אלגברה מודרנית

24 בנובמבר 2005

תוכן עניינים

1 הקדמה

בקובץ זה נמצאים סיכומי הרצאות של פרופ' רועי משולם בסמסטר אביב 2005.
הודפס ע"י חגי ערן.

הקורס דן בנושאים:

- אריתמטיקה - מספרים שלמים
- חבורות
- חוגים
- שדות סופיים

2 אריתמטיקה

$\mathbb{N}$ - מספרים טבעיים
$\mathbb{Z}$ - מספרים שלמים (כולל השליליים)
$a|b$ - a מחלק את b.
לכל $b, a \geq 1$ יש $q, r \in \mathbb{Z}$ יחידים כך ש

$$b = q \cdot a + r$$

$$0 \leq r < a$$

r הוא שארית של חלוקת b ב-a.
כיצד מוצאים את q ו-r?
עבור x ממשי,

$$\lfloor x \rfloor \leq x \leq \lfloor x \rfloor + 1$$

$$\begin{aligned} q &= \left\lfloor \frac{b}{a} \right\rfloor \\ r &= b - \left\lfloor \frac{b}{a} \right\rfloor a \end{aligned}$$

צ"ל

$$\begin{aligned} a &\leq b - \left\lfloor \frac{b}{a} \right\rfloor a < a \\ \left\lfloor \frac{b}{a} \right\rfloor a &\leq b < a + \left\lfloor \frac{b}{a} \right\rfloor a = \left(1 + \left\lfloor \frac{b}{a} \right\rfloor\right) a \end{aligned}$$

2.1 מחלק משותף גדול ביותר

יסומן $\text{greatest common divisor } (a, b) = \gcd(a, b)$
ממ"מ - מחלק משותף מקסימלי, ממג"ב - מחלק משותף גדול ביותר.

דוגמה:

$(8, 12) = 4$
$(3, 12) = 3$
$(3, -12) = 3$

2.1.1 אלגוריתם למציאת ממג"ב

נניח ש-$a < b$. אחד מהם שונה מאפס.
נחלק עם שארית:

$$\begin{aligned} b &= qa + r \\ (a,b) &= (r,a) \\ &= \left(b - \left\lfloor \frac{b}{a} \right\rfloor a, a\right) \end{aligned}$$

הוכחה: עלינו להוכיח כי המחלק המקסימלי של a, b והמחלק המקסימלי של $b - \left\lfloor \frac{b}{a} \right\rfloor a, a$ שווים, ועושים זאת על ידי ההוכחה ששתי קבוצות המחלקים שוות.
נניח $x|a, b$, אז x מחלק את a, ומחלק את b, ובוודאי ש-x מחלק את $b - \left\lfloor \frac{b}{a} \right\rfloor a$.
כיוון שני. נניח $x|b - \left\lfloor \frac{b}{a} \right\rfloor a, a$. נסמן

$$b = \left(b - \left\lfloor \frac{b}{a} \right\rfloor a\right) + \left\lfloor \frac{b}{a} \right\rfloor a$$

x מחלק את שניהם, ולכן $x|b$.

2.1.2 אלגוריתם אוקלידס

כעת ניתן למצוא ממ"מ באלגוריתם הבא:

1. מחלקים את המספר הגדול בקטן עם שארית, ומוצאים את הממ"מ של השארית והמספר הקטן.
2. כאשר מגיעים לשארית 0, המחלק הוא המחלק המשותף המקסימלי.

סיבוכיות ליניארית בקלט.

טענה 2.1 לכל a, b שלא שניהם 0, קיימים x, y שלמים כך ש

$$ax + by = (a,b)$$

$$\begin{aligned} m &= \min\{ax + by | a, b \in \mathbb{Z}, ax + by > 0\} \\ d &= (a,b) \end{aligned}$$

נראה ש-$d \leq m$:
d מחלק את ax ואת by, לכן $d|ax + by$, ולכן $d \leq ax + by$ ולכן $d \leq m$.
כיוון הפוך, $m \leq d$:
נראה שלכל x, y ,$m|ax + by$, ובפרט $m|a, b$ ולכן $m \leq (a,b) = d$.
כלומר כל איבר מינימלי בקבוצה מחלק את כל אברי הקבוצה.
על דרך השלילה, קיימים x, y כך ש-m אינו מחלק את $ax + by$.

$$ax + by = qm + r$$

$$0 < r < m$$

$$\begin{aligned} r &= ax + by - qm \\ &= ax + by - q(ax_0 + by_0) \\ &= a(x - qx_0) + b(y - qy_0) < m \end{aligned}$$

סתירה למינימליות m.

מציאת x, y הוכחנו קודם (אוקלידס) ש-

$$d = (a, b) = \left(b - \left\lfloor \frac{b}{a} \right\rfloor a, a\right)$$

נניח ש

$$\left(b - \left\lfloor \frac{b}{a} \right\rfloor a\right) x' + ay' = d$$

$$a\left(y' - \left\lfloor \frac{b}{a} \right\rfloor x'\right) + bx' = d$$

נוכל לבחור $x = y' - \left\lfloor \frac{b}{a} \right\rfloor x'$ ו-$y = x'$ אז מצאנו

$$ax + by = d$$

a	b	$\left\lfloor \frac{b}{a} \right\rfloor$	x	y
51	81	1	8	-5
30	51	1	-5	3
21	30	1	3	-2
9	21	2	-2	1
3	9	3	1	0
0	3	3	0	1

$(a, b) = 1$ אומרים ש-a ו-b זרים.

