מבנים אלגבריים 1

יובל קפלן

סיכום הרצאות פרופ׳ אלכסנדר לובוצקי בקורס ״מבנים אלגבריים 1״
(80445) באוניברסיטה העברית, 8–2007.

תוכן מחברת זו הוקלד ונערך על־ידי יובל קפלן. אין המרצה אחראי לכל טעות שנפלה בו. סודר באמצעות $\LaTeX 2_\varepsilon$ ב־21 בפברואר 2008. עדכונים ותיקונים יופיעו ב־http://www.limsoup.net/. לתגובות, לתיקונים ובכל עניין אחר, אנא כתבו ל־yuvak@gmx.net.

סיכומים נוספים בסדרה:

2006–7	חשבון אינפיניטסימלי 1	אלגברה לינארית 1
	חשבון אינפיניטסימלי 2	אלגברה לינארית 2
	תורת הקבוצות	
2007–8	מבנים אלגבריים 1	תורת ההסתברות 1

תוכן עניינים

1 תורת החבורות

1.1 הגדרה

22.10.2007

חבורה

הגדרה. **חבורה** היא מערכת $(G,\cdot,e)$ כאשר G קבוצה, $\cdot$ פעולה בינארית[1] ו־$e\in G$, כך ש־

1. קשירות: $\forall a,b\in G\quad \exists! a\cdot b\in G$
2. אסוציאטיביות: $\forall a,b,c\in G\quad (a\cdot b)\cdot c=a\cdot(b\cdot c)$
3. e איבר יחידה: $\forall a\in G\quad a\cdot e=e\cdot a=a$
4. קיום איבר הפכי: $\forall a\in G\quad \exists b\in G\ :\ a\cdot b=b\cdot a=e$

חבורה חילופית

הגדרה. חבורה נקראת **חילופית (קומוטטיבית, אבלית)** אם $\forall a,b\in G\quad ab=ba$.

דוגמה. $(\mathbb{Z},+,0)$ חבורה; באופן כללי, אם F שדה, $(F,+,0)$ ו־$(F\setminus\{0\},\cdot,1)$ חבורות.
כל מרחב וקטורי, עם פעולת החיבור, הוא חבורה אבלית.

דוגמה. תהי $S_n=\mathrm{perm}(\{1,\dots,n\})$ קבוצת כל הפונקציות החח״ע ועל מ־$\{1,\dots,n\}$ לעצמה, ביחס לפעולת ההרכבה. האיבר הנייטרלי הוא תמורת הזהות. פעולת ההרכבה אסוציאטיבית.[2] עבור $2<n$, חבורה זו אינה קומוטטיבית.

דוגמה. יהי F שדה. הקבוצה $GL_n(F)=\{A\in M_n(F)\mid \det A\neq 0\}$ ביחס לפעולת הכפל עם איבר היחידה $e_G=I$ היא חבורה.[3]

טענה 1: האיבר ההפכי b של a יחיד. (נסמנו a^{-1}.[4])

הוכחה. אם $ac_1=e$ ו־$ac_2=e$, מאחר שקיים b כך ש־$ba=e$, נכפול את שתי המשוואות ב־b ונשתמש באסוציאטיביות:

$$\begin{aligned} b(ac_1) &= (ba)c_1=ec_1=c_1\\ b(ac_2) &= (ba)c_2=ec_2=c_2 \end{aligned}$$

מכיוון ש־$ac_1=ac_2$, גם $b(ac_1)=b(ac_2)$, ונקבל $c_1=c_2$.

מסקנה 2: למשוואה מהצורה $ax=d$ או $xa=d$ יש פתרון יחיד.

הוכחה ($ax=d$). יש פתרון, $x=a^{-1}d$. בהוכחת הטענה השתמשנו רק בעובדה ש־$ac_1=ac_2$, לכן נקבל יחידות גם כאן.

הגדרה. יהיו H, G שתי חבורות.

הומומורפיזם

1. פונקציה $\varphi:G\to H$ נקראת **הומומורפיזם** אם לכל $a,b\in G$, $\varphi(a\cdot b)=\varphi(a)\cdot\varphi(b)$.

[1] לא בהכרח כפל. הסיבה לשימוש בסימן $\cdot$ היא שמקובל ש־$+$ מייצג פעולה קומוטטיבית, מה שלא בהכרח מתקיים.
[2] כי $(f\circ(g\circ h))(x)=((f\circ g)\circ h)(x)=f(g(h(x)))=f(g\circ h(x))=f\circ(g\circ h)(x)$.
[3] GL הוא קיצור של General Linear [Group].
[4] לא $\frac{1}{a}$ – לא ברור האם $\frac{c}{a}$ הוא $\frac{1}{a}\cdot c$ או $\frac{1}{a}$, והרי אין דרישה לקומוטטיביות.

דוגמה. כל טרנספורמציה לינארית בין שני מרחבים וקטוריים שומרת על החיבור, לכן היא הומומורפיזם.

2. הומומורפיזם φ ייקרא **מונומורפיזם** אם φ חד־חד ערכית.
3. הומומורפיזם φ ייקרא **אפימורפיזם** אם φ על.
4. הומומורפיזם φ ייקרא **איזומורפיזם** אם φ חח״ע ועל.

חבורות איזומורפיות

אם קיים $\varphi : G \to H$ איזומורפיזם, נאמר ש־G ו־H **איזומורפיות** ($G \cong H$).

טענה 3: אם $\varphi : G \to H$ הומומורפיזם בין חבורות, אזי $\varphi(e_G) = e_H$.[5]

הוכחה. למה 1.3: אם $b \in G$ ו־$ab = b$, אזי $a = e$.

הוכחה. למשוואה $xb = b$ יש פתרון יחיד, והוא e.

כעת, $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G)$. אז על־פי הלמה, $\varphi(e_G) = e_H$.

1.2 חבורות סופיות

ניתן לייצג חבורה כטבלה (״לוח כפל״). (אם החבורה קומוטטיבית, טבלה זו תהיה סימטרית.) משמעות מסקנה 2 היא שבכל שורה יופיעו כל איברי החבורה פעם אחת בדיוק (השורה תהיה תמורה של איברי החבורה): $\forall a, b \quad \exists! x \ : \ ax = b$. זה נכון גם לגבי עמודות: $\forall a, b \quad \exists! x \ : \ xa = b$. אז כל חבורה היא בעצם ״ריבוע לטיני״ (״ריבוע קסם״).

1.2.1 חבורות מסדר 1

החבורה היחידה האפשרית מסדר 1 היא $G = (\{e\}, \cdot, e)$ כך ש־$e \cdot e = e$. זוהי **החבורה הטריוויאלית**.

מרחב ה־0 (המרחב הווקטורי שמכיל רק את ה־0, שהוא למעשה חבורה) איזומורפי לחבורה הטריוויאלית. כלומר, $(\{e\}, \cdot, e) \cong (\{0\}, +, 0)$, ובפרט קיימת חבורה מסדר 1.

1.2.2 חבורות מסדר 2

נסמן את האיברים ב־e ו־a. מתכונות הפעולה $\cdot$, בהכרח נקבל –

$\cdot$	e	a
e	e	a
a	a	

נותר למצוא מהו $a \cdot a$; אך בהכרח $a \cdot a = e$, שאם לא כן $e = a$. מכאן, יכולה להיות רק חבורה אחת מסדר 2, עד־כדי איזומורפיזם (כל הגדרה אחרת של הפעולה $\cdot$ לא תוביל לחבורה).

למעשה, חסרה הוכחת קיום; ניתן לספק אותה על־ידי דוגמה: השדה $\mathbb{Z}_2$ הוא חבורה מסדר 2: $G = (\{e, a\}, \cdot, e) \cong (\{0, 1\}, +, 0) = \mathbb{Z}_2$.

[5] טענה זו אנלוגית לטענה כי $\varphi(0) = 0$ עבור טרל״נ φ, מאלגברה לינארית 1.

1.2.3 חבורות מסדר 3

נסמן את האיברים ב־e, a ו־b. בהכרח נקבל –

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

אי־אפשר להגדיר $a \cdot a = e$, כי אז נקבל $b \cdot a = b$ ו־$a = e$; לכן בהכרח $a \cdot a = b$, ונקבל –

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

גם כאן, זו האפשרות היחידה לחבורה מסדר 3. דוגמה לחבורה כזו היא $\mathbb{Z}_3$.

1.2.4 חבורות מסדר 4

נסמן את האיברים ב־e, a, b ו־c. בהרח נקבל –

$\cdot$	e	a	b	c
e	e	a	b	c
a	a			
b	b			
c	c			

$a \cdot a \neq a$; כעת ישנן שלוש אפשרויות:

$a \cdot a = e$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e		
b	b			
c	c			

$a \cdot a = b$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b		
b	b			
c	c			

$a \cdot a = c$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	c		
b	b			
c	c			

ובהכרח –

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	$e/\mathbf{a}$	$a/\mathbf{e}$
c	c	b	$a/\mathbf{e}$	$e/\mathbf{a}$

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	c	e	b
b	b	e	c	a
c	c	b	a	e

האפשרות השנייה (המודגשת) עבור $a \cdot a = e$ איזומורפית לאפשרות המתקבלת עבור $a \cdot a = b$ (על־ידי איזומורפיזם φ עבורו $\varphi(a) = b$, $\varphi(b) = a$, $\varphi(e) = e$, $\varphi(c) = c$). כמו־כן, אפשרויות אלה איזומורפיות לאפשרות המתקבלת עבור $a \cdot a = c$ (כתרגיל). מצד שני, האפשרות המתקבלות

עבור $a \cdot a = b$ אינה איזומורפית לאפשרות הראשונה המתקבלת עבור $a \cdot a = e$: קבוצות איברי האלכסון שונות, ולכן אין איזומורפיזם שיוכל לשמור על האלכסון.

דוגמה לחבורה מהדגם $a \cdot a = e$ היא $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(1,0),(0,1),(1,1)\}$, בה $a + a = 0$ לכל איבר a; דוגמה לחבורה מהדגם $a \cdot a = b$ היא $\mathbb{Z}_4 = \{0,1,2,3\}$.

1.3 תת־חבורות

תת־חבורה **הגדרה.** אם G חבורה, תת־קבוצה H של G תיקרא **תת־חבורה (חבורה חלקית)** אם – 24.10.2007

1. $H \neq \varnothing$;
2. לכל $a, b \in H$ גם $a \cdot b \in H$;
3. לכל $a \in H$ גם $a^{-1} \in H$.

כלומר, H חבורה ביחס לאותה פעולה של G.[6] מסמנים $H \leq G$.

מסקנה 4: מהתכונות, $e \in H$.

טענה 5: G חבורה, $H \subseteq G$ תת־קבוצה לא ריקה. אזי H חבורה חלקית $\iff$ לכל $a, b \in H$ גם $a^{-1}b \in H$.

הוכחה. כתרגיל.

טענה 6: אם $\{H_i\}_{i \in I}$ אוסף של תת־חבורות של G, אזי $H = \bigcap_{i \in I} H_i$ גם היא חבורה חלקית.

הוכחה. לכל i, $e \in H_i$ לכן $e \in \bigcap H_i = H$ ובפרט H אינה ריקה ותנאי 1 מתקיים.

אם $a, b \in H$ אזי לכל i, $a, b \in H_i$ ולכן לכל i, $a \cdot b \in H_i$ (אלו תת־חבורות); מכאן, $a \cdot b \in H$, ותנאי 2 מתקיים.

אם $a \in H$ אזי לכל i, $a \in H_i$ ולכן לכל i, $a^{-1} \in H_i$; מכאן, $a^{-1} \in H$, ותנאי 3 מתקיים.

דוגמה. $G = \mathbb{Z}$, $H_2 = 7\mathbb{Z}$, $H_1 = 5\mathbb{Z}$. אז $H_1 \cap H_2 = 35\mathbb{Z}$ חבורה חלקית.

הטענה המקבילה לאיחוד תת־חבורות אינה מתקיימת: בדוגמה הנ"ל, $H_1 \cup H_2$ איננה חבורה חלקית – למשל, 5 ו־7 נמצאים בה, אך $7 + 5$ לא.

מסקנה 7: תהא G חבורה ו־$S \subseteq G$ תת־קבוצה. נסמן $\hat{S} = \bigcap\{H \ : \ H \leq G \ \wedge \ S \subseteq H\}$ – חיתוך כל החבורות החלקיות של G המכילות את S. אזי $\hat{S}$ חבורה חלקית של G, וזו החבורה החלקית המינימלית המכילה את S.[7]

[6] חשוב לשים לב לכך שמדובר באותה פעולה: למשל, אמנם $\mathbb{R}$ חבורה ביחס לחיבור (עם איבר יחידה 0) ותת־הקבוצה $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ מהווה חבורה ביחס לכפל (עם איבר יחידה 1), אך $\mathbb{R}^*$ איננה חבורה חלקית של $\mathbb{R}$.

[7] דבר זה אנלוגי למרחב וקטורי הנפרש על־ידי קבוצת וקטורים.

טענה 8: $S \subseteq G$ תת־קבוצה. נסמן –

$$\langle S\rangle = \{x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n} \ : \ n \in \mathbb{N} \cup \{0\}, \varepsilon_i = \pm 1, x_i \in S\}$$

(זהו אוסף כל ה"מילים" המורכבות מאיברי S, כאשר המילה באורך 0 היא e). אזי $\langle S\rangle = \hat{S}$ היא **החבורה החלקית הנוצרת על־ידי** S. החבורה הנוצרת

הוכחה. נראה ש־$\langle S\rangle$ היא חבורה חלקית. ואכן, $e \in \langle S\rangle$; אם $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}, y_1^{\delta_1} \cdots y_m^{\delta_m} \in S$ אזי $x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n} \cdot y_1^{\delta_1} \cdots y_m^{\delta_m} \in \langle S\rangle$; ולבסוף, $(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n})^{-1} = x_n^{-\varepsilon_n} \cdots x_1^{-\varepsilon_1}$ ולכן גם ההפכי ב־$\langle S\rangle$.[8] אז $\langle S\rangle$ חבורה חלקית.

ברור ש־$S \subseteq \langle S\rangle \leq G$; לכן $\hat{S} \leq \langle S\rangle$, על־פי הגדרת $\hat{S}$.

בכיוון ההפוך, $\hat{S}$ היא חבורה חלקית המכילה את S ולכן גם את $S^{-1} = \{s^{-1} \ : \ s \in S\}$; אז היא מכילה גם את אוסף כל המכפלות של איברים מ־S ומ־S^{-1} מכל אורך, ולכן מכילה את $\langle S\rangle$.

1.4 חבורות ציקליות

29.10.2007

דוגמה. $G = (\mathbb{Z}, +, 0)$. עבור $S = \{3\}$ נקבל $\langle S\rangle = 3\mathbb{Z}$. עבור $T = \{5, 7\}$ נקבל $\langle T\rangle = \mathbb{Z}$: נוכל לקבל $1 = 3 \cdot 5 - 2 \cdot 7$. באופן כללי יותר, אם $a, b \in \mathbb{Z}$, קיימים $x, y \in \mathbb{Z}$ כך ש־$xa + yb = 1$ אם"ם $(a, b) = 1$.[9] זה מתקיים אם"ם $\langle a, b\rangle \cong \mathbb{Z}$, כי $\langle -1\rangle = \langle 1\rangle = \mathbb{Z}$.

אם $G = \mathbb{Z}_n = \{0, \ldots, n-1\}$, $\mathbb{Z}_n = \langle 1\rangle$; באופן כללי, אם $1 \leq a < n$ ו־$(a, n) = 1$, $\langle a\rangle = \mathbb{Z}_n$. (כתרגיל.)

הגדרה. אם קיים $a \in G$ כך ש־$G = \langle a\rangle$, נאמר ש־G **חבורה מעגלית (ציקלית)**. חבורה ציקלית

טענה 9: אם G חבורה ציקלית, אזי אם G אינסופית, $G \cong \mathbb{Z}$, ואם G סופית מסדר n, $G \cong \mathbb{Z}_n$.[10]

הוכחה. יש $a \in G$ כך ש־$G = \langle a\rangle$, כלומר כל איבר ב־G הוא "מילה" ב־a וב־a^{-1}, ולכן כל איבר ב־G הוא מהצורה a^k עבור $k \in \mathbb{Z}$.[11]

אם כל האיברים a^k שונים זה מזה, בפרט G אינסופית. נגדיר העתקה $\varphi : \mathbb{Z} \to G$ על־ידי $\varphi(k) = a^k$. זהו הומומורפיזם כי $\varphi(k + l) = a^{k+l} = a^k a^l = \varphi(k) \cdot \varphi(l)$.[12] זה על, כי $G = \langle a\rangle$, וזה חח"ע כי אמרנו שכל האיברים שונים זה מזה. לכן φ איזומורפיזם.

אם יש $k \neq l \in \mathbb{Z}$ כך ש־$a^k = a^l$, נכפול ב־a^{-1} l פעמים ונקבל $a^{k-l} = e$. בה"כ $k - l > 0$ (אחרת $e = (a^{k-l})^{-1} = a^{l-k}$), כלומר יש $m > 0$ כך ש־$a^m = e$. יהי n החיובי הראשון כך ש־$a^n = e$; נטען כי $G = \{e, a, a^2, \ldots, a^{n-1}\}$, ואלו איברים שונים. אם $k \geq n$, נחלק את k ב־n ונקבל $k = rn + s$ (כאשר $0 \leq s < n$), ואז $a^k = a^{rn+s} = (a^n)^r a^s = e^r a^s = ea^s = a^s$ (ובאופן דומה עבור k שלילי). אלו איברים שונים כי אם $1 \leq j < i < n$ ו־$a^i = a^j$, אז $a^{i-j} = e$,

[8] השתמשנו בכך ש־$a = (a^{-1})^{-1}$.

[9] דהיינו, המחלק המשותף הגדול ביותר של a ו־b הוא 1 (הם זרים).

[10] מהטענה נובע שחבורה ציקלית היא לכל היותר בת־מניה.

[11] זה אומר, בפרט, שחבורה ציקלית היא אבלית; ההיפך, כמובן, אינו נכון ($\mathbb{R}$ למשל אבלית ולא ציקלית).

[12] יש לשים לב ש־$+$ היא הפעולה של $\mathbb{Z}$ ו־$\cdot$ היא הפעולה של G.

בסתירה למינימליות n. נגדיר $\varphi : \mathbb{Z}_n \to G$ על־ידי $\varphi(k) = a^k$. מהדיון הקודם נובע ש־φ חח״ע ועל; φ הומומורפיזם: $\varphi(k+r) = a^{k+r} = a^k a^r = \varphi(k)\varphi(r)$.

סדר של איבר

הגדרה. G חבורה, $a \in G$. $o(a) = \min\{n \ : \ n > 0,\ a^n = e\}$ הוא **הסדר** של a. אם אין n כזה, נאמר שהסדר של a הוא אינסופי.

משקנה 10: אם $a \in G$ ו־$H = \langle a \rangle$ החבורה החלקית הנוצרת על־ידי a, אזי $|H| = o(a)$.

1.5 מחלקות של חבורות חלקיות

הגדרה. תהי G חבורה, H תת־חבורה. עבור $a, b \in G$, נאמר ש־$a \equiv b \pmod H$ אם $a^{-1}b \in H$.

טענה 11: יחס זה הוא יחס שקילות.

הוכחה. נבדוק את קיום התכונות:[13]

1. רפלקסיביות: $e = a^{-1}a \in H \iff a \equiv a \pmod H$; זה אכן מתקיים, כי H חבורה חלקית.
2. סימטריות: נניח $a \equiv b \pmod H$. אזי $a^{-1}b \in H$ ולכן גם $(a^{-1}b)^{-1} = b^{-1}a \in H$, כי H חבורה חלקית. כלומר, $b \equiv a \pmod H$.
3. טרנזיטיביות: נניח $a \equiv b \pmod H$ ו־$b \equiv c \pmod H$. אז $a^{-1}b \in H$ ו־$b^{-1}c \in H$. H חבורה חלקית, לכן גם $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$. כלומר, $a \equiv c \pmod H$.

יחס שקילות זה מחלק את החבורה G (כקבוצה) למחלקות שקילות זרות; אם $a \in G$, נסמן $[a] = \{b \ : \ a \equiv b \pmod H\}$. זוהי ה**מחלקה** של a.

דוגמה. $[e] = H$, כי $a = e^{-1}a \in H$ לכל a.

טענה 12: אם $a \in G$ אזי $[a] = a \cdot H = \{ah \ : \ h \in H\}$.[14]

הוכחה. נראה קודם ש־$aH \subseteq [a]$: ואכן, אם $b = ah \in H$, אזי $a^{-1}b = a^{-1}ah = h \in H$ ולכן $b \in [a]$.

להיפך, אם $b \in [a]$ אזי $h = a^{-1}b \in H$. אז $b = aa^{-1}b = ah \in aH$.

מחלקות

הגדרה. aH נקראת **המחלקה השמאלית** של H המכילה את a. באופן אנלוגי, Ha היא **המחלקה הימנית** של H המכילה את a.[15] [16]

אינדקס

הגדרה. מספר המחלקות השמאליות של H ב־G, שיסומן $[G : H]$, נקרא **האינדקס של H ב־G**.

[13] להגדרת יחס ויחס שקילות, ר׳ סיכומים בתורת הקבוצות.
[14] בקונטקסט של מרחבים וקטוריים, זה מקביל לישרייה.
[15] לשם הגדרת מחלקה ימנית, משתמשים ביחס השקילות $a \equiv b \pmod H \iff ab^{-1} \in H$.
[16] בדרך כלל, $aH \neq Ha$.

דוגמה. $[\mathbb{Z} : 7\mathbb{Z}] = 7$ (ובאופן כללי, $[\mathbb{Z} : n\mathbb{Z}] = n$).

טענה 13: אם $[a]$ ו־$[b]$ מחלקות שקילות (שמאליות) של H, יש פונקציה חח״ע ועל $f : [a] \to [b]$ (ובפרט, $|[a]| = |[b]|$).

הוכחה. למה 1.13: כל איבר $c \in [a]$ ניתן לכתיבה באופן יחיד כ־$c = ah$ עבור $h \in H$.

הוכחה. $ah_1 = ah_2$ אזי $h_1 = h_2$.

נגדיר $f : [a] \to [b]$ על־ידי $f(ah) = bh$. זה על כי כל איברי $[b]$ הם מהצורה bh, וזה חח״ע כי אם $f(ah_1) = f(ah_2)$ אז $bh_1 = bh_2$ ומכאן $h_1 = h_2$ ו־$ah_1 = ah_2$.

