emptyset\ne(H\cap F)\lhd F$ כי $\theta\in(H\cap F)$

(למה א')

לכן ∀ $A\cap F = F \Longleftarrow F\leq H$ תת-חבורה.

לכן H מכילה מחזור באורך 3 ולכן $H=A_6$ מלמה ב'.

אפשר להניח שכל התמורות ב-H פרט לזהות מזיזות את כל המספרים מ- $(1,\dots,6)$:

$(12)(3456)=\alpha$

$(123)(456)=\beta$

אם $\alpha^2(1)=1$ מצד שני $\alpha^2\in H$, $id\neq\alpha^2$, סתירה.

נניח כי $\gamma=(234)$

$$\underset{H\ni}{\rho}=\beta(\gamma\,\underset{\in H}{(\beta^{-1}\gamma^{-1})})\in H$$

$$(123)(456)(234)[(123)(456)]^{-1}\cdot(243)=(315)(243)\Rightarrow\rho(6)=6$$

מגיעים לכך ש σ מעבירה
את $\{2,3,4\}$ לעצמה בסתירה להנחה.

<u>הוכחת המשפט:</u>

A_n פשוטה.

נניח $\{1\}\neq H\lhd A_n$ נראה כי H מכילה מחזור מאורך 3. ומלמה ב' $H=A_n$.

נניח $id\neq\beta\in H$ $\beta(i)=j$ $(i\neq j)$

נבחר מחזור מאורך 3, α, כך ש: $\alpha(i)=i$ ו- $\alpha(j)\neq j$

אם $\alpha\beta\neq\beta\alpha$ כי,

$\alpha\circ\beta(i)=\alpha(j)\neq j$

$\beta\circ\alpha(i)=\beta(i)=j$

לכן $\rho=\alpha\beta\alpha^{-1}\beta^{-1}\neq 1$

$$\rho=(\alpha\underset{\in H}{\beta\alpha^{-1}})\underset{\in H}{\beta^{-1}}\in H$$

אבל: $\rho=\alpha(\beta\alpha^{-1}\beta^{-1})$

לכן ρ היא מכפלה של 2 מחזורים מאורך 3 ולכן ρ מזיזה

לכל היותר 6 מספרים ונסמנם $i_1,i_2,\dots,i_6$ נגדיר:

$A_6\cong F=\{\theta\in A_n \mid$ θ לא מזיזה מספרים פרט ל: $\{i_1,\dots,i_6\}\}$

$\Longleftarrow F$ פשוטה (מלמה ג') $\rho\in(H\cap F)\lhd F$

$\Longleftarrow H\cap F=F \Longleftarrow H\geq F$

לכן H מכילה מחזור מאורך 3 ולכן מלמה ב' $H=A_n$.

$\blacksquare$

<u>הגדרה</u>: G חבורה פועלת על קבוצה X אם יש העתקה

$$f: G\times X \longrightarrow X$$

(נסמן: $f(g,x)=g\cdot x$)

המקיימת $1\cdot x = x$

$$g(hx)=(gh)x$$

הראינו שזה שקול לכך שקיים הומומורפיזם $\varphi: G \longrightarrow Per(X)$

<u>הגדרה</u>: אם G פועלת על X, $x\in X$ אז <u>המסלול</u> של x הוא:

$$O(x)=\{gx \mid g\in G\}$$

<u>הגדרה</u>: פעולה תקרא <u>טרנזיטיבית</u> אם קיים מסלול אחד (לכל האיברים).

ראינו כי $O(x)\cap O(y)\neq\phi \Longrightarrow O(x)=O(y)$

<u>דוגמאות לפעולות</u>:

① S_n פועלת על $\{1,2,\ldots,n\}$

② V מרחב וקטורי, $GL(V)$ טרנספורמציות לינאריות הפיכות, אז $GL(V)$ פועלת על V.

③ G חבורה, G פועלת על עצמה ע"י כפל משמאל (זה יהיה טרנזיטיבי)

④ G חבורה, G פועלת על עצמה ע"י הצמדה

הראינו $x,y\in G$! $x^G\cap y^G\neq\phi \Longrightarrow x^G=y^G$

זהו מקרה פרטי לכך שאם G פועלת על X $x,y\in X$

אז $O(x)\cap O(y)\neq\phi \Longrightarrow O(x)=O(y)$

<u>יש לשים לב</u>: אם $gx=y \Longrightarrow x=g^{-1}y$ כלומר אם אפשר <u>להגיע</u> מ-a ל-b

אפשר להגיע מ-b ל-a (מחלקות צמידות זה פשוט מסלולים תחת פעולת ההצמדה)

הגדרה: G פועלת על X. יהי $x\in X$

המייצב של x ב- G הוא $Stab_G(x)=\{g\in G \mid gx=x\}$

והמייצב (קל לראות) הוא תת חבורה של G.

למשל, בדוגמא ④ (ההצמדה) המייצב הוא **המרכז** של x $C_G(x)$.

למשל, בדוגמא של הכפל משמאל, החבורה הטריוויאלית $\{e\}$ היא המייצב של כל $g\in G$.

ראינו, כי $|x^G|=[G:C_G(x)]$

גם באופן כללי, $|O(x)|=[G:Stab_G(x)]$

(הוכחה כמו אז, נגדיר העתקה: $gx \longmapsto g\cdot Stab_G(x)$

זה יתן העתקה חח"ע ועל מ- $O(x)$ ל- $G/Stab_G(x)$)

כי קבוצה, לאו דווקא חבורה.

הגדרה: $T:\mathbb{R}^n\to\mathbb{R}^n$, $\mathbb{R}^n$ עם המכפלה הסקלרית הרגילה, נקראת **איזומטריה** אם $\|T(x)-T(y)\|=\|x-y\|$

(עם הנורמה האוקלידית)

דוגמאות:

(א) עבור $\omega_0\in V$ נגדיר הזזה ב- ω_0 $T_{\omega_0}(v)=v+\omega_0$ (?) לבדוק

(ב) T טרנספורמציה לינארית אורתוגונלית

($\|T(x)\|=\|x\|$, או $\langle T(x),T(y)\rangle=\langle x,y\rangle$, או T לוקחת בסיס אורתונורמלי לבסיס אורתונורמלי. $(T^*=T^{-1})$.

אז T איזומטריה כי: $\|T(x)-T(y)\| \underset{\text{מהלינאריות}}{=} \|T(x-y)\| \underset{\text{מהאורתוגונליות}}{=} \|x-y\|$

למה: איזומטריה הקובעת את הראשית (כלומר $T(0)=0$) היא טרנספורמציה לינארית אורתוגונלית.

30-11-2006

הוכחה:

טענה: אם T איזומטריה ו-T קובעת את הראשית ואת איברי הבסיס הסטנדרטי אז $T=id$.

הוכחה: יהי $x=(x_1,\dots,x_n)$ ב X כלשהו. ! $T(x)=(y_1,y_2,\dots,y_n)$

T קובעת את הראשית $\Longleftarrow$

$$\|Tx\|^2=\|Tx-T0\|^2=\|x-0\|=\|x\|^2$$

$$\Longleftrightarrow \quad y_1^2+y_2^2+\dots+y_n^2=x_1^2+x_2^2+\dots+x_n^2$$

T קובעת את $e_1=(1,0,\dots,0)$.

$$\|x-e_1\|^2=\|T(x)-T(e_1)\|^2=\|T(x)-e_1\|^2$$

$$\Longleftarrow \quad (y_1-1)^2+y_2^2+\dots+y_n^2=$$

$$=(x_1-1)^2+x_2^2+\dots+x_n^2$$

$$\Longleftarrow \quad 2y_1=2x_1$$

$$\Downarrow$$

$$y_1=x_1$$

באופן דומה נקבל $x_i=y_i$ (ע"י חיסור של e_i)

זה אומר ש: $T(x)=x \Longrightarrow T(x)=id$ וזהו סוף הוכחת הטענה.

נחזור עתה להוכחת הלמה:

נסמן $T(e_i)=u_i$. נטען ש-$\{u_i\}$ בסיס אורתונורמלי.

(זה מושאר כתרגיל) כדאי להסתכל בשיוויון $\|e_i-e_j\|^2=\|u_i-u_j\|^2$

אז $\{u_i\}$ אורתונורמלי.

נגדיר את S להיות הטרנספורמציה הלינארית המקיימת $S(e_i)=u_i$

ועכשיו נראה ש- S טרנספורמציה לינארית (והיא תהיה אורתוגונלית כי היא מעבירה בסיס אורתונורמלי מסוים לבסיס אורתונורמלי אחר; ואז נקבל לפי הלמה שהיא הפיכה, כלומר מתלכדת עם T ואז T תהיה טרנספורמציה לינארית אורתוגונלית)

אז S אורתוגונלית ולכן הפיכה, ההרכבה $S^{-1}\circ T$ היא איזומטריה (הרכבה של איזומטריות) והיא קובעת את אפס ואת הבסיס הסטנדרטי

$\Longleftarrow$ (מהטענה) $S^{-1}\circ T=id \Longleftarrow T=S$.

טענה: כל איזומטריה T היא הרכבה של טרנספורמציה לינארית אורתוגונלית והזזה.

הוכחה: אם $T(0)=w$ אז $\underset{\text{הזזה ב-}w}{T_{w}}\circ T = S$ איזומטריה הקובעת את 0.

ולכן S טרנספורמציה לינארית אורתוגונלית $T=T_w\circ S$

חבורת הטרנספורמציות הלינאריות האורתוגונליות על $\mathbb{R}^n$ מסומנת $O_n(\mathbb{R})$

תרגיל: המיצב של כל נקודה תחת פעולת חבורת האיזומטריות איזומורפי ל $\mathbb{R}^n$.

הגדרה: מטריצה $S\in O_n(\mathbb{R})$ תקרא סיבוב אם $\det S=1$

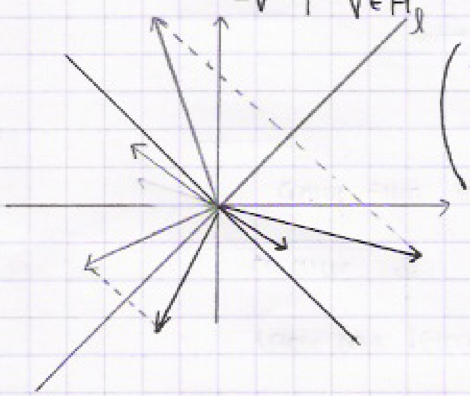
S תקרא הופכת אוריינטציה אם $\det S=-1$

(תזכורת: $S^{-1}={}^tS$ — S טרנספוס
$1=|S\cdot {}^tS|=|S|\cdot|{}^tS|=|S|^2$)

דוגמה: יהי H תת-מרחב של $\mathbb{R}^n$ ממימד $n-1$

השיקוף ביחס ל-H היא טרנספורמציה לינארית הקובעת את H

(כלומר $\forall v\in H$ $T(v)=v$) והופכת את הוקטור $v\in H^{\perp}$ ל- $-v$



ביחס לבסיס מתאים המטריצה של T היא

$$\begin{pmatrix}1&&&&\\&1&&&\\&&\ddots&&\\&&&1&\\&&&&-1\end{pmatrix}$$

(כלומר נבחר בסיס אורתונורמלי ל-H, ונוסיף $v\in H^{\perp}$ כך ש $\|v\|=1$)

דוגמה: $\mathbb{R}^2$. המטריצות האורתוגונליות הן מאחת מהצורות:

$$A=\begin{pmatrix}\cos\theta&\sin\theta\\-\sin\theta&\cos\theta\end{pmatrix}$$ מטריצת סיבוב בזווית θ

$$B=\begin{pmatrix}\cos\theta&\sin\theta\\\sin\theta&-\cos\theta\end{pmatrix}$$ מטריצה הופכת אוריינטציה בזווית θ מתאימה לכל S.

דוגמה: $v_1=(\cos\frac{\theta}{2},\sin\frac{\theta}{2})$ וקטור עצמי עם ערך עצמי 1

$v_2=(-\sin\frac{\theta}{2},\cos\frac{\theta}{2})$ וקטור עצמי עם ערך עצמי -1

אם $v=\lambda_1v_1+\lambda_2v_2$ אז:

$$Sv=S(\lambda_1v_1+\lambda_2v_2)=\lambda_1v_1-\lambda_2v_2$$

זהו שיקוף ביחס לישר ש-v_1 פורש

מסקנה:

טרנספורמציה ליניארית אורתוגונלית ב- $O_2(\mathbb{R})$ היא סיבוב או שיקוף.