טענה 2.2 אם $a|bc$ ו-$(a, b) = 1$ אז $a|c$.

הוכחה: קיימים x, y כך ש-

$$ax + by = 1$$

$$acx + bcy = c$$

המחובר הראשון מתחלק ב-a. המחובר השני גם הוא מתחלק ב-a כיוון ש-$a|bc$. לכן $a|c$. ■

2.2 מספר ראשוני

p יקרא ראשוני אם מחלקיו היחידים הם $\pm 1, \pm p$.

טענה 2.3 כל טבעי $1 \leq n$ הוא מכפלה של ראשוניים

טענה 2.4 אם $n = p_1 ... p_k = q_1 ... q_l$ ו-p_i, q_i ראשוניים אז $k = l$ וקיימת תמורה π, $p_i = q_{\pi(i)}$.

הוכחה: אינדוקציה על n.
בסיס - n ראשוני.
הנחת האינדוקציה לכל $m < n$, m ניתן להצגה כמפלה של ראשוניים.
צעד - ל-n מחלק $1 < a < n$

$$\begin{aligned} n &= ab \\ 1 &< b < n \end{aligned}$$

לכן לפי הנחת האינדוקציה

$$\begin{aligned} a &= p_1...p_k \\ b &= q_1...q_l \\ n &= p_1...p_k q_1...q_l \end{aligned}$$

■

הוכחת נוספת:
הוכחה: מספיק להראות שקיים i כך ש-$p_1 = q_i$ (כי אז נצמצם ונחזור על התהליך)

$$p_1 | q_1...q_l$$

אם $p_1 = q_1$ מצאנו, אחרת $p_1 \neq q_1$ ואז $(p_1, q_1) = 1$ שני ראשוניים שונים הם זרים.
חוזרים על התהליך $p_1 | q_2...q_l$ ... התהליך יעצר כאשר $p_1 = q_i$.
לעתים מסמנים $2 = p_1 < p_2 < ...$ סדרת הראשוניים. אז כל $n \geq 2$ הוא מכפלה

$$n = p_1^{\alpha_1}...p_k^{\alpha_k}$$

$\alpha_i \geq 0$.
נוכל למצוא כך את הממ"מ:

$$\begin{aligned} a &= p_1^{\alpha_1}...p_k^{\alpha_k} \\ b &= p_1^{\beta_1}...p_k^{\beta_k} \\ (a,b) &= p_1^{\gamma_1}...p_k^{\gamma_k} \\ \gamma_i &= \min\{\alpha_i, \beta_i\} \end{aligned}$$

■

2.3 יחס שקילות

הגדרה 2.5 אוסף R של זוגות סדורים (a,b) כאשר $a,b \in S$ הוא יחס בינארי מעל הקבוצה S.

$$R \subset S \times S$$

נסמן $(a,b) \in R \Leftrightarrow a\ b$.

הגדרה 2.6 ~ יקרא יחס שקילות אם

1. רפלקסיביות $a\ a$
2. סימטריות $a\ b \Leftarrow b\ a$
3. טרנזיטיביות $a\ b, b\ c \Rightarrow a\ c$

דוגמאות

1. $S = \mathbb{Z}$
   $a\ b$ אם $a \leq b$.
   היחס רפלקסיבי, טרנזיטיבי אך איננו סימטרי. לא יחס שקילות.
2. S סטודנטים בכיתה. $a\ b$ אם הסטודנטים יושבים אחד ליד השני, או אם הם אותו בן אדם.
   היחס רפלקסיבי, סימטרי, אך איננו טרזיטיבי.

3. $a\ b$ אם a, b מאותה עיר.

היחס רפלקסיבי, סימטרי וטרזיטיבי. יחס שקילות.

4. $S = \mathbb{Z}$

$a\ b$ אם $a - b$ זוגי.

a שקול לעצמו כיוון ש-0 הוא זוגי.

יחס סימטרי, כיוון שאם a זוגי אז גם $-a$ זוגי.

אם $a\ b, b\ c$ אז

$$a - c = (a - b) + (b - c)$$

לכן $a\ c$

5. יחס השקילות מודולו n

$a \equiv b\,(mod\ n)$ אם $n|a - b$

6. S משולשים במישור.

$T_1\ T_2$ אם T_1, T_2 חופפים.

2.3.1 מחלקת שקילות

הגדרה 2.7 מחלקת השקילות של a היא קבוצת האיברים השקולים לו.

$$C(a) = \{b \in S : b\ a\}$$

מחלקות השקילות מחלקות את המרחב לקבוצות זרות.

טענה 2.8 $C(a) = C(b) \Leftrightarrow a\ b$

טענה 2.9 $C(a) \cap C(b) = \emptyset \Leftrightarrow a \not\sim b$

הוכחה: $a\ b$ צ"ל $C(a) = C(b)$.

נבחר $z \in C(a)$, ונוכיח ש-$z \in C(b)$.