מסקנה 14: אם G סופית, אזי $|G| = [G : H] \cdot |H|$.

הוכחה. בכל מחלקה יש אותו מספר איברים ויש $[G : H]$ מחלקות.

מסקנה 15 (משפט לגראנז׳): אם G סופית ו־H חבורה חלקית, אזי $|H| \mid |G|$.

31.10.2007

יהי עכשיו g איבר כלשהו ב־G, ונסמן ב־H את החבורה החלקית של G הנוצרת על־ידי g. H ציקלית. אם G סופית, גם H סופית, ואז $H \cong \mathbb{Z}_n$ כאשר $n = o(g)$.[17] כלומר, מצאנו ב־G תת־חבורה שגודלה כסדר g.

מסקנה 16: אם G סופית, אזי לכל $g \in G$, $o(g) \mid |G|$.

מסקנה 17: לכל $g \in G$, $g^{|G|} = e$.

הוכחה. $|G| = o(g) \cdot r$, אז $g^{|G|} = g^{o(g)\cdot r} = (g^{o(g)})^r = e^r = e$.

מסקנה 18: אם G חבורה מסדר ראשוני p, אזי $G \cong \mathbb{Z}_p$.

הוכחה. יהי $e \neq g \in G$. אזי $o(g) \mid |G| = p$ ו־$o(g) \neq 1$ כי $g \neq e$. לכן $o(g) = p$.[18] $H = \langle g \rangle$ היא מסדר p, ולכן $H = G$. אז G נוצרת על־ידי g, כלומר היא ציקלית מסדר p – ולכן איזומורפית ל־$\mathbb{Z}_p$.

בעזרת שימוש בחבורות, משפטים בתורת המספרים נעשים פשוטים להוכחה:

משפט 19 (פרמה הקטן): אם p ראשוני ו־$a \in \mathbb{Z}$, אזי $a^p \equiv a \pmod{p}$. (כלומר, $p \mid a^p - a$.)

הוכחה. אם $p \mid a$, ברור. לכן נניח $(a, p) = 1$. נתבונן בחבורה הכפלית $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$ עם פעולת הכפל מודולו p.[19] זו חבורה מסדר $p - 1$, לכן מהמסקנה, לכל $b \in \{1, \ldots, p-1\} \in \mathbb{Z}_p^*$ מתקיים $b^{p-1} \equiv 1 \pmod{p}$, ולכן אם $a \in \mathbb{Z}$ כלשהו עם $(a, p) = 1$, אזי יש $b \in \mathbb{Z}_p^*$ כך ש־$a \equiv b \pmod{p}$, ולכן $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$. נכפול את שני הצדדים ב־$a$ ונקבל $a^p \equiv a \pmod{p}$.

[17] כי $H = \{e, g, g^2, \ldots, g^{n-1}\}$.

[18] מחלק של מספר ראשוני שאינו 1 הוא הראשוני עצמו.

[19] זו החבורה הכפלית של השדה $\mathbb{Z}_p$; $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$.

הגדרה. יהי n מספר טבעי; נסמן $\mathbb{Z}_n^* = \{1 \leq a < n \mid (a,n) = 1\}$. **פונקציית אוילר** מוגדרת על־ידי $\varphi(n) = |\mathbb{Z}_n^*|$.

דוגמה. $\varphi(p) = p-1$, אם p ראשוני; $\varphi(6) = 2$; $\varphi(15) = 8$; אם p ו־q ראשוניים, $\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1)(q-1)$.

טענה 20: 1. אם $(m,n) = 1$ אזי $\varphi(mn) = \varphi(m)\varphi(n)$.

2. $\varphi(p^r) = (p-1)p^{r-1}$ עבור p ראשוני.

טענה 21: $\mathbb{Z}_n^*$ היא חבורה מסדר $\varphi(n)$; זו חבורת האיברים ההפיכים בחוג $\mathbb{Z}_n$.

הוכחה. תרגיל: $a \in \mathbb{Z}_n^* \iff$ קיים $b \in \mathbb{Z}_n^*$ כך ש־$ab \equiv 1 \pmod{n}$.
מכפלת שני הפיכים הפיכה: $(ab)^{-1} = b^{-1}a^{-1}$.

משפט 22 (אוילר): $a, n \in \mathbb{Z}$ עם $(a,n) = 1$, אזי $a^{\varphi(n)} \equiv 1 \pmod{n}$.[20]

הוכחה. בלי הגבלת הכלליות, אפשר להניח ש־$0 \leq a < n$, ואז $a \in \mathbb{Z}_n^*$ כי $(a - q \cdot n, n) = 1$ אם $(a,n) = 1$.[21] אז $a^{\varphi(n)} \equiv 1 \pmod{n}$, כי $\mathbb{Z}_n^*$ חבורה מסדר $\varphi(n)$, ועל־פי המסקנה ממשפט לגראנז'.

1.6 חבורות התמורות

5.11.2007

תהי X קבוצה. נסמן $\mathrm{Per}(X) = \{f : X \to X \mid f$ חח"ע ועל$\}$ – אוסף התמורות של X. זו חבורה ביחס לפעולת ההרכבה: איבר היחידה הוא העתקת הזהות; לכל $f : X \to X$ חח"ע ועל יש $f^{-1} : X \to X$ כך ש־$f^{-1} \circ f = f \circ f^{-1} = id$; הרכבת שתי פונקציות מקיימת את החוק האסוציאטיבי: $(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$.

דוגמה. אם X סופית, נניח $X = \{1, 2, \ldots, n\}$, נסמן $\mathrm{Per}(X) = \mathrm{Sym}(n) = S_n = \Sigma_n$. חבורה זו נקראת **החבורה הסימטרית על n אותיות**; גודלה $|S_n| = n!$.

משפט 23 (קיילי): לכל חבורה G קיימת קבוצה X כך ש־G איזומורפית לחבורה חלקית של $\mathrm{Per}(X)$.[22] כלומר, קיימים קבוצה X ומונומורפיזם $\varphi : G \to \mathrm{Per}(X)$.

הוכחה. נבחר $X = G$ (כקבוצה). עבור כל $a \in G$ נגדיר $l_a : G \to G$ על־ידי $l_a(x) = ax$ ($x \in G$). l_a חח"ע: נניח $ax_1 = l_a(x_1) = l_a(x_2) = ax_2$; בחבורה אפשר לצמצם, לכן $x_1 = x_2$. כמו־כן, l_a על: אם $y \in X = G$, נקבל $l_a(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y = ey = y$. לכן $l_a \in \mathrm{Per}(X)$.

נגדיר הומומורפיזם $\varphi : G \to \mathrm{Per}(X)$ על־ידי $\varphi(a) = l_a$ לכל $a \in G$. נותר להראות כי (א) φ הומומורפיזם וכי (ב) φ חח"ע.

[20] זוהי הכללה של משפט פרמה הקטן.

[21] אם p מחלק גם את n וגם את $a - q \cdot n$, אז בהכרח p מחלק גם את a.

[22] משמעות המשפט היא שכל החבורות איזומורפיות לחבורות תמורות וחבורות חלקיות שלהן.

(א) $l_{ab} = \varphi(a\cdot b) \stackrel{?}{=} \varphi(a)\circ\varphi(b) = l_a \circ l_b$. $l_{ab}(x) = (ab)x$ ו־$(l_a \circ l_b)(x) = a(bx)$; שוויון מתקיים, מאסוציאטיביות.
(ב) צריך להוכיח כי אם $\varphi(a) = \varphi(b)$ אזי $a = b$: זאת אומרת, אם $l_a = l_b$ אזי $a = b$. נפעילן על e: $a = l_a(e) = l_b(e) = b$.

מההוכחה נובע כי אם G סופית מסדר n, היא ניתנת לשיכון ב־S_n (כלומר, איזומורפית לחבורה חלקית של S_n).

1.6.1 החבורה $S_n = \mathrm{Sym}(n)$

תמורה $\pi \in S_n$ מקובל לסמן כך: $\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$.

דוגמה. עבור $n = 5$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 5 & 2 \end{pmatrix}$ ו־$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 4 & 1 \end{pmatrix}$, נקבל
$\pi\circ\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 1 & 3 \end{pmatrix}$ ו־$\sigma\circ\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}$.

שיטה אחרת לכתוב תמורות היא כתיב מחזורים: בדוגמה לעיל, נקבל $\sigma = (1\ 3\ 4\ 5\ 2)$, $\pi = (1\ 5)(2\ 3)(4) = (1\ 5)(2\ 3)$, $\pi\circ\sigma = (1\ 2\ 5\ 3\ 4)$, $\sigma\circ\pi = (1\ 2\ 4\ 5\ 3)$. מכאן ברור ש־$o(\pi\circ\sigma) = 5$, $o(\pi) = 2$ וכו'. דוגמה נוספת: עבור $\varphi = (1\ 3\ 5)(2\ 4)$, $o(\varphi) = 6$.

הגדרה. $\varphi \in S_n$ נקראת **ציקלוס**[23] מסדר r אם קיימים $Y = \{i_1,\dots,i_r\} \subseteq \{1,\dots,n\}$ ($r \le n$) כך שמתקיים $\varphi(i_1) = i_2, \varphi(i_2) = i_3, \dots, \varphi(i_{r-1}) = i_r, \varphi(i_r) = i_1$ ולכל $j \notin Y$, $\varphi(j) = j$.
הקבוצה $Y = \{i_1,\dots,i_r\}$ נקראת **התומך** של φ.

דוגמה. $\varphi = (1\ 2\ 3) \in S_5$ הוא מחזור מסדר 3. $(3\ 2\ 4)$ גם מסדר 3. σ שהוגדרה קודם הוא ציקלוס מסדר 5, אך π אינו ציקלוס, אלא הרכבה של שני מחזורים.

טענה 24: אם σ ציקלוס מסדר r, אזי $o(\sigma) = r$.

טענה 25: כל תמורה ב־S_n היא מכפלה של ציקלוסים זרים (כלומר, בעלי תומכים זרים).

דוגמה. $n = 10$; את התמורה $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 6 & 2 & 4 & 1 & 7 & 3 & 9 & 10 & 8 \end{pmatrix}$ ניתן לכתוב כ־$\pi = (1\ 5)(2\ 6\ 7\ 3)(8\ 9\ 10)$.

טענה 26: ציקלוסים זרים מתחלפים זה עם זה.

מסקנה 27: אם $\pi = \varphi_1\circ\varphi_2\circ\dots\circ\varphi_l$ כאשר φ_i הם מחזורים זרים, אזי $o(\pi)$ שווה למכנה המשותף של $o(\varphi_i)$, כלומר למספר הטבעי הקטן ביותר המתחלק על־ידי $o(\varphi_i)$ לכל $i = 1,\dots,l$.
(הטענה איננה נכונה עבור מכפלת מעגלים לא־זרים.)

[23] גם **מחזור/מעגל**.

7.11.2007

כל איבר $\pi \in S_n$ ניתן לכתיבה כמכפלת מחזורים זרים:

$$\pi = (a_1\ a_2\ \dots\ a_{r_1})(b_1\ b_2\ \dots\ b_{r_2})\dots$$

כל מעגל ניתן לכתיבה כמכפלת חילופים (לאו דווקא זרים):

$$(a_1\ a_2\ \dots\ a_r) = (a_1\ a_r)(a_1\ a_{r-1})\dots(a_1\ a_2)$$

– מעגל מסדר r הוא, למעשה, מכפלת $r-1$ טרנספוזיציות.

מסקנה 28: כל תמורה ב־S_n ניתנת לכתיבה כמכפלה של לכל היותר n טרנספוזיציות.

הוכחה. כל תמורה π ניתנת לכתיבה כמכפלה של מעגלים באורכים $r_1,\dots,r_l$ כך ש־$\sum r_i \le n$, וכל מעגל באורך r_i ניתן לכתיבה כמכפלה של r_i-1 חילופים. לכן π ניתנת לכתיבה כמכפלה של $\sum_{i=1}^{l}(r_i-1) < n$ חילופים.

בנוסף, כל חילוף $(a\ b)$ ניתן לכתיבה כמכפלת חילופים מהצורה $(i\ \ i+1)$: אם $a<b$,

$$(a\ b) = (a\ a+1)(a+1\ a+2)\dots(b-2\ b-1)(b-1\ b)\dots(a+1\ a+2)(a\ \ a+1)$$

מסקנה 29: כל תמורה π ניתנת לכתיבה כמכפלה של עד $2n^2$ חילופים מהצורה $(i\ \ i+1)$.

הוכחה. כל חילוף כללי $(a\ b)$ הוא מכפלה של עד $2n$ חילופים מהצורה $(i\ \ i+1)$.

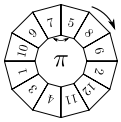
מסקנה 30: הקבוצה $\{(1\ 2),(2\ 3),\dots,(n-1\ n)\}$ יוצרת את S_n.

טענה 31: S_n נוצרת על־ידי שני איברים: $S_n = \langle\sigma,\tau\rangle$ כאשר $\tau = (1\ 2)$, $\sigma = (1\ 2\ \dots\ n)$.

הוכחה. מספיק להוכיח שכל חילוף $(i\ \ i+1)$ ניתן לכתיבה כמילה ב־τ ו־σ (והפכיהם). ואכן, $(i\ \ i+1) = (i+1\ \ i) = \sigma^{i-1}\tau\sigma^{n-(i-1)} = \sigma^{i-1}\tau\sigma^{-(i-1)}$.[24]

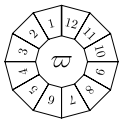
קיבלנו ש־$(i\ \ i+1)$ היא מילה באורך $n+1$ ב־σ ו־τ, ולכן כל איבר ב־S_n ניתן לכתיבה כמילה באורך $O(n^3)$ על־ידי τ ו־σ. למעשה, $O(n^2)$ מספיק: נשים לב שבכתיבת התמורה כ־$(a\ b) = \dots(a+1\ \ a+2)(a\ \ a+1)$ נקבל $\sigma^{a+1}\tau\sigma^{-(a+1)}\cdot\sigma^{a}\tau\sigma^{-a}\cdot\sigma^{a-1}\tau\sigma^{-a+1}$, ויתקבלו צמצומים, כך שבסופו של דבר נקבל שהחילוף $(a\ b)$ הוא למעשה מילה באורך $O(n)$ של σ ו־τ (במקום $O(n^2)$).

דוגמה (Bubblesort). אנו מעוניינים לסדר רצף מספרים לפי סדר עולה באמצעות "מכונה" שיכולה להסתובב ולהחליף בין האיברים שליד הקוטב. נשים לב שפעולות אלה שקולות לכתיבת הפרמוטציה שרשומה על המכונה כמילה ב־σ (סיבוב) ו־τ (החלפה). למשל,



נסתכל על אוסף השלשות (i,j,k): קבוצה כזו תיקרא **רעה** ביחס לתמורה π אם אינה מסודרת בכיוון השעון. נתבונן בתמורה ϖ:

[24] למעשה, $\sigma^{-(i-1)}$ מעביר את i ל־1 ואת $i+1$ ל־2, τ מחליף ביניהם ו־σ^{i-1} "מחזיר" אותם ל־$i+1$ ול־i, בהתאמה.



בתמורה $\varpi = \sigma^{-1}$ כל השלשות רעות. יש $\binom{n}{3} \sim \frac{n^3}{6}$ שלשות כאלו. הסיבוב σ וחזקותיו לא מתקן שלשות כלל, ואילו ההחלפה τ מתקנת לכל היותר n שלשות (אלה שכוללות את שני האיברים שהוחלפו). כלומר, כדי לסדר את ϖ הגרועה הזו, צריך לפחות $\frac{\frac{n^3}{6}}{n} \sim \frac{n^2}{6}$ פעולות: כלומר, היא תיכתב כמילה באורך $O(n^2)$.[25]

זוגיות תמורה

הגדרה. תמורה π נקראת **זוגית** אם היא ניתנת לכתיבה כמכפלת מספר זוגי של חילופים. אחרת, תיקרא **אי־זוגית**.

סימן תמורה

אם π זוגית, נסמן $\operatorname{sgn}\pi = +1$; אחרת, $\operatorname{sgn}\pi = -1$.

טענה 32: יהי f הפולינום ב־n משתנים $x_1, \ldots, x_n$ הנתון על־ידי $f = \prod_{1 \le i < j \le n}(x_i - x_j)$. תהא φ תמורה. נסמן $f^\varphi = \prod_{i<j}(x_{\varphi(i)} - x_{\varphi(j)})$. אזי $f^\varphi = \operatorname{sgn}(\varphi) \cdot f$.

הוכחה. נניח ש־φ מכפלה של מספר זוגי של חילופים. הפעלת φ על f פירושה הפעלת מספר זוגי של חילופים על f.

למה 1.32: כל חילוף משנה את הסימן.

הוכחה. $\varphi = (i\ j)$ כאשר $i < j$. עבור $a < j$ או $a > j$, $x_a - x_i = x_a - x_{\varphi(j)}$ ו־$x_a - x_j = x_a - x_{\varphi(i)}$. עבור $i < b < j$,

$$(x_{\varphi(j)} - x_b)(x_b - x_{\varphi(i)}) = (x_j - x_b)(x_b - x_i) = (x_i - x_b)(x_b - x_j)$$

כל אלה מופיעים בדיוק כך בפולינום $\prod_{i<j}(x_i - x_j)$; המקום היחיד בו ההחלפה איננה מתבטלת הוא $(x_i - x_j)$, שהופך ל־$-(x_i - x_j) = (x_j - x_i)$.

לכן בסך־הכל φ אינה משנה את f. באופן דומה, אם φ מכפלה של מספר אי־זוגי של חילופים, אזי $f^\varphi = -f$. בסך הכל, $f^\varphi = \operatorname{sgn}\varphi \cdot f$.

מסקנה 33: אם φ ניתנת לכתיבה כמכפלה זוגית של חילופים, אזי כל כתיבה שלה כמכפלת חילופים היא מכפלה של מספר זוגי של חילופים; באופן דומה, לגבי תמורה אי־זוגית.

למעשה, φ זוגית אם־ם $|\{(i,j) \mid i < j \wedge \varphi(i) > \varphi(j)\}|$ זוגי. מכאן, שיטה מהירה לבדיקת סימנה של תמורה: בכתיבת תמורה π, מעבירים קו בין i ו־$\pi(i)$; זוגיות התמורה שקולה לזוגיות מספר ההצטלבויות.

שיטה נוספת: נתבונן בכתיב המחזורים של תמורה. נשים לב כי מעגל באורך זוגי הוא תמורה אי־זוגית ומעגל באורך אי־זוגי הוא תמורה זוגית. אז זוגיות התמורה שקולה לזוגיות מספר המעגלים שארכם זוגי בכתיבתה כמכפלת מעגלים.

דוגמה. התמורה $\pi = (1\ 6)(2\ 5)(3\ 7\ 4)$ היא זוגית.

[25] קודם הראינו שניתן לכתוב כל תמורה כמכפלת באורך $O(n^2)$ חילופים; עכשיו מצאנו מילה שלא ניתן לכתוב כמכפלת פחות מ־$O(n^2)$ חילופים. לכן לא ניתן לתת חסם טוב יותר.

1.6.2 יחס הצמידות ב־S_n

הצמדה יהי G חבורה כלשהי; איברים $a, b \in G$ נקראים **צמודים** אם קיים $g \in G$ כך ש־$g^{-1}ag = b$. זהו יחס שקילות; מחלקות השקילות נקראות **מחלקות צמידות**.

טענה 34: תהיינה π ו־π' שתי תמורות ב־S_n. נכתוב אותן כמכפלת מעגלים זרים באורכים יורדים:[26]

$$\begin{aligned}\pi &= (a_1^1\ \dots\ a_{r_1}^1)\dots(a_1^l\ \dots\ a_{r_l}^l)\\ \pi' &= (b_1^1\ \dots\ b_{s_1}^1)\dots(b_1^{l'}\ \dots\ b_{s_{l'}}^{l'})\end{aligned}$$

אזי π ו־π' צמודות אמ"ם $l = l'$ ו־$r_1 = s_1, \dots, r_l = s_{l'}$.

דוגמה. התמורה $\pi = (3\ 4\ 7)(5\ 2)(6\ 1)$ צמודה לתמורות $\pi' = (6\ 2\ 4)(7\ 1)(3\ 5)$ ו־$\pi'' = (7\ 1\ 3)(2\ 5)(1\ 6)$.

הוכחה. תהי $g \in S_n$. הצמדה ב־g שקולה להפעלתה על התכנים:

$$g(a_1^1\ \dots\ a_{r_1}^1)\dots(a_1^l\ \dots\ a_{r_l}^l)g^{-1} = (g(a_1^1)\ \dots\ g(a_{r_1}^1))\dots(g(a_1^l)\ \dots\ g(a_{r_l}^l))$$

לכן לתמורות צמודות אותו מבנה ציקלי, ואם לשתי תמורות אותו מבנה ציקלי, ניתן להגדיר תמורה מצמידה (לאו דווקא באופן יחיד).

12.11.2007 **דוגמה.** $x = (1\ 5\ 7)(2\ 6)(3\ 8)$, $g = (1\ 6\ 7\ 4)(5\ 8)$. אז –

$$\begin{aligned}gxg^{-1} &= (1)(2\ 7)(3\ 5)(4\ 6\ 8)\\ &= (6\ 8\ 4)(2\ 7)(3\ 5)\\ &= (g(1)\ g(5)\ g(7))(g(2)\ g(6))(g(3)\ g(8))\end{aligned}$$

פונקציית החלוקה **פונקציית החלוקה** היא הפונקציה $\sigma : \mathbb{N} \to \mathbb{N}$ כך ש־$\sigma(n)$ הוא מספר האפשרויות לכתוב את n כסכום מספרים טבעיים חיוביים בסדר יורד.[27]

דוגמה.
$\sigma(1) = 1$
$\sigma(2) = 2$ (שכן $2 = 2, 2 = 1 + 1$)
$\sigma(3) = 3$ ($3 = 3 = 2 + 1 = 1 + 1 + 1$)
$\sigma(4) = 5$ ($4 = 4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$)

מסקנה 35: מספר מחלקות הצמידות ב־S_n הוא $\sigma(n)$.

הוכחה. המבנה הציקלי הוא הקובע את מחלקות הצמידות; מספר האפשרויות למבנים ציקליים הוא $\sigma(n)$.

1.7 אוטומורפיזמים ואוטומורפיזמים פנימיים

אוטומורפיזם **הגדרה.** תהא G חבורה. הומומורפיזם מ־G ל־G שהוא חח"ע ועל ייקרא **אוטומורפיזם**.