(הערה/הגדרה: $SO_n(\mathbb{R})$ - חבורת הסיבובים של $\mathbb{R}^n$

תת-חבורה של $O_n(\mathbb{R})$ $\quad \underset{\text{האינדקס}}{2 =} [O_n(\mathbb{R}) : SO_n(\mathbb{R})]$)

הסבר לגבי האינדקס:

$$\det : O_n(\mathbb{R}) \longrightarrow \{\pm 1\}$$ (הדטרמיננטה היא פונקציה)

$$\ker(\det) = SO_n(\mathbb{R})$$

$$\Longrightarrow \left| O_n(\mathbb{R}) / SO_n(\mathbb{R}) \right| = \left| \{\pm 1\} \right| = 2$$

נניח $G \le O_2(\mathbb{R})$ תת-חבורה סופית.

נתבונן ב- $H \le G$ תת-החבורה של סיבובים מ-G.

נסמן עבור $T \in H$ נסמן $\Theta(T)$ אם T היא סיבוב בזווית Θ,

כלומר את זווית הסיבוב של Θ.

נבחר $T \in H$ עבורו $\Theta(T)$ מינימלי. עבור $R \in H$ (סיבוב כלשהו)

יש $m \in \mathbb{N}$ כך ש: $m\Theta(T) \le \Theta(R) \le (m+1)\Theta(T)$

אז:

$$0 < \Theta(T^{-m}R) < \Theta(T)$$

מהמינימליות $\Theta(T^{-m}R) = 0 \Longrightarrow T^{-m}R = id$

או במילים אחרות $R = T^m$

לכן H חבורה ציקלית. $H = \langle T \rangle$

אם $H = G$ אז G חבורה ציקלית $|G| = n$, T סיבוב בזווית $\frac{2\pi}{n}$

...נמשיך בשיעור הבא...

7-12-2006

amie@math.huji.ac.il

הגדרה: (א) G חבורת-p אם G מסדר p^n $\quad |G|=p^n$

זה נכון אם ורק אם כל איבר ב-G הוא מסדר p^r.

(חבורות p-סלו הם מקרה פרטי חבורות-p)

② $Z(G)=\{g\in G \mid gh=hg \ \forall h\in G\}$ = המרכז של G

© $C_G(x)=\{g\in G \mid gx=xg\}$ = המרכֵּז של x ב-G (מרכֵּז הוא כל אשר מסדרים)

③ $H\le G$ $\quad N_G(H)=\{g\in G \mid gHg^{-1}=H\}$ המנרמל של H.

פתרון שאלות מתרגיל בית מס' 6:

⑥ $G\le GL_d(\mathbb{Z}_p)$ פועלת על $X=V$

$X=\bigcup_{x\in X} O(x)$ (איחוד המסלולים = זהו איחוד זר ולכן ניתן להתכל X הסכום של הגדלים)

אז $|V|=p^d$

ראינו ש: $|O(x)| \,\big|\, |G|=p^n$ (גודל מסלול מחלק את סדר החבורה)

לכן כל מסלול הוא מסדר חזקה של p. המסלול של אפס הוא מגודל 1.

אם כל שאר הנקודות אין נקודות שבת אז הגדלים של שאר המסלולים הם חזקה חיובית של p לכן היינו מקבלים $|V|\equiv 1 \pmod p$ סתירה!

⑦ א. X אוסף הישרים ב-V (תת-מרחב ממימד 1 ב-V)

אם למשל $x\in X$ $\quad x=\mathrm{span}\{v\}$ $\quad (0\neq v\in V)$

$gx=sp\{gv\}$ $\quad (v'\in X \Leftarrow v'=\lambda v \quad gv'=\lambda gv$ ב- $\mathrm{span}\{gv\})$

נתבונן ב- $\mathrm{span}\{e_1\}$

נניח $x=\mathrm{span}\{v\}$ אז נשלים את v לבסיס של המרחב $v_1,v_2,\dots,v_d$

ונסדר העתקה שמעבירה את $e_1,e_2,\dots,e_d$ ל- $v_1\dots v_d$ בהתאמה.

נתבונן ב:

$$g=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \\ \vdots & & & \\ a_{n1} & \cdots & & a_{nn}\end{pmatrix}\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}=\begin{pmatrix}a\\0\\\vdots\\0\end{pmatrix}$$

כלומר

$$=\begin{pmatrix}a_{11}\\a_{21}\\\vdots\\a_{n1}\end{pmatrix}$$

לכן $a_{i1}=0$ עבור $i\neq 1$

הרעיון של ההמשך הוא דומה, רק נסביר כמה דברים:

הגדרה: יהי V מרחב וקטורי. אז דגל של תתי-מרחבים ב-V היא סדרה עולה של תתי-מרחבים:

$$\{0\} = V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_k \subsetneq V$$

(תתי המרחבים (ואלה יכולים להיות מכל מיני מימדים ולכן הטיפוס של הדגל נקבע לפי סדרת המימדים של תתי-המרחבים).

נאמר שדגל הוא מטיפוס $(n_1, \dots, n_k)$ אם המימד של V_i הוא n_i:
כלומר: $\dim V_i = n_i$.

דגל הוא מלא אם לכל $1 \le i \le d$ המימד של V_i הוא i כלומר: $\dim V_i = i$.

כדי להראות שהפעולה של GL_d על דגלים מטיפוס נתון היא טרנזיטיבית מספיק להראות שהיא טרנזיטיבית על דגלים מלאים.

כי, נניח שהוכחנו ו- $X_1 = \{0\} \subsetneq V_{i_1} \subsetneq V_{i_2} \dots \subseteq V$

$X_2 = \{0\} \subsetneq U_{i_1} \subseteq U_{i_2} \dots \subseteq V$

שני דגלים מאותו טיפוס, אז נשלים אותם לדגלים מלאים.

נסמנם: $\tilde{X}_1, \tilde{X}_2$ נניח $g\tilde{X}_1 = \tilde{X}_2$ אז ברור שגם

$gX_1 = gX_2$

אם אנחנו רוצים להראות טרנזיטיביות, ניקח דגל אחד ונראה שממנו ניתן להגיע לכל דגל אחר:

נסמן: $f = 0 \subsetneq sp\{e_1\} \subsetneq sp\{e_1, e_2\} \dots \subsetneq sp\{e_1, \dots, e_{d-1}\} \subseteq V$

נניח ש- f' דגל מלא אחר, הוא מהצורה:

$$\{0\} \subsetneq sp\{v_1\} \subseteq sp\{v_1, v_2\} \subsetneq \dots \subsetneq sp\{v_1, \dots, v_{d-1}\} \subseteq V$$

צריך להראות שיש מטריצה הפיכה שלוקחת את e_i ל- v_i.

זוהי אלגברה לינארית בסיסית ונשאיר את זה לנו, לחזור לזה...

(הרעיון בסופו של דבר הוא אותו הרעיון של סעיף א' רק שיש לנו פחות חופש לבחור)

המשמעות של "לקבע את המייצב של הדגל הנה":

המייצב מורכב ממטריצות $g \in GL_d$ רק ש- $ge_1 = \lambda e_1$

$ge_2 \in sp\{e_1, e_2\}$

$\Leftarrow ge_2 = \lambda_2 e_1 + \mu_2 e_2$

(המשך):

7-12-2006 ②

⋮

$g e_n = \lambda_n e_1 + \mu_n e_2 + \dots + f_n e_3 + \dots$

בשבוע שעבר דיברנו על איזומטריות והשתמשנו בסימון:

$O_n(\mathbb{R})$ = מטריצות אורתוגונליות (הדטרמיננטה היא 1 או -1)

ראינו שב-$\mathbb{R}^2$, יש שני סוגי מטריצות ב- $O_2(\mathbb{R})$

$A = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$ = מטריצת סיבוב בזווית θ. $(\det = 1)$

$B = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$ = שיקוף $(\det B = -1)$ ול-B ערכים עצמיים $1, -1$

המתאימים וקטורים עצמיים:

$(-\sin\frac{\theta}{2}, \cos\frac{\theta}{2})$,

$(\cos\frac{\theta}{2}, \sin\frac{\theta}{2})$

(בהתאמה)

עתה, נניח $G \le O_2(\mathbb{R})$ סופית.

סימון: $H \le G$ תת-החבורה של סיבובים ב-G.

ראינו ש- H חבורה ציקלית $H = \langle T \rangle$ ואם $|H| = n$ אז T סיבוב בזווית $\frac{2\pi}{n}$.

נניח $S \in G$ שיקוף (איבר בחבורה). במחלקה $S \cdot H$ יש n שיקופים.

מאידך אם $R \in G$ שיקוף אז $S \cdot R \in H$ ולכן $\Leftarrow$ $R \in S^{-1}H = SH$

לכן $G = \ \cup SH \Rightarrow |G| = 2n$

בנוסף לזה, $G = \langle T, S \rangle$ (G נוצרת ע"י סיבוב וע"י שיקוף)

כי: $T^n = id$ (אנו יודעים), $S^2 = 1$, $(ST)^2 = 1 \Rightarrow STST = 1 \Rightarrow STS = T^{-1}$

(הגדרה: חבורה מסדר 2n, אשר נוצרת ע"י שני איברים S, T כאשר $S^2 = 1$, $T^n = 1$ ו- $STS = T^{-1}$ נקראית חבורה דיהדרלית ומסמנים D_{2n}

מסקנה:

תת-חבורה סופית של $O_2(\mathbb{R})$ היא ציקלית או דיהדרלית.

נסמן $R = S \cdot T$. זה שיקוף. $G = \langle S, R \rangle$

לכן D_{2n} נוצרת ע"י שני שיקופים.

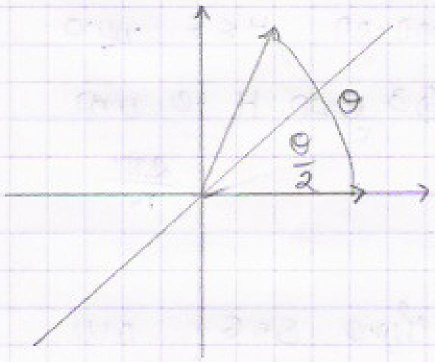
ניקח למשל S שיקוף ביחס לציר X.

$$T = \begin{pmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ -\sin\frac{2\pi}{n} & \cos\frac{2\pi}{n} \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$\Leftarrow \quad R = \begin{pmatrix} \cos\frac{2\pi}{n} & \sin\frac{2\pi}{n} \\ \sin\frac{2\pi}{n} & -\cos\frac{2\pi}{n} \end{pmatrix}$$

תזכורת: ראינו קודם ש: $B = \begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$ שיקוף ביחס לישר בזווית $\frac{\theta}{2}$ מציר ה-X.

אז R שנתונה לנו היא שיקוף ביחס לישר בזווית $\frac{\pi}{n}$ מציר ה-X.



הגדרה: בהינתן צורה במישור Δ נגדיר

$$S(\Delta) = \{ S \in O_2(\mathbb{R}) \mid S(\Delta) = \Delta \}$$

חבורת הסימטריות של Δ.

למשל $S(O) = O_2(\mathbb{R})$. (כל הסיבובים והשיקופים הם סימטריות של מעגל)

עבור משולש, יש הומומורפיזם חח"ע $S(\Delta) \longrightarrow Per(X)$

X - הקודקודים של Δ.

לכן $S(\Delta)$ סופית.

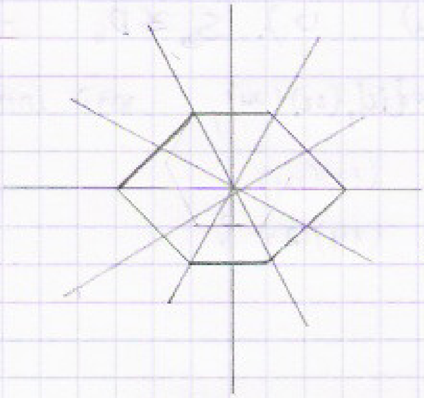
דוגמא: משולש כללי Δ $\quad S(\Delta) \cong 1$ (כי אורך הצלעות חייב להשמר)

משולש שווה שוקיים  $\quad S(\Delta) \cong \mathbb{Z}_2$

משולש שווה צלעות $\quad S(\Delta) \cong S_3$ $\quad (S_3 = \text{מתמורות})$

7-12-2006 באופן כללי, אם ישנו מצולע משוכלל: ③

נסתכל במשושה לצורך הסבר



ישנם 6 סיבובים

וישנם 6 שיקופים

כך מקבלים החבורה הדיהדרלית D_{12}

עבור מצולע משוכלל עם n צלעות,

$$S(\Delta)=D_{2n}$$

הערה: $|S(\Delta)|=2n$ פועלת על הצלעות טרנזיטיבית,

יש n צלעות וגודל המייצב של כל אחת 2 (הזהות או שיקוף דרך האמצע)

לכן $|S(\Delta)|=2\cdot n$

טענה: תהי G חבורה סופית. $a,b\in G$ איברים מסדר 2

$G=\langle a,b\rangle$ (נוצרת ע"י a,b) אז $G\cong D_{2n}$ (n כלשהו)

הוכחה: נסמן $s=a\cdot b$ ונניח ש- $o(s)=n$ (הסדר של s)

$$a\cdot sa=aaba=ba=$$
$$=b^{-1}a^{-1}=s^{-1}$$

אז היחסים המתאימים מתקיימים.