$z\ a$, אבל $a\ b$ לכן מן הטרנזיטיביות נובע ש-$z\ b$, $z \in C(b)$.

כיוון שני, $C(a) = C(b)$ וצ"ל $a\ b$.

$b \in C(b)$ וגם $a \in C(b)$ ולכן $a\ b$.

$C(a) \cap C(b) = \emptyset$ אז $a \sim b$.

$a\ b$. נניח על דרך השלילה ש-$C(a) \cap C(b) \neq \emptyset$.

קיים $z \in C(a) \cap C(b)$. מכאן $z\ a$ וגם $z\ b$. אבל אז $a\ b$ בסתירה להנחה. ■

מסקנה 2.10 מחלקות שקילות הן או זהות, או זרות. המרחב מתפרק כאיחוד מחלקות שקילות.

2.4 יחס השקילות מודולו n

הגדרה 2.11 $a \equiv b\,(mod\ n)$ אם $n \mid a - b$

1. מספר מחלקות השקילות השונות הוא n. $V_0, V_1, ..., V_{n-1}$.

למשל עבור $n = 3$:

$$\begin{aligned} V_0 &= ...-3, 0, 3, 6, ... \\ V_1 &= ...-2, 1, 4, 7, ... \\ V_2 &= ...-1, 2, 5, 8, ... \end{aligned}$$

$$\mathbb{Z} = V_0 \cup V_1 \cup V_2$$

תכונות מיוחדות של שקילות מודולו n $(\equiv_n)$

1. אם $a \equiv_n b$, $c \equiv_n d$ אז $a+c \equiv_n b+d$

הוכחה: מכיוון ש-

$$\begin{array}{rcl} n & | & a-b \\ n & | & c-d \end{array}$$

$$\begin{array}{rcl} (a+c)-(b+d) & = & (a-b)+(b-d) \\ n & | & (a+c)-(b+d) \end{array}$$

וגם $ac \equiv_n bd$

$$\begin{array}{rcl} a & = & b+xn \\ c & = & d+yn \\ ac & = & (b+xn)(d+yn) = bd+n(nxy+xd+by) \\ n & | & ac-bd \end{array}$$

■

2. אם $(a,n)=1$ וגם $ab \equiv_n ac$ אזי $b \equiv_n c$. אם a ו-n זרים, אז ניתן לצמצם את משוואת השקילות ב-a. במקרים אחרים אסור לצמצם.

הוכחה: מכיוון ש-

$$\begin{array}{rcl} n & | & ab-ac = a(b-c) \\ n & | & b-c \\ b & \equiv_n & c \end{array}$$

■

2.5 המשפט הקטן של פרמה

משפט 2.12 p ראשוני, ו-$1 \leq a \leq p-1$ (למעשה נראה זאת עבור $(a,p)=1$) אזי

$$a^{p-1} \equiv_p 1$$

לדוגמה $p=7; a=2$

$$a^{p-1} = 64 \equiv 1 \, (mod\ 7)$$

נתבונן בטבלה

i	$ia \, (mod\ p)$
1	a
2	$2a$
3	$3a$
...	...
$p-1$	$(p-1)\,a$

למה 2.13 אם $1 \leq i < j \leq p-1$ אזי $ia \not\equiv_p ja$
אם הפרשם $(j-i)\,a$ היה מתחלק ב-p אזי $p \mid j-i$ או $p \mid a$. שניהם לא מתקיימים ולכן הגענו לסתירה.
הוכחת המשפט:

בשתי העמודות בטבלה מופיעים כל המספרים $1, \ldots, p-1$ בדיוק פעם אחת. אם נכפול את כל השורות אחת בשניה נקבל שיוויון:

$$1 \cdot 2 \ldots \cdot (p-1) \equiv_p (a)\,(2a)\,(3a) \ldots (a)\,(p-1)$$

נשנה את סדר המכפלה

$$1 \cdot 2 \ldots \cdot (p-1) \equiv_p a^{p-1} \cdot 1 \cdot 2 \ldots \cdot (p-1)$$

מכיוון ש-p ראשוני, ניתן לצמצם ב-$(p-1)!$ ($(p, (p-1)!) = 1$) ולכן

$$1 \equiv_p a^{p-1}$$

משפט זה שימושי לבדיקת ראשוניות של מספרים גדולים. ניתן בעזרתו לפסול מספרים שאינם ראשוניים.

3 חבורות

3.1 הגדרת החבורה

הגדרה 3.1 קבוצה G עם פעולה בין כל שני איברים $a \circ b$. $(G, \circ)$ תיקרא חבורה (Group) אם מתקיימים

1. סגירות: לכל $(a,b) \in G \times G$ מתקיים $a \circ b \in G$
2. אסוציאטיביות: $(a \circ b) \circ c = a \circ (b \circ c)$
3. קיום איבר יחידה e: לכל $a \in G$ $a \circ e = e \circ a = a$
4. קיום איבר הופכי: לכל $a \in G$ קיים b יחיד שיסומן $b = a^{-1}$ כך ש-$b \circ a = a \circ b = e$.

3.1.1 תכונות החבורה

טענה 3.2 קיים איבר ניטרלי יחיד.