[26] ניתן לעשות זאת, שכן מעגלים זרים מתחלפים.
[27] $\sigma(n) \sim e^{\sqrt{n}}$.

טענה 36: אוסף האוטומורפיזמים של G מהווה חבורה ביחס לפעולת ההרכבה; חבורה זו תסומן $\mathrm{Aut}(G)$.[28]

הוכחה. איבר יחידה: id.

קשירות: הרכבת שני הומומורפיזמים היא הומומורפיזם, והרכבת פונקציות חח"ע ועל היא חח"ע ועל.

קיום הפכי: הפונקציה ההפכית היא חח"ע ועל; יש לבדוק שהיא גם הומומורפיזם. יהי $\alpha : G \to G$ אוטומורפיזם. $\alpha^{-1} : G \to G$ מוגדר על־ידי $\alpha^{-1}(x) = y$ אם $\alpha(y) = x$. יש להראות כי $\alpha^{-1}(x_1x_2) = \alpha^{-1}(x_1)\alpha^{-1}(x_2)$. נסמן $\alpha^{-1}(x_1) = y_1$, $\alpha^{-1}(x_2) = y_2$. אז מתקיים $\alpha(y_1) = x_1$ ו־$\alpha(y_2) = x_2$, ולכן $\alpha(y_1y_2) = \alpha(y_1)\alpha(y_2) = x_1x_2$. לכן נקבל $\alpha^{-1}(x_1x_2) = y_1y_2 = \alpha^{-1}(x_1)\alpha^{-1}(x_2)$, ו־$\alpha^{-1}$ הומומורפיזם. קיבלנו שההפכי גם הוא אוטומורפיזם.

1.7.1 האוטומורפיזמים הפנימיים

תהא G חבורה, ויהי $g \in G$. נגדיר $i_g : G \to G$ על־ידי $i_g(x) = gxg^{-1}$ ($x \in G$).

טענה 37: i_g אוטומורפיזם של G.

הוכחה. i_g הומומורפיזם כי $i_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = i_g(x) \cdot i_g(y)$.

i_g חח"ע: נניח $i_g(x) = i_g(y)$, כלומר $gxg^{-1} = gyg^1 \Longleftarrow x = y$

i_g על: $i_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = x$

טענה 38: ההעתקה $i : G \to \mathrm{Aut}(G)$ המוגדרת על־ידי $i(g) = i_g$ היא הומומורפיזם.

הוכחה. צ"ל $i(g_1g_2) = i(g_1) \circ i(g_2)$. כדי להוכיח זאת, נראה שפועלים באותו אופן על כל x ב־G:

$$\begin{aligned} i(g_1g_2)(x) &\stackrel{?}{=} (i(g_1) \circ i(g_2))(x) \\ i_{g_1g_2}(x) &\stackrel{?}{=} i_{g_1} \circ i_{g_2}(x) \\ (g_1g_2)x(g_1g_2)^{-1} &\stackrel{?}{=} i_{g_1}(g_2xg_2^{-1}) \\ (g_1g_2)x(g_2^{-1}g_1^{-1}) &\stackrel{!}{=} g_1(g_2xg_2^{-1})g_1^{-1} \end{aligned}$$

מסקנה 39: אוסף האוטומורפיזמים הפנימיים של חבורה G מהווה חבורה חלקית של $\mathrm{Aut}(G)$.

הוכחה. זו בדיוק התמונה של ההומומורפיזם i.

טענה 40: $\ker i = Z(G)$, כאשר $Z(G)$, או **המרכז** (centre) של G, הוא אוסף איברי G המתחלפים עם כל איברי G.

בחבורה אבלית, כל אוטומורפיזם פנימי הוא הזהות.

[28] זו תת־חבורה של $\mathrm{Per}(G)$.

1.8 חבורות חלקיות נורמליות וחבורות מנה

חבורה חלקית נורמלית

הגדרה. חבורה חלקית H של G נקראת **נורמלית** ($H \trianglelefteq G$) אם לכל $g \in G$, $gHg^{-1} = H$.[29]

טענה 41: G חבורה, H חבורה חלקית. אזי התנאים הבאים שקולים:

א. $H \lhd G$;

ב. לכל $g \in G$, $gH = Hg$;

ג. כל מחלקה שמאלית היא מחלקה ימנית.

הוכחה. ((א) $\Leftarrow$ (ב)) $gHg^{-1} = H$ ולכן $gH = Hg$, וגמרנו.

((ב) $\Leftarrow$ (א)) $gH = Hg$; נכפול את שתי הקבוצות ב־g^{-1} (משמאל) ונקבל $gHg^{-1} = H$.

((ב) $\Leftarrow$ (ג)) ברור.

((ג) $\Leftarrow$ (ב)) אם gH מחלקה שמאלית, אנו יודעים שהיא גם מחלקה ימנית. כלומר, $gH = Hg'$ לאיזשהו $g' \in G$. אבל זה אומר ש־$g \in g \cdot e \in Hg'$, כלומר g ו־g' באותה מחלקת שקילות של מחלקות ימניות,ולכן $Hg = Hg'$.

חבורת מנה

הגדרה. תהא G חבורה ו־$N \trianglelefteq G$ תת־חבורה נורמלית. **חבורת המנה** G/N מוגדרת כך: איבריה הם המחלקות השמאליות[30] של N ב־G; הכפל מוגדר על־ידי $(g_1N) \cdot (g_2N) = g_1g_2N$ (כאשר $g_1, g_2 \in G$).

זו אכן חבורה: איבר היחידה הוא $eN = N$, שהרי $(g_1N)(eN) = (g_1e)N = g_1N$, ו־$(gN)^{-1} = g^{-1}N$, כי $(eN)(g_1N) = (eg_1)N = g_1N$; איבר הפכי מוגדר על־ידי $(gN)(g^{-1}N) = (gg^{-1})N = eN$ (וכן משמאל); אסוציאטיביות מתקיימת מקיומה ב־G:

$$\begin{aligned}[(g_1N)(g_2N)](g_3N) &\stackrel{?}{=} (g_1N)[(g_2N)(g_3N)] \\ (g_1g_2N)(g_3N) &\stackrel{?}{=} (g_1N)(g_2g_3N) \\ (g_1g_2)g_3N &\stackrel{!}{=} g_1(g_2g_3)N\end{aligned}$$

כמו כן, הכפל מוגדר היטב: אם $g_1N = x_1N$ ו־$g_2N = x_2N$, צ"ל $g_1g_2N \stackrel{?}{=} x_1x_2N$, כלומר $g_1g_2(x_1x_2)^{-1} \in N$. אבל $g_2N = x_2N$, ולכן מתקיים $g_2x_2^{-1} = n' \in N$. אם כן, $g_1g_2(x_1x_2)^{-1} = g_1g_2x_2^{-1}x_1^{-1} = g_1n'x_1^{-1} = (g_1n'g_1^{-1})(g_1x_1^{-1}) \in N$, מכיוון ש־$N$ נורמלית (ולכן $g_1n'g_1^{-1} \in N$) ו־$g_1N = x_1N$ (ולכן $g_1x_1^{-1} \in N$).

דוגמה. $G = \mathbb{Z}, N = m\mathbb{Z}$. אז $G/N = \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$.

14.11.2007

טענה 42: $N \leq G$ חבורה חלקית. אזי התנאים הבאים שקולים:

א. $N \lhd G$ (דהיינו, לכל $g \in G$, $g^{-1}Ng = N$);

ב. לכל $g \in G$, $gNg^{-1} \subseteq N$;

[29] כלומר, H נורמלית אם היא, כקבוצה, נשמרת במקום על־ידי כל אוטומורפיזם פנימי. (לא כל איברי H בהכרח נשמרים.) בחבורה אבלית, כל חבורה חלקית היא נורמלית, שכן כל האוטומורפיזמים הפנימיים הם העתקת הזהות.

[30] או הימניות; זה לא משנה, שהרי N נורמלית.

ג. לכל $g \in G$ ולכל $n \in N$, $g^{-1}ng \in N$.

הוכחה. ((א) $\Leftarrow$ (ב) $\Leftarrow$ (ג)) טריוויאלי.

((ג) $\Leftarrow$ (א)) ברור ש־(ג) גורר שלכל $g \in G$, $g^{-1}Ng \subseteq N$; עלינו להראות שמתקיים שוויון, כלומר לכל $n \in N$ קיים $n_0 \in N$ כך ש־$g^{-1}n_0g = n$. ואכן, נבחר $n_0 = gng^{-1}$; אז $n_0 \in N$ על־פי (ג), כי $n_0 = gng^{-1} = (g^{-1})^{-1}ng^{-1} \in N$, ואז $g^{-1}n_0g = g^{-1}(gng^{-1})g = n$ וגמרנו.

נעיר שייתכן מצב ש־H חבורה חלקית ו־$g \in G$ כך ש־$g^{-1}Hg \subsetneq H$, אך לא ייתכן שזה קורה לכל $g \in G$.

דוגמה. F שדה, $G = GL_n(F)$, $N = SL_n(F)$[31]. אזי $N \lhd G$: עבור $n \in N$, $g \in G$, נקבל $\det(g^{-1}ng) = \det(g^{-1})\det(n)\det(g) = \det(g)^{-1} \cdot 1 \cdot \det(g) = 1$, ולכן $g^{-1}ng \in N$.

דוגמה. $G = S_n$, $N = A_n$[32].

$((a_1\ b_1)\dots(a_l\ b_l))^{-1} = (a_l\ b_l)^{-1}\dots(a_1\ b_1)^{-1} = (a_l\ b_l)\dots(a_1\ b_1)$ ולכן $g \in S_n$ זוגית אם"ם g^{-1} זוגית. לכן אם n זוגית ו־g תמורה כלשהי, אם g מכפלה של l חילופים ו־n מכפלה של $2m$ חילופים, אזי $g^{-1}ng$ מכפלה של $l + 2m + l = 2l + 2m$ חילופים ולכן זוגית וב־N.

טענה 43: G חבורה, $\varphi : G \to M$ הומומורפיזם. נסמן $N = \ker\varphi$. אזי $N \lhd G$.

הוכחה. יהיו $n \in N$ ו־$g \in G$. צריך להוכיח $g^{-1}ng \in N$, כלומר $\varphi(g^{-1}ng) = e_M$. ואכן, $\varphi(g^{-1}ng) = \varphi(g^{-1})\varphi(n)\varphi(g) = \varphi(g)^{-1}e_M\varphi(g) = e_M$.

דוגמה. כדי להראות $A_n \lhd S_n$, יכולנו לומר ש־$\mathrm{sgn} : S_n \to \{\pm 1\}$ הומומורפיזם, ואז $A_n = \ker(\mathrm{sgn})$.

הטענה נכונה גם בכיוון ההפוך:

טענה 44: לכל חבורה חלקית נורמלית N של G קיימת חבורה M ואפימורפיזם $\varphi : G \to M$ כך ש־$N = \ker\varphi$.

הוכחה. תהא $M = G/N$. זאת אומרת, איברי M הם המחלקות השמאליות של N ב־G. ראינו שאוסף המחלקות מהווה חבורה ביחס להגדרת הכפל $g_1N \cdot g_2N = g_1g_2N$. נגדיר העתקה $\varphi : G \to G/N$ על־ידי $\varphi(g) = gN$. זהו הומומורפיזם, כי אם $g_1, g_2 \in G$, $(g_1N)(g_2N) = \varphi(g_1)\varphi(g_2) \overset{?}{=} \varphi(g_1g_2) = (g_1g_2)N$. כמו כן, $e_{G/N} = eN = N$ ולכן $\ker\varphi = \{g \in G \mid gN = N\} = \{g \in G \mid g \in N\} = N$, כנדרש.

[31] $SL_n(F) = \{A \in GL_n(F) \mid \det A = 1\}$.

[32] A_n היא חבורת התמורות הזוגיות על $\{1, \dots, n\}$.

1.9 משפטי ההומומורפיזם

משפט 45 (ההומומורפיזם הראשון): תהיינה G ו־M חבורות, $\varphi : G \to M$ הומומורפיזם. נסמן $\bar{G} = \operatorname{Im}\varphi$. אזי $\bar{G} \cong G/\ker\varphi$.

הוכחה. יש לנו אפימורפיזם $\varphi : G \to \bar{G}$. נגדיר העתקה $\bar{\varphi} : G/N \to \bar{G}$ (כאשר $N = \ker\varphi$) ונראה שהיא איזומורפיזם.

לכל $g \in G$, נגדיר $\bar{\varphi}(gN) = \varphi(g)$. יש לבדוק ש־$\bar{\varphi}$ אינה תלויה בנציג: אם $gN = g'N$, $g' = gn$ ל־$n \in N$ כלשהו ונקבל $\varphi(g') = \varphi(gn) = \varphi(g)\varphi(n) = \varphi(g)e_{\bar{G}} = \varphi(g)$.

$\bar{\varphi}$ הומומורפיזם:

$$\begin{aligned} \bar{\varphi}((g_1N)(g_2N)) &\overset{?}{=} \bar{\varphi}(g_1N)\cdot\bar{\varphi}(g_2N) \\ \bar{\varphi}(g_1g_2N) &\overset{?}{=} \varphi(g_1)\varphi(g_2) \\ \varphi(g_1g_2) &\overset{!}{=} \varphi(g_1)\varphi(g_2) \end{aligned}$$

$\bar{\varphi}$ על: צריך להראות שלכל $h \in \bar{G}$ קיים $gN \in G/N$ כך ש־$\bar{\varphi}(gN) = h$. ידוע שקיים $g \in G$ כך ש־$\varphi(g) = h$ (כי φ על $\bar{G}$), ואז $\bar{\varphi}(gN) = \varphi(g) = h$.

$\bar{\varphi}$ חח״ע: ניעזר **בלמה:** אם $\psi : G \to H$ הומומורפיזם, אזי ψ חח״ע אם״ם $\ker\psi = \{e_G\}$. כלומר, עלינו להוכיח שאם $\bar{\varphi}(gN) = e_{\bar{G}}$ אזי $gN = N$. ואכן, אם $\varphi(g) = \bar{\varphi}(gN) = e_{\bar{G}}$, מתקיים $g \in \ker\varphi = N$, כלומר $gN = eN = N$ ולכן $g \in N$.

דוגמה. F שדה, $G = GL_n(F)$. אזי $\det : GL_n(F) \to F^*$ הומומורפיזם מ־$GL_n(F)$ ל־$F^* = F \setminus \{0\}$, שהיא חבורה ביחס לפעולת הכפל. הגרעין הוא $SL_n(F)$. התמונה היא F^*, כי אם $a \in F^*$, הדטרמיננטה של המטריצה שעל אלכסונה פעם אחת a והשאר 1 היא a. מכאן, $GL_n(F)/SL_n(F) \cong F^*$.

דוגמה. $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $\varphi(x) = x \pmod n$. אז $\ker\varphi = n\mathbb{Z}$, ומכאן $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

דוגמה. $f : \mathbb{R}_+ \to S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, $f(x) = e^{2\pi ix}$. זהו הומומורפיזם כי $f(x+y) = e^{2\pi i(x+y)} = e^{2\pi ix}e^{2\pi iy} = f(x)f(y)$. $\ker f = \mathbb{Z}$, ומכאן $\mathbb{R}/\mathbb{Z} \cong S^1$.

דוגמה. $\operatorname{sgn} : S_n \to \{\pm 1\}$, $\ker\operatorname{sgn} = A_n$; לכן $S_n/A_n \cong \{\pm 1\} \cong \mathbb{Z}_2$.

למה 46: אם G חבורה, $N \lhd G$ ו־$H \leq G$, אזי $HN = NH$[33] חבורה חלקית של G. 19.11.2007

הוכחה. אם $h \in H$, $n \in N$, $hn = hnh^{-1}h = n'h$ (מנורמליות N) ולכן $HN \subseteq NH$. בכיוון השני, $nh = hh^{-1}nh = hn''$ ולכן $NH \subseteq HN$. לכן מתקיים שוויון.

HN היא חבורה חלקית: יהיו $h_1, h_2 \in H$, $n_1, n_2 \in N$. נעיר כי מנורמליות N, $h_2^{-1}n_1h_2 = n_0$. אז $(h_1n_1)(h_2n_2) = h_1h_2(h_2^{-1}n_1h_2)n_2 = h_1h_2n_0n_2 \in HN$. בנוסף, $(hn)^{-1} = n^{-1}h^{-1} \in NH = HN$.

[33] מגדירים $HN = \{hn \mid h \in H, n \in N\}$.

נעיר גם כי HN מכילה את N ואת H (שכן $e \in N \cap H$) וכי $N \lhd HN$. לכן אפשר לדבר על HN/N.

משפט 47 (ההומומורפיזם השני): G חבורה, $N \lhd G$, $H \leq G$. אזי $HN/N \cong H/H \cap N$. (זאת אומרת, $H \cap N \lhd H$ ומתקיים האיזומורפיזם.)

הוכחה. נגדיר הומומורפיזם $\varphi : H \to HN/N (\leq G/N)$ על־ידי $\varphi(h) = hN$.[34] φ הוא על, כי אם $gN \in HN/N$ אזי g ניתן לכתיבה כ־$g = h_1 n_1$ ואז $gN = h_1 n_1 N = h_1 N$ ולכן $\varphi(h_1) = h_1 N = gN$.[35]

בנוסף, $\ker \varphi = \{h \in H \mid \varphi(h) = e_{HN/N} \Leftrightarrow hN = N \Leftrightarrow h \in N\} = H \cap N$.

לכן לפי משפט ההומומורפיזם הראשון, $HN/N \cong H/H \cap N$.

משפט 48 (ההתאמה): G חבורה, $N \lhd G$. אזי ההומומורפיזם הטבעי $\pi : G \to G/N$[36] משרה התאמה חח״ע ועל $\bar{\pi}$ בין הקבוצות $\{L \mid N \leq L \leq G\}$ לבין $\{M \mid M \leq G/N\}$, הניתנת על־ידי $L \mapsto \pi L$, $M \mapsto \{g \in G \mid \pi(g) \in M\} = \pi^{-1}(M)$.

הוכחה. ברור שאם L חבורה חלקית של G המכילה את N אזי $\pi(L)$ חבורה חלקית של G/N. כמו כן, $\pi^{-1}(M)$ גם היא חבורה חלקית:

למה 1.48: אם $\varphi : G \to S$ הומומורפיזם ו־$T \leq S$, אזי $\varphi^{-1}(T)$ חבורה חלקית של G המכילה את $\ker \varphi$.

הוכחה. $g_1, g_2 \in \varphi^{-1}(T)$; אזי $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1)(\varphi(g_2))^{-1} \in T$. לכן $g_1 g_2^{-1} \in \varphi^{-1}(T)$.

$\bar{\pi}$ על: תהא M חבורה חלקית של G/N. נסמן $L = \pi^{-1}(M)$ ונראה $\pi(L) = M$. אך זה ברור, כי $\pi(L) = \pi(\pi^{-1}(M)) \leq M$, ומתקיים שוויון כי לכל $m \in M$ יש $g \in G$ כך ש־$\pi(g) = m$ (שהרי π על), ו־$g \in \pi^{-1}(M)$ מהגדרה.

$\bar{\pi}$ חח״ע: יהיו L_1 ו־L_2 שתי חבורות חלקיות של G המכילות את N כך ש־$\pi(L_1) = \pi(L_2)$. נראה ש־$L_1 \subseteq L_2$, ומסימטרייה ינבע גם ההיפך. יהי $l_1 \in L_1$. אזי קיים $l_2 \in L_2$ כך ש־$\pi(l_1) = \pi(l_2)$, כלומר $l_1 N = l_2 N$; לכן קיים $n \in N$ כך ש־$l_1 = l_2 n$. אבל $N \subseteq L_2$ ולכן $l_2 n \in L_2$, כלומר $l_1 \in L_2$.

משפט 49 (ההומומורפיזם השלישי): G חבורה, N ו־K חבורות חלקיות נורמליות של G כך ש־$N \subseteq K$. אזי $K/N \lhd G/N$ וכן $G/K \cong (G/N)/(K/N)$.

הוכחה. נבדוק קודם ש־$K/N \lhd G/N$: יהיו $gN \in G/N$, $kN \in K/N$. אז מתקיים $(gN)(kN)(gN)^{-1} = (gN)(kN)(g^{-1}N) = (gkg^{-1})N = k'N \in K/N$.

[34] זהו הומומורפיזם כי $\varphi(h_1 h_2) = (h_1 h_2)N = (h_1 N)(h_2 N) = \varphi(h_1)\varphi(h_2)$.

[35] למעשה אמרנו שלכל מחלקה של N יש נציג מ־H.

[36] זהו ההומומורפיזם $g \overset{\pi}{\mapsto} gN$.

נגדיר הומומורפיזם $\psi : G/N \to G/K$ על־ידי $\psi(gN) = gK$. ψ מוגדרת היטב, כי אם $g_1N = g_2N$ אזי $g_1 = g_2n$ ($n \in N \subseteq K$) ולכן $g_1K = g_2nK = g_2K$. לכן $\psi(g_1N) = \psi(g_2N)$. בנוסף, ψ היא על כי אם $gK \in G/K$ אזי $\psi(gN) = gK$.

$$\ker\psi = \{gN \mid \psi(gN) = gK = eK\} = \{gN \mid g \in K\} = K/N.$$

בסך הכל, ψ אפימורפיזם מ־G/N ל־G/K שגרעינו K/N, ולכן הדרוש מתקבל לפי משפט ההומומורפיזם הראשון.

1.10 סדרות נורמליות

21.11.2007

למה 50 (זאסנהאוס): G חבורה, $B \lhd B^*$, $A \lhd A^*$ ארבע חבורות חלקיות של G. אזי מתקיים $A(A^* \cap B) \lhd A(A^* \cap B^*)$ ו־$B(B^* \cap A) \lhd B(B^* \cap A^*)$, וכן מתקיים האיזומורפיזם $A(A^* \cap B^*)/A(A^* \cap B) \cong B(B^* \cap A^*)/B(B^* \cap A)$.

למה 1.50: א. אם $B \lhd B^*$, A שלוש חבורות חלקיות של G, אזי $A \cap B \lhd A \cap B^*$.

ב. אם N ו־K חבורות חלקיות נורמליות של G, אזי KN נורמלית.

הוכחה. א. יהיו $g \in A \cap B^*$ ו־$n \in A \cap B$. יש להראות $g^{-1}ng \in A \cap B$. מאחר ש־$n \in B$, $g \in B^*$ ו־$B \lhd B^*$, הרי $g^{-1}ng \in B$. מצד שני, $g \in A$ ו־$n \in A$ ולכן $g^{-1}ng \in A$. אז $g^{-1}ng \in A \cap B$.