נשאר להראות $|G|=2n$

למה: $a\cdot s^i\neq 1 \quad \forall i$

הוכחת הלמה: מספיק להניח $i\neq 0,1$

בשלילה נבחר i מינימלי כך ש: $a\cdot s^i=1$

$$1=a\cdot s^i=aabs^{i-1}=bs^{i-1}$$

נכפיל ב- b משני הצדדים ונקבל: $1=s^{i-1}b=$

$$=s^{i-2}abb=s^{i-2}a$$

מאותו דומה $1=as^{i-2}$ סתירה!

נובע ש: $as^i\neq s^j \quad \forall i,j$

אנו יודעים כי $|\langle a,s\rangle|\geq 2n \Leftarrow \langle a,s\rangle\supseteq\langle s\rangle\cup a\langle s\rangle$

כדי להראות שיוויון נראה ש- $H=\{a^is^j \mid i=0,1,\ j=0\ldots n-1\}$ חבורה

תמשך

←

(כמובן מופיעים מכפלות מהצורה as^ias^j, s^is^j, as^is^j, s^ias^j.)

<u>דוגמאות:</u> $S_3 \cong D_6$ (כי $(12)(23)$ יוצרים את S_3)

חבורת קליין $V=\{id, (12)(34), (13)(24), (14)(23)\}$

$V \cong D_4$

מבנים אלגבריים - תרגול מס' 8

<u>הגדרה:</u> תהי G חבורה סופית. $|G|=p^\alpha m$ (p,m) זרים.
חבורת p-סילו של G היא תת-חבורה H, $|H|=p^\alpha$

<u>משפטי סילו:</u>

1. לכל G, קיימת חבורת p-סילו
2. אם יש n חבורות p-סילו אז $n \,||G|$ ו- $n\equiv 1 \bmod p$
3. כל חבורות p-סילו הן צמודות.

<u>הערה:</u> יש חבורת p-סילו יחידה אם ורק אם היא נורמלית.

<u>שאלות מתרגיל 7:</u>

<u>שאלה 3:</u>

<u>טענה:</u> אין חבורה פשוטה מסדר 30.

<u>הוכחה:</u> בעזרת מניית איברים.

נניח כי G פשוטה $30=2\cdot3\cdot5$

יש חבורות 5-סילו מסדר 5. כמה כאלו יש?
אין חבורה אחת ולכן יש 6 חבורות 5-סילו והחיתוך של כל שתי תת-חבורות 5-סילו הוא $\{e\}$ הסדר של כל איבר שלא בחיתוך הוא 5.
וקיבלנו $6\cdot4=24$ איברים מסדר 5 (שונים).

יש חבורות 3-סילו מסדר 3. כמה כאלו יש? אין חבורה אחת ולכן יש 10 חבורות 3-סילו והחיתוך של כל 2 ת"ח הוא $\{e\}$ (כי הם מסדר ראשוני ולכן ציקליות)
$20=10\cdot2$ איברים מסדר 3 (שונים)

וקיבלנו מסה"כ 44 איברים שונים - סתירה (כי בחבורה יש מסה"כ 30 איברים)
$\blacksquare$

טענה: אין חבורה פשוטה מסדר 12

הוכחה: $12=2^2\cdot 3$

כמו קודם נחשב: יש 4 חבורות 3-סילו, שתורמות $4\cdot 2=8$ איברים מסדר 3.

יש חבורות 2-סילו, וסדרן הוא 4. יש 3 כאלו (החבורות האלו לאו דווקא ציקליות). סדר האיברים הוא 2 או 4

החיתוך לא בהכרח ריק אבל החיתוך של כל 2 תת-חבורות הוא לכל היותר מסדר 2.

ונקבל לפחות 6 איברים נוספים (אברים מסדר 2,4 + היחידה)

וקיבלנו $8+6=14$ איברים. סתירה!

$\boxed{}$

דוגמא: חבורות 2-סילו ב-S_4. $24=2^3\cdot 3$

$$P_1=\langle (1,3),(1234)\rangle=\{e,(13),(1234),(14)(23),(24),(12)(34),(13)(24),(1432)\}$$

P_1 אינה נורמלית. למשל חסרים הילופים.

לכן יש 3 חבורות 2-סילו מסדר 8.

$$gP_1g^{-1}=g_2 \qquad g'P_1g'^{-1}=g_3$$

נסמן: $S_4\rhd V=\{e,(12)(34),(14)(23),(13)(24)\}$

V נמצא ב-P_i עבור $i=1,2,3$ כי הוא נשמר תחת הצמדה. ולכן חיתוך של כל 2 תת-חבורות הוא V.

טענה: אין תת-חבורה פשוטה מסדר 36. $36=2^2\cdot 3^2$

הוכחה:

דרך א': יש תת-חבורה 3-סילו מסדר 9 כלומר מאינדקס 4, נסמנה H.

G פועלת על מחלקות H. $g(kH)=gkH$

לכן יש הומומורפיזם $\varphi: G\longrightarrow S_4$ (כי הפרמוטציה על מחלקות H הן מגודל 4)

במקרה של פעולה על מחלקות $\ker\varphi\le H$ כי $g\in\ker\varphi$ אז $g(H)=H$

וזה קורה עבור $\forall g\in H$.

G פשוטה $\Longleftarrow$ $\ker\varphi=\{e\}$ ואז φ חח"ע.

14-12-2006 סתירה, כי $|S_4|=24$ ו- $|G|=36$.

דרך ב': G פשוטה לכן יש 4 חבורות 3-סילו.

נסתכל על $X=\{P_1,\dots,P_4\}$ אזי G פועלת על-ידי הצמדה: $g(P_i)=gP_ig^{-1}$

ונקבל אחרת: P_j $i\neq j$

לכן יש $\psi: G\longrightarrow S_4$ כי $|X|=4$.

אזי $\ker\psi\leq N_G(P_1)$

אם $g\in\ker\psi$ אז $g(P_1)=gP_1g^{-1}=P_1 \Longleftrightarrow g\in N_G(P_1)$.

האם $N_G(P_1)=G$? לא כי זה כמו לומר ש- $P_1\lhd G$ וזה לא יתכן

כי G פשוטה לכן ψ חח"ע וסתירה כמקודם.

∎

משפט הוכחנו שאם G חבורה מסדר p^2 אז היא אבלית. כי אם G חבורת p אז $Z(G)\neq\{e\}$ וזו $Z(G)=G$ או ש- $|Z(G)|=p$

אבל אז טענו כי אם G לא אבלית אז $G/Z(G)$ לא ציקלית.

הגדרה: חבורת הקווטרניונים היא חבורה מסדר 8 $Q=\langle a,b\rangle$

עם היחסים: $bab^{-1}=a^{-1}$, $a^4=1$ $b^2=a^2$

בתרגיל ראינו את החבורה:

$$G=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix},\ \pm\begin{pmatrix}0&1\\1&0\end{pmatrix},\ \pm\begin{pmatrix}0&1\\-1&0\end{pmatrix},\ \pm\begin{pmatrix}1&0\\0&-1\end{pmatrix}\right\}$$

$$G\cong Q$$

Q חבורה מסדר 2^3 שאינה אבלית.

מהו $Z(G)$? $Z(G)=\left\{\pm\begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}$

$G/Z(G)$ מסדר 4, מכאן אבלית.

לכן $G/Z(G)$ אבלית לא גורר כי G אבלית.

אם $G/Z(G)$ ציקלית $\Longleftarrow$ G אבלית.

נתבונן ב- $GL_d(\mathbb{Z}_p)$ (עובד לכל שדה סופי אחר)

נחשב את $|GL_d(\mathbb{Z}_p)|$:

צריך לבחור d וקטורים בלתי-תלויים לינארית מעל $\mathbb{Z}_p$.

לבחירה הראשונה יש p^d-1 (פחות וקטור האפס) אפשרויות.

לבחירה השניה יש p^d-p אפשרויות (פחות אלו שתלויים לינארית בקודם)

וכן הלאה..

מבחירה ה- d יש p^d-p^{d-1} אפשרויות לכן:

$$|GL_d(\mathbb{Z}_p)| = \prod_{i=0}^{d-1}(p^d-p^i) =$$

$$= p^{(1+2+\dots+d-1)} \cdot \prod_{i=1}^{d}(p^i-1) = p^{\frac{(d-1)d}{2}} \cdot \prod_{i=1}^{d}(p^i-1)$$

אז החזקה הגבוהה ביותר שמחלקת את הסדר של $GL_d(\mathbb{Z}_p)$ היא: $p^{\frac{(d-1)d}{2}}$

ולכן $p^{\frac{(d-1)d}{2}}$ חזקת p הגבוהה ביותר המחלקת את סדר החבורה.

נראה שקיימת חבורת p-סילו.

$$U = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \right\}$$

(תרגיל: U תת-חבורה.)

יש חופש רק לבחור את האיברים מעל האלכסון. יש בדיוק $\sum_{i=1}^{d-1} i = \frac{(d-1)d}{2}$

איברים כאלו ולכן $|U| = p^{\frac{d(d-1)}{2}}$.

נחזור קצת למחלקות כפולות:

הגדרה: יהיו H, K תת-חבורות של G. $g \in G$.

$$HgK = \{hgk \mid h \in H, k \in K\}$$

נקראת מחלקה כפולה ביחס ל- H ו- K.

14-12-2006

טענה: עבור חבורה G. $K,H \le G$ תת-חבורות
$g \in G$:

1. יש מחלקה כפולה יחידה המכילה את g.
2. חיתוך שתי מחלקות כפולות שונות הוא ריק.
3. G איחוד זר של מחלקות כפולות ביחס ל- H ול- K.
4. מחלקה כפולה ביחס ל- H,K היא איחוד מחלקות ימניות של H ולכן איחוד מחלקות שמאליות של K. ו- HgK מכילה $[K : K\cap(g^{-1}Hg)]$ מחלקות ימניות של H.

הוכחה:

1. $g \in HgK$

אם $g \in HxK$ אז $HgK = Hh_xk_xK = HxK$

$1 \Rightarrow 2 \Rightarrow 3$.

4. מחלקה ימנית של H המוכלת ב- HgK היא מהצורה Hgk עבור $k\in K$

$$Hgk_1 = Hgk_2 \iff Hgk_1k_2^{-1}g^{-1} = H \iff gk_1k_2^{-1}g^{-1} \in H$$
$$\iff K \ni k_1k_2^{-1} \in g^{-1}Hg \iff k_1k_2^{-1} \in K\cap(g^{-1}Hg)$$
$$\iff (K\cap(g^{-1}Hg))k_1 = (K\cap(g^{-1}Hg))k_2$$

ולכן יש בדיוק $[K : K\cap(g^{-1}Hg)]$ מחלקות ימניות של H המוכלות ב- HgK

∎

למה: תהי L חבורה. H חבורת p-סילו של L. אז לכל תת-חבורה $K \le L$ קיים $x \in L$ כך ש: $K\cap x^{-1}Hx$ חבורת p-סילו של K.

הוכחה: $[L:H] = \sum_{x\in X} [K : K\cap x^{-1}Hx]$

X הוא אוסף מלא של נציגים של מחלקות כפולות ביחס ל- H ו- K.

$p \nmid [L:H]$ כי H חבורת p-סילו.

ולכן קיים $x \in X$ כך ש: $p \nmid [K : K\cap(x^{-1}Hx)]$ מצד שני $K\cap x^{-1}Hx$ תת-חבורה של $x^{-1}Hx$ שהיא חבורת p, ולכן היא בעצמה חבורת p. $p \nmid [K : K\cap x^{-1}Hx] \Leftarrow K\cap x^{-1}Hx$ חבורת p-סילו של K.