הוכחה: נניח $f \in G$ איבר ניטרלי נוסף. נכפול אותו באיבר הניטרלי המקורי e:

$$f = ef = e$$

לכן יש רק איבר ניטרלי אחד. ■

טענה 3.3 לכל $a \in G$ קיים הפכי יחיד b שנסמנו a^{-1}.

הוכחה: נניח b, c הופכיים ל-a.

$$\begin{aligned} ab &= ac = e \\ b\,(ab) &= b\,(ac) \\ (ba)\,b &= (ba)\,c \\ eb &= ec \\ b &= c \end{aligned}$$

■

3.2 דוגמאות לחבורות

3.2.1 חבורת התמורות

A קבוצה סופית (למשל $\{1,...,n\}$)

הגדרה 3.4 תמורה (פרמוטציה) היא העתקה חח"ע מ-A על עצמה. $\sigma : A \to A$.

הרכבת תמורות עבור שתי תמורות $\pi, \sigma : A \to A$ ניתן להרכיב אותן ולקבל תמורה חדשה

$$\begin{aligned} \pi \cdot \sigma : A &\to A \\ \pi \cdot \sigma (a) &= \pi (\sigma (a)) \end{aligned}$$

- הרכבת תמורות תלויה בסדר.
- לכל תמורה σ קיימת תמורה הופכית יחידה π כך ש-

$$\pi \cdot \sigma = \sigma \cdot \pi = id$$

קבוצת התמורות S_n נסמן ב-S_A את קבוצת התמורות על A. אם $A = \{1,...,n\}$ נסמן $S_n = S_A$.

$$|S_n| = n!$$

3.2.2 תכונות פעולת ההרכבה על S_n

1. **סגירות:** $\sigma, \pi \in S_n$ גורר $\pi \cdot \sigma \in S_n$
2. **אסוציאטיביות:** $(\sigma \cdot \pi) \cdot \tau = \sigma \cdot (\pi \cdot \tau)$ - זה נכון להרכבה של כל פונקציה.

$$\begin{aligned} ((\sigma \cdot \pi) \cdot \tau)(i) &= \sigma((\pi \cdot \tau)(i)) = \sigma(\pi(\tau(i))) \\ (\sigma \cdot (\pi \cdot \tau))(i) &= (\sigma \cdot \pi)(\tau(i)) = \sigma(\pi(\tau(i))) \end{aligned}$$

3. **קיום איבר יחידה:** יש e המקיים לכל $\sigma \in S_n$

$$\sigma \cdot e = e \cdot \sigma = \sigma$$

$$e = id$$

4. **קיום איבר הופכי:** לכל $\sigma \in S_n$ קיים τ יחיד המקיים

$$\sigma \cdot \tau = \tau \cdot \sigma = id$$

3.2.3 חבורת הסימטריות

C_n - כל הסימטריות האפשריות על n איברים.

דוגמה נתון מרובע שקודקודיו ממוספרים $1,2,3,4$ נגד כיוון השעון. מהן התמורות על $1,...,4$ אשר ניתון למימוש ע"י סיבוב המישור?

- סיבוב ב-$\frac{\pi}{2}$ נגד כיוון השעון יעביר את הקודקודים $1,2,3,4$ ע"י התמורה $R_{\frac{\pi}{2}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$
- סיבוב ב-π נגד כיוון השעון מתאים לתמורה $R_{\pi} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$
- $R_{\frac{3\pi}{2}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$
- סיבוב מלא יתן את תמורת הזהות: $R_0 = R_{\pi} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

נסמן את קבוצת התמורות הסימטריות

$$C_4 = \left\{ id = R_0, R_{\frac{\pi}{2}}, R_{\pi}, R_{\frac{3\pi}{2}} \right\}$$

טענה: הקבוצה C_4 מקיימת את כל 4 תכונות S_4 ביחס לפעולת ההרכבה.

1. C_4 סגור להרכבה.

$$R_{\alpha} \cdot R_{\beta} = R_{\alpha+\beta}$$

מכיוון ש-α, β כפולות של $\frac{\pi}{2}$ גם סכומן הוא כפולה של $\frac{\pi}{2}$.

2. C_4 אסוציאטיבית כמו כל הרכבה של תמורות.
3. קיים איבר יחידה - R_0.
4. קיים איבר הופכי

$$R_{\alpha}^{-1} = R_{-\alpha}$$

דוגמאות נוספות

- שיקופים במישור:

$$S_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$S_{\frac{\pi}{4}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

$$S_{\frac{\pi}{2}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$S_{\frac{\pi}{2}} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

קבוצת השיקופים איננה חבורה ביחס לפעולת ההרכבה כי אין לה איבר יחידה. אבל קבוצת איחוד השיקופים והסיבובים D_4 היא אכן חבורה.

1. סגירות: לדוגמה

$$S_{\frac{\pi}{4}} \circ S_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = R_{\frac{\pi}{2}}$$

ניתן להמשיך ולבדוק ידנית את שאר לוח הכפל אולם אפשר לקצר:

$$R_\alpha \circ R_\beta = R_{\alpha+\beta}$$

$$S_\alpha \circ S_\beta = R_{2(\alpha-\beta)}$$

$$S_\alpha \circ R_\beta = S_{\alpha-\frac{\beta}{2}}$$

הוכחה:

$$\begin{aligned} S_\alpha \circ S_{\alpha-\frac{\beta}{2}} &= R_{2\left(\alpha-\alpha+\frac{\beta}{2}\right)} = R_\beta \\ S_\alpha \circ S_\alpha \circ S_{\alpha-\frac{\beta}{2}} &= S_{\alpha-\frac{\beta}{2}} = S_\alpha \circ R_\beta \end{aligned}$$

3.2.4 עוד דוגמאות לחבורות

- $G = \mathbb{Z}$ עם פעולת החיבור הרגילה.