ב. כתרגיל.

הוכחה. לפי (א) בלמה, $A \cap B^* \lhd A^* \cap B^*$, ובאופן דומה, $A^* \cap B \lhd A^* \cap B^*$. לפי (ב), $D = (A^* \cap B)(A \cap B^*) \lhd A^* \cap B^*$.

נגדיר $f : B(B^* \cap A^*) \to A^* \cap B^*/D$ לכל $x = bc \in B(B^* \cap A^*)$ (כאשר $b \in B$, $c \in B^* \cap A^*$[37]) על־ידי $f(x) = f(bc) = cD$.

למה 2.50: א. f מוגדרת היטב;

ב. f על;

ג. f הומומורפיזם;

ד. $\ker f = B(B^* \cap A)$.

הוכחה. א. נניח כי $x = bc = b'c'$ עבור $b, b' \in B$ ו־$c, c' \in B^* \cap A^*$. אזי מתקיים $c'c^{-1} \in B \cap (B^* \cap A^*) = B \cap A^* \leq B^* \cap A^* \ni c'c^{-1} = b'^{-1}b \in B$, ומכאן $c'D = cD$.

ב. אם $y \in A^* \cap B^*$ אזי $x = ey \in B(B^* \cap A^*)$ ו־$f(x) = yD$.

ג. יהיו $x = bc$, $b, b_1 \in B$ (עבור $y = b_1c_1 \in A^* \cap B^*$, c, c_1). אז

$$f(x)f(y) = (cD)(c_1D) = cc_1D = f((bcb_1c^{-1})cc_1) = f(bcb_1c_1) = f(xy)$$

(שהרי $b(cb_1c^{-1}) \in B$, כי $B \lhd B^*$ ו־$c \in B^* \cap A^* \leq B^*$.)

[37] $B(B^* \cap A^*)$ היא חבורה חלקית (מכפלת חבורה חלקית בחבורה חלקית נורמלית).

ד. $$\begin{aligned}\ker f &= \{x \in B(B^* \cap A^*) \mid f(x) = e_{A^* \cap B^*/D}\} \\ &= \{x = bc \mid cD = D\} \\ &= \{x = bc \mid c \in D\} \\ &= BD = B(A^* \cap B)(A \cap B^*) = B(B^* \cap A) \end{aligned}$$
($B(A^* \cap B) = B$ כי $A^* \cap B \leq B$).

לפי הלמה ומשפט ההומומורפיזם הראשון, $B(B^* \cap A^*)/B(B^* \cap A) \cong A^* \cap B^*/D$. מסימטרייה, החבורה שבאגף ימין איזומורפית גם ל־$A(A^* \cap B^*)/A(A^* \cap B)$, וגמרנו.

1.10.1 סדרות נורמליות

סדרה נורמלית

הגדרה. תהא G חבורה; סדרת חבורות חלקיות $G = G_0 \geq G_1 \geq \ldots \geq G_l = \{e\}$ תיקרא **סדרה נורמלית** אם לכל $i = 0, \ldots, l-1$, $G_i \rhd G_{i+1}$.

עידון של סדרה

הגדרה. אם $G = G_0 \geq \ldots \geq G_l = \{0\}$, $G = H_0 \geq \ldots \geq H_m = \{0\}$ סדרות נורמליות ב־G, נאמר שהשנייה היא **עידון** של השנייה אם $\{G_0, \ldots, G_l\} \subseteq \{H_0, \ldots, H_m\}$.

דוגמה. הסדרות $\mathbb{Z}_{10} - \{0, 2, 4, 6, 8\} - \{0\}$ ו־$\mathbb{Z}_{10} - \{0, 5\} - \{0\}$ אינן עידון אחת של השנייה. (טכנית, תמיד אפשר לעדן (על־ידי הוספת חבורה שכבר מופיעה בסדרה, למשל); מעשית, כאן אי־אפשר.)

שקילות סדרות נורמליות

הגדרה. שתי סדרות נורמליות $\{G_i\}_{i=0}^{l}$ ו־$\{H_j\}_{j=0}^{m}$ תיקראנה **שקולות** אם $m = l$ וקיימת תמורה $\alpha : \{0, \ldots, n-1\} \to \{0, \ldots, n-1\}$ כך ש־$G_i/G_{i+1} \cong H_{\alpha(j)}/H_{\alpha(j)+1}$.

משפט 51 (העידון של שרייר): תהא G חבורה, $\{G_i\}_{i=0}^{l}$ ו־$\{H_j\}_{j=0}^{m}$ סדרות נורמליות ב־G. אזי יש להן עידונים שקולים.

הוכחה. נגדיר $G_{ij} = G_{i+1}(G_i \cap H_j)$ עבור $i = 0, \ldots, l-1$, $j = 0, \ldots, m-1$. אם נסמן $G_{i+1} = A$, $G_i = A^*$, $H_j = B$, $H_{j-1} = B^*$, נקבל, לפי הלמה של זאסנהאוס, $G_{ij} = A(A^* \cap B) \lhd A(A^* \cap B^*) = G_{i+1}(G_i \cap H_{j-1}) = G_{i,j-1}$, $j = 1, \ldots, m-1$ ל־j כלומר $G_{ij} \lhd G_{i,j-1}$, וכן עבור $j = 0$, $G_{i,0} = G_i = G_{i+1}(G_i \cap H_0)$. קיבלנו עידון

$$G_0 = G_{0,0} \geq G_{0,1} \geq \ldots \geq G_{0,m-1} \geq G_{1,0} = G_1 \geq \ldots \geq G_{1,m-1} \geq G_{2,0} \geq \ldots$$

באופן דומה, נעדן את הסדרה H_j על־ידי $H_{ij} = H_{j+1}(H_j \cap G_i)$. מתקיים $H_{0,j} = H_j$ ו־$H_{j+1} \leq H_{ij} \leq H_j$. קיבלנו עידון

$$H_0 = H_{0,0} \geq H_{1,0} \geq \ldots \geq H_{l-1,0} \geq H_{0,1} = H_1 \geq \ldots$$

נוסיף $\{e\}$ בשתי הסדרות בסוף.

אלה שני עידונים של הסדרות מאורך $lm+1 = ml+1$. נותר להוכיח שמתקיים $G_{i,j}/G_{i,j+1} \cong H_{i,j}/H_{i+1,j}$ (לא בהכרח לפי הסדר). כלומר, יש להוכיח כי

$$G_{i+1}(G_i \cap H_j)/G_{i+1}(G_i \cap H_{j+1}) \cong H_{j+1}(H_j \cap G_i)/H_{j+1}(H_j \cap G_{i+1})$$

ואכן, אם נסמן $A = G_{i+1}$, $A^* = G_i$, $B = H_{j+1}$, $B^* = H_j$, נקבל זאת מהלמה של זאסנהאוס.

1.10.2 סדרות הרכב

חבורה פשוטה **הגדרה.** חבורה G נקראת **פשוטה** אם החבורות החלקיות הנורמליות היחידות שלה הן $\{e\}$ ו־G. 26.11.2007

סדרת הרכב **הגדרה.** סדרה נורמלית $G = G_0 \geq \ldots \geq G_n = \{e\}$ נקראת **סדרת הרכב** אם לכל $i = 0, \ldots, n-1$, G_i/G_{i+1} חבורה פשוטה.

סדרת הרכב נקראת גם **סדרת ג׳ורדן־הולדר**. החבורות המופיעות כמנות בסדרת הרכב נקראות **גורמי הרכב** (או **גורמי ג׳ורדן־הולדר**) של החבורה.

כזכור, משפט ההתאמה נותן התאמה חח״ע ועל בין החבורות החלקיות של חבורה A המכילות חבורה חלקית נורמלית N לבין החבורות החלקיות של A/N, והתאמה זו מעבירה חבורות חלקיות נורמליות ב־A לחבורות חלקיות נורמליות ב־A/N. נפעילו על $A = G_i$ ו־$N = G_{i+1}$ ונסיק ש־G_i/G_{i+1} פשוטה אם״ם G_{i+1} חבורה חלקית־ממש נורמלית מקסימלית ב־G_i.[38]

משפט 52 (ג׳ורדן־הולדר): כל שתי סדרות הרכב ב־G הן שקולות. (בפרט, יש להן אותו אורך.)

הוכחה. על־פי משפט העידון של שרייר, יש לשתי הסדרות עידונים שקולים. עידונים שכאלה יכולים להיות רק חזרה על חבורות חלקיות בסדרה שכבר מופיעות. התאמה בין עידונים אלו מעבירה חבורות מנה לא־טריוויאליות ללא־טריוויאליות (וטריוויאליות לטריוויאליות), לכן הסדרות שקולות גם קודם לכן.

טענה 53: בחבורה סופית יש סדרת הרכב.[39]

הוכחה. באינדוקציה על הסדר של G. נניח שנכון לכל החבורות הקטנות מ־G. אם G פשוטה, אזי $G \geq \{e\}$ סדרת הרכב. אם G לא פשוטה, יש ב־G חבורה חלקית נורמלית מקסימלית (וזאת בגלל הסופיות); נקרא לה G_1. $G \geq G_1$ ו־G/G_1 פשוטה לא־טריוויאלית. כמו־כן, הסדר של G_1 קטן ממש מהסדר של G, לכן לפי הנחת האינדוקציה יש ב־G_1 סדרת הרכב, וגמרנו.

1.10.3 חבורות פתירות

חבורה פתירה **הגדרה.** חבורה G נקראת **פתירה** אם יש לה סדרה נורמלית $G = G_0 \geq \ldots \geq G_n = \{e\}$ עם G_i/G_{i+1} אבלית לכל $i = 0, \ldots, n-1$. 28.11.2007

[38] חבורה חלקית נורמלית B של A תיקרא **מקסימלית נורמלית** אם $B \subseteq C \lhd A$ אזי $C = B$ או $C = A$. (לא מדובר בחבורה הנורמלית ״הכי גדולה״, אלא בחבורה נורמלית ש״אין גדולה ממנה״ המכילה אותה.)

[39] לא בהכרח נכון בחבורה אינסופית.

נסמן $G' = G^{(1)} = [G,G] = \langle g^{-1}h^{-1}gh \mid g,h \in G \rangle$.

טענה 54: $G/[G,G]$ אבלית, ו־$[G,G]$ היא החבורה החלקית הנורמלית N הקטנה ביותר של G כך ש־G/N אבלית.

נגדיר באינדוקציה $G^{(0)} = G$, $G^{(1)} = [G,G]$, $G^{(i+1)} = [G^{(i)}, G^{(i)}]$.

טענה 55: חבורה G היא פתירה אם"ם קיים $n \in \mathbb{N}$ כך ש־$G^{(n)} = \{e\}$.

טענה 56: חבורה סופית G היא פתירה אם"ם כל גורם הרכב שלה הוא חבורה ציקלית מסדר ראשוני.

למה 1.56: חבורה אבלית פשוטה היא ציקלית מסדר ראשוני.

1.11 חבורות פשוטות

26.11.2007

דוגמה. $\mathbb{Z}_p$ עבור p ראשוני הן חבורות פשוטות. (למעשה, מבין האבליות הסופיות, אלו הפשוטות היחידות.)

משפט 57: החבורות האלטרנטיביות A_n (חבורות התמורות הזוגיות על קבוצה בת n עצמים) הן פשוטות לכל $n \geq 5$.[40]

למה 1.57: החבורה A_n נוצרת על־ידי אוסף הציקלוסים מסדר 3.

הוכחה. כזכור, הוכחנו ש־S_n נוצרת על־ידי ציקלוסים מסדר 2. התמורות הזוגיות הן אותן תמורות שנכתבות כמכפלת מספר זוגי של חילופים. מכאן, A_n נוצרת על־ידי כל התמורות מהצורה $(x\ y)(z\ w)$. לכן מספיק להראות שכל תמורה מהצורה $(x\ y)(z\ w)$ היא מכפלת שלשות: אם $z = x$ ו־$w = y$, $(x\ y)(x\ y) = e$. אם $z = y$, נקבל $(x\ y)(y\ w) = (x\ y\ w)$. אחרת, $(x\ y)(z\ w) = (x\ y)(y\ z)(y\ z)(z\ w) = (x\ y\ z)(y\ z\ w)$.

למה 2.57: A_5 פשוטה. (כתרגיל.)

למה 3.57: לכל $n \geq 5$, השלשות ב־A_n צמודות זו לזו.

הוכחה. יש להראות ש־$(x\ y\ z)$ צמוד ל־$(a\ b\ c)$ ב־A_n. אנו יודעים שקיים $g \in S_n$ כך ש־$g(x\ y\ z)g^{-1} = (a\ b\ c)$. אם $g \in A_n$, גמרנו. אחרת, ניקח $u \neq v$ שונים מ־x, y, z (יש כאלה, כי $n \geq 5$). אז $(u\ v)$ מתחלף עם $(x\ y\ z)$, ונקבל

$$\begin{aligned}((u\ v)g)^{-1}(x\ y\ z)((u\ v)g)) &= g^{-1}(u\ v)^{-1}(x\ y\ z)(u\ v)g \\ &= g^{-1}(u\ v)^{-1}(u\ v)(x\ y\ z)g \\ &= (a\ b\ c)\end{aligned}$$

ו־$(u\ v)g \in A_n$.

[40] זה נכון גם עבור $n = 1, 2, 3$.

הוכחה. אנו רוצים להוכיח שאם $K \lhd A_n$ ($n \geq 5$) ו־$K \neq \{e\}$ אזי $K = A_n$. מספיק שנוכיח ש־K מכילה ציקלוס אחד באורך 3, כי אז מנורמליות ינבע שמכילה את כל הציקלוסים מאורך 3, ומכיוון שאוסף זה יוצר את A_n, נקבל $K = A_n$.

תהא $K \lhd A_n$ ויהי $e \neq k \in K$ $\{e\} \neq K$. נתבונן $k = (a\ b\ c\ d\ \ldots)(r\ s\ u\ z\ \ldots)\ldots$. נתבונן בשלשה $t = (b\ a\ x)$, כאשר $x \neq c$ (אם $k = (a\ b)\ldots$, x יכול להיות איבר כלשהו). נתבונן ב־$K \ni (tkt^{-1})k^{-1} = (b\ a\ x)k(a\ b\ x)k^{-1} = (b\ a\ x)(k(a)\ k(b)\ k(x)) = (b\ a\ x)(b\ c\ y)$. תמורה זו נמצאת גם ב־$A_5 \cong Alt\{a,b,c,x,y\}$. כלומר, מצאנו ב־$A_n$ עותק של A_5, שיש לו חיתוך לא־טריוויאלי עם K. A_5 פשוטה, אבל $\{e\} \neq K \cap A_5 \lhd A_5$ ולכן $K \cap A_5 = A_5$ – כלומר, $K \cap A_5$ מכילה את כל התמורות הזוגיות על $\{a,b,c,x,y\}$ ובפרט מכילה שלשה.

1.12 פעולה של חבורה על קבוצה

פעולה של חבורה על קבוצה 28.11.2007

הגדרה. G חבורה, X קבוצה. נאמר ש־G **פועלת על** X אם קיימת פונקציה $\alpha : G \times X \to X$ המקיימת (א) $\alpha(e,x) = x$; (ב) $\alpha(g_1g_2,x) = \alpha(g_1,\alpha(g_2,x))$ לכל $x \in X$ ו־$g_1,g_2 \in G$.

טענה 58: α כזו מגדירה הומומורפיזם $\varphi : G \to \operatorname{Per} X$ הניתן על־ידי $\varphi(g)(x) = \alpha(g,x)$ (לכל $g \in G$, $x \in X$), ולהיפך – כל הומומורפיזם $\varphi : G \to \operatorname{Per} X$ מגדיר פעולה של G על X באופן הבא: $\alpha(g,x) = (\varphi(g))(x)$.

הוכחה. בהינתן α, נגדיר φ כנ"ל. צריך לבדוק ש־φ הומומורפיזם לתוך $\operatorname{Per} X$. על־פי ההגדרה, $\varphi(g)$ העתקה מ־X ל־X. היא חח"ע ועל כי יש לה הפכי, $\varphi(g^{-1})$. נבדוק:

$$\begin{aligned}\varphi(g^{-1})(\varphi(g)(x)) &= \varphi(g^{-1})(\alpha(g,x)) \\ &= \alpha(g^{-1},\alpha(g,x)) \\ &= \alpha(g^{-1}g,x) = \alpha(e,x) = x\end{aligned}$$

אם כך, $\varphi(g^{-1}) \circ \varphi(g) = id\,|_X$, ובאופן דומה, $\varphi(g) \circ \varphi(g^{-1}) = id\,|_X$. לכן $\varphi(g)$ הפיך, כלומר זו פרמוטציה של X.

φ הומומורפיזם: צריך להראות שלכל $x \in X$,

$$\begin{aligned}\varphi(g_1g_2)(x) &\stackrel{?}{=} \varphi(g_1)(\varphi(g_2)(x)) \\ \alpha(g_1g_2,x) &\stackrel{?}{=} \alpha(g_1,\varphi(g_2)(x)) \\ \alpha(g_1g_2,x) &\stackrel{!}{=} \alpha(g_1,\alpha(g_2,x))\end{aligned}$$

ולהיפך, בהינתן הומומורפיזם $\varphi : G \to \operatorname{Per} X$, נגדיר α כנ"ל. צריך לבדוק שהתכונות מתקיימות:

(א) $\alpha(e,x) = \varphi(e)(x) = id\,|_X\,(x) = x$

(ב) $\alpha(g_1g_2,x) = \varphi(g_1g_2)(x) = \varphi(g_1)(\varphi(g_2)(x)) = \alpha(g_1,\alpha(g_2,x))$

בדרך כלל, כאשר הפעולה של G על X ברורה, נסמן בפשטות $g.x$ או רק gx.

דוגמה. תהא G חבורה, H חבורה חלקית. נסמן ב־X את קבוצת המחלקות השמאליות של H ב־G (לפעמים מסמנים זאת $X = G/H$, על־אף שזו לא בהכרח חבורת מנה). G פועלת על X כך: $g.(yH) = gyH$ ($yH = x \in X$, $g \in G$). זה מוגדר היטב, כי אם $yH = y'H$, כלומר $y^{-1}y' \in H$, אזי גם $gyH = gy'H$, כי $(gy)^{-1}gy' = y^{-1}g^{-1}gy' = y^{-1}y' \in H$.

נבדוק את קיום התכונות:

(א) $e.yH = eyH = yH$

(ב) $(g_1g_2).(yH) = (g_1g_2)yH = g_1(g_2y)H = g_1.(g_2y)H = g_1.(g_2.yH)$

במקרה הפרטי $H = \{e\}$, נקבל את פעולת G על עצמה על־ידי כפל משמאל; השתמשנו בפעולה זו במשפט קיילי על־מנת לשכן את G בתוך $\operatorname{Per} G$.

דוגמה (פעולת ההצמדה של G על עצמה). $X = G$; לכל $g \in G, x \in X$, $g.x = gxg^{-1}$.
זו פעולה: $e.x = x$; $(g_1g_2).x = (g_1g_2)x(g_1g_2)^{-1} = g_1(g_2xg_2^{-1})g_1^{-1} = g_1.(g_2.x)$.

מסקנה 59: G חבורה כלשהי, H חבורה חלקית של G מאינדקס n. אזי קיימת חבורה חלקית נורמלית $N \lhd G$ כך ש־$N \leq H$ ו־$[G : N] \leq n!$.

הוכחה. נתבונן בפעולה של G על X קבוצת המחלקות השמאליות של H ב־G. $|X| = n$. זה מגדיר הומומורפיזם $\varphi : G \to \operatorname{Per} X = S_n$. נסתכל בגרעין $N = \ker\varphi$. מאחר ש־$G/\ker\varphi \cong \operatorname{Im}\varphi$, נקבל $[G : N] \leq n!$.[41] לכל $k \in N$ מתקיים $kH = k(eH) = k.eH = eH = H$; ולכן $k \in H$ ו־$N \leq H$.

מסלול **הגדרה.** אם G חבורה הפועלת על קבוצה X, עבור $x \in X$ נסמן $[x] = o(x) = \{g.x \mid g \in G\}$ **– המסלול של $\mathbf{x}$ על־ידי $\mathbf{G}$**.

למה 60: G פועלת על X, $x, y \in X$. אזי $[x] = [y]$ או $[x] \cap [y] = \varnothing$.

הוכחה. מספיק להוכיח שאם $z \in [x] \cap [y]$ אזי $[y] \subseteq [x]$ (ואז, באופן סימטרי, גם $[x] \subseteq [y]$). ואכן, קיימים $g_1, g_2 \in G$ כך ש־$g_1.x = z = g_2.y$, ולכן $x = (g_1^{-1}g_2).y$. יהי $u \in [x]$. אז $u = g_3.x$, ו־$u = g_3.((g_1^{-1}g_2).y) = (g_3g_1^{-1}g_2).y \in [y]$.

מייצב **הגדרה.** יהי $x \in X$. $G_x = \{g \in G \mid g.x = x\}$ הוא **המייצב של $\mathbf{x}$ ב־$\mathbf{G}$**.

טענה 61: א. G_x חבורה חלקית של G;

ב. יש התאמה חח״ע ועל בין איברי המסלול $[x]$ למחלקות השמאליות של G_x ב־G. בפרט, אם $[x]$ סופי, $[G : G_x] = |[x]|$. התאמה זו ניתנת על־ידי $gG_x \mapsto g.x$.

הוכחה (ב). ההתאמה מוגדרת היטב כי אם $gG_x = g_0G_x$ אזי $g = g_0t$ עבור $t \in G_x$, ואז $g.x = (g_0t).x = g_0.(t.x) = g_0.x$.

ההתאמה היא על: אם $y \in [x]$ אזי קיים $g \in G$ כך ש־$g.x = y$ ולכן $gG_x \mapsto g.x = y$.

ההתאמה היא חח״ע: נניח שההתאמה העבירה את g_1G_x ואת g_2G_x לאותו איבר. אזי $g_1.x = g_2.x$, זאת אומרת $(g_1^{-1}g_2).x = x$, כלומר $g_1^{-1}g_2 \in G_x$ ולכן $g_1G_x = g_2G_x$.

[41] מקיום האיזומורפיזם, $|G/\ker\varphi| = |\operatorname{Im}\varphi| \leq |S_n| = n!$.

מסקנה 62: אם G חבורה סופית הפועלת על קבוצה X, אזי לכל $x \in X$, $|[x]| \mid |G|$.