∎

ממשפט קיילי כל חבורה סופית היא תת-חבורה של S_n (איזומורפית ל___)

אבל, S_n איזומורפית למטריצת תמורות ב- $GL_n(\mathbb{F})$ לכל שדה $\mathbb{F}$.

בפרט עבור $\mathbb{F}=\mathbb{Z}_p$

28-12-2006

מבנים אלגבריים - תרגול מס' 10

תרגילי רשות: (שהיה בשיעורי בית, נפתור חלק מהסעיפים)

(1) G חבורה. $|G|=p^k$, $k>1$ צריך להוכיח כי G אינה פשוטה.

אם $Z(G)=G$ אז G אינה פשוטה כי היא אבלית (וכל תת-חבורה שלה היא נורמלית)

G אבלית היא פשוטה אם ורק אם היא ציקלית מסדר ראשוני,

כי אם G אבלית כל תת-חבורה שלה היא נורמלית ולכן G אבלית היא פשוטה

אם ורק אם אין לה תת-חבורות בכלל.

אם G לא אבלית $G\neq Z(G)\neq\{1\}$ $Z(G)\triangleleft G$ G לא פשוטה.

(2) צריך להוכיח שעבור כל מספר שאינו ראשוני בין 2 ל-50 היא אינה פשוטה

(4) כדי להוכיח $Z(G)\neq 1$ בחבורת p נראה כי G פועלת ע"י הצמדה על אברי

G המסלולים בגודל p^k $k=0 \Longleftrightarrow O(x)=\{x\} \Longleftrightarrow x\in Z(G)$

$1\in Z(G)$ $|G|=p^n$ $|G|=\sum|O(x)|$ ⇐ חייב להיות עוד איבר ב-$Z(G)$

עבור $H\triangleleft G$ G פועלת על ידי הצמדה על אברי H $|H|=p^r$ לכן

מאותו נימוק יש $1\neq h\in H$ $ghg^{-1}=h$ $\forall g\in G \Longrightarrow h\in Z(G)$

(6) G חבורה. נגדיר עבור $a,b\in G$ $[a,b]=aba^{-1}b^{-1}$

$[a,b]=1 \Longleftrightarrow a,b$ מתחלפים.

<u>הגדרה</u>: חבורת הקומוטטור של G (החבורה הנגזרת) היא החבורה הנוצרת ע"י

כל הקומוטטורים $G'=[G,G]=\langle[a,b]\mid a,b\in G\rangle$

(7) $G'\triangleleft G$ כדי לבדוק עבור חבורה אם היא נורמלית מספיק לבדוק על היוצרים

$$g[a,b]g^{-1}=gaba^{-1}b^{-1}g^{-1}=(gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1})$$

$ga^{-1}g^{-1}=(gag^{-1})^{-1}$ $(gb^{-1}g^{-1})=(gbg^{-1})^{-1}$ לכן $=[(gag^{-1}),(gbg^{-1})]$

אם $f:G\to G$ הומומורפיזם אז $f([a,b])=[f(a),f(b)]$

בפרט, ההצמדה ב-$g\in G$ היא איזומורפיזם מ-G ל-G.

<u>הערה</u>: אם $g\in G$ אז נגדיר $\gamma_g:G\to G$ ע"י $x\mapsto gxg^{-1}$

γ_g הומומורפיזם $\gamma_g(xy)=gxyg^{-1}=$

$=gxg^{-1}gyg^{-1}=\gamma_g(x)\gamma_g(y)$

γ_g איזומורפיזם כי $\gamma_{g^{-1}}$ היא ההפכית שלה.

אם $H\leq G$ הצמצום של ההצמדה ל-H $\gamma_g|_H$ נותן איזומורפיזם מ-H ל-gHg^{-1}

לכן כל חבורות p-סילו הן איזומורפיות לכן כדי לדעת מאיזה טיפוס הן מספיק לבדוק אחת מהן.

(ב) G/G' אבלית

ואם $G' \le H \trianglelefteq G$ אז G/H אבלית.

G/G' אבלית אם ורק אם כל הקומוטטורים שלה הם 1

$[G'a, G'b] = (G'a)(G'b)(G'a^{-1})(G'b^{-1}) = G'aba^{-1}b^{-1} = G'\cdot 1$ $\quad a,b \in G$

כי $aba^{-1}b^{-1} \in G'$

(ג) $H \trianglelefteq G$ ו- G/H אבלית אז $G' \le H$ לכן G' תת-החבורה הנורמלית המינימלית עבורה חבורת המנה היא אבלית

<u>הוכחה:</u> נתון $\forall a,b \ HaHb = HbHa$

<u>הגדרה:</u> תהי G חבורה. סדרה $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_n = \{1\}$
כך ש $G_{i+1} \trianglelefteq G_i$ תקרא נורמלית. חבורות המנה הן G_{i+1}/G_i.

החבורה נקראת פתירה אם יש לה סדרה נורמלית בה חבורות המנה הן אבליות.

<u>תרגיל 9, שאלה 3:</u>

G חבורה; נגדיר באינדוקציה $G^0 = G$, $G^1 = G'$, $G^{i+1} = (G^i)'$

<u>טענה:</u> G פתירה $\iff$ קיים n כך ש $G^{(n)} = \{1\}$

חבורות הקומוטטור נותנות סדרה של חבורות, הנותנת נורמלית בשנייה עם חבורות מנה אבליות (הראינו) $G = G^0 \trianglerighteq G' \trianglerighteq \dots \trianglerighteq 1$

לכן אם קיים n כך ש $G^n = \{1\}$ אז נקבל ש-G פתירה

<u>למה:</u> G פתירה: $G = G_0 \trianglerighteq G_{n-1} \dots \trianglerighteq G_n = 1$.

אזי $G^{(i)} \le G_i \quad \forall i$

(<u>הערה:</u> מכאן נובעת הטענה, כי אז $G^n = \{1\}$).

באינדוקציה: $G \le G^{(0)} = G_0$

נניח ש $G^{(i)} \le G_i \Longleftarrow G^{i+1} = (G^i)' \le G_i'$

G_i/G_{i+1} אבלית, $G_{i+1} \trianglelefteq G_i \Longleftarrow$ (הוכחנו קודם) $G_i' \le G_{i+1}$

וקיבלנו ש $G^{i+1} \le G_{i+1}$ כנדרש.

<u>נראה איך 3 עוזר לפתור את ב:</u>

(א) אם $H \leq G$ אז $H^{(i)} \leq G^{(i)}$ לכן G פתירה $\Leftarrow$ $G^{(n)}=1$ עבור n כלשהו $\Leftarrow$ $H^{(n)}=1$ $\Leftarrow$ H פתירה.

(ב) $f: G \to H$ הומומורפיזם $f(G^{(i)})=(f(G))^{(i)}$ (תרגיל, להוכיח באינדוקציה)

מסקנה: אם $N \trianglelefteq G$ $K=G/N$ $f: G \to K$ ההעתקה הטבעית

אז $(f(G)^{(i)})=K^{(i)}$ ($K^{(i)}$ מכילה את התת-המחלקות של איברים ב-$G^{(i)}$)

$\Leftarrow$ אם $G^{(n)}=1$ $\Leftarrow$ $f(G^{(n)})=1$ $\Leftarrow$ $K^{(n)}=1$

$\Leftarrow$ לכן G פתירה גורר G/N פתירה.

(ג) אם N נורמלית ב-G פתירה ! $K=G/N$ $K^{(n)}=1 \Leftarrow G^{(n)} \leq N$

$N^{(m)}=1$ $(G^{(n)})$ $(G^{(n)})^{(m)}=1$

<u>טענה:</u> $(G^{(n)})^{(m)} \geq G^{n+m}$ (תרגיל - אינדוקציה)

<u>שאלה 1 (א) מהבוחן</u>

G חבורה, $H \lneq G$ אזי יש $x \in G$ שאינו צמוד לאף $h \in H$

<u>הגדרה:</u> x צמוד לאיבר ב-H אם ורק אם $x \in \bigcup_{g \in G} gHg^{-1}$

אם H נורמלית $\bigcup gHg^{-1}=H$ ואז הטענה ברורה

נניח כי H אינה נורמלית

נבדוק מה גודל $\bigcup_{g \in G} gHg^{-1}$ כי $|gHg^{-1}|=|H|$ כי תת-חבורות צמודות הן איזומורפיות. כמה תת-חבורות צמודות כאלו יש? G פועלת על הצמודות של H ע"י הצמדה. הפעולה טרנזיטיבית. מס' החבורות הצמודות ל-H $=|O(H)|=|X|$

$$|X|=[G:N_G(H)]=|G|/|N_G(H)|$$

$H \subseteq N_G(H) \Leftarrow H \leq |N_G(H)|$ $|X| \leq \frac{|G|}{|H|}$

האיחוד אינו זר כי $1 \in gHg^{-1}$ לכל $g \in G$

והנחנו שיש יותר מתת-חבורה צמודה 1. לכן, $|\bigcup_g gHg^{-1}| < \frac{|G|}{|H|} \cdot |H|$

4-1-2007 (1)

מבנים אלגבריים - תרגול מס' 11

נעשה חזרה על דברים שעשינו בהרצאה.

הגדרה:

קבוצה R עם שתי פעולות דו-מקומיות $+,\cdot$ רק ש- R סגורה תחת $\cdot,+$ ומתקיימים התנאים:

(א) R חבורה אבלית ביחס ל $+$. (אסוציאטיביות החיבור, קומוטטיביות החיבור, קיום איבר 0 $0+a=a+0=a$ $\forall a\in R$. קיום איבר נגדי)

(ב) אסוציאטיביות הכפל: $(ab)c=a(bc)$ $\forall a,b,c\in R$

(ג) קיום איבר נטרלי לכפל $0\neq 1\in R$ עבורו $a\cdot 1=1\cdot a=a$

הערה: לפעמים לא דורשים את (ג) ואם (ג) מתקיים קוראים ל- R "חוג עם יחידה".

(ד) דיסטריביוטיביות: $a(b+c)=ab+ac$

$(b+c)a=ba+ca$

$S\subseteq R$ תקרא תת-חוג אם היא חוג תחת הפעולות $+,\cdot$ מ- R.

הערה: חיתוך של תת-חוגים הוא חוג. לכן אפשר להגדיר עבור הקבוצה $X\subset R$ את החוג הנוצר ע"י X כחיתוך כל תתי החוגים המכילים את X.

דוגמאות: (א) $\mathbb{Z}$ - השלמים.

(הגדרה: חוג R יקרא 'קומוטטיבי' אם $ab=ba$ $\forall a,b\in R$)

(ב) כל שדה F

(הגדרה: חוג R יקרא 'חוג חילוק' אם לכל $0\neq a\in R$ קיים $b\in R$ כך ש- $ab=ba=1$) (קיום הפכי ביחס לכפל)

(הגדרה: איבר $a\in R$ יקרא הפיך אם קיים $b\in R$ כך ש- $ab=ba=1$, למשל, בשלמים האיברים ההפיכים היחידים הם 1 ו- (-1))

(ג) $\mathbb{Z}[\sqrt{2}]=\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\}$

זהו חוג, נראה רק סגירות לכפל לצורך ההמחשה: $(a+b\sqrt{2})(c+d\sqrt{2})=$

$=(ac+2bd)+(ad+bc)\sqrt{2}$

זהו תת-חוג של הממשיים $\mathbb{R}$

ולכן הרבה תכונות שמתקיימות מ- $\mathbb{R}$ אין צורך לבדוק כאן.

מאותן דומה, ניתן לחשוב על: $\mathbb{Q}[\sqrt{2}]=\{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\}$

$\mathbb{Q}[\sqrt{2}]$ הוא שדה.

(כי $(a+b\sqrt{2})(a-b\sqrt{2})=a^2-2b^2$

ואפשר לחלק ב a^2-2b^2 (תרגיל))

דוגמא נוספת מאותה משפחה של חוגים:

$\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$ – חוג השלמים של גאוס.