1. קשירות: מתקיים. סכום מספרים הוא מספר שלם.
2. אסוציאטיביות: חוק הקיבוץ בחיבור.
3. איבר יחידה: אפס.
4. איבר הופכי ל-a הוא $-a$.

הגדרה 3.5 אם בחבורה G מתקיים $ab = ba$ לכל a, b החבורה נקראת קומוטטיבית, או אבלית.

- $G = \mathbb{R}$ עם $+$
- $G = \mathbb{Q}$ רציונליים עם $+$
- $G = \mathbb{R}$ פעולת הכפל - זוהי איננה חבורה כי ל-0 אין אבר הופכי.
- $G = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ עם פעולת הכפל. זוהי חבורה:

1. סגירות. לכל $a, b \neq 0$ $ab \neq 0$.
2. אסוצ': לפי פעולת הכפל.
3. איבר יחידה 1.
4. איבר הופכי ל-a : $\frac{1}{a}$.

- $G = \mathbb{Z} \setminus \{0\}$ עם פעולת הכפל. זו איננה חבורה. למעט ± 1 לאף איבר אין הופכי.
- $G = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ עם פעולת הכפל היא חבורה.
- $G = GL_2(\mathbb{R})$ כל המטריצות בגודל 2×2 כאשר הדטרמיננטה של המטריצות שונה מאפס. הפעולה היא פעולה הכפל.

1. קשירות: $A, B \in GL_2(\mathbb{R})$. המכפלה היא מטריצה 2×2. דטרמיננטת המכפלה שווה למכפלת הדטרמיננטות, ולכן גם $AB \in GL_2(\mathbb{R})$.

2. אסוציאטיביות: $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ מיצגת העתקה ליניארית $A : R^2 \to R^2$ על ידי $A \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$
אנחנו רוצים להראות ש-

$$A(BC) = (AB)C$$

מספיק להראות שהשוויון מתקיים להעתקות ליניאריות. עובדה זו נכונה לכל הרכבת פונקציות

$$\begin{aligned} (A(BC)) \begin{pmatrix} x \\ y \end{pmatrix} &= A\left(B\left(C\begin{pmatrix} x \\ y \end{pmatrix}\right)\right) \\ ((AB)C) \begin{pmatrix} x \\ y \end{pmatrix} &= A\left(B\left(C\begin{pmatrix} x \\ y \end{pmatrix}\right)\right) \end{aligned}$$

1. איבר יחידה: I.
2. הופכי:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

- $G = GL_1(\mathbb{R})$ זוהי בדיוק $\mathbb{R}^*$
- $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$ האם זוהי חבורה?

1. סגירות נובעת מחוק מכפלת הדטרמיננטות.
2. אסוציאטיביות נובעת מהרכבת העתקות.
3. איבר יחידה I
4. איבר הופכי:

$$1 = |I| = \left|AA^{-1}\right| = |A|\left|A^{-1}\right| = \left|A^{-1}\right|$$

3.3 חבורת השאריות מודולו n

$\mathbb{Z}_n = \{0, \ldots, n\}$ עם הפעולה $a +_n b = (a + b) \pmod{n}$.
האיבר הניטרלי הוא 0.
הופכי ל-a יהיה b כאשר

$$b = \begin{cases} n - a & 1 \le a \le n - 1 \\ 0 & a = 0 \end{cases}$$

תבורה זו נקראת חבורה חיבורית של שאריות מודולו n.

הגדרה 3.6 G היא חבורה ציקלית מסדר n עם קיים $a \in G$ כך ש-

$$G = \left\{1, a, a^2, \ldots, a^{n-1}\right\}$$

ו-

$$a^n = 1$$

לחבורה זו התכונה שניתן לקבל את כל חבריה על ידי חיבורי המספר 1:

$$\mathbb{Z}_n = \left\{ 1, 1+1, 1+1+1, \ldots, \underbrace{1+\cdots+1}_{n-1}, \underbrace{1+\cdots+1=0}_{n} \right\}$$

לכן זוהי חבורה ציקלית. תכונה זו ראינו גם בחבורה C_n חבורת הסיבובים במישור ששומרים על קודקודי מצולע משוכלל עם n קודקודים.

3.3.1 פעולת הכפל ב-$\mathbb{Z}_n$ והחבורה $\mathbb{Z}^*$

נגדיר $j = a \cdot b$ על ידי $j \equiv_n ab$ היחידי ב-$\mathbb{Z}_n$.
האם $(\mathbb{Z}, \cdot)$ היא חבורה?
ל-0 אין הופכי.
האם $(\mathbb{Z} \setminus \{0\}, \cdot)$ חבורה? לא תמיד. למשל $\mathbb{Z}_4 \setminus \{0\}$ איננו חבורה. למספר 2 אין הופכי בקבוצה זה.