מסקנה 63: אם G חבורה סופית ו־C מחלקת צמידות ב־G, אזי $|C| \mid |G|$ (כי C מסלול של פעולת G על עצמה על־ידי הצמדה).

חבורת־p **הגדרה.** חבורה סופית מסדר p^n עבור p ראשוני נקראת **חבורת־p**.

מסקנה 64: עבור G חבורת־p, $Z(G) \neq \{e\}$.

הוכחה. תהי G חבורת־p. כל מחלקת צמידות היא מסדר חזקת p. נניח שמחלקות הצמידות הן $C_1, C_2, \ldots, C_r$, $|C_i| = p^{\alpha_i}$. $|C_i| = 1 \iff c \in C_i$ הוא במרכז[42]. בכל מקרה אחר, $p \mid |C_i|$. אבל $C_1 = \{e\}$, $|C_1| = 1$, ומכאן נובע שבהכרח יש עוד (לפחות $p-1$) מחלקות צמידות מגודל 1.

באופן פורמלי יותר –

נשים לב שכאשר מתבוננים בפעולת ההצמדה, $G_x = \{g \in G \mid gx = xg\} = C_G(x)$. $|x^G| = [G : G_x] = [G : C_G(x)] = 1$ אז $x \in Z(G)$ אם"ם $|G| = [G : C_G(x)] + |Z(G)|$ סופית, אם G נציגי מחלקות צמידות לא־טריוויאליות שאינן $x_1, \ldots, x_t$ כאשר $p^n = |Z(G)| + \sum_{i=1}^{t} [G : C_G(x_i)]$. בפרט, אם G חבורת־p, נקבל $i = 1, \ldots, t$ לכל $[G : C_G(x_i)] \mid |G| = p^n$, ומצד שני $[G : C_G(x_i)] > 1$ (כי אחרת $x_i \in Z(G)$), ולכן $p \mid \sum_{i=1}^{t} [G : C_G(x_i)]$, ולכן $p \mid |Z(G)|$. אבל $|Z(G)| \geq 1$ כי $e \in Z(G)$, ולכן $|Z(G)| \geq p$ וסיימנו.

מסקנה 65: כל חבורת־p פתירה.

הוכחה. נתבונן ב־$G/Z(G)$. זו חבורת־p, לכן יש לה מרכז לא טריוויאלי (אלא אם כן $Z(G) = G$): $Z(G/Z(G)) \neq \{e\}$. נסמן $Z_1(G) = Z(G)$. לפי משפט ההתאמה, יש $Z_2(G)$ חבורה חלקית נורמלית של G המכילה את $Z_1(G)$ כך ש־$Z_2(G)/Z_1(G) = Z(G/Z_1(G))$. בדרך זו נבנה סדרת חבורות חלקיות נורמליות ב־G כך ש־$\{e\} \lhd Z_1(G) \lhd \ldots \lhd Z_l(G) = G$, והמנות $Z_{i+1}(G)/Z_i(G)$ אבליות. לכן G פתירה.

נקודת שבת **הגדרה.** $x \in X$ נקרא **נקודת שבת** של G אם לכל $g \in G$, $g.x = x$; דהיינו, אם"ם $G_x = G$ 3.12.2007
אם"ם $o(x) = \{x\}$.

דוגמה. G פועלת על G על־ידי כפל משמאל: $g.x = gx$, $x, g \in G$. אם $x \in G$, $o(x) = G$ כי לכל $y \in G$ קיים $g \in G$ כך ש־$gx = y$. $G_x = \{g \in G \mid gx = x\} = \{e\}$.

דוגמה. G פועלת על $X = G$ על־ידי $g.x = gxg^{-1}$. מחלקת הצמידות של x היא $x^G = o(x)$. $G_x = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\} = C_G(x)$.

[42] Centre; קבוצת האיברים שמתחלפים עם כל איברי החבורה. מסומן $Z(G)$.

1.13 משפטי סילו

משפט 66 (קושי): תהא G סופית, p ראשוני, ונניח $p \mid |G|$. אזי יש ב־G איבר מסדר p.

הוכחה. נגדיר $X = \{(g_0, \ldots, g_{p-1}) \mid g_i \in G,\ \prod_{i=0}^{p-1} g_i = e\}$. אז $X \subseteq G^p$. החבורה $C_p = \mathbb{Z}/p\mathbb{Z}$ פועלת על G^p על־ידי $i.(g_0, \ldots, g_{p-1}) = (g_{0+i}, \ldots, g_{p-1+i \pmod p})$ (זהו סיבוב שמאלה). קל לראות שזו פעולה. היא שומרת על הקבוצה X: אם $\prod_{i=0}^{p-1} g_i = e$, כלומר $g_0 \cdots g_{p-1} = e$, צריך להראות שגם $g_{0+i} \cdots g_{p-1+i \pmod p} = e$; עבור $i = 1$, $g_0 \cdots g_{p-1} = e \iff g_1 \cdots g_{p-1} = g_0^{-1} \iff g_1 \cdots g_{p-1} g_0 = e$, ועבור $i = 2, \ldots, p-1$ – באינדוקציה. לכן מוגדרת פעולה של $C_p = \mathbb{Z}/p\mathbb{Z}$ על X.

$|X| = |G|^{p-1}$, כי אפשר לבחור את $g_0, \ldots, g_{p-2}$ שרירותית וזה קובע לחלוטין את g_{p-1}. לכן $p \mid |X|$.

מאחר שהחבורה הפועלת על X היא מסדר p, גודל כל מסלול בפעולת C_p על X מחלק את p, ולכן הוא מסדר p או מסדר 1. כלומר, או שהמסלול מסדר p או ש־x נקודת שבת. יש לפחות נקודת שבת אחת: $(e, \ldots, e)$. מכאן יש לפחות עוד נקודת שבת אחת: $|X|$ הוא מספר נקודות השבת ועוד p פעמים מספר המסלולים מסדר p; לכן p מחלק את מספר נקודות השבת, שגדול מ־ או שווה ל־1, ולכן הוא לפחות p. נקודת שבת היא וקטור $(h, \ldots, h) \in X$ עבור $h \in G$ כך ש־$h^p = e$. הסדר של h מחלק את p, ומאחר ש־$h \neq e$, הרי $o(h) = p$ ומצאנו איבר כנדרש.

חבורת p־סילו

הגדרה. תהי G חבורה מסדר $n = p^r m$, כאשר p ראשוני ו־$p \nmid m$. חבורה חלקית P של G מסדר p^r תיקרא **חבורת p־סילו** של G.

משפט 67 (סילו): G חבורה סופית מסדר $n = p^r m$, p ראשוני, $p \nmid m$. אזי –

א. יש ל־G חבורה חלקית P מסדר p^r, כלומר יש חבורת p־סילו;

ב. כל חבורת־p ב־G מוכלת בחבורת p־סילו כלשהי;

ג. כל שתי חבורות p־סילו ב־G צמודות זו לזו;

ד. אם l הוא מספר חבורות p־סילו ב־G, אזי $l \equiv 1 \pmod p$, ו־$l \mid m$.

דוגמה. נשתמש במשפט סילו כדי להוכיח שכל חבורה מסדר 48 פתירה.

למה: אם G חבורה, $N \lhd G$ כך ש־N פתירה ו־G/N פתירה, אזי G פתירה. (כתרגיל.)

תהא G חבורה מסדר 48. $48 = 2^4 \cdot 3$, לכן לפי משפט סילו יש ב־G חבורה חלקית P מסדר 16 ואינדקס 3. P מכילה חבורה חלקית נורמלית N מאינדקס $\geq 3!$, ו־N חבורת־2 ולכן פתירה.[43] G/N חבורה מסדר ≥ 6 ולכן פתירה.[44]

הוכחה. א. נסמן ב־X את קבוצת כל תת־הקבוצות של G מסדר p^r. $|X| = \binom{p^r m}{p^r}$.

למה 1.67: אם $p \nmid m$, אזי $p \nmid \binom{p^r m}{p^r}$. (כתרגיל.)

[43] ניזכר שכל חבורת־p היא פתירה.

[44] חבורות מסדרים ≥ 5 הן חבורות־p ולכן פתירות; ההוכחה שחבורה K מסדר 6 היא פתירה (למעשה, $K \cong \mathbb{Z}/6\mathbb{Z}$ או $K \cong S_3$) – כתרגיל.

G פועלת על X באופן הבא: אם $B \in X$, $g \in G$, $g.B = \{gb \mid b \in B\}$. מאחר ש־$p \nmid |X|$, יש לפחות קבוצה אחת B_0 מסדר p^r שגודל המסלול שלה בפעולת G אינו מתחלק ב־p. נסמן $H = G_{B_0} = \{g \in G \mid gB_0 = B_0\}$ המייצב של B_0. זו חבורה חלקית של G מאינדקס זר ל־p.[45] כלומר, הסדר של H מחלק את $p^r m$ ו־$\frac{p^r m}{|H|}$ איננו מתחלק ב־p. לכן $p^r \mid |H|$, ובפרט $|H| \geq p^r$. מצד שני, יהי $b_0 \in B_0$ איבר קבוע ונגדיר פונקציה $f : H \to B_0$ על־ידי $f(h) = h \cdot b_0 \in B_0$. נטען ש־$f$ חח״ע: זה ברור, כי אם $f(h_1) = f(h_2)$, $h_1 b_0 = h_2 b_0$ ולכן $h_1 = h_2$. לכן $|H| \leq |B_0| = p^r$. בסך הכל $|H| = p^r$, וגמרנו.

5.12.2007 בטרם נמשיך את הוכחת הסעיפים הנוספים במשפט סילו, נתבונן בפעולה של חבורה G על קבוצת החבורות החלקיות של G המוגדרת על־ידי $g.H = gHg^{-1}$ עבור $g \in G$ ו־$H \in X$.[46] זו פעולה.

המייצב של H בפעולה זו הוא

$$G_H = \{g \in G \mid g.H = H\} = \{g \in G \mid gHg^{-1} = H\} = N_G(H)$$

– **הנורמליזטור** של H. מתקיימות התכונות הבאות:

1. $N_G(H)$ חבורה חלקית של G;
2. $N_G(H) \supseteq H$;
3. $H \lhd N_G(H)$ ו־$N_G(H)$ הוא החבורה החלקית המקסימלית של G ביחס לתכונה זו;
4. מספר החבורות החלקיות של G הצמודות ל־H שווה ל־$[G : N_G(H)]$, כי קבוצת כל החבורות החלקיות של G הצמודות ל־H היא המסלול של H תחת פעולת G, שגודלו שווה לאינדקס המייצב;
5. מספר החבורות החלקיות הצמודות ל־H, $[G : N_G(H)] = \frac{|G|}{|N_G(H)|}$, מחלק את $[G : H] = \frac{|G|}{|H|}$, כי מתקיים $H \leq N_G(H) \leq G$ ואז

$$[G : H] = \frac{|G|}{|H|} = \frac{|G|}{|N_G(H)|} \cdot \frac{|N_G(H)|}{|H|} = [G : N_G(H)][N_G(H) : H]$$

נחזור להוכחת משפט סילו:

ב. תהא P חבורת p־סילו של G. תהא $Y = \{P_1, \ldots, P_k\}$ קבוצת החבורות החלקיות הצמודות ל־P, כלומר המסלול של P בפעולת G על־ידי הצמדה על חבורות חלקיות. לפי הדיון לעיל, $k \mid m = [G : P]$. בפרט, k זר ל־p ($p \nmid k$).

תהא Q חבורת־p כלשהי חלקית ל־G. Q פועלת על Y על־ידי הצמדה. המסלולים של Q בפעולתה על Y הם מסדר חזקת־p (שהרי אורך מסלול של חבורה מחלק את סדר החבורה), ולכן סדריהם $1, p, \ldots, p^s$ (כאשר $|Q| = p^s$).

יש לפחות מסלול אחד בגודל 1 (כלומר, נקודת שבת): סכום ארכי המסלולים (הזרים) הוא $|Y| = k$, ואם כולם מתחלקים ב־p, נובע ש־k מתחלק ב־p, אך $p \nmid k$ ולכן קיים

[45] האינדקס הוא אורך המסלול של B_0, שזר ל־p.

[46] הצמדה, כזכור, היא אוטומורפיזם של G, ולכן gHg^{-1} גם היא חבורה חלקית.

$1 \le i_0 \le k$ כך ש־P_{i_0} נקודת שבת של Q, כלומר לכל $q \in Q$, $qP_{i_0}q^{-1} = P_{i_0}$. $q.P_{i_0}$
אז $q \in N_G(P_i)$ ולכן $Q \le N_G(P_{i_0})$. נסמן $D = N_G(P_{i_0})$, $\bar{P} = P_{i_0}$. אז $\bar{P} \lhd D$,
$Q \le D$. מתקיים $|D| = p^r m_0$ עבור $m_0 \mid m$, כי $|\bar{P}| = p^r$ ומוכלת ב־D ו־$G \le D$.
נסתכל בחבורה $Q\bar{P}$. זו חבורה חלקית. יתר על כן, $Q\bar{P}/\bar{P} \cong Q/\bar{P} \cap Q$. $Q/\bar{P} \cap Q$
היא מסדר חזקת־p, כי זו חבורת מנה של Q, ולכן $|Q\bar{P}/\bar{P}| = [Q\bar{P} : \bar{P}]$ גם הוא חזקת
p. $|Q\bar{P}| = [Q\bar{P} : \bar{P}]|\bar{P}|$, אם כן, גם הוא חזקת p. אבל אין ב־G חבורה חלקית מסדר
חזקת p גדולה מ־p^r, ולכן $|Q\bar{P}| = p^r$, כלומר $Q\bar{P} = \bar{P}$ ולכן $Q \le \bar{P}$.

ג. למעשה, בהוכחת (ב) הראינו שכל חבורת־p ב־G מוכלת באחד מצמודי P; בפרט, אם Q עצמה היא p־סילו, היא מוכלת באחד מצמודי P. אבל חבורות אלה הן מגודל זהה, ולכן Q שווה לאחד מצמודי P.

ד. בסימונים הקודמים, $l = k \mid m$.[47] $l \equiv 1 \pmod p$ נוכיח עכשיו ש־l. נתבונן בפעולת P על $Y = \{P_1, \dots, P_l\}$: המסלולים של P ב־Y הם או מגודל 1 או מתחלקים ב־p. אבל יש נקודת שבת – P עצמה, כאיבר של Y; אין נקודת שבת נוספת, כי אם P מייצבת את P_i אזי $P \le N_G(P_i)$ ו־$P \le P_i$ (הוכחנו זאת עבור חבורת־p כלשהי Q), ומכיוון שהן מאותו סדר, $P = P_i$. בסך הכל קיבלנו ש־P מקבעת במקום רק את עצמה וכל שאר המסלולים הם מסדרים המתחלקים ב־p. מאחר ש־Y היא איחוד של מסלולים זרים, $l \equiv 1 \pmod p$.

מסקנה 68: חבורת p־סילו נורמלית $\iff$ היא יחידה ($l = 1$).

דוגמה. חבורה מסדר 35 היא אבלית, ולמעשה ציקלית.

הוכחה. $5 \cdot 7 = 35$. תהא G חבורה מסדר 35. יש ב־G חבורה חלקית A מסדר 7 – חבורת 7־סילו. מספר חבורות 7־סילו l מחלק את 5, $l \equiv 1 \pmod 7$, לכן $l = 1$ ולכן $A \lhd G$. יש ב־G חבורת 5־סילו B. מספר חבורות 5־סילו t מקיים $t \mid 7$, $t \equiv 1 \pmod 5$ ולכן $t = 1$. לכן גם $B \lhd G$.

$e = a^7$, $A = \langle a \rangle$ ציקלית מסדר 7; $b^5 = e$, $B = \langle b \rangle$ כי B ציקלית מסדר 5.[48]
נסתכל ב־$A \ni a^{-1}b^{-1}ab \in B$: מתקיים $a^{-1}b^{-1}ab \in A \cap B$. אך $|A \cap B| \mid 5, 7$
ולכן $A \cap B = \{e\}$. אז $a^{-1}b^{-1}ab = e$, ומכאן $ab = ba$.
החבורה G נוצרת על־ידי a ו־b, כי $H = \langle a, b \rangle$ חבורה חלקית של G המכילה גם את A וגם את B, ולכן $|H| \mid 5$ ו־$|H| \mid 7$ ולכן $|H| \mid 35$ ו־$|H| = 35$, כלומר $H = G$.

למה 1.68: אם חבורה נוצרת על־ידי איברים המתחלפים ביניהם, אזי היא אבלית. (כתרגיל.)

יתר על כן, G ציקלית מסדר 35, כלומר $G \cong \mathbb{Z}_{35}$: על־מנת להוכיח זאת, מספיק להראות קיום איבר מסדר 35. נסתכל ב־$g = ab$: ברור ש־$g^{35} = e$, כי הוא בתוך חבורה מסדר 35 ו־$o(g) \mid |G|$ לפי כך ש־$o(g) = |\langle g \rangle|$ ומשפט לגראנז'. לכן $o(g) = 1, 5, 7, 35$.

[47] ראינו זאת בתחילת הוכחת (ב).
[48] חבורה מסדר ראשוני היא תמיד ציקלית.

אם $o(g) = 1$ אז $g = e$, כלומר $A \ni a = b^{-1} \in B$ ו־$a = b = e$, בסתירה. אם $o(g) = 5$, נקבל $g^5 = (ab)^5 = a^5b^5 = a^5 \neq e$, כי $o(a) = 7$; אם $o(g) = 7$, נקבל $g^7 = (ab)^7 = a^7b^7 = b^7 = b^2 \neq e$. לכן $o(b) = 5$, כנדרש. $o(g) = 35$, כנדרש.

10.12.2007

משפט 69: כל החבורות מסדר < 60 הן פתירות.

כדאי לזכור:

1. $N \lhd G$, N פתירה ו־G/N פתירה $\Longleftrightarrow$ G פתירה (כמסקנה, כל חבורת־p פתירה);
2. חבורה חלקית מאינדקס 2 היא נורמלית;
3. חבורה חלקית מאינדקס n מכילה חבורה חלקית $N \lhd G$ עם $[G : N] \leq n!$;
4. $r_p(G) \mid [G : P]$ ו־$r_p(G) \equiv 1 \pmod{p}$, כאשר P חבורת p־סילו (כאשר $r_p(G)$ הוא מספר חבורות p־סילו של G);
5. חבורת p־סילו של G נורמלית ב־G אם"ם $r_p(G) = 1$;
6. G/N איזומורפית לתת־חבורה של S_n, ולפי לגראנז' $|G/N| \mid n!$;
7. אם $|G| = pq$, p ראשוני, $(p, q) = 1$, $p > q$, אזי p־סילו נורמלית.

הוכחה. $r_p(G) \equiv 1 \pmod{p}$. אבל $r_p(G) \mid q$, $p > q$, ולכן $r_p(G) = 1$.

הוכחה. 1: $\{e\}$

p **2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 57, 59:** ציקליות מסדר ראשוני.

p^r **4, 8, 9, 16, 25, 27, 32, 49:** חבורות p־סילו.

$pq, p > q$ **6, 10, 14, 20, 21, 22, 26, 28, 34, 35, 38, 39, 42, 44, 46, 52, 55, 58:** ניתן לכתוב, למשל, $20 = 5 \cdot 2^2$, ואם נסמן $p = 5$, $q = 4$, נקבל לפי (7) שיש חבורת p־סילו נורמלית. כאן, למעשה, אנו מסתמכים על מה שהראינו קודם – כבר הראינו שחבורת p־סילו הזו, שסדרה קטן ממש מסדר החבורה הנדונה, היא פתירה.

$3p^r$ **12, 15, 24, 33, 48, 51:** למשל, $12 = 3 \cdot 2^2$; חבורות 2־סילו הן מאינדקס 3, ולכן יש חבורה חלקית נורמלית מאינדקס ≥ 6; חבורה זו תקיים $G \neq N \neq \{e\}$. N ו־G/N פתירות (על־פי מה שהראינו כבר), ולפי (1), G פתירה.

$2p^r$ **18, 50, 54:** על־פי (2): למשל, $18 = 2 \cdot 3^2$, וחבורת 3־סילו נורמלית (כי היא מאינדקס 2).

30: $30 = 2 \cdot 3 \cdot 5$. אז $r_5 \equiv 1 \pmod{5}$ ו־$r_5 \mid 6$, ולכן $r_5 = 1$, שאז סיימנו, או $r_5 = 6$. כל חבורת 5־סילו היא ציקלית מסדר ראשוני, ולכן חיתוך כל שתיים כאלו מכיל רק את e. אז יש $6(5 - 1) = 24$ איברים מסדר 5 ואיבר אחד מסדר 1. כעת, $r_3 \equiv 1 \pmod{3}$ ו־$r_3 \mid 10$. אז $r_3 = 1$ וסיימנו, כי אחרת $r_3 = 10$ ואז יש $10(3 - 1) = 20$ איברים נוספים, שסדרם 3, וזה בלתי אפשרי. לכן חבורת 5־סילו או חבורת 3־סילו נורמלית, והחבורה פתירה.

$4p^r$ **36:** $36 = 3^2 2^2$; אז חבורת 3־סילו מכילה חבורה חלקית נורמלית מאינדקס $\geq 4! = 24$.

$5p^r$ **40, 45:** למשל, $40 = 5 \cdot 2^3$; $r_5 \equiv 1 \pmod{5}$ ו־$r_5 \mid 8$, ולכן $r_5 = 1$.

56: $56 = 7 \cdot 8$; $r_7 \equiv 1 \pmod{7}$ ו־$r_7 \mid 8$, לכן $r_7 = 1$, שאז סיימנו, או $r_7 = 8$. יש $8 \cdot 6$ איברים מסדר 7 (שישה מכל חבורת 7־סילו) ואיבר אחד מסדר 1 (e, שגם נמצא בכל חבורת 7־סילו).

בכל חבורת 2־סילו יש שמונה איברים, מתוכם אחד טריוויאלי והשאר לא. $r_2 = 1$ וסיימנו, כי אחרת יש לפחות 8 איברים מסדרים 2, 4 או 8, ונקבל שיש יותר מ־$1 + 8 \cdot 6 + 8 = 57$ איברים, בסתירה.

1.14 חבורות אבליות

תהא A חבורה אבלית; נסמן בדרך־כלל את הפעולה ב־$+$ ואת איבר היחידה ב־0.

דוגמה. כל חבורה ציקלית היא אבלית.