זהו תת-חוג של $\mathbb{C}$ ( ) זהו תת-החוג הנוצר ע"י $\mathbb{Z}\cup\{i\}$)

③ פונקציות רציפות $f:[0,1]\to\mathbb{R}$ עם החיבור והכפל:

$(f+g)(x)=f(x)+g(x) \qquad (f\cdot g)(x)=f(x)g(x)$

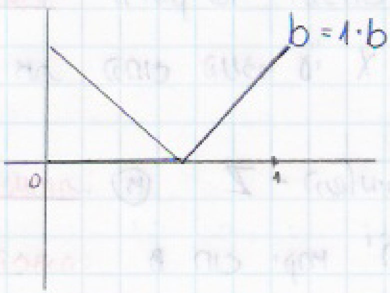
חוג קומוטטיבי.

<u>הגדרה</u>: איבר $a\in R$ יקרא מחלק אפס אם קיים $0\neq b\in R$ כך ש $ab=0$

חוג ללא מחלקי אפס יקרא תחום שלמות. (לפעמים מוסיפים את הביטוי לחוגים קומוטטיביים).

<u>בחוג חילוק</u> R אין מחלקי אפס.

$a\neq 0 \quad ab=0 \Longleftarrow b=1\cdot b=a^{-1}ab=0$



בדוגמא ③ יש מחלקי אפס

④ $\mathbb{Z}_n$ חוג. הוא שדה $\Longleftrightarrow$ n ראשוני

הוא תחום שלמות $\Longleftrightarrow$ n ראשוני.

הגדרה (או יותר דיוק סימון): R חוג, נסמן את אוסף האיברים ההפיכים ב-R ע"י R^*. R^* היא <u>חבורה</u> ביחס לכפל.

4-1-2007

① אם R חוג אז גם $M_n(R)$ - המטריצות $n\times n$ עם איברים מ- R הוא חוג. עבור $n\ge 2$ $M_n(R)$ לא קומוטטיבי עם מחלקי אפס.

לדוגמא: $\begin{pmatrix}0&1\\0&0\end{pmatrix}\begin{pmatrix}1&0\\0&0\end{pmatrix}=\begin{pmatrix}0&0\\0&0\end{pmatrix}$, (זוהי דוגמא למחלקי אפס)

מצד שני: $\begin{pmatrix}1&0\\0&0\end{pmatrix}\begin{pmatrix}0&1\\0&0\end{pmatrix}=\begin{pmatrix}0&1\\0&0\end{pmatrix}$ (רואים כי הכפל אינו קומוטטיבי)

ניתן לזהות את R עם תת-חוג של $M_n(R)$ ע"י המטריצות הסקלריות:

$$R\ni a\longmapsto\begin{pmatrix}a&&\\&a\ddots&\\&&a\end{pmatrix}$$

(העתקה חח"ע ועל והומומורפיזם [שיכון בהמשך])

⊛ נניח ש- R קומוטטיבי.

אפשר להגדיר עבור מטריצה $A\in M_n(R)$ את $\det A$.

מתקיימת הנוסחה לפיתוח דטרמיננטה לפי שורה ועמודה: $\det A=\sum_{j=1}^{n}(-1)^{i+j}a_{ij}A_{ij}$

מתקבל שגם (שלמדנו בלינארית) $(\mathrm{Adj}A)\cdot A=A\cdot(\mathrm{Adj}A)=\begin{pmatrix}\det A&&\\&\ddots&\\&&\det A\end{pmatrix}$

לא חייבים לזכור את הגדרה של Adj A

בנוסף לכך מתקיימת נוסחת הכפל $\det AB=\det A\cdot\det B$. וברור ש $\det I_n=1$

הדטרמיננטה של מטריצת היחידה.

אם A הפיכה אז: $1=\det I_n=\det A\cdot A^{-1}=\det A\cdot\det A^{-1}$

מסקנה: $A\in M_n(R)$ הפיכה $\iff$ $\det A\in R^*$

דוגמא: $S=M_n(\mathbb{Z})$

$A\in M_n(\mathbb{Z})$ הפיכה $\iff$ $\det A=\pm1$

למשל: $\begin{pmatrix}2&1\\1&2\end{pmatrix}$ אינה הפיכה ב- $M_2(\mathbb{Z})$

③ הקווטרניונים $\mathbb{H}$ (ע"ש המילטון)

"הופכים" את $\mathbb{R}^4$ לחוג.

מתאימים:

$$1 \longleftrightarrow (1,0,0,0)$$

$$i \longleftrightarrow (0,1,0,0)$$

$$j \longleftrightarrow (0,0,1,0)$$

$$k \longleftrightarrow (0,0,0,1)$$

הכפל מוגדר ע"י $i^2=j^2=k^2=-1$ $\quad ij=k \quad jk=i \quad ki=j$

הערה: האיברים הממשיים מתחלפים עם כולם. $\quad ik=-j \quad kj=-i \quad ji=-k$

לאיברים כלליים הכפל מוגדר בעזרת דיסטריבוטיביות

(הכפל של איברים כלליים עם ההמחשה):

$$(a+bi+cj+dk)(\alpha+\beta i+\gamma j+\delta k) = a\alpha+a\beta i+a\gamma j+a\delta k$$
$$+b\alpha i-b\beta+b\gamma k-b\delta j$$
$$+\dots$$

עבור $x=a+bi+cj+dk$ נגדיר $\bar{x}=a-bi-cj-dk$

מתקבל $x\bar{x}=a^2+b^2+c^2+d^2$ אם $x\neq 0$ אז $a^2+b^2+c^2+d^2>0$

לכן $x\cdot\frac{\bar{x}}{a^2+b^2+c^2+d^2}=1 \Longleftarrow x$ הפיך.

נקבל ש $\mathbb{H}$ הוא חוג חילוק.

$Q=\{\pm 1,\pm i,\pm j,\pm k\}$ חבורה ביחס לכפל, חבורת הקווטרניונים

היא איזומורפית לחבורה $G=\left\{\pm\begin{pmatrix}1&\\&1\end{pmatrix},\pm\begin{pmatrix}i&\\&-i\end{pmatrix},\pm\begin{pmatrix}&1\\-1&\end{pmatrix},\pm\begin{pmatrix}&i\\i&\end{pmatrix}\right\}$ (מהתרגיל 4)

ח) חוג הפולינומים מעל $\mathbb{R}$.

$\mathbb{R}[x]$ $\quad a_0+a_1x+\dots+a_nx^n \quad a_i\in\mathbb{R}$

חוג קומוטטיבי:

$\mathbb{R}[x,y]$ $\quad a+bx+cy+dxy+ex^2+fy^2+hxy^2+\dots$

$$\mathbb{R}[x,y]=(\mathbb{R}[x])[y]$$

ניתן להגדיר חוג פולינומים בכמה משתנים $\mathbb{R}[x_1,\dots,x_n]$

נחזור עכשיו לתורת החבורות ונלמד למה חשובה.

הלמה של ברנסייד (מדברים על חבורה סופית שפועלת על קבוצה סופית - מעניין אותנו מספר המסלולים של הפעולה)

הגדרה: תהי G חבורה. X קבוצה. G פועלת על X

$Fix(g)=\{x\in X \mid gx=x\}$ $\quad g\in G$ (נקודות שבת)

דוגמא: S_4 פועלת על $\{1,2,3,4\}$ אז $fix((1\,2))=\{3,4\}$

משפט: תהי G חבורה סופית. X קבוצה סופית. G פועלת על X.

נסמן ב- N את מספר המסלולים לפעולה אז:

$$N=\frac{1}{|G|}\sum_{g\in G}|fix(g)|$$

הוכחה: אם $x\in X$ אז, ע"פ ההגדרה, $x\in fix(g) \Longleftrightarrow g\in Stab_G(x)$

(אז מס' הפעמים שנספור אותו זה בדיוק הגודל של המייצב). לכן סופרים את $x\in X$ $|Stab_G(x)|$ פעמים.

נ"ב $y\in O(x)$ אז קיים $g\in G$ רק ש: $Stab_G(y)=gStab_G(x)g^{-1}$

($gx=y$). אז בפרט $|Stab_G(x)|=|Stab_G(y)|$. כמה תורמים כל האיברים במסלול של x?

האיברים במסלול של X, תורמים ל $\sum|fix(g)|$ בסה"כ:

$\underbrace{|O(x)|\cdot|Stab_G(x)|}_{=|G|}$ לכן כל איברי X תורמים: $N\cdot|G|$

ומכאן נובעת הלמה, המשפט.

$\boxtimes$

מסקנה: תהי G סופית, הפועלת על X סופית ו-$|X|>1$.

טרנזיטיבית אז קיים איבר $\exists g\in G$ כך ש- $gx\neq x$ $\forall x\in X$ (כלומר קיים איבר ללא נקודת שבת)

הוכחה: לפי הלמה של ברנסייד $1=\frac{1}{|G|}\sum_{g\in G}|fix(g)|$

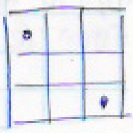
תמיד מתקיים $fix(id)=X$ (כי כל איבר כפול היחידה הוא עצמו)

לכן אם לכל $g\in G$ יש נקודת שבת אז $\sum_{g\in G}|fix(g)|>|G|$

(וזה לא יתכן)

דוגמא: (לבעיה קומבינטורית)

נאמר שמייצרים תמונות כיהוי מאוזן הבא:



מחלקים את הכיבוע לתשע ומנקבים שני חורים בשניים מהריבועים. כמה קונפיגורציות ניתנות לציור?

יש $\binom{9}{2}=36$ קונפיגורציות שונות.

D_4 (חבורת הסימטריות של הריבוע). פועלת על הקונפיגורציות

מזהים שני "כרטיסים" כאלה כשהם נמצאים באותו המסלול. (ניתן להגיע מאחד לשני ע"י סיבוב או שיקוף)

ומחפשים בעצם את מס' המסלולים. זה מספר הכרטיסים שאפשר להבדיל ביניהם. נחשב את $|fix(g)|$ לכל $g\in D_4$

נעשה זאת באמצעות הלמה של ברנסייד.

11/1/07

מבנים אלגבריים - תרגיל מס' 12

(תודה למהבה על שלושת התרגילים האחרונים)

5) ג.

חזיק להתאים בין אוקר:

$$X = a + bi + cj + dk \longleftrightarrow \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}$$

$H \longrightarrow R : \varphi$ הומו'

אם $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(a \cdot b) = \varphi(a)\varphi(b)$

ואם להוי חוג עם יחוד אז $\varphi(1_H) = 1_R$.

אם (נמצא) מט' מתאימות ל- i, j, k אז φ נקבעת ביחודות. צריך שתתקיימו היחסים בין i, j, k יחודה.

לכן, מספיק שנראה כי $G \cong Q$.

$$\pm 1 \longrightarrow \pm I$$

$$\pm i \longrightarrow \pm \begin{pmatrix} -i & \\ & i \end{pmatrix}$$

$$\pm j \longrightarrow \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

$$\pm k \longrightarrow \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$X = a + bi + cj + dk$

$$\varphi(X) = aI + b\begin{pmatrix}-i & 0\\ 0 & i\end{pmatrix} + c\begin{pmatrix}0 & i\\ i & 0\end{pmatrix} + d\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

$$= \begin{pmatrix}a-bi & d+ci\\ -d+ci & a+bi\end{pmatrix}$$

והרי כי זו העתקה חח"ע ועל (מהמט' המרוכבים).

הגדרה: יהי R חוג, אז $I \subseteq R$ נקראת <u>אידיאל</u> <u>שמאלי (ימני)</u> אם I תת-חוג סגור לחיבור ו- לכל $a \in R$ $i \in I$ $ai \in I$ $(ia \in I)$.

הגדרה: <u>אידיאל</u> (דו-צדדי) $I \subseteq R$ הוא גם אידיאל שמאלי וגם אידיאל ימני.

בחוג קומוט' כל אידיאל הוא דו-צדדי.

הגדרה: יהי $X \subseteq R$ קב' <u>האידיאל הנוצר ע"י X</u> הוא האידיאל המינימלי המכיל את X.

דוגמה: אם $a \in R$ אז האידיאל הנוצר ע"י a מסומן (a). (אידיאל ראשי).

לדוג', האידיאל השמאלי הנוצר ע"י $a \in R$ הוא מהצורה $I = \{r \cdot a \mid r \in R\}$.

בחוג כללי האידיאל הדו-צדדי הנוצר ע"י $a \in R$ הוא מהצורה
$$I = \{\sum r_i a s_i \mid r_i, s_i \in R\}$$
(תרגיל - קל לבדוק).

בחוג קומו', $I = \{ra \mid r \in R\}$ (אידיאל ראשי)

לדוגמה: $nZ \lhd Z = (n)$

הגדרה: R קומוטטיבי. אידיאל I, הנוצר ע"י איבר $a \in R$ נקרא <u>אידיאל ראשי</u>.