הגדרה 3.7 נגדיר $\mathbb{Z}_n^* = \{0 \leq a \leq n-1 \mid (a,n) = 1\}$

טענה 3.8 $(\mathbb{Z}_n^*, \cdot)$ היא חבורה.

הוכחה: קשירות:

$$\begin{array}{rcl} (b,n) & = & (a,n) = 1 \\ & \Downarrow & \\ (ab,n) & = & 1 \end{array}$$

אסוציאטיביות: מתקיים באופן כללי ב-$\mathbb{Z}_n$.
איבר יחידה: 1 זר ל-n.
הופכי:

$$\begin{array}{rcl} (a,n) & = & 1 \\ & \Downarrow & \\ \exists x,y : ax + ny & = & 1 \\ ax - 1 & = & -ny \\ ny & \mid & ax - 1 \\ ax & \equiv & 1 \pmod{n} \end{array}$$

אז אפשר לבחור

$$a^{-1} = x \pmod{n}$$

■

3.3.2 מהו מספר האיברים ב-$\mathbb{Z}_n^*$?

- כאשר $n = p$ ראשוני, $\left|\mathbb{Z}_p^*\right| = p - 1$
- כאשר $n = p^2$, מספר המספרים בין 0 ל-$p^2 - 1$ הזרים ל-p^2. כמה מספרים אינם זרים ל-p^2? רק המספרים $0, p, 2p, \ldots, (p-1)\,p$ שמספרם הוא p. לכן $\left|\mathbb{Z}_{p^2}^*\right| = p^2 - p$
- $\left|\mathbb{Z}_{p^3}^*\right| = p^3 - p^2$ מכיוון שהמספרים בתחום שמתחלקים ב-p הם $0, p, 2p, \ldots, (p^2-1)\,p$.
- $\left|\mathbb{Z}_{p^n}^*\right| = p^n - p^{n-1}$

- כאשר $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. ($p_i$ זרים בזוגות)

טענה 3.9 $|\mathbb{Z}_n^*| = \left(p_1^{n_1} - p_1^{n_1-1}\right) \cdots \left(p_1^{n_k} - p_1^{n_k-1}\right)$

נוסחה זו נקראת פונקציית אוילר ומסומנת $\phi(n)$.
מקרה פרטי:

$$\phi(pq) = (p-1)(q-1)$$

נסמן A - קבוצת המספרים בין 0 ל-$pq-1$ שמתחלקים ב-p ו-B קבוצת המספרים בין 0 ל-$pq-1$ שמתחלקים ב-q.

$$\phi(pq) = pq - |A \cup B| = pq - |A| - |B| + |A \cap B| = pq - p + 1 - q + 1 - 1$$

הוכחה: יהיו $m_1, \ldots, m_k$ זרים בזוגות. נגדיר העתקה

$$F : \mathbb{Z}_{m_1,\ldots,m_k} \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$$

מספר האיברים בתחום הוא $m_1 \cdots m_k$, ומספר האיברים בטווח הוא $m_1 \cdots m_k$.

$$F(x) = (x \,(\mathrm{mod} m_1), \ldots, x \,(\mathrm{mod} m_k))$$

נראה שההעתקה היא חח"ע ועל. די להראות ש-F חח"ע (כי הגודל שווה). נניח ש-$F(x) = F(y)$:

$$(x \,(\mathrm{mod} m_1), \ldots, x \,(\mathrm{mod} m_k)) = (y \,(\mathrm{mod} m_1), \ldots, y \,(\mathrm{mod} m_k))$$

כלומר

$$\begin{array}{rcl} m_1 & | & x - y \\ & \vdots & \\ m_k & | & x - y \end{array}$$

לכן בגלל ש-$m_1, \ldots, m_k$ זרים:

$$m_1 \cdots m_k \mid x - y$$

כלומר

$$x \equiv y \,(\mathrm{mod}\ m_1 \cdots m_k)$$

ו-F חח"ע. ■

3.4 משפט השאריות הסיני

$m_1, \ldots, m_k$ זרים בזוגות. לכל $a_1, \ldots, a_k$ קיים $0 \le x < m_1 \cdots m_k$ יחיד המקיים

$$\begin{array}{rcl} x & \equiv_{m_1} & a_1 \\ & \vdots & \\ x & \equiv_{m_k} & a_k \end{array}$$

הוכחה: הראנו שההעתקה F היא על. אפשר להניח עתה כי $0 \leq a_i < m_i$ ולכן קיים $x \in \mathbb{Z}_{m_1 \cdots m_k}$ כך ש-

$$F(x) = (a_1, \ldots, a_k)$$

■

ההוכחה אינה קונסטרוקטיבית. היא לא נותנת דרך מהירה למצוא את ה-x המתאים.
איך למצוא את x באופן מפורש? נעיין ב-$1 \leq i \leq k$ מסויים.

$$\left(m_i, \prod_{j \neq i} m_j\right) = 1$$

ל-$\prod_{j \neq i} m_j$ יש הפכי ב-$\mathbb{Z}^*_{m_i}$. נסמן ב-c_iאת הפכי זה, כלומר

$$\left(\prod_{j \neq i} m_j\right) c_i \equiv 1 \pmod{m_i}$$

פתרון למערכת (לאו דווקא בין $(0, \prod m_i)$ הוא

$$x = \sum_{i=1}^{k} a_i \left(\prod_{j \neq i} m_j\right) c_i$$

נראה למשל כי $x \equiv a_1 \pmod{m_1}$:

$$x \equiv a_1 \prod_{j \neq 1} m_j c_1 \pmod{m_1}$$

כי כל יתר המחוברים הם מכפלות של m_1 ולכן לא תורמים דבר לשארית. מכיוון שהגדרנו את c_1 להיות ההופכי של $\prod_{j \neq 1} m_j$:

$$x \equiv a_1 \pmod{m_1}$$

כנ"ל לגבי $m_2, \ldots, m_k$.