סכום ישר

הגדרה. יהי $\{G_i\}_{i\in I}$ אוסף של חבורות; **סכומן הישר** $G = \bigoplus_{i=1}^{n} G_i$ זו חבורת ה־n־יות $\{g = (g_1, \ldots, g_n) \mid g_i \in G_i\}$, עם פעולת הכפל $gh = (g_1 \cdot_1 h_1, g_2 \cdot_2 h_2, \ldots, g_n \cdot_n h_n)$.
זו חבורה, וניתן לזהות את G_i כחבורה חלקית של G על־ידי $g_i \mapsto (e, \ldots, e, g_i, e, \ldots, e)$. $G_i \lhd G$ (לאחר הזיהוי).

דוגמה. סכום ישר של חבורות אבליות (ובפרט של חבורות ציקליות) הוא אבלי.

דוגמה. $\mathbb{Q}_+$ המספרים הרציונאליים ביחס לחיבור. היא לא ציקלית, כי כל איברי החבורה החלקית הנוצרת על־ידי מספר רציונאלי $\frac{a}{b}$ הם בעלי מכנה שמחלק את b, ולכן לא נוכל לקבל כל מספר רציונאלי. כל תת־חבורה נוצרת סופית של $\mathbb{Q}_+$ היא ציקלית (כתרגיל). אז $\mathbb{Q}_+$ איננה נוצרת סופית. (דוגמה לקבוצת יוצרים: $\{\frac{1}{n!} \mid n \in \mathbb{N}\}$.)

דוגמה. $\mathbb{Q}_\times$ המספרים הרציונאליים ביחס לכפל. היא לא ציקלית וגם לא נוצרת סופית. (דוגמאה לקבוצת יוצרים: $\langle p \text{ ראשוני} \mid p\rangle$. $\mathbb{Q}_\times = \langle -1, p\rangle$. כמו־כן, $\mathbb{Q}_\times^{\geq 0} \bigoplus_{p \text{ ראשוני}} \langle p\rangle$.)

12.12.2007

A חבורה אבלית. אם $n \in \mathbb{N}$, $na = a + \ldots + a$ n פעמים. אם $n \in \mathbb{Z} \setminus \mathbb{N}$ אזי $na = -((-a) + \ldots + (-a))$ $-n$ פעמים.
מתקיים $0_{\mathbb{Z}} \cdot a = 0_A$, $m \cdot 0_A = 0_A$, $m(a +_A b) = ma +_A mb$, $(m+n)a = ma +_A na$ ($m, n \in \mathbb{Z}$ ו־$a, b \in A$). תכונות אלה דומות למה שהיה מתקיים ב־A כמרחב וקטורי מעל $\mathbb{Z}$, אך $\mathbb{Z}$ איננו שדה.

1.14.1 בסיסים לחבורות

בסיס

הגדרה. A חבורה אבלית, $X = \{\alpha_1, \ldots, \alpha_n\}$ תת־קבוצה של A. נאמר ש־X **בסיס** של A אם כל $a \in A$ ניתן לכתיבה באופן יחיד כ־$a = a_1\alpha_1 + \ldots + a_n\alpha_n$ כאשר $a_1, \ldots, a_n \in \mathbb{Z}$. (כלומר, X יוצרת את A באופן יחיד.)

לא לכל חבורה אבלית יש בסיס: אם A סופית וציקלית, למשל $A = \mathbb{Z}_n$, לכל α מתקיים $0\alpha = n\alpha = 0$, ולכן ההצגה לא יחידה.

טענה 70: לחבורה סופית אין בסיס.

דוגמה. $A=\mathbb{Z}^n=\mathbb{Z}\oplus\ldots\oplus\mathbb{Z}$ וניקח $X=\{e_1,\ldots,e_n\}$.[49] אזי X בסיס ל־A, כי לכל $\alpha=(a_1,\ldots,a_n)\in A$ מתקיים $\alpha=a_1e_1+\ldots+a_ne_n$ והצגה זו יחידה (בפרט כי אלו וקטורי בסיס ל־$\mathbb{R}^n$, וההצגה היחידה נשמרת).

במקרה זה, $\{2e_1,\ldots,2e_n\}$ איננו בסיס: הוא איננו פורש, כי לא ניתן בעזרתו לייצג וקטורים בעלי קואורדינטות אי־זוגיות.

בסיס לחבורה הוא לא יחיד:

טענה 71: אם $X=\{\alpha_1,\ldots,\alpha_n\}$ בסיס ל־A, אזי $Y=\{\bar\alpha_1,\alpha_2,\ldots,\alpha_n\}$, כאשר מגדירים $\bar\alpha_1=\alpha_1+\sum_{i=2}^n c_i\alpha_i$,[50] גם הוא בסיס ל־$A$.

1.14.2 חבורות אבליות חפשיות

חבורה חפשית

הגדרה. אם A אבלית, $X=\{\alpha_1,\ldots,\alpha_n\}$ תת־קבוצה, נאמר A **חבורה חפשית על** X אם לכל חבורה אבלית D ולכל העתקה קבוצתית $\varphi:X\to D$ קיימת המשכה יחידה $\tilde\varphi:A\to D$ שהיא הומומורפיזם (ו־$\tilde\varphi(\alpha_i)=\varphi(\alpha_i)$ לכל $1\le i\le n$).

משפט 72: תהא A חבורה אבלית ו־$X=\{\alpha_1,\ldots,\alpha_n\}$ תת־קבוצה של A. אזי התנאים הבאים שקולים:

א. X בסיס של A;

ב. A חפשית על X;

ג. קיים איזומורפיזם $\tilde\varphi:\mathbb{Z}^n\to A$ כך ש־$\tilde\varphi(e_i)=\alpha_i$ לכל $i=1,\ldots,n$.

הוכחה. ((א) $\Leftarrow$ (ב)) תהא D חבורה אבלית ו־φ העתקה קבוצתית $\varphi:X\to D$. צריך להוכיח שקיים הומומורפיזם יחיד $\tilde\varphi:A\to D$ כך ש־$\tilde\varphi(\alpha_i)=\varphi(\alpha_i)$. יהי $\alpha\in A$; אזי מאחר ש־X בסיס, α ניתן לכתיבה באופן יחיד כ־$\alpha=\sum_{i=1}^n m_i\alpha_i$, $m_i\in\mathbb{Z}$. נגדיר $\tilde\varphi(\alpha)=\sum_{i=1}^n m_i\varphi(\alpha_i)$. ברור שזו הדרך היחידה להגדיר את $\tilde\varphi$ אם רוצים שיהיה הומומורפיזם המתלכד עם φ על X. נשאר לבדוק ש־$\tilde\varphi$ אכן הומומורפיזם של חבורות (כתרגיל; משתמשים בכך ש־D קומוטטיבית).

((ב) $\Leftarrow$ (ג)) נניח A חפשית על $X=\{\alpha_1,\ldots,\alpha_n\}$ ונגדיר $\psi:X\to\mathbb{Z}^n$ על־ידי $\psi(\alpha_i)=e_i$ ל־$i=1,\ldots,n$. מאחר ש־A חפשית על X, קיים הומומורפיזם $\tilde\psi:A\to\mathbb{Z}^n$ כך ש־$\tilde\psi(\alpha_i)=e_i$. מצד שני, $\{e_1,\ldots,e_n\}$ בסיס של $\mathbb{Z}^n$, ולכן קיים הומומורפיזם $\tilde\varphi:\mathbb{Z}^n\to A$ המקיים $\tilde\varphi(e_i)=\alpha_i$. נראה שהומומורפיזמים אלה הפכיים זה לזה. $\tilde\psi\circ\tilde\varphi(e_i)=\tilde\psi(\alpha_i)=e_i$, ומאחר ש־$\{e_1,\ldots,e_n\}$ יוצרת את $\mathbb{Z}^n$, $\tilde\psi\circ\tilde\varphi=id\mid_{\mathbb{Z}^n}$. (זה אומר ש־$\tilde\varphi$ חח״ע ו־$\tilde\psi$ על.) באופן דומה, $\tilde\varphi\circ\tilde\psi(\alpha_i)=\tilde\varphi(e_i)=\alpha_i$. כדי להראות ש־$\tilde\psi\circ\tilde\varphi$ גם הוא הזהות יש להוכיח ש־$X=\{\alpha_1,\ldots,\alpha_n\}$ יוצרת את A.

---

[49] $e_i=(0,\ldots,0,\overset{i}{1},0,\ldots,0)$.

[50] כפל של α_1 בסקלר יציב תנאי על הקואורדינטה הראשונה, והקבוצה שתתקבל לא תפרוש.

למה 1.72: אם A חפשית על $X = \{\alpha_1, \ldots, \alpha_n\}$ אז X יוצרת את A.

הוכחה. תהא $B = \langle \alpha_1, \ldots, \alpha_n \rangle$ החבורה החלקית של A הנוצרת על־ידי $\alpha_1, \ldots, \alpha_n$. יש להראות $B = A$, כלומר $A/B = \{0\}$. נגדיר שתי העתקות $\tilde{\varphi}_1, \tilde{\varphi}_2 : A \to A/B$ על־ידי $\tilde{\varphi}_1$ ההומומורפיזם הטבעי, $\tilde{\varphi}_2$ העתקת האפס. אז לכל i, $\tilde{\varphi}_1(\alpha_i) = B = 0_{A/B}$ ו־$\tilde{\varphi}_2(\alpha_i) = 0_{A/B}$, כלומר $\tilde{\varphi}_1 \mid_X = \tilde{\varphi}_2 \mid_X$. לפי הגדרת חבורה חפשית, יש המשכה יחידה, ולכן $\tilde{\varphi}_1 \equiv \tilde{\varphi}_2$. בפרט, לשתי ההתעקות אותה תמונה, כלומר $A/B = \{0_{A/B}\}$.

((ג) $\Leftarrow$ (א)) ברור, כי $\{e_1, \ldots, e_n\}$ בסיס של $\mathbb{Z}^n$.

משפט 73: תהא A חבורה אבלית עם בסיס $X = \{\alpha_1, \ldots, \alpha_n\}$. תהא B חבורה חלקית של A. אזי קיים ל־A בסיס $Y = \{\bar{\alpha}_1, \ldots, \bar{\alpha}_n\}$ כך ש־$B = \langle m_1\bar{\alpha}_1, \ldots, m_k\bar{\alpha}_k \rangle$, $k \leq n$ ו־$m_i \in \mathbb{Z}$ ומתקיים $m_1 \mid m_2 \mid \ldots \mid m_k$.

הוכחה. באינדוקציה על n. אם $n = 1$, A חפשית על $\{\alpha_1\}$ אז $A \cong \mathbb{Z}$ ואנו יודעים שכל החבורות החלקיות של $\mathbb{Z}$ הן מהצורה $B = \langle m \cdot 1 \rangle$.

נניח שהטענה נכונה ל־$n-1$ ונוכיח ל־n. בהינתן בסיס כלשהו $\mathcal{A}$ של A וחבורה חלקית $B \neq \{0\}$ של A, נסמן $f(\mathcal{A}, B)$ – השלם החיובי m הקטן ביותר כך שקיים $0 \neq \beta \in B$ שבכתיבתו על־פי הבסיס $\mathcal{A}$ מופיע m כאחד המקדמים. לנו נתונה B; יהי m המספר הקטן ביותר מבין $f(\mathcal{A}, B)$, כאשר $\mathcal{A}$ רץ על כל בסיסי A. נניח ש־m זה מתקבל עם בסיס $\mathcal{A} = \{\alpha'_1, \ldots, \alpha'_n\}$, ונניח $B \ni \beta = m\alpha'_1 + a_2\alpha'_2 + \ldots + a_n\alpha'_n$.

למה 1.73: $m \mid a_i$ לכל $i = 2, \ldots, n$.

הוכחה. נכתוב $a_i = q_i m + r_i$ ($0 \leq r_i < m$). נוכיח $r_i = 0$. נחליף את הבסיס $\mathcal{A}$ בבסיס $\mathcal{A}_0 = \{\bar{\alpha}_1, \alpha'_2, \ldots, \alpha'_n\}$ כך ש־$\bar{\alpha}_1 = \alpha'_1 + \sum_{i=2}^n q_i\alpha'_i$, ועכשיו $\beta = m\bar{\alpha}_1 + \sum_{i=2}^n r_i\alpha'_i$. מדרך בחירת m, נובע ש־$r_i = 0$, שאם לא כן, r_i מקדם קטן יותר של איבר של B ביחס לבסיס כלשהו. לכן $\beta = m\bar{\alpha}_1$.

תהא $A' = \langle \alpha'_2, \ldots, \alpha'_n \rangle$. אזי $\alpha'_2, \ldots, \alpha'_n$ הוא בסיס של A', כלומר A' חפשית על $n-1$ יוצרים. נסמן $B' = B \cap A'$. זוהי חבורה חלקית של A'.

למה 2.73: $B = \langle \beta = m\bar{\alpha}_1 \rangle \oplus B'$, דהיינו $\langle \beta \rangle \cap B' = \{0\}$ וכל איבר של B ניתן לכתיבה כ־$c\beta + \beta'$ עבור $c \in \mathbb{Z}$, $\beta' \in B'$.

17.12.2007

הוכחה. נניח $0 \neq \gamma \in \langle \beta \rangle \cap B'$, כלומר $\gamma = r\beta = rm\bar{\alpha}_1$ ו־$A' \ni \gamma = \sum_{i=2}^n a_i\alpha'_i$. אבל $\{\bar{\alpha}_1, \alpha'_2, \ldots, \alpha'_n\}$ בסיס, ולכן כתיבתו של γ יחידה – סתירה.[51]

עלינו להראות שכל איבר δ של B ניתן לכתיבה כ־$\delta = c\beta + \beta'$, כאשר $c \in \mathbb{Z}$ ו־$\beta' \in B'$. נסמן $\delta = a\bar{\alpha}_1 + \delta'$ כאשר $\delta' \in A'$. אז $m \mid a$: נכתוב $a = qm + r$ עבור $0 \leq r < m$, ונתבונן ב־

[51] יכולנו להוכיח זאת בדרך החיוב, ואז היינו מקבלים $\gamma = 0$.

$$\begin{aligned} B \ni \delta - q\beta &= (a\bar{\alpha}_1 + \delta') - qm\bar{\alpha}_1 \\ &= (a - qm)\bar{\alpha}_1 + \delta' \\ &= r\bar{\alpha}_1 + \delta' \end{aligned}$$

מאחר ש־δ' הוא צירוף לינארי של $\alpha'_2, \ldots, \alpha'_n$, נקבל סתירה לדרך בחירת m אלא אם כן $r = 0$. אז $m \mid a$, כלומר $a = mq$ ולכן $\delta = mq\bar{\alpha}_1 + \delta' = q(m\bar{\alpha}_1) + \delta' = q\beta + \delta'$. מתקיים $\delta' \in A'$ וכן $\delta' = \delta - q\beta \in B$, לכן $\delta' \in A' \cap B = B'$, כנדרש.

לפי הנחת האינדוקציה יש ל־A' בסיס $\bar{\alpha}_2, \ldots, \bar{\alpha}_n$ כך ש־$B' = \langle m_2\bar{\alpha}_2, \ldots, m_k\bar{\alpha}_k\rangle$ ו־$m_2 \mid m_3 \mid \ldots \mid m_k$, $k - 1 \leq n - 1$ ($k \leq n$). נשים לב ש־$\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n$ בסיס של A, ומהלמה נקבל ש־$B = \langle m\bar{\alpha}_1, m_2\bar{\alpha}_2, \ldots, m_k\bar{\alpha}_k\rangle$. נותר להוכיח $m \mid m_2$.

נכתוב $m_2 = qm + r$ עבור $0 \leq r < m$. נסמן $\tilde{\alpha}_1 = \bar{\alpha}_1 + q\bar{\alpha}_2$ ואז $\{\tilde{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n\}$ בסיס ל־A, לפי טענה 71. נתבונן עכשיו ב־

$$\begin{aligned} B \ni m\bar{\alpha}_1 + m_2\bar{\alpha}_2 &= m\bar{\alpha}_1 + mq\bar{\alpha}_2 + r\bar{\alpha}_2 \\ &= m(\bar{\alpha}_1 + q\bar{\alpha}_2) + r\bar{\alpha}_2 \\ &= m\tilde{\alpha}_1 + r\bar{\alpha}_2 \end{aligned}$$

מצאנו איבר ב־B עם כתיבה על־פי בסיס תוך שימוש ב־r, ולכן $r = 0$. לכן $m_1 = m \mid m_2$, וסיימנו.

מסקנה 74: חבורה חלקית של חבורה אבלית חפשית על n יוצרים היא חפשית על $k \leq n$ יוצרים.[52]

הוכחה. ראינו שאם $B \leq A$ אזי ביחס לבסיס $X = \{\bar{\alpha}_1, \ldots, \bar{\alpha}_n\}$ של A, B נוצרת על־ידי $Y = \{m_1\bar{\alpha}_1, \ldots, m_k\alpha_k\}$. נטען ש־$Y$ בסיס של B, כי כל איבר ב־B הוא צירוף לינארי של איברי Y, $B \ni \beta = \sum_{i=1}^{k} a_i(m_i\bar{\alpha}_i)$, כי הם יוצרים, ו־$a_i$ נקבעים באופן יחיד כי $a_i m_i$ נקבעים באופן יחיד מכך ש־X בסיס.

הערה: אם M חבורה אבלית נוצרת סופית על־ידי n איברים, אזי M (איזומורפית ל)חבורת מנה של החבורה החפשית על n יוצרים, כי אם A חפשית על $\{\alpha_1, \ldots, \alpha_n\}$ ו־M נוצרת על־ידי $\{\gamma_1, \ldots, \gamma_n\} \subseteq M$, את ההעתקה הקבוצתית $\alpha_i \mapsto \gamma_i$ ניתן להרחיב להומומורפיזם $\tilde{\varphi} : A \to M$, שהוא על כי $\{\gamma_1, \ldots, \gamma_n\}$ יוצרת את M. לכן $M \cong A/B$, $B = \ker\tilde{\varphi}$.

מסקנה 75: אם M חבורה אבלית נוצרת סופית עם מספר יוצרים מינימלי n, אזי קיימים שלמים חיוביים $m_k \mid \ldots \mid m_1$ ($k \leq n$) כך ש־$M \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_k\mathbb{Z} \oplus \mathbb{Z}^{n-k}$. בפרט, כל חבורה אבלית נוצרת סופית היא סכום ישר של חבורות ציקליות.

הוכחה. בסימונים כמקודם, $M \cong A/B$. לפי משפט 73, קיים ל־A בסיס $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$ כך ש־$B = \langle m_1\bar{\alpha}_1, \ldots, m_k\bar{\alpha}_k\rangle$ כאשר $k \leq n$ ו־$m_k \mid \ldots \mid m_1$. לכן

$$A/B \cong \mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_k\mathbb{Z} \oplus \overbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}^{n-k \text{ פעמים}}$$

(הסבר בתרגול.)

[52] בחבורה שאיננה קומוטטיבית, מספר היוצרים של תת־חבורה עשוי להיות גדול יותר.

מסקנה 76: חבורה סופית אבלית M היא סכום ישר של חבורות ציקליות. יתר על כן, אפשר שהיא איזומורפית לסכום $\mathbb{Z}/m_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/m_k\mathbb{Z}$ כאשר $m_1 \mid m_2 \mid \ldots \mid m_k$.

טענה 77: כל חבורה אבלית סופית M היא (איזומורפית ל)סכום ישר של חבורות p־סילו שלה.

מסקנה 78: אם M חבורת־p אבלית סופית, כלומר M מסדר p^r, אזי קיימים $r_1 \leq \ldots \leq r_k$, $\sum_{i=1}^{k} r_i = r$ כך ש־$M \cong \mathbb{Z}/p^{r_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p^{r_k}\mathbb{Z}$.

הוכחה. מסקנה מיידית מהמסקנה הקודמת.

טענה 79: הפירוק הנ"ל יחיד.

מסקנה 80: מספר החבורות האבליות מסדר p^r הוא $\sigma(r)$ (σ היא פונקציית החלוקה).[53]

הוכחה. מספר החבורות האבליות מסדר p^r שווה למספר האפשרויות לכתוב את r כסכום $r_1 + \ldots + r_k = r$ כאשר $1 \leq r_1 \leq \ldots \leq r_k$, ומספר זה שווה ל־$\sigma(r)$, על־פי הגדרה.

מסקנה 81: יהי $n \in \mathbb{N}$, ויהי $n = p_1^{d_1} p_2^{d_2} \cdot \ldots \cdot p_l^{d_l}$ פירוקו למכפלת ראשוניים ($p_i \neq p_j$ לכל $i \neq j$). אז מספר החבורות האבליות מסדר n הוא $\sigma(d_1) \cdot \ldots \cdot \sigma(d_l)$, ובפרט תלוי רק בחזקות ולא בראשוניים.

הוכחה. זוהי מסקנה מהטענה שכל חבורה אבלית היא מכפלת חבורות p־סילו שלה ומהמסקנה הקודמת.

[53] שימו לב שמספר החבורות האבליות מסדר p^r תלוי ב־r בלבד ולא ב־p.

2 תורת החוגים

2.1 הגדרה

24.12.2007

חוג

הגדרה. **חוג** הוא קבוצה R עם איבר 0 (האפס) ושתי פעולות בינאריות $+ : R \times R \to R$, $\cdot : R \times R \to R$ המקיימות –

1. $(R, 0, +)$ היא חבורה קומוטטיבית
2. אסוציאטיביות: $\forall r, s, t \in R \quad r \cdot (s \cdot t) = (r \cdot s) \cdot t$
3. דיסטריביוטיביות: $r(s + t) = rs + rt$, $(s + t)r = sr + tr$

חוג קומוטטיבי

אם דורשים גם $rs = sr$, R נקרא **חוג קומוטטיבי**.

חוג עם יחידה

אם דורשים קיום איבר $1 \neq 0$ המקיים $1 \cdot r = r \cdot 1 = r$, אזי R נקרא **חוג עם יחידה**.

דוגמה. שדה הינו חוג קומוטטיבי עם יחידה המקיים בנוסף שלכל $r \neq 0$ ישנו s כך ש־$r \cdot s = 1$.

דוגמה. $\mathbb{Z}$ – השלמים.