וחוג R ייקרא <u>חוג ראשי</u> אם כל האידיאלים בו הם ראשיים.

טענה: Z חוג, ראשי. $F[x]$ חוג ראשי.

עמ' 2 (נוכיח בכתה).

הערה: אם $I\triangleleft R$ ו- $1\in I$ אז $I=R$

קשדה F אין אידיאלים לא טריוויאלים. כי אם $0\neq a\in I$

אז $I\ni a^{-1}a=1$ ולכן גם $1\in I$).

כלל, בחוג חילוק אין אידיאלים שמאליים או ימניים לא

טריוויאלים.

מאידך, אם R קומוטטיבי שאין בו אידיאלים לא טריוויאלים

אז R שדה (תרגיל השבוע).

הגדרה: $I\triangleleft R$ אידיאל דו"צ. מגדירים את החוג

R/I - חוג המנה. בחיבור כמו כי החבורה (חבורה!) אבלית

צריך רק להגדיר את הכפל: $(a+I)(b+I)=ab+I$.

ונוכיח בשיעור שזה אכן מוגדר היטב.

יש העתקה טבעית, $u: R\to R/I$
$r\mapsto r+I$

הומו', ע"ל. ו- $\ker u=I$.

כל אידיאל דו"צ הוא גרעין של איזשהו הומו'!!!

יש התאמה.

(בחבורות ראינו כי אם G חבורה ו- $N\triangleleft G$ אז

יש התאמה בין תת קבוצות G המכילות את N לבין תת

של G/N).

יש התאמה בין תת של אידיאלים של R/I לבין אידיאלים $R\supseteq J$

המכילים את I הנתונה ע"י:

$$I\subseteq J\triangleleft R \longrightarrow u(J)$$

$$u^{-1}(\tilde{J}) \leftarrow \tilde{J}\triangleleft R/I$$

(u ההעתקה הטבעית)

הגדרה: ~~תחו~~ חוג קומ' R נקרא תחום שלמות אם

אין בו מחלקי אפס.

כל שדה הוא תחום שלמות.

תת חוג של תחום שלמות הוא תחום שלמות.

יש תחומי שלמות שאינם שדות. (השלמים, Z).

עמ' 3

האם כל ~~תת~~ תחום שלמות הוא תת חוג של שדה?

נראה שאכן כן

בהינתן תחום שלמות R נבנה את שדה השברים של R. ! $R \subset F$ תת חוג.

תהי $S = R \setminus \{0\}$. נגדיר יחס שקילות על $R \times S$ ע"י $(r_1, s_1) \sim (r_2, s_2) \iff r_1 s_2 = r_2 s_1$ $\left(\frac{r_1}{s_1} = \frac{r_2}{s_2}\right)$

רפלקס' וסימטריות ברורות. נראה טרנז':

נניח $(r_1, s_1) \sim (r_2, s_2)$ וכן $(r_2, s_2) \sim (r_3, s_3)$

אזי $r_1 s_2 = r_2 s_1$ ו- $r_2 s_3 = r_3 s_2$

$$\Rightarrow (r_1 s_3) s_2 = r_1 s_2 s_3 = r_2 s_1 s_3 =$$

$$= r_2 s_3 s_1 = r_3 s_2 s_1 = (r_3 s_1) s_2 \quad \text{(קומו')}$$

$$\Rightarrow (r_1 s_3) s_2 = (r_3 s_1) s_2$$

(מצמצום אגפים R תחום שלמות)

$$\Rightarrow r_1 s_3 = r_3 s_1$$

$$\Rightarrow (r_1, s_1) \sim (r_3, s_3)$$

נסמן את מחלקת השקילות של (r, s) ב- $\frac{r}{s}$.

הערה: $\frac{r'}{s'} = \frac{s \cdot r'}{s' \cdot s}$ (אפשר לצמצם).

נסמן את קב' מחלקות השקילות ב- $S^{-1}R$ (או R_S, $R[S^{-1}]$).

נגדיר חיבור וכפל:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$

$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

נראה כי החיבור מוגדר היטב:

נניח כי: $\frac{r_1}{s_1} = \frac{r_1'}{s_1'}$ ו- $\frac{r_2}{s_2} = \frac{r_2'}{s_2'}$

רוצים להראות כי: $(r_1 s_2 + r_2 s_1) s_1' s_2' = (r_1' s_2' + r_2' s_1') s_1 s_2$

$$r_1' s_2' s_1 s_2 + r_2' s_1' s_1 s_2 = r_1 s_1' s_2 s_2' + r_2 s_1 s_1' s_2' =$$

$$= s_1' s_2' (r_1 s_2 + r_2 s_1) \quad \checkmark$$

הכפל מוגדר היטב תרגיל.

טענה: $S^{-1}R$ הוא חוג עם יחידה ויש הומו' חח"ע: $\Psi: R \to S^{-1}R$ כלומר גם שיכון. $\Psi(r)=\frac{r}{1}$. ולכן קיבלנו כי R הוא תת חוג של $S^{-1}R$

הוכחה: תרגיל. בדיקה ישירה.

(נזכיר כי $\frac{0}{1}$ הינו איבר האפס. $\frac{1}{1}$ איבר היחידה. ו- $-\frac{r}{s}=\frac{-r}{s}$.)

כלל Ψ הומו' ברור.

Ψ חח"ע כי $\Psi(r)=\frac{0}{1}=\frac{r}{1}$ ויקבל כי $r=r\cdot 1=0\cdot 1=0$. כלומר $\ker\Psi=\{0\}$ ולכן Ψ חח"ע.

השתמשנו בתכונות S האיבר היחידה נמצא בה וכי היא סגורה לכפל. כאן נשתמש בתכונה נוספת.

טענה: $S^{-1}R$ הוא שדה.

הוכחה: אם $r/s\neq 0$ אז $r\neq 0$ ולכן $r\in S$ ולכן $s/r\in S^{-1}R$. וקל לראות כי $\frac{s}{r}\cdot\frac{r}{s}=1$.
כאן השתמשנו בהכלה S כולל את R ומלבד 0 לא נמצא בה.

דוגמאות:

אם $R=F[x]$ אז $S^{-1}R=F[x]=\left\{\frac{f(x)}{g(x)} \mid g(x)\not\equiv 0\right\}$

$R=F[x_1,\dots,x_n] \longrightarrow F(x_1,\dots,x_n)=\left\{\frac{f(x_1,\dots,x_n)}{g(x_1,\dots,x_n)}\right\}$ $(g\neq 0)$

הכללה:

יהי R תחום שלמות $S\subset R\setminus\{0\}$ $1\in S$ ו- S סגורה תחת כפל אז $S^{-1}R$ הוא חוג. ויש שיכון טבעי: $\Psi: R\to S^{-1}R$ המוגדר ע"י $\Psi(r)=\frac{r}{1}$ חח"ע.

טענה: יהיו R, T חוגים קומוטטיביים. $S\subset R\setminus\{0\}$ ללא מחלקי אפס, $1\in S$ וסגורה לכפל. ויהי $\varphi: R\to T$ הומו' כך שמתקיים: $\varphi(s)$ הפיך ב-T לכל $s\in S$.

אז ניתן להרחיב את $\varphi: R\to T$ להומו'
(באופן יחיד) $\bar\varphi: S^{-1}R\to T$ ע"י
$\bar\varphi(\frac{r}{s})=\varphi(r)\cdot\varphi^{-1}(s)$. $\ker\bar\varphi=S^{-1}\ker\varphi$
$=\{a/s \mid a\in\ker\varphi\}$

הוכחה: תרגיל. מספיק להראות כי $\bar\varphi$ הומו'.
בפרט אם φ חח"ע אז גם $\bar\varphi$ חח"ע.
$\ker\bar\varphi=S^{-1}\ker\varphi=\{a/s \mid a\in\ker\varphi\}$ ← (המשך ההוכחה).

דוגמה: כל תת-חוג R של $\mathbb{Q}$ מכיל את $\mathbb{Z}$.
($1\in R$ ולכן גם $\Sigma 1\in R$ וכו' ...)
בפרט, אם R שדה אז נקבל כי $\mathbb{Q}\subset R$.
$\varphi: \mathbb{Z}\xrightarrow{\text{חח"ע}} R$ כל איברי $\mathbb{Z}$ הפיכים ב-R
כי R שדה ולכן $\bar\varphi$ חח"ע: $\mathbb{Q}\to R$
כלומר לרציונלים אין תת שדות חוץ מהרציונלים עצמם.

(1) דוגמא: יהי R תחום שלמות. $0\neq s\in R$ (ונתבונן)
ב- $S=\{s^i \mid i\in\mathbb{N}\}$ אז: $S^{-1}R=\{r/s^i \mid i\in\mathbb{N}\}$
למשל בשלמים, $\mathbb{Z}[\frac{1}{2}]=\{\frac{n}{2^i} \mid i\in\mathbb{N}\}$ ← (סימון כמו $S^{-1}R$)
(כל הרציונלים שבמכנה יש חזקת 2).
אם $s|t$ אז נקבל כי $\mathbb{Z}[\frac{1}{s}]\subseteq\mathbb{Z}[\frac{1}{t}]$
כי אם $as=t$ אז $\frac{1}{s}=\frac{a}{t}$.
מדויק אם $t\nmid s^i$ $\forall i\in\mathbb{N}$ אז $\mathbb{Z}[\frac{1}{s}]\subsetneq\mathbb{Z}[\frac{1}{t}]$
למה? כי אם $n/s^i=1/t$ אז $nt=s^i$ קונטרה
להנחה ולכן $1/t\notin\mathbb{Z}[\frac{1}{s}]$.

$$\mathbb{Z}\subsetneq\mathbb{Z}[\tfrac{1}{2}]\subsetneq\mathbb{Z}[\tfrac{1}{6}]\subsetneq\mathbb{Z}[\tfrac{1}{30}]\subsetneq\cdots$$

(2) דוגמא: P ראשוני. $S=\{n\in\mathbb{Z} \mid P\nmid n\}$
סגירות לכפל: מהגדרה של ראשוני: אם $P|a\cdot b$
אז $P|b$ או $P|a$. $S^{-1}R=\{\frac{n}{m} \mid P\nmid m\}$.

18/1/07 תרגול מקוון (1)

מבנים אלגבריים - תרגול 13
(תודה לרבקה)

בשלמים אנחנו מכירים את המשפט היסודי של האריתמטיקה:
לכל $n\in\mathbb{Z}$ יש פירוק $n=p_1\cdots p_k$ למכפלה של מס' ראשוניים. הפירוק יחיד עד כדי שינוי סדר וכפל איברים ראשוניים ב-1-.

בהינתן חוג R תחום חוג שלמות, לאו דווקא קיים או יחיד
ללא מחלקי אפס. אלא אם נאמר אחרת.
נראה במקרה הזה למצוא פירוק דומה.

הגדרה: R תחום שלמות. $a,b\in R$ אז $a|b$ אם קיים $c\in R$ כך ש- $ac=b$.

הגדרה: a ו- b כלשהם נקראים חברים אם $a|b$ ו- $b|a$.

דוגמא: ב- $\mathbb{Z}$: $6,-6$
ב- $\mathbb{R}[x]$: $3x+6,\ x+2$

a,b חברים אמ"מ $b=au$, כאשר u הפיך.

("⇒") $a|b \Rightarrow au=b$
$b|a \Rightarrow bv=a$

$a=auv \Rightarrow a(1-uv)=0$
R תחום שלמות, $a\neq 0 \Rightarrow uv=1$.

תרגום למונחי אידאלים:
$a|b \Leftrightarrow Ra\supseteq Rb$
a,b חברים $\Leftrightarrow Ra=Rb$

הגדרה: איבר לא הפיך $0\neq p\in R$ יקרא אי-פריק אם $p=a\cdot b \Rightarrow a$ הפיך (b חבר של p) או b הפיך (a חבר של p)

נשים לב: אם $c=a\cdot b$ ו- u הפיך אז גם $c=(au)(bu^{-1})$. (ולכן לא נראה את ההפיכים - בהגדרה של הפירוק...)

הגדרה: לאיבר $r\in R$ יש פירוק אם $r=p_1\cdots p_n$ כאשר p_i אי-פריקים.

נאמר שהפירוק יחיד אם כאשר $r=q_1\cdots q_m$ אז $m=n$ וקיימת תמורה $\sigma\in S_n$ כך ש- $q_{\sigma(i)}$ חבר של p_i.