טענה 3.10 $\mathbb{Z}^*_{m_1 \cdots m_k} \xrightarrow{F} \mathbb{Z}^*_{m_1} \times \cdots \times \mathbb{Z}^*_{m_k}$
התמונה של F על $\mathbb{Z}^*_{m_1 \cdots m_k}$ היא בדיוק $\mathbb{Z}^*_{m_1} \times \cdots \times \mathbb{Z}^*_{m_k}$ ובפרט $\left|\mathbb{Z}^*_{m_1 \cdots m_k}\right| = \left|\mathbb{Z}^*_{m_1} \times \cdots \times \mathbb{Z}^*_{m_k}\right|$ כלומר $\phi(m_1 \cdots m_k) = \phi(m_1) \cdots \phi(m_k)$.

הוכחה: יהי $x \in \mathbb{Z}^*_{m_1 \cdots m_k}$
מכיוון ש-x זר לכל אחד מ-$m_1, \ldots, m_k$ - נניח בשלילה של-$x \bmod m_1$ ול-m_1 יש גורם משותף $p > 1$ אז גם $p \mid m_1, x$ בסתירה לכך ש-x זר למכפלת ה-m_i. לכן

$$F(x) = (x \bmod m_1, \ldots, x \bmod m_k) \in \mathbb{Z}^*_{m_1} \times \cdots \times \mathbb{Z}^*_{m_k}$$

נותר להראות שלכל $(a_1, \ldots, a_k) \in \mathbb{Z}^*_{m_1} \times \cdots \times \mathbb{Z}^*_{m_k}$ קיים $x \in \mathbb{Z}^*_{m_1 \cdots m_k}$ כך ש-

$$F(x) = (a_1, \ldots, a_k)$$

יהי x המקיים את המשוואה, אז x זר ל-$m_1 \cdots m_k$ כי אחרת היה קיים i ו-$p > 1$ כך ש-$p \mid m_i, x$ ואז

$$p \mid x \,(\mathrm{mod} m_i) \equiv a_i$$

ואז a_i לא זר ל-m_i, וזו סתירה.
לכן F היא חח"ע ו-$\left|\mathbb{Z}^*_{m_1 \cdots m_k}\right| = \left|\mathbb{Z}^*_{m_1} \times \cdots \times \mathbb{Z}^*_{m_k}\right|$. ■

3.5 חבורות חלקיות

הגדרה 3.11 נתונה חבורה $(G,\cdot)$. $H\subset G$ תקרא חבורה חלקית או תת-חבורה אם $(H,\cdot)$ חבורה. נסמן $H<G$.

טענה 3.12 $H\subset G$ ת"ח אסם לכל $a,b\in H$ מתקיים $ab^{-1}\in H$.

הוכחה: נניח $H\subset G$ ת"ח. ברור מאקסיומות החבורה שמתקיים $ab^{-1}\in H$.
נניח לכל $a,b\in H$ מתקיים $ab^{-1}\in H$.
אסוציאטיביות נובעת מאסוציאטיביות G.
נקח $a\in H$ אז ע"פ ההנחה $1=aa^{-1}\in H$ לכן קיים איבר יחידה ב-H.
נקח $1,b\in H$ אז $1b^{-1}=b\in H$ ולכן גם $b^{-1}\in H$.
$a,b^{-1}\in H$ ולכן ע"פ ההנחה $ab=a\left(b^{-1}\right)^{-1}\in H$ ולכן החבורה H סגורה.
לסיכום H חבורה. ■

3.5.1 דוגמאות

$G=(\mathbb{Z},+)$ ו-$H=5\mathbb{Z}$ ($n\mathbb{Z}=\{x\mathbb{Z}:n\mid x\}$). H היא תת חבורה של G.
לעומת זאת $H=\{n:n\geq 0\}$ איננה תת חבורה כי היא אינה מכילה איבר הפכי לכל איבר.
$G=(\mathbb{Z}_{15},+)$. נקח את הקבוצה $H=\{0,3,6,9,12\}$ ונבדוק האם זוהי תת חבורה של G. צריך לבדוק האם לכל $a,b\in H$ גם $ab^{-1}\in H$.

$$ab^{-1}=a-b$$

אם $3\mid a,b$ אז גם $3\mid a-b$ ולכן $a-b\in H$.