חוג פולינומים

דוגמה (חוגי פולינומים). F שדה, X משתנה. $F[X]$ הוא **חוג הפולינומים** במשתנה X מעל F. איבריו הם מהצורה $f(X) = a_0 + a_1X + \ldots + a_nX^n$. $a_i \in F$ הם המקדמים; a_0 הוא המקדם החפשי; $a_n \neq 0$ הוא המקדם העליון; n היא מעלת (דרגת) הפולינום f.

$$\begin{aligned} \textstyle\sum a_iX^i + \sum b_iX^i &= \sum (a_i + b_i)X^i \\ (\textstyle\sum a_iX^i)(\sum b_iX^i) &= \sum_{i,j} a_ib_jx^{i+j} = \sum_k (\sum_{i+j=k} a_ib_j)X^k \end{aligned}$$

(יש לבדוק את קיום התכונות). $F[X]$ הוא חוג קומוטטיבי עם יחידה: $0_F = 0$, $1_F = 1$.

ניתן גם להגדיר חוגי פולינומים ביותר ממשתנה אחד, למשל $\sum a_{ij}X^iY^j \in F[X, Y]$. תכונות חוגים כאלה שונות מאוד מתכונות חוגי פולינומים במשתנה בודד.

דוגמה (חוג המטריצות). F משדה, $M_n(F)$ אוסף המטריצות $n \times n$ מעל שדה F עם כפל וחיבור רגילים של מטריצות. מתקיים $A(B+C) = AB+AC$, $(B+C)A = BA+CA$, $A(BC) = (AB)C$. זהו חוג לא קומוטטיבי (עבור $n \geq 2$, בדרך־כלל $AB \neq BA$) עם יחידה I (מטריצת הזהות), איבר אפס 0.

דוגמה (חוג האנדומורפיזמים). V מרחב וקטורי מעל שדה F, $R = End(V)$ אוסף הטרנספורמציות הלינאריות $T : V \to V$. נגדיר פעולות $(T_1 + T_2)(v) = T_1(v) + T_2(v)$, $(T_1 \cdot T_2)(v) = T_1(T_2(v))$. $0(v) = 0$, $1(v) = v$. יש לבדוק את קיום אקסיומות החוג. נראה קיום דיסטריביוטיביות:

$$\forall v \in V \quad (T_1 + T_2)(S(v)) = T_1(S(v)) + T_2(S(v))$$

– מהגדרת החיבור;

$$\forall v \in V \quad S(T_1(v) + T_2(v)) = S(T_1(v)) + S(T_2(v))$$

– מהגדרת החיבור ומלינאריות S.[54] החוג המוגדר כך נקרא **חוג האנדומורפיזמים של מרחב וקטורי** V.

[54] קיבלנו, בעצם, שהסיבות לדיסטריביוטיביות מכל כיוון שונות.

דוגמה (חוגי חבורה). תהא Γ חבורה ויהי F שדה. נסמן ב־$F[\Gamma]$ את אוסף הביטויים הסופיים[55] $\sum_{g\in\Gamma} a_g g$ כאשר $a_g \in F$. הפעולות מוגדרות כך:

$$\begin{aligned}\textstyle\sum_{g\in\Gamma} a_g g + \sum_{g\in\Gamma} b_g g &= \sum_{g\in\Gamma}(a_g + b_g)g \\ (\textstyle\sum_{g\in\Gamma} a_g g)(\sum_{g\in\Gamma} b_g g) &= \sum_{g,h} a_g \cdot_F b_h g \cdot_\Gamma h\end{aligned}$$

אסוציאטיביות, למשל, נובעת מאסוציאטיביות בחבורה ובשדה:

$$\Big((\sum a_g g)(\sum b_h h)\Big)(\sum c_k k) = (\sum a_g b_h gh)(\sum c_k k) = \sum (a_g b_h)c_k (gh)k$$

החוג המוגדר כך נקרא **חוג החבורה** של Γ עם מקדמים בשדה F.

דוגמה. $F = \mathbb{R}$, $\Gamma = C_3 = \{e, g, g^2\}$ ($g^3 = e$). אז $F[\Gamma] = \{ae + bg + cg^2 \mid a, b, c \in \mathbb{R}\}$.

בחוג החבורה $F[\Gamma]$ יש איברים שונים מ־0 שמכפלתם 0, כלומר יש מחלקי אפס:

$$(e + g + g^2)(g - e) = g + g^2 + e - e - g - g^2 = 0$$

דוגמה. $C[0,1]$ אוסף הפונקציות הרציפות בקטע $[0,1]$ עם $(f+g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x) \cdot g(x)$, $0(x) = 0$, $1(x) = 1$.

הגדרה. יהי R חוג עם יחידה. איבר $r \in R$ נקרא **הפיך** אם קיים $s \in R$ כך ש־$rs = sr = 1$. איבר הפיך

דוגמה. נמצא את האיברים ההפיכים ב־$C[0,1]$: צריך להתקיים $f(x)g(x) = 1$, כלומר $g(x) = \frac{1}{f(x)}$; ו־$\frac{1}{f(x)}$ רציפה אם $f(x) \neq 0$.

טענה 82: אוסף האיברים ההפיכים בחוג R מהווה חבורה כפלית, המסומנת $R^\times$.

דוגמה. $\mathbb{Z}^\times = \{\pm 1\}$; $\mathbb{R}[X]^\times = \mathbb{R}^+ = \mathbb{R} \setminus \{0\}$

הוכחה. אקסיומת האסוציאטיביות $r(st) = (rs)t$ מתקיימת בחוג, וכן לכל $r \in R^\times$ קיים $s \in R^\times$ כך ש־$rs = sr = 1$, וכן אם $r_1 s_1 = s_1 r_1 = 1$, $r_2 s_2 = s_2 r_2 = 1$, אזי $(r_1 r_2)(s_2 s_1) = r_1(r_2 s_2)s_1 = r_1 1 s_1 = r_1 s_1 = 1$.

2.2 תת־חוגים

הגדרה. **תת־חוג** של חוג R הינו תת־קבוצה S המהווה תת־חבורה ביחס ל־$+$ וסגורה ביחס לכפל ($r, s \in S \implies r \cdot s \in S$). אם R חוג עם יחידה, נדרוש $1 \in S$. תת־חוג

דוגמה.

1. $M_n(\mathbb{R}) \leq M_n(\mathbb{C})$
2. $\Delta \leq \Gamma$ אזי $F[\Delta] \leq F[\Gamma]$
3. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$ (תת־שדה הוא תת־חוג)
4. $\mathbb{R}[X] \leq \mathbb{R}[X, Y]$

[55] הכוונה, כמובן, לביטויים סופיים בארכם. דרישה זו באה מכיוון שיש לקבץ מקדמים בפעולת הכפל, כפי שנראה מיד, וזה יהיה בלתי־אפשרי במקרה האינסופי כי איננו בהכרח יודעים איך לחבר אינסוף איברים בשדה כלשהו.

2.3 הומומורפיזמים

הומומורפיזם של חוגים

הגדרה. **הומומורפיזם** $\varphi : R \to S$ בין חוגים הינו העתקה המתאימה לכל איבר $r \in R$ איבר $\varphi(r) \in S$ כך ש־

א. φ הינה הומומורפיזם של חבורות קומוטטיביות ביחס ל־$+_R$ ו־$+_S$: כלומר, $\varphi(0_R) = 0_S$ ו־$\varphi(a+b) = \varphi(a) + \varphi(b)$;

ב. $\varphi(r \cdot s) = \varphi(r) \cdot \varphi(s)$;

ג. אם יש יחידה, $\varphi(1_R) = 1_S$.

דוגמה. יהי $\varphi : \mathbb{R}[X,Y] \to \mathbb{R}[X,Y]$ כך ש־$\varphi \mid_{\mathbb{R}} = id$, $\varphi(X) = f$, $\varphi(Y) = g$. אז $\varphi(\sum a_{ij} X^i Y^j) = \sum a_{ij} f^i g^j$.

לכל שני פולינומים $f, g \in \mathbb{R}[X,Y]$, הנוסחה הנ"ל מגדירה הומומורפיזם. (בדוק!)

בעיה פתוחה: מתי (כלומר, מה התנאי על f ו־g) φ הוא איזומורפיזם? (במקרה הלינארי $f = aX + bY$, $g = cX + dY$, זה מתקיים אם"ם $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ הפיכה.)

2.4 אידיאלים וחוגי מנה

יהי $\varphi : R \to S$ הומומורפיזם. $\operatorname{Im}\varphi$ הינו תת־חוג של S, כי ידוע שהוא תת־חבורה וכן $\varphi(r_1)\varphi(r_2) = \varphi(r_1 r_2)$.

$\ker\varphi$ הינו תת־חבורה חיבורית של החוג R. יהיו $a \in \ker\varphi$ ו־$r \in R$; אזי מתקיים $\varphi(ar) = \varphi(a)\varphi(r) = 0$ ו־$\varphi(ra) = \varphi(r)\varphi(a) = 0$. לכן לכל $a \in \ker\varphi$ ולכל $r \in R$, $ra, ar \in \ker\varphi$.

אידיאל

26.12.2007

הגדרה. R חוג; תת־קבוצה I של R תיקרא **אידיאל** (דו־צדדי) אם מתקיים (1) I תת־חבורה חיבורית של R; (2א) לכל $r \in R$ ולכל $a \in I$, $r \cdot a \in I$; (2ב) לכל $r \in R$ ולכל $a \in I$, $a \cdot r \in I$.

אידיאל שמאלי מקיים (1) ו־(2א); אידיאל ימני מקיים (1) ו־(2ב). אידיאל דו־צדדי מסומן $I \lhd R$.

דוגמה. $2\mathbb{Z} \subseteq \mathbb{Z}$, ובכלל $n\mathbb{Z} \subseteq \mathbb{Z}$ לכל n טבעי, הם אידיאלים.

דוגמה. גרעין של הומומורפיזם הוא אידיאל: $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0$, $\varphi(ar) = \varphi(a)\varphi(r) = 0 \cdot \varphi(r) = 0$ ולכן $ar, ra \in \ker\varphi$.

בפרט, אם R הוא חוג עם יחידה ו־$1 \in \ker\varphi$, אז $\varphi \equiv 0$, שהרי מתקיים לכל $a \in R$ $\varphi(a) = \varphi(a \cdot 1) = \varphi(a)\varphi(1) = \varphi(a) \cdot 0 = 0$.)

חוג מנה

הגדרה. יהי R חוג ו־I אידיאל ב־R. I חבורה־חלקית נורמלית של החבורה החיבורית של R, לכן R/I מוגדר כחבורת מנה, שאיבריה $a + I$ עבור $a \in R$. נהפוך את R/I ל**חוג מנה** על־ידי הגדרת כפל: עבור $a, b \in R$, $(a+I)(b+I) = ab + I$.

טענה 83: הכפל מוגדר היטב, ועם פעולה זו, R/I אכן חוג.

הוכחה. הכפל מוגדר היטב: נניח ש־$a+I=a'+I$ ו־$b+I=b'+I$. אז $a=a'+j$ עבור $j\in I$, $b=b'+l$ עבור $l\in I$. אז

$$\begin{aligned}(a+I)(b+I) &= ((a'+j)+I)((b'+l)+I)\\ &= (a'+j)(b'+l)+I\\ &= (a'(b'+l)+j(b'+l)+I\\ &= a'b'+a'l+jb'+jl+I=a'b'+I\end{aligned}$$

שכן $a'l\in I$ כי I אידיאל שמאלי ו־$jb',jl\in I$ כי I אידיאל ימני.

אסוציאטיביות: לכל $a,b,c\in R$,

$$\begin{aligned}(a+I)((b+I)(c+I)) &\stackrel{?}{=} ((a+I)(b+I))(c+I)\\ (a+I)(bc+I) &\stackrel{?}{=} (ab+I)(c+I)\\ a(bc)+I &\stackrel{!}{=} (ab)c+I\end{aligned}$$

מאסוציאטיביות R.

דיסטריביוטיביות (משמאל; מימין, באופן דומה):

$$\begin{aligned}(a+I)((b+I)+(c+I)) &\stackrel{?}{=} (a+I)(b+I)+(a+I)(c+I)\\ (a+I)((b+c)+I) &\stackrel{?}{=} (ab+I)+(ac+I)\\ a(b+c)+I &\stackrel{!}{=} (ab+ac)+I\end{aligned}$$

מדיסטריביוטיביות R משמאל.

2.5 משפטי ההומומורפיזם

ההשלכה הטבעית $\pi:R\to R/I$ המוגדרת על־ידי $a\overset{\pi}{\mapsto}a+I$ היא הומומורפיזם של חוגים: $\pi(ab)=ab+I=(a+I)(b+I)=\pi(a)\pi(b)$. זה הומומורפיזם על שגרעינו I, ומכאן שכל אידיאל הוא גרעין של הומומורפיזם.

משפט 84 (ההומומורפיזם הראשון): יהיו R ו־S חוגים, $\varphi:R\to S$ הומומורפיזם. נסמן $I=\ker\varphi$. אז $\operatorname{Im}\varphi$ תת־חוג של S ו־$R/I\cong\operatorname{Im}\varphi$.

הוכחה. אנו כבר יודעים ש־φ משרה איזומורפיזם של חבורות אדיטיביות $\tilde\varphi:R/I\to\operatorname{im}\varphi$ הנתון על־ידי $\tilde\varphi(a+I)=\varphi(a)$ ($a\in R$). לכן כל שנותר להוכיח הוא ש־$\tilde\varphi$ גם הומומורפיזם של חוגים, כלומר שומר את הכפל:

$$\begin{aligned}\tilde\varphi((a+I)(b+I)) &\stackrel{?}{=} \tilde\varphi(a+I)+\tilde\varphi(b+I)\\ \tilde\varphi(ab+I) &\stackrel{?}{=} \varphi(a)\varphi(b)\\ \varphi(ab) &\stackrel{!}{=} \varphi(a)\varphi(b)\end{aligned}$$

משפט 85 (ההתאמה): R חוג, $I\lhd R$ אידיאל. אזי יש התאמה בין תת־חוגים של R/I לתת־חוגים של R המכילים את I, ויש התאמה בין אידיאלים (ימניים/שמאליים) של R/I לבין אידיאלים (ימניים/שמאליים, בהתאמה) של R המכילים את I.

הוכחה. ראינו שיש התאמה חח״ע ועל בין החבורות החלקיות האדיטיביות של $(R,+)$ המכילות את I לבין החבורות החלקיות האדיטיביות של R/I כך שאם L חבורה חלקית של $(R,+)$ המכילה את I, מתאימים לה את $\bar{L}=\{l+I \mid l\in L\}$; ולהיפך, אם M חבורה חלקית של $(R/I,+)$, מותאמת לה $\tilde{M}=\{a\in R \mid a+I\in M\}$. מתקיים $\tilde{\bar{L}}=L$ עבור חבורה חלקית L המכילה את I, $\bar{\tilde{M}}=M$ לכל חבורה חלקית M של $(R/I,+)$.

כדי להוכיח את המשפט, יש להראות ש־(א) אם L כמקודם תת־חוג אז $\bar{L}$ תת־חוג, ואם M תת־חוג אז $\tilde{M}$ תת־חוג; (ב) אם L אידיאל (ימני/שמאלי) אזי $\bar{L}$ אידיאל (ימני/שמאלי, בהתאמה), ואם M אידיאל (ימני/שמאלי) אזי $\tilde{M}$ אידיאל (ימני/שמאלי, בהתאמה). נוכיח את (ב); (א) – תרגיל דומה.

יהי L אידיאל ב־R/I המכיל את I. יש להראות ש־$\bar{L}=\{l+I \mid l\in L\}$ אידיאל ב־R/I. יהי $a+I$ איבר כלשהו של R/I; אז $(a+I)(l+I)=al+I\in\bar{L}$ כי L אידיאל שמאלי, ובאופן דומה $(l+I)(a+I)\in\bar{L}$, ולכן $\bar{L}$ אידיאל.

נניח עכשיו ש־M אידיאל ב־R/I. יש להראות ש־$\tilde{M}=\{r\in R \mid r+I\in M\}$ אידיאל. יהיו $a\in R, m\in\tilde{M}$; אז $m+I\in M$, ויש להראות $am, ma\in\tilde{M}$, כלומר $am+I, ma+I\in M$. ואכן, $am+I=(a+I)(m+I)\in M$ כי M אידיאל שמאלי, ו־$ma+I=(m+I)(a+I)\in M$ כי M אידיאל ימני.

משפט 86 (ההומומורפיזם השני): R חוג, I אידיאל ב־R ו־H תת־חוג של R. אזי $H\cap I$ אידיאל ב־H ו־$(H+I)/I\cong H/(H\cap I)$.

הוכחה. $I\cap H$ אידיאל ב־H: יהיו $l\in H\cap I$ ו־$h\in H$. $H\ni hl\in I$, כלומר $hl\in H\cap I$, כי H תת־חוג ו־I אידיאל; באופן דומה, $lh\in H\cap I$.

אנו יודעים ש־$H+I/I\cong H/H\cap I$ כחבורות אדיטיביות על־ידי האיזומורפיזם $h+H\cap I\overset{\psi}{\mapsto}h+I$. נשאר רק לבדוק את הכפל:

$$\begin{aligned}\psi((h_1+H\cap I)(h_2+H\cap I)) &\overset{?}{=} \psi(h_1+H\cap I)\psi(h_2+H\cap I)\\ \psi(h_1h_2+H\cap I) &\overset{?}{=} (h_1+I)(h_2+I)\\ h_1h_2+I &\overset{!}{=} h_1h_2+I\end{aligned}$$

משפט 87 (ההומומורפיזם השלישי): אם I ו־K אידיאלים (דו־צדדיים) ב־R ו־$K\leq I$, אזי $R/I\cong(R/K)/(I/K)$.

הוכחה. אנו יודעים שיש איזומורפיזם של חבורות אדיטיביות $r+I\overset{\psi}{\mapsto}(r+K)+I/K$.[56] צריך להראות שזה גם הומומורפיזם של חוגים, כלומר שומר על הכפל:

$$\begin{aligned}\psi((r_1+K+I/K)(r_2+K+I/K)) &\overset{?}{=} \psi(r_1+K+I/K)\psi(r_2+K+I/K)\\ \psi((r_1+K)(r_2+K)+I/K) &\overset{?}{=} (r_1+I)(r_2+I)\\ \psi((r_1r_2+K)+I/K) &\overset{!}{=} r_1r_2+I\end{aligned}$$

[56] כמובן, אין המדובר באותה פעולת חיבור: $(r+_R K)+_{R/K} I/K$.

2.6 תחומי שלמות, תחומים ראשיים וחוגים אוקלידיים

2.6.1 תחומי שלמות

31.12.2007

תחום שלמות

הגדרה. **תחום שלמות** הוא חוג קומוטטיבי R בלי מחלקי אפס; כלומר, אם $a,b \in R$ כך ש־$ab=0$, אזי $a=0$ או $b=0$.

דוגמה. $\mathbb{Z}/12\mathbb{Z}$ איננו תחום שלמות – $3 \cdot 4 = 0$. אבל שדות ותת־חוגים שלהם הם תחומי שלמות.

משפט 88: כל תחום שלמות ניתן לשכן בשדה.[57]

הוכחה. (לשם כך, מגדירים יחס שקילות – $(a,b) \sim (c,d)$ אם $ad=bc$, בדיוק כפי שבונים את הרציונאלים מהשלמים.)

טענה 89: תחום שלמות $R \neq \{0\}$ סופי הוא שדה.

הוכחה. יהי $0 \neq a \in R$. הכפלה משמאל ב־a היא תמורה על R, כי $ab_1 = ab_2$ אז $a(b_1-b_2)=0$, ומכיוון ש־$a \neq 0$ ואין מחלקי 0 בהכרח $b_1 - b_2 = 0$, כלומר $b_1 = b_2$, ומסופיות R, חח״ע $\Leftarrow$ על. לכן קיים c כך ש־$ac = a$. יתר על כן, לכל $b \in R$ קיים $d_b \in R$ כך ש־$ad_b = b$, ולכן $b \cdot c = ad_b c = acd_b = ad_b = b$. לכן c איבר יחידה לכפל.

לכל $b \neq 0$ ב־R מתקיים שהכפלה ב־b היא תמורה, לכן קיים $f_b \in R$ כך ש־$bf_b = c = 1$. לכן R שדה.

2.6.2 חוגים אוקלידיים

חוג אוקלידי

הגדרה. תחום שלמות עם יחידה R ייקרא **חוג אוקלידי** אם יש פונקציה $d : R \setminus \{0\} \to \mathbb{Z}_{\geq 0}$ כך ש־(א) לכל $R \ni a,b \neq 0$, $d(a) \leq d(ab)$; (ב) חלוקה עם שארית: לכל $a,b \in R$ כך ש־$a \neq 0$ קיימים $q,r \in R$ כך ש־$b = qa + r$ ואם $r \neq 0$, $d(r) \lneq d(a)$.

דוגמה. $R = \mathbb{Z}$, $d(a) = |a|$.

דוגמה (חוג הפולינומים במשתנה אחד). שדה F, $R = F[X]$:[58] עבור הפולינום $f(X) = a_m X^m + \ldots + a_1 X + a_0$, $a_m \neq 0$, נגדיר $d(f(X)) = \deg f(x) = m$.

דוגמה (חוג השלמים של גאוס). $R = \mathbb{Z}[i] = \{a + bi \mid a,b \in \mathbb{Z}\}$ ($i = \sqrt{-1}$) הוא חוג אוקלידי, כאשר $d(a+bi) = a^2 + b^2$.

דוגמה. שדה F הוא חוג אוקלידי: נגדיר $d : F \setminus \{0\} \to \mathbb{N} \cup \{0\}$ על־ידי $d(a) = 0$ לכל $a \in F \setminus \{0\}$.

[57] כלומר, כל תחום שלמות הוא תת־חוג של שדה כלשהו, ולמעשה זו הדוגמה היחידה לתחומי שלמות.

[58] זהו תחום שלמות, כי המקדם של x^{n+m} במכפלת פולינום ממעלה m ופולינום ממעלה n איננו 0, מכך ש־F שדה.

2.6.3 תחומים ראשיים

אידיאל ראשי **הגדרה.** אם R חוג ו־$a \in R$, אזי $Ra = \{ra \mid r \in R\}$ הוא **האידיאל השמאלי** הנוצר על־ידי a, aR – **האידיאל הימני** הנוצר על־ידי a. אם R חוג קומוטטיבי, $Ra = aR$ נקרא **האידיאל הראשי** הנוצר על־ידי a.

תחום ראשי **הגדרה. תחום ראשי** הוא חוג קומוטטיבי שבו כל אידיאל הוא ראשי.