דוגמאות:

⊛ ב-$\mathbb{Z}$. אי-פריקים הם הראשוניים.

⊛ ב-$\mathbb{C}[x]$. אם $f(x)\in\mathbb{C}[x]$ אז $\alpha\in\mathbb{C}$ שורש של $f(x)$ אמ"מ $(x-\alpha)|f(x)$. מהמשפט היסודי של האלגברה, לכל $f(x)\in\mathbb{C}[x]$ $\quad f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$

לכן האי-פריקים ב-$\mathbb{C}[x]$ הם הפולינומים לינאריים (ממעלה ראשונה). (אם $ax+b=g(x)\cdot h(x)$ אז בהכ"ל $\deg(h)=0$ $\Leftarrow$ h הפיך).

⊛ ב-$\mathbb{R}[x]$. הפולינום x^2+1 הוא אי-פריק. אחרת היה מתפרק למכפלת פולינום לינאריים ואז היה לו שורש ב-$\mathbb{R}$.

כל פולינום $f(x)\in\mathbb{R}[x]$ ניתן לפירוק מעל $\mathbb{C}$ כך:

$$f(x)=(x-u_1)(x-\bar{u}_1)\cdots(x-u_r)(x-\bar{u}_r)\cdot$$
$$=(x-\lambda_1)\cdots(x-\lambda_m)$$

($u_i\notin\mathbb{R}$, $u_i\in\mathbb{C}$, $\lambda_i\in\mathbb{R}$)

נשים לב כי: $(x-u)(x-\bar{u})=x^2-(u+\bar{u})x+u\bar{u}\in\mathbb{R}[x]$

לכן אפשר לכתוב את $f(x)$ כמכפלת פולינומים לינאריים ופולינומים ריבועיים שאין להם שורש ב-$\mathbb{R}$. ואלו, כלומר הלינאריים והריבועיים ללא שורש ב-$\mathbb{R}$ הם האי-פריקים.

⊛ $x^2+x+1\in\mathbb{Z}_2[x]$ אי פריק. כי אין לו שורש ב-$\mathbb{Z}_2$.

הגדרה: תחום שלמות R יקרא תחום פריקות חד-ערכית (פח"ע) אם לכל איבר $r\in R$ (לא הפיך) יש פירוק יחיד. (U.F.D)

הגדרה: תחום שלמות R יקרא אוקלידי אם קיימת פונק' $d:R\setminus\{0\}\longrightarrow\mathbb{N}$ המקיימת: ① $d(ab)\geq d(a)$ כלומר אם $x|y$ אז $d(x)\leq d(y)$. ② לכל $a,b\in R$ יש $r,q\in R$ כך שמתקיים: $b=qa+r$ ו-$r=0$ או $d(r)<d(a)$

המשך

דוגמאות:

$\mathbb{Z}$ עם $d=|\,|$

$F[X]$ עם $d=\deg$

$\mathbb{Z}[i]$ עם $d=|\,|^2$ $\quad d(a+bi)=a^2+b^2$

טענה: בחוג אוקלידי כל אידיאל הוא ראשי, נוצר ע"י איבר אחד, $a\in R$. לכן R אוקלידי $\Leftarrow$ R תחום ראשי (תחום ראשי תחום שלמות).

אם $I\triangleleft R$ נבחר $a\in I$ כך ש- $d(a)$ מינימלי של (בעזרת חלוקה עם שארית נקבל כי $I=Ra$.

בחוג אוקלידי R, אידיאל I נוצר ע"י $a\in I$ כך ש- $d(a)$ מינימלי.

לכן, אם $a|b$ ו- $d(a)=d(b)$ אז a ו- b חברים.

כי $b\in Ra$, אבל Ra נוצר ע"י כל $x\in Ra$ עם $d(x)$ מינימלי, בפרט ע"י b.

לכן אם $a=b\cdot c$ פירוק אמיתי (לא הפיכים ולא חברים) אז $d(a)>d(b),d(c)$

מכאן אפשר להוכיח כי לכל $r\in R$, R אוקלידי, יש פירוק.

באינדוקציה על $d(r)$.

הגדרה: איבר $p\in R$ ייקרא ראשוני אם $p|ab$ $\Leftarrow$ $p|a$ או $p|b$.

p ראשוני הוא אי-פריק כי אם $p=ab$ אז בפרט $p|ab$ ולכן $p|a$ או $p|b$ אבל $a,b|p$ ולכן או a או b חברים של p.

(לא תמיד אי-פריק הוא ראשוני).

למה: אם $p\in R$ ראשוני ו- $r_1,\dots,r_n$ אז $p|r_1\cdots r_n$ אז $p|r_i$ עבור i כלשהו ואם r_i הוא אי-פריק ובפרט ראשוני אז p ו- r_i חברים.

מסקנה: אם $r=p_1\cdots p_n$ פירוק למכפלת ראשוניים אז הפירוק יחיד.

(הדי הוכחה): אם $r=p_1\cdots p_n = q_1\cdots q_m$ ו-$\overset{\text{שני פירוקים}}{}$ p_i ראשונים אז קה"כ $p_1 \mid q_1$ אז $up_1=q_1$ כאשר u הפיך. נקבל: $up_1 q_2\cdots q_m = p_1\cdots p_n$
R תחום שלמות, אז אפשר לחלק ב-p_1 וממשיכים להשוות את הפירוקים, באינד'.

על מנת להראות פירוקות יחידות צריך להראות כל אי-פריק הוא ראשוני.

תרגום לאידיאלים:

$p\in R$ אי-פריק $\Leftrightarrow$ $Rp \subsetneq Ra$ אז a הפיך
ו-$Ra=R$

אם R תחום ראשי אז נקבל כי אם $Rp\subsetneq I \triangleleft R$ אז $I=R$. $\Leftrightarrow$ Rp אידיאל מקס'. $\Leftrightarrow$ R/Rp שדה.

$p\in R$ ראשוני $\Leftrightarrow$ $ab\in Rp$ ① אז $a\in Rp$ או $b\in Rp$
② אם $RaRb\in Rp$ אז $Ra\subseteq Rp$ או $Rb\in Rp$
③ R/Rp תחום שלמות

נימוק אם $\bar{a}=a+Rp$ $\bar{a}\bar{b}=\bar{0}$ $\Rightarrow R/Rp$ אז $\bar{a}\bar{b}=\bar{0}$
$\Leftarrow ab\in Rp \Leftarrow a\in Rp$ או $b\in Rp \Leftarrow \bar{a}=\bar{0}$ או $\bar{b}=\bar{0}$.

הגדרה: יהי R חוג קוו' עם יחידה. אידיאל $P\triangleleft R$ ייקרא ראשוני אם: $ab\in P$ ① $\Leftarrow a\in P$ או $b\in P$
אמ"מ $I,J\triangleleft R$ ② ו-$IJ\subseteq P$ אז $I\subseteq P$ או $J\subseteq P$
אמ"מ R/p ③ תחום שלמות.

תמיד אידיאל מקס' הוא אידיאל ראשוני! (כי אם P מקס' אז R/p שדה ובפרט תחום שלמות).

תחום ראשי, בפרט אוקלידי, (לא בהכרח), $p\in R$ אי-פריק אמ"מ Rp מקס'. אמ"מ $\Leftarrow Rp$ ראשוני $\Leftarrow p$ ראשוני. ולכן אם יש פירוקים ב-R הם יהיו חד ערכיים. בפרט, חוג אוקלידי הוא תחום פח"ע.

הערה: תחומים ראשיים הם תחומי פח"ע.

בתחום ראשי כל אידיאל ראשוני P הוא מהצורה Rp
כאשר p ראשוני ($p\in R$). אם $P\neq 0$ אז p אי-פריק
ולכן $Rp=P$ מקס'.

מסקנה: בתחום ראשי כל אידיאל ראשוני שונה מ-(0) הוא מקסימלי.

דוגמאות:

א) $R=\mathbb{Z}[x]$.

נגדיר העתקה: $\psi:\mathbb{Z}[x]\to\mathbb{Z}$. $\psi(f)=f(0)$

זהו הומו' על ולכן $\mathbb{Z}\cong \mathbb{Z}[x]/_{\ker\psi}$ ולכן $\ker\psi$
הוא ראשוני ולא מקס' כי $\mathbb{Z}$ תחום שלמות.
$0\neq \ker\psi=\mathbb{Z}[x]\cdot x$.

$\Leftarrow$ $\mathbb{Z}[x]$ תחום שלמות שאינו ראשי.

(למעשה זה, נראה אח"כ כי זהו תחום פח"ע שאינו ראשי)
דוגמא לאידיאל לא ראשי: $I=(2,x)$ (האידיאל שנוצר ע"י 2 ו-x,
$(\mathbb{Z}[x]\cdot 2+\mathbb{Z}[x]\cdot x)$ נניח כי I נוצר ע"י a אז $a|2$
ומשיקולי דרגה $a\in\mathbb{Z}$ ולכן $a=\pm2$ אבל $\pm2\nmid x$. (תרגיל)

ב) $R=F[x_1,x_2]$.

נגדיר הומו': $\psi:F[x_1,x_2]\longrightarrow F[x_1]$ ע"י: $\psi(f(x_1,x_2))=f(x_1,0)$.
זהו הומו' על, ושוב יש לנו כי:
$$F[x_1,x_2]/_{\ker\psi}\cong F[x_1]$$
ו-$F[x_1]$ הוא תחום שלמות שאינו שדה ולכן $\ker\psi$ הוא
ראשוני שאינו מקס'. $\ker\psi=F[x_1,x_2]\cdot x_2$.
דוג' לאידיאל לא ראשי: אם $I=(x_1,x_2)$ (האידיאל שנוצר
ע"י x_1,x_2) הוא אידיאל שאינו ראשי. (תרגיל)

משפט: אם R תחום פח"ע אז גם $R[x]$ תחום פח"ע.

מסקנה: $\mathbb{Z}[x]$ ו- $F[x_1,x_2]$ תחומי פח"ע.

ג) $\mathbb{Z}[\sqrt{10}]$ תחום שלמות שאינו תחום פריקות ח"ע.

הוכחה: נשים לב ש- $(7+2\sqrt{10})(7-2\sqrt{10})=9=3\cdot3$

אם נניח כי 3 הוא אי-פריק בחוג נקבל את מה שרצינו:

נניח כי $3=(a+b\sqrt{10})(x+y\sqrt{10})$ $\Leftarrow$ $ay+bx=0$

אז $ay=-bx$.

בה"כ a,b זרים, אחרת, נניח $d|a$, $d|b$,

ו- $e|x$ ו- $e|x$ ו-

$(a+b\sqrt{10})(x+y\sqrt{10})=cd=(a'+b'\sqrt{10})(c'+d'\sqrt{10})$ אז $\in\mathbb{Z}$

$\Leftarrow$ $c|3$ ו- $d|3$ $\Leftarrow$ בה"כ $d=1$.

ולכן $a|x$ ו- $b|y$. נסמן: $x=a\cdot x_1$ ו- $y=b\cdot y_1$

$\Leftarrow$ $aby_1=ba$ $\Leftarrow$ $y_1=-x_1$

$$3=(a+b\sqrt{10})(ax_1-bx_1\sqrt{10})=$$

$$=x_1(a+b\sqrt{10})(a-b\sqrt{10})\in\mathbb{Z}$$

$x_1=1$ או $x_1=3$. אם $x_1=3$ זה לא פירוק

ולכן $x_1=1$ ולכן: $3=(a+b\sqrt{10})(a-b\sqrt{10})=a^2-10b^2$

ומקבלים כי $a^2\equiv 3 \mod 10$ וזה לא יתכן

מבנים אלגבריים - תרגול 14 (תודה לשמעון)

דוגמאות לתחומי שלמות שאינם פריקות חע:

הגדרה: תחום שלמות R ייקרא תחום פריקות חד-ערכית אם לכל איבר $r\in R$ (לא הפיך) יש פירוק יחיד.

א. $\mathbb{Z}[\sqrt{10}]=\{a+b\sqrt{10}\mid a,b\in\mathbb{Z}\}$. זהו אכן תחום שלמות כי זהו תת-חוג של $\mathbb{R}$.