1. חבורה ציקלית
   C_n היא חבורה ציקלית מסדר n:

$$C_n=\left\{a^i:0\leq i\leq a-1\right\}$$

   עבור $k\mid n$ נקח את

$$H=\left\{a^{ki}:0\leq i<\frac{n}{k}\right\}$$

   וזוהי תת חבורה של C_n מכיוון ש-

$$a^{ki}a^{-kj}=a^{k(i-j)}\in H$$

2. $G=GL_2(\mathbb{R})$ מטריצות 2×2 הפיכות
   ונבחר $H=SL_2(\mathbb{R})=\{A:\det A=1\}$. זוהי תת חבורה.
3. $G=(\mathbb{R}^*,\cdot)$
   ונקח $H=\mathbb{R}_+^*$ אז $H<G$.
   לעומת זאת $K=\{x:x<0\}$ איננה תת חבורה כי היא איננה מכילה את 1.
4. תת מרחב וקטורי
5. $G=\left(\mathbb{R}^3,+\right)$
   נבחר $H=\{(x,y,z):x+2y+3z=0\}$ מישור כלשהו שעובר דרך הראשית. אוסף הפתרונות של מערכת ליניארית הוא תת מרחב של $\mathbb{R}^3$ ולכן H תהיה תת חבורה של G.
6. חבורת התמורות
   $C_n\subset D_n\subset S_n$
7. החבורה הסיבובית היא תת חבורה של החבורה הדיהדרילית והיא תת חבורה של חבורת התמורות.

3.5.2 שקילות מדולו תת חבורה

הגדרה 3.13 G חבורה ו$G > H$ ת"ח אז נגדיר

$$a \equiv b \pmod{H}$$

אם $a^{-1}b \in H$.

לדוגמה
$H = SL_2(\mathbb{R}) < G = GL_2(\mathbb{R})$. האיברים

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, b = \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{4} \end{pmatrix}$$

מקיימים $a \equiv b \pmod{H}$ כי

$$\det a^{-1}b = \det \begin{pmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = 1$$

טענה 3.14 שקילות מודולו תת חבורה הוא יחס שקילות

הוכחה: נראה כי הוא מקיים את שלושת התנאים:

1. $a \equiv a$ מכיוון ש-$a^{-1}a = 1 \in H$
2. $a \equiv b \Leftrightarrow b \equiv a$ כי אם $a \equiv b$ אז

$$\begin{aligned} a^{-1}b &\in H \\ b^{-1}a &= \left(a^{-1}b\right)^{-1} \in H \end{aligned}$$

3. אם $a \equiv b$ ו-$b \equiv c$ אז

$$\begin{aligned} a^{-1}b &\in H \\ b^{-1}c &\in H \end{aligned}$$

ולכן

$$a^{-1}bb^{-1}c = a^{-1}c \in H$$

כלומר $a \equiv c$

■

מחלקות השקילות

טענה 3.15 מחלקת השקילות של a מודולו H היא הקוסט השמאלי של H - aH:

$$C(a) = \{b : a \equiv b \pmod{H}\} = aH = \{ah : h \in H\}$$

הוכחה: מצד אחד

$$ah \in aH \Rightarrow \left(a^{-1}\right)ah = h \in H \Rightarrow a \equiv ah$$

כיוון שני

$$a \equiv b \Rightarrow a^{-1}b = h \in H \Rightarrow b = ah$$

■

לדוגמה $G = GL_2(\mathbb{R})$, $H = SL_2(\mathbb{R})$. כמה מחלקות שקילות יש?

$$C\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = SL_2(\mathbb{R})$$

$$C\left(\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\right) = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} SL_2(\mathbb{R})$$

טענה 3.16 ניתן לחלק את G למחלקות שקילות זרות $\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} SL_2(\mathbb{R})$ $t \neq 0$ שאיחודן הוא $GL_2(\mathbb{R})$.

$$\bigcup_{a \in G} aH = G$$

3.5.3 פירוק לקוסטים שמאליים

טענה 3.17 אנחנו יודעים מתכונות יחס השקילות כי לכל שתי מחלקות שקילות aH ו-bH מתקיים $aH = bH$ או $aH \cap bH = \emptyset$ וכמו כן $\bigcup_{a \in G} aH = G$.
נבחר נציג יחיד מכל מחלקת שקילות $a_1, a_2, \ldots$ ונסמן $A = \{a_1, a_2, \ldots\}$ אז

$$\bigcup_{a \in A} aH = G$$

וגם

$$aH \cap bH = \emptyset \quad a \neq b \in A$$

(כי כך בחרנו את A) וקיבלנו פירוק לקוסטים זרים.

נניח ש-G סופית. ותהי $H < G$ ת"ח. אז יש פירוק

$$G = \bigcup_{i=1}^{t} a_i H$$

(H סופית, ולכן גם מספר מחלקות השקילות)

טענה 3.18 לכל הקוסטים אותו הגודל:

$$|a_i H| = |a_j H| = |H|$$

הוכחה: נסמן $H = \{h_1, \ldots, h_k\}$ ואז

$$aH = \{ah_1, \ldots, ah_k\}$$

די להראות שאם $i \neq j$ גם $ah_i \neq ah_j$. אבל אם

$$ah_i = ah_j$$

נכפול ב-a^{-1} משמאל

$$h_i = h_j$$

בסתירה. ■

3.6 משפט לגרנז'

מסקנה 3.19 משפט לגרנז'
אם G סופית, $H < G$ אזי $|H| \mid |