דוגמה (תחום שלמות שאיננו ראשי). $R = \mathbb{Z}[X]$, ויהי I האידיאל הנוצר על־ידי 2 ו־X. נסתכל בהומומורפיזם $\mathbb{Z}[X] \overset{\varphi_1: x \mapsto 0}{\mapsto} \mathbb{Z} \overset{\varphi_2: a \mapsto a \pmod 2}{\mapsto} \mathbb{Z}/2\mathbb{Z}$: הרכבת ההומומורפיזמים $\varphi_2 \circ \varphi_1 : \mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z}$ גם היא הומומורפיזם; $I = \ker(\varphi_2 \circ \varphi_1)$ הוא האידיאל המינימלי המכיל את 2 ואת X. I נוצר על־ידי 2 ו־X אבל לא על־ידי איבר אחד, כלומר איננו ראשי: אילו היה $f(X) \in \mathbb{Z}[X] = R$ כך ש־$I = Rf(X)$, כלומר $g(X) \in R$ כך ש־$2 = g(X)f(X)$, היינו מקבלים ש־$f(X) = c \in \mathbb{Z}$ סקלר; אז $X = h(X) \cdot c$ עבור $R \ni h(X) = aX + b$ ($a, b \in \mathbb{Z}$); מכאן נקבל $a \cdot c = 1$ (זהו המקדם של X ב־$h(X) \cdot c$), כלומר $c = \pm 1$. אבל אם $f(X) = \pm 1$ אז $Rf(X) = R \neq I$.

טענה 90: חוג אוקלידי הוא תחום ראשי.

הוכחה. יהי $I \lhd R$. אם $I = \{0\}$ אז $I = R \cdot 0$ וגמרנו. נניח ש־$I \neq \{0\}$ ונבחר $0 \neq a \in I$ עם $d(a)$ מינימלי. נטען ש־$I = Ra$: ברור ש־$Ra \subseteq I$, שהרי $a \in I$ ו־I אידיאל. צריך עכשיו להראות שאם $b \in I$ כלשהו אזי קיים $c \in R$ כך ש־$b = ca$. על־פי תכונת החילוק עם שארית, קיימים $q, r \in R$ כך ש־$b = qa + r$; אם $r = 0$, ניקח $c = q$ וגמרנו, או $d(r) \lneq d(a)$ ואז $r = b - qa \in I$, בסתירה לבחירת a.

איבר הפיך **הגדרה.** איבר a ב־R נקרא **הפיך** אם קיים $b \in R$ כך ש־$ab = 1$, כאשר 1 איבר היחידה ביחס לכפל[59].

דוגמה. האיברים ההפיכים ב־$\mathbb{Z}$ הם $\{\pm 1\}$; האיברים ההפיכים ב־$F[X]$, כאשר F שדה, הם $F \setminus \{0\}$; האיברים ההפיכים ב־$R = \mathbb{Z}[i]$ הם $\{\pm 1, \pm i\}$.

איברים ידידים **הגדרה.** איברים $a, b \in R$ נקראים **ידידים**[60] ב־R אם קיים $e \in R$ הפיך כך ש־$ae = b$. (יחס הידידות הוא יחס שקילות.)

ראינו שכל איבר ב־I מנורמה מינימלית יוצר את I. בפרט, אם $a, b \in I$ שניהם מנורמה מינימלית, אזי $I = Ra = Rb$, כלומר יש $c_1, c_2 \in R$ כך ש־$a = bc_2, b = ac_1$. כעת, $b = ac_1 = bc_2c_1$, כלומר $b(1 - c_2c_1) = 0$, ומכיוון שאין מחלקי 0, נקבל $1 - c_2c_1 = 0$ ולכן $c_2c_1 = 1$, כלומר c_1 ו־c_2 הפיכים.

[59] $a \cdot 1 = a$; איבר זה יחיד בתחום שלמות, שכן $a = a \cdot 1 = a \cdot 1'$ אז $a(1 - 1') = 0$ ולכן $1 = 1'$.

[60] associates.

טענה 91: התנאים הבאים שקולים עבור $a, b \in R$: (א) a ו־b ידידים; (ב) $Ra = Rb$.

הוכחה. ((א) $\Leftarrow$ (ב)) אם a ו־b ידידים, אזי קיים $e \in R$ הפיך עבורו $a = be$. מתקיים $Ra = Rbe = Reb = Rb$, כי עבור d כלשהו $ed = 1$ ואז $Re \supseteq Rde = R1 = R$ ולכן $Re = R$.

((ב) $\Leftarrow$ (א)) אז $I = Ra = Rb$, כלומר, קיימים $c_1, c_2 \in R$ כך ש־$a \in Rb$ ו־$b \in Ra$; $ac_1 = b$ ו־$bc_2 = a$. לכן $b(1 - c_2c_1) = 0$, ולכן $1 - c_2c_1 = 0$. $1 = c_2c_1$, כלומר c_1 ו־c_2 הפיכים, כלומר a ו־b ידידים.

טענה 92: התנאים הבאים שקולים: (א) $c \in R$ הפיך; (ב) c ידיד של 1; (ג) $Rc = R$, כלומר האידיאל הנוצר על־ידי c הוא כל R.

הוכחה. ידידי 1 הם בדיוק ההפיכים, ולכן (א) $\Leftrightarrow$ (ב); $Rc = R = R1$ אם"ם c ו־1 ידידים (לפי הטענה הקודמת), ולכן אם"ם c הפיך.

טענה 93: $d(1) \leq d(a)$ לכל $a \in R$.

הוכחה. $d(1) \leq d(1 \cdot a) = d(a)$, על־פי התנאי הראשון על d.

2.1.2008 **הגדרה.** R חוג קומוטטיבי, $a, b \in R$. נאמר ש־a **מחלק** את b ($a \mid b$) אם קיים $c \in R$ כך ש־$b = ac$. מחלקים

לפיכך, ניתן לומר באופן שקול להגדרה מקודם שאיבר $u \in R$ **הפיך** אם מחלק את 1. כמו כן, אם $a \mid b$ ו־$a \mid a$, a **ידיד** של b.[61]

למה 94: 1. $a \in R$ הפיך אם"ם $d(a) = d(1)$;

2. אם $0 \neq a, c \in R$ ו־$d(ac) = d(a)$, אזי c הפיך.

הוכחה. 1. אם a הפיך אזי קיים a' כך ש־$aa' = 1$, ולכן $d(1) = d(aa') \geq d(a)$. מצד שני, $d(1) \leq d(1 \cdot a) = d(a)$. לכן $d(a) = 1$.
מצד שני, אם $d(a) = d(1)$, בפרט a מנורמה מינימלית ולכן $Ra = R$; אז קיים $a' \in R$ כך ש־$aa' = 1$, ולכן a הפיך.

2. נסתכל באידיאל $I = Ra$ ובאידיאל $J = Rac = Rca$. ברור ש־$J \leq I$. מצד שני, $a, ac \in I$ מאותה נורמה, ולכן גם ac יוצר את I. כלומר, קיים c' כך ש־$(ac)c' = a$. לכן $a(cc' - 1) = 0$ ולכן $cc' = 1$ ו־c הפיך.

הגדרה. R תחום שלמות. איבר $p \in R$ ייקרא **ראשוני** אם אינו הפיך ומקיים שלכל $a, b \in R$, אם $p \mid ab$ אזי $p \mid a$ או $p \mid b$. איבר ראשוני

הגדרה. R תחום שלמות. איבר $q \in R$ ייקרא **אי־פריק** אם אינו הפיך ומקיים שאם $q = ab$ אזי a הפיך או b הפיך. איבר אי־פריק

[61] כיוון אחד של השקילות: אם $a = bc$ ו־$b = ad$, אז $b = bcd$ ולכן $cd = 1$, כלומר c ו־d הפיכים. השני – כתרגיל.

דוגמה. $R = \mathbb{Z}[\sqrt{-5}]$; 2 אי־פריק אך איננו ראשוני: $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$, כלומר $2 \mid (1+\sqrt{-5})(1-\sqrt{-5})$, כך איננו מחלק אף אחד מהגורמים.

טענה 95: R תחום שלמות. איבר ראשוני הוא אי־פריק.

הוכחה. יהי p ראשוני, ונניח $p = ab$. בפרט, $p \mid ab$, ולכן $p \mid a$ או $p \mid b$. בלי הגבלת הכלליות נניח $p \mid a$, כלומר $a = pc$ ולכן $p = ab = pcb$, ומכאן $p(1-cb) = 0$. $p \neq 0$ ואין מחלקי 0; אז $1 - cb = 0$, זאת אומרת $cb = 1$. כלומר, b הפיך.

טענה: בחוג אוקלידי, כל אי־פריק הוא ראשוני. (נוכיח זאת מיד.)

משפט 96: R חוג אוקלידי; אזי כל איבר a לא־הפיך ניתן לכתיבה כמכפלת איברים ראשוניים. יתר על כן, אם $a = p_1 \cdot \ldots \cdot p_m$ ו־$a = q_1 \cdot \ldots \cdot q_l$ כאשר p_i ו־q_j ($i = 1, \ldots, m$, $j = 1, \ldots, l$) ראשוניים, אזי $l = m$, ואחרי שינוי סדר, p_i ידיד של q_i לכל $i = 1, \ldots, m$.

הוכחה. קיום הפירוק: באינדוקציה על $d(a)$. אם $d(a)$ קטן ביותר, אזי $d(a) = d(1)$ ולכן a הפיך והטענה נכונה.

נניח שהוכחנו לכל האיברים c עם $d(c) < d(a)$ ונוכיח ל־a. אם a ראשוני, גמרנו. אחרת, a לא אי־פריק, כלומר ניתן לכתוב $a = bc$ כאשר לא b ולא c הפיך. זה אומר ש־$d(b), d(c) \lneq d(a)$ (כי ראינו שאם $d(b) = d(bc)$ אזי c הפיך), לכן לפי הנחת האינדוקציה b מכפלת ראשוניים ו־c מכפלת ראשוניים ולכן a מכפלת ראשוניים.

הוכחת היחידות: באינדוקציה על $d(a)$. אם $d(a)$ מינימלי אז גמרנו. עכשיו נניח $d(a)$ לא מינימלי, כלומר a לא הפיך ויש כתיבה $a = p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_l$.

p_1 ראשוני ו־$p_1 \mid q_1(q_2 \cdot \ldots \cdot q_l)$, ואז או $p_1 \mid q_1$ או $p_1 \mid q_2 \cdot \ldots \cdot q_l$. נמשיך ונקבל $p_1 \mid q_{j_0}$ ל־j_0 כלשהו. מכאן, $q_{j_0} = p_1 g$; q_{j_0} ראשוני ולכן אי־פריק, אז g הפיך, כלומר p_1 ו־q_{j_0} ידידים.

בלי הגבלת הכלליות נניח $j_0 = 1$. אז $p_1 p_2 \cdot \ldots \cdot p_m = p_1 g q_2 \cdot \ldots \cdot q_l$. נעביר אגף ונקבל $p_1(p_2 \cdot \ldots \cdot p_m - g_1 q_2 \cdot \ldots \cdot q_l) = 0$, ומאחר שאין מחלקי 0, $p_2 \cdot \ldots \cdot p_m = (gq_2)q_3 \cdot \ldots \cdot q_l$. נשים לב ש־$gp_2$ גם הוא ראשוני.[62] יתר על כן, $d(p_2 \cdot \ldots \cdot p_m) < d(p_1 p_2 \cdot \ldots \cdot p_m)$ על־פי למה 94, ולכן, על־פי הנחת האינדוקציה מיושמת על $p_2 \cdot \ldots \cdot p_m = (gq_2)q_3 \cdot \ldots \cdot q_l$, $l - 1 = m - 1$ (כלומר, $l = m$) ולאחר שינוי סדר $p_2 \sim gq_2 \sim q_2$, $p_i \sim q_i$ ל־$i \geq 3$.

2.6.4 מחלק משותף מקסימלי

מחלק משותף מקסימלי

הגדרה. יהי R חוג אוקלידי, $a, b \in R$. $d \in R$ ייקרא **מחלק משותף מקסימלי** של a ו־b ויסומן $d = \gcd(a, b)$ אם מקיים (א) $d \mid a$ ו־$d \mid b$; (ב) אם $c \mid a$ ו־$c \mid b$ אזי $c \mid d$.

איברים זרים

הגדרה. $a, b \in R$ ייקראו **זרים** אם $\gcd(a, b) = 1$.

[62] תרגיל: מכפלת ראשוני והפיך היא מספר ראשוני.

משפט 97: R חוג ראשי. לכל $0 \neq a, b \in R$ קיים $\gcd$, והוא יחיד עד־כדי ידידות.

7.1.2008 **הוכחה.** יהי I האידיאל הנוצר על־ידי a ו־b, כלומר $I = Ra + Rb = \{ra + sb \mid r, s \in R\}$. זהו אידיאל (בחוג) ראשי, כלומר $I = Rd$ לאיזשהו d. אז $d \mid a$ ו־$d \mid b$, כי $a, b \in I$; נשים לב ש־d עצמו הוא מהצורה $d = r_0 a + s_0 b$, ולכן אם $c \mid a$ ו־$c \mid b$, מתקיים $c \mid r_0 a + s_0 b = d$.

טענה 98: בחוג אוקלידי R, $p \in R$ ראשוני אם"ם p אי־פריק.

הוכחה. (ראשוני $\Leftarrow$ אי־פריק) לכיוון זה מספיק תחום שלמות; טענה 95.

(אי־פריק $\Leftarrow$ ראשוני) לכיוון זה צריך חוג ראשי.

למה 1.98: אם $c \mid ab$ ו־$(c, a) = 1$ אזי $c \mid b$.

הוכחה. אם $(c, a) = 1$, קיימים $r_0, s_0 \in R$ כך ש־$r_0 c + s_0 a = 1$, ו־$c \mid ab$ ולכן $cm = ab$. אז $b = b \cdot 1 = b \cdot r_0 c + s_0 ab$, ולפיכך $c \mid b$, כי $c \mid br_0 c$ ו־$c \mid s_0 ab$.

יהי p אי־פריק וננית $p \mid ab$. צריך להראות ש־$p \mid a$ או $p \mid b$. נסתכל ב־$d = \gcd(p, a)$. $d \mid p$, כלומר $p = dc$ ל־c כלשהו, ולכן d הפיך או c הפיך, כי p אי־פריק. אם c הפיך, p ידיד של d, כלומר גם $p = (a, p)$ ובפרט $p \mid a$. אם d הפיך, d ידיד של 1 ולכן $\gcd(p, a) = 1$. מתקיים, אם כן, $p \mid ab$ ו־$(p, a) = 1$; תנאי הלמה מתקיימים, ולכן $p \mid b$.

2.6.5 האלגוריתם של אוקלידס

האלגוריתם של אוקלידס

יהי R חוג אוקלידי ויהיו $a, b \in R$. למציאת $\gcd(a, b)$ נפעל כך:

$$\begin{aligned}
b &= q_0 a + r_1 && d(r_1) < d(a) \\
a &= q_1 r_1 + r_2 && d(r_2) < d(r_1) \\
r_1 &= q_2 r_2 + r_3 && d(r_3) < d(r_2) \\
r_2 &= q_3 r_3 + r_4 && d(r_4) < d(r_3) \\
&\vdots \\
r_{m-2} &= q_{m-1} r_{m-1} + r_m \\
r_{m-1} &= q_m r_m + 0
\end{aligned}$$

התהליך בהכרח נעצר, כי d יורד ממש בכל צעד.

טענה 99: $r_m = \gcd(a, b)$.

הוכחה. נוכיח באינדוקציה אחורית ש־$r_m \mid r_i$ לכל i: לפי השורה האחרונה, $r_m \mid r_{m-1}$, ומכאן לפי השורה שלפניה $r_m \mid r_{m-2} \Leftarrow r_m \mid r_{m-3} \Leftarrow \ldots \Leftarrow r_m \mid r_1$. $r_m \mid r_1, r_2$, אז מהשורה השנייה $r_m \mid a$ ואז מהראשונה גם $r_m \mid b$.

יהי $c \in R$ וננית $c \mid a$ וגם $c \mid b$. מהשורה הראשונה, $c \mid r_1$; מהשורה השנייה, $c \mid r_2$. נמשיך כך עד שמהשורה לפני האחרונה נקבל $c \mid r_m$.

דוגמה. $\gcd(759, 323) = 1$:

$$\begin{aligned} 759 &= 2 \cdot 323 + 113 \\ 323 &= 2 \cdot 113 + 97 \\ 113 &= 1 \cdot 97 + 16 \\ 97 &= 6 \cdot 16 + 1 \\ 16 &= 16 \cdot 1 \end{aligned}$$

בדרך־כלל תהליך זה מהיר מאוד, בפרט לעומת הדרך למציאת $\gcd$ על־ידי פירוק לראשוניים, שהיא בעיה קשה בהרבה.

שני איברים סמוכים בסדרת פיבונאצ'י ($1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \ldots$) נותנים את הרצף הארוך ביותר:

$$\begin{aligned} 89 &= 1 \cdot 55 + 34 \\ 55 &= 1 \cdot 34 + 21 \\ 34 &= 1 \cdot 21 + 13 \\ &\vdots \end{aligned}$$

2.7 חוגים פשוטים

חוג פשוט **הגדרה.** חוג R ייקרא **חוג פשוט** אם מתקיים $I = R \iff I \lhd R$ או $I = 0$.

דוגמה. F שדה. $M_n(F)$ הוא חוג פשוט (כתרגיל).

נעיר רק שבחוג (פשוט) זה יש אידיאלים חד־צדדיים: למשל, אוסף המטריצות מהצורה

$$\begin{pmatrix} * & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ * & 0 & \ldots & 0 \end{pmatrix}$$

מהווה אידיאל שמאלי (וכנ"ל, רק עם שורה במקום עמודה – אידיאל ימני).

טענה 100: אם R חוג פשוט קומוטטיבי עם יחידה, אזי R שדה.

הוכחה. צריך להראות שלכל $0 \neq a \in R$ קיים $a' \in R$ כך ש־$aa' = 1$. נסתכל באידיאל Ra. זה אידיאל (דו־צדדי) ב־R שונה מ־0 (כי מכיל את $1 \cdot a = a$), ולכן $Ra = R$, בגלל הפשטות. בפרט, קיים $a' \in R$ כך ש־$a'a = 1$, ולכן יש הפכי.

מסקנה 101: אם R חוג קומוטטיבי עם יחידה ו־$M \lhd R$ אידיאל מקסימלי[63], אזי R/M שדה.[64]

הוכחה. לפי משפט ההתאמה, יש התאמה חח"ע ועל בין האידיאלים של R/M לאידיאלים של R המכילים את M. נובע מכאן של־R/M יש רק אידיאל ה־0 וכל החוג, כלומר הוא פשוט ולכן שדה.

[63] זאת אומרת, $M \lneq R$ ואם $I \lhd R$ ו־$M \leq I \leq R$ אזי $I = M$ או $I = R$. (לפי הגדרה זו, חוג פשוט הוא חוג בו 0 הוא אידיאל מקסימלי.)

[64] למעשה, R/M שדה אם"ם M מקסימלי.

2.8 אידיאלים ראשוניים

אידיאל ראשוני

הגדרה. R חוג קומוטטיבי עם יחידה. אידיאל $I \lhd R$ נקרא **אידיאל ראשוני** אם כאשר $ab \in I$ אז $a \in I$ או $b \in I$.

דוגמה. $6\mathbb{Z}$ איננו אידיאל ראשוני: $2 \cdot 3 = 6 \in 6\mathbb{Z}$, אך $2, 3 \notin 6\mathbb{Z}$.

טענה 102: R חוג קומוטטיבי עם יחידה; אידיאל $I \lhd R$ ראשוני אם"ם R/I תחום שלמות.

הוכחה. R/I הוא קומוטטיבי עם יחידה. נניח I ראשוני; יהיו $x, y \in R/I$ כך ש־$x \cdot y = 0_{R/I}$, כלומר $x = a + I$, $y = b + I$ עבור $a, b \in R$, ו־$xy = (a+I)(b+I) = ab + I$. זה 0 ב־R/I, אז $ab + I = I$, כלומר $ab \in I$. I אידיאל ראשוני, לכן a או b ב־I. בלי הגבלת הכלליות, נניח $a \in I$, ולכן $x = a + I = I = 0_{R/I}$. לכן R/I תחום שלמות.

בכיוון השני, נניח R/I תחום שלמות ונוכיח ש־I ראשוני: יהיו $a, b \in R$ ונניח $ab \in I$. נסתכל ב־$a + I, b + I \in R/I$ ונכפול אותם: $(a + I)(b + I) = ab + I = I = 0_{R/I}$. R/I תחום שלמות, ולכן $a + I = 0_{R/I}$ או $b + I = 0_{R/I}$. בלי הגבלת הכלליות, $a + I = 0_{R/I}$, זאת אומרת $a + I = I$, כלומר $a \in I$.

מסקנה 103: אידיאל מקסימלי הוא ראשוני.

הוכחה. $I \lhd R$ מקסימלי $\Longleftarrow$ R/I שדה $\Longleftarrow$ R/I תחום שלמות $\Longleftarrow$ I ראשוני.

משפט 104: R חוג אוקלידי, $I \lhd R$; אזי התנאים הבאים שקולים:

א. I מקסימלי;

ב. R/I שדה;

ג. R/I תחום שלמות;

ד. I ראשוני.

הוכחה. (א) $\Leftrightarrow$ (ב), (ג) $\Leftrightarrow$ (ד), (ב) $\Leftrightarrow$ (ג). נותר להוכיח (ד) $\Leftarrow$ (א): אם I אידיאל ראשוני, צריך להראות ש־I מקסימלי. נניח שלא, כלומר קיים $I \lneq J \lneq R$, $J \lhd R$. כל אידיאל הוא ראשי, אז $I = Ra$, $J = Rd$.

למה 1.104: a ראשוני ב־R; או, באופן שקול, a אי־פריק. (כלומר, יוצר של אידיאל ראשוני הוא אי־פריק.)

הוכחה. $a = c_1 c_2$. Ra אידיאל ראשוני ו־$(c_1 + I)(c_2 + I) = a + I$; מכאן c_1 או c_2 ב־I. בלי הגבלת הכלליות, $c_1 \in I$, ואז $a \mid c_1$ וגם $c_1 \mid a$. נובע ש־c_2 הפיך.

$J = Rd \supseteq I = Ra$, אזי $d \mid a$, כלומר $a = dc$. אבל לפי הלמה a אי־פריק ולכן d הפיך – ואז $J = R$, בסתירה – או c הפיך – ואז a ו־d חברים, ולכן $Ra = Rd$, כלומר $I = J$, ושוב סתירה.