נמצא דוג' למס' שיש לו שני פירוקים בחוג:

$$3\cdot3=9=(7+2\sqrt{10})(7-2\sqrt{10})$$

אולי אפשר לפרק את הגורמים עוד ולקבל פירוק שקול?
נוכיח כי 3 אי-פריק ולכן $3\cdot3$ פירוק של 9 לאי-פריקים.
ואם $\mathbb{Z}[\sqrt{10}]$ הוא תחום פח"י אז $3\cdot3$ היה צריך להיות שקול ל: $(7+2\sqrt{10})(7-2\sqrt{10})$, כלומר, 3 חבר של $7\pm2\sqrt{10}$, וזה לא נכון. (תרגיל, בדוק למצוא הפיך, u רק ש $3\cdot u=7\pm2\sqrt{10}$).
נניח: $3=(a+b\sqrt{10})(x+y\sqrt{10})$.

טענה: ניתן להניח כי $g.c.d(a,b)=1$, כי נניח כי $d=g.c.d(a,b)$ ו- $e=g.c.d(x,y)$ אז $3=de(\ )(\ )$ ($\in\mathbb{Z}$) $\Leftarrow$ $d\mid3,\ e\mid3$
בה"כ $d=1$.

מהשוויון נובע כי $ay+bx=0$ $\Leftrightarrow$ $ay=-bx$
a,b זרים $\Leftarrow$ $a\mid x$ ו- $b\mid y$. נכתוב $x=a\cdot x_1$, $y=b\cdot y_1$
ונקבל: $a\cdot by_1=-bax_1$ $\Leftarrow$ $x_1=-y_1$.
קיבלנו כי: $3=(a+b\sqrt{10})(ax_1-by_1\sqrt{10})=x_1(a+b\sqrt{10})(a-b\sqrt{10})$
$\Leftarrow$ $x_1\mid3$. אם $x_1=3$ אז גם $a\pm b\sqrt{10}$ הפיכים והפירוק לא אמיתי.

אם $x_1=1$ אזי $3=(a+b\sqrt{10})(a-b\sqrt{10})=a^2-10b^2$
ובפרט נקבל כי: $a^2\equiv3\pmod{10}$.
a^2 נקבע ע"י מס' האחדות, ולכן: $a^2=1,4,5,6,9,0\pmod{10}$
$\Leftarrow$ $x_1\neq1$ $\Leftarrow$ אין פירוק ל-3.
ומצאנו שני פירוקים שונים ל-9.

ב. $R=\mathbb{Z}[\sqrt{-5}]$ · תחום שלמות כתת-חוג של $\mathbb{C}$.

דוגמא: $(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2\cdot 3$

נניח $2=a\cdot b$, $a,b\in R$.

אז: $4=|a|^2|b|^2$ ולכן $|a|^2=1,2,4$

נניח $a=a_1+a_2\sqrt{-5}$, אז: $a_1^2+5a_2^2=|a|^2=1$

$\Rightarrow a_1=\pm1,\ a_2=0 \Rightarrow a=\pm1$ בפרט הפיך.

אם $|a|^2=4$ אז $|b|^2=1$ ואז b הפיך.

המשוואה $a_1^2+5a_2^2=2$ לא ניתנת, לכן 2 אי פריק.

טיעון דומה עובד ל-3 ול- $1\pm\sqrt{-5}$.

$2,3,1\pm\sqrt{-5}$ הם אברים אי-פריקים סוציניים.

שימו לב: $2\mid(1+\sqrt{-5})(1-\sqrt{-5})$ אבל לא מחלק ~~אף~~ אף אחד מהגורמים במכפלה.

הערה: אם R תחום הח"ע אז כל אי-פריק הוא ראשוני

כי אם $p\mid ab$ (p אי-פריק) · נניח $c\cdot p=a\cdot b$, נפרק את

שני האגפים ו- $c_1\cdots c_n\cdot p=a_1\cdots a_k\cdot b_1\cdots b_l$ כמכפלות אי-פריקים.

p חייב להופיע בפירוק של a או של b ולכן הוא מחלק

או את a או את b ולכן ראשוני.

נזכור שטענו כי אם p אי-פריק ב-R ו- $Rp\subsetneq Ra$ אז

a הפיך ו- $Ra=R$. בפרט, החוג ראשי, נקבל כי אם

p אי"פ אז Rp מקס', ובפרט ראשוני.

אז אנו צריכים למצוא אידאל שאינו ראשי ש- $R2$ מוכל בו

ממש. $I=(2,1+\sqrt{-5})=2R+(1+\sqrt{-5})R \supsetneq 2R=(2)$ ו- $I\neq R$,

תרגיל. (למשל $1\notin I$). ולכן האידאל $2R$ אינו ראשוני.

תרגיל 13:

① $R=F[x]$, $I\lhd F[x]$, אז ל- $F[x]/I$ מבנה של מ"ו מעל F.

$u: F[x]\longrightarrow F[x]/I$ כך ש- $u(f)=f+I$.

הסעיף הראשון שהעתקה u נותן לשכן את F ב- $F[x]/I$,

ואז מושרה מבנה של מ"ו על $F[x]/I$ מעל F.

הסעיף ג': אם $f(x)$ פולינום ממעלה n אז $F[x]/(f(x))$ מ"ו

קטא

ממימד n מעל F.

טענה: $1, \bar{x}, \bar{x}^2, \dots, \bar{x}^{n-1}$ בסיס ל- $F[x]/(f(x))$ כאשר $\bar{p}=p+I$

הוכחה: ברור ש- $1, \bar{x}, \dots, \bar{x}^k, \dots$ פורשים את $F[x]/(f(x))$.

בתוך המנה: $a_0+a_1\bar{x}+\dots+a_n\bar{x}^n \underset{\text{הגדרה}}{=} \overline{a_0+a_1x+\dots+a_nx^n} = \overline{f(x)} = \bar{0}$

$\Leftarrow$ $\bar{x}^n = -\frac{a_0}{a_n} - \frac{a_1}{a_n}\bar{x} - \dots - \frac{a_{n-1}}{a_n}\bar{x}^{n-1}$ $(a_n \neq 0)$

ובאינדוקציה $\bar{x}^k \in Sp(1, \bar{x}, \dots, \bar{x}^{n-1})$ לכל $k \in \mathbb{N}$. ולכן

$$F[x]/(f(x)) = Sp\{1, \bar{x}, \dots, \bar{x}^{n-1}\}$$

הם בת"ל כי: $\bar{0} = c_0+c_1\bar{x}+\dots+c_{n-1}\bar{x}^{n-1} = \overline{c_0+c_1x+\dots+c_{n-1}x^{n-1}}$

$\Leftarrow$ $p(x) = c_0+c_1x+\dots+c_{n-1}x^{n-1} \in (f(x))$

$\Leftarrow$ $f(x)|p(x)$, אבל $\deg(p(x)) < \deg(f(x))$

$\Leftarrow$ $p(x)=0$ $\Leftarrow$ $c_i=0$ $\forall i$. ∎

אם $f(x)$ הוא אי פריק אז $(f(x))$ מקסי. (כי $F[x]$ חוג אוקלידי) ולכן $F[x]/(f(x))$ שדה.

הערה: יהי $f(x) \in F[x]$ פולינום ממעלה 2 או 3, אז $f(x)$ אי-פריק אמ"מ ל- $f(x)$ אין שורש ב- F.

הוכחה: אם ל- $f(x)$ שורש α אז $(x-\alpha)|f(x)$ ולכן f פריק. לכן $\overset{\text{הכיוון}}{\Leftarrow}$ תמיד נכון (לכל פולינום בכל דרגה).

($\Rightarrow$) אם $f(x)=g(x)h(x)$ פריק אמיתי אז בה"כ $\deg(g(x))=1$. נניח $g(x)=ax+b$ אז:

$f(x) = (ax+b)h(x) = a(x-(-\frac{b}{a}))h(x) \Rightarrow$

$\Leftarrow$ $-\frac{b}{a}$ שורש של $f(x)$ בסתירה.

נבנה לוח כפל וחיבור לשדה בן 4 איברים.

$F=\mathbb{Z}_2$. $f(x)=1+x+x^2$ אי-פריק מעל $\mathbb{Z}_2$.

$\mathbb{Z}_2[x]/(1+x+x^2) = F_4$ שדה, ומרחב וקטורי ממימד 2 מעל $\mathbb{Z}_2$

לכן גודלו 4; $F_4 = \{0, 1, \bar{x}, 1+\bar{x}\}$

נשים לב ש- $\bar{X}^2 = -1-\bar{X} \underset{char 2}{=} 1+\bar{X}$ (תכונות אלגוריתם)

לוח חיבור:

+	0	1	$\bar{X}$	$1+\bar{X}$
0	0	1	$\bar{X}$	$1+\bar{X}$
1	1	0	$1+\bar{X}$	$\bar{X}$
$\bar{X}$	$\bar{X}$	$1+\bar{X}$	0	1
$1+\bar{X}$	$1+\bar{X}$	$\bar{X}$	1	0

לוח כפל:

·	0	1	$\bar{X}$	$1+\bar{X}$
0	0	0	0	0
1	0	1	$\bar{X}$	$1+\bar{X}$
$\bar{X}$	0	$\bar{X}$	$1+\bar{X}$	1
$1+\bar{X}$	0	$1+\bar{X}$	1	$\bar{X}$

$\bar{X}+\bar{X}^2 = \bar{X}+1+\bar{X} = 1$

כדי למצוא לוח חיבור וכפל ל- F_8 ניקח את
$g(x) = 1+x+x^3$
$g(x)$ אי-פריק מעל $\mathbb{Z}_2$, לכן $\mathbb{Z}_2[x]/(g(x))$ שדה
מגודל 8: $F_8 = \{0, 1, \bar{X}, \bar{X}^2, 1+\bar{X}, 1+\bar{X}^2, \bar{X}+\bar{X}^2, 1+\bar{X}+\bar{X}^2\}$
בלוח חיבור הפשט מחברים (מציין השדה הוא 2)
כדי לבנות לוח כפל יש לחשב את $\bar{X}^3$ ו- $\bar{X}^4$:
$\bar{X}^3 = 1+\bar{X}$, $\bar{X}^4 = \bar{X}+\bar{X}^2$
ומכאן, כמו קודם אפשר לבנות גם לוח כפל.

$\mathbb{Z}[i]$. זהו חוג אוקלידי עם $d(a+bi) = a^2+b^2$.
אם $p \neq 2$ ראשוני, $p = a^2+b^2$ אז $p = 1 \pmod 4$.
בה"כ $a^2 \equiv 1 \pmod 4$ ו- $b^2 \equiv 0 \pmod 4$.
רוצים להראות כי אם $p \equiv \pmod 4$ אז p סכום שני ריבועים.
אם p ראשוני ב- $\mathbb{Z}$, ו- p לא ראשוני ב- $\mathbb{Z}[i]$ אז

$p=a^2+b^2$.

כי: p לא ראשוני ב- $\mathbb{Z}[i]$, ונניח כי $a+bi|p$.

אם $x|y$ ידוע אז $\bar{x}|\bar{y}$, ולכן $a-bi|p$ ולכן

$d(a+bi)=a^2+b^2=(a+bi)(a-bi)$ מחלק את p ולכן

$p=a^2+b^2$.

כדי להוכיח את המשפט צריך להראות כי אם $p\equiv 1 \pmod 4$

אז p אינו ראשוני ב- $\mathbb{Z}[i]$.

מיהם הראשוניים ב- $\mathbb{Z}[i]$?

טענה: הראשוניים הם איברים $a+bi$ כך ש- $d(a+bi)=p$

p - ראשוני ו- ראשוניים ב- $\mathbb{Z}$, $p\in\mathbb{Z}$ כך ש- $p=3(4)$

אם $p\equiv 3(4)$ אז p ראשוני ב- $\mathbb{Z}[i]$ כי אחרת

p סכום שני ריבועים.

נניח $d(a+bi)=p$. p ראשוני ונניח $x+yi|a+bi$

לכן $x-yi|a-bi$ ולכן $d(x+yi)|d(a+bi)$

$\Leftarrow$ $d(x+yi)=1$ או $d(x+yi)=p$ ולכן $x+yi$

הפיך או חבר. לכן, $a+bi$ ראשוני.

נשאר להראות שאלו הם בדיוק הראשוניים.

לא (נספיק...)

אם $x\in\mathbb{Z}[i]$ פריק אז $x=y\cdot z$ ו- $d(x)=d(y)d(z)$

לכן $d(x)$ פריק ב- $\mathbb{Z}$ (כי $d(y),d(z)\neq 1$)...

צריך להראות כי אם $d(x)$ אינו ראשוני ב- $\mathbb{Z}$ אז

או $d(x)=p^2\equiv 3\ (4)$ או ש- x אינו ראשוני ב- $\mathbb{Z}[i]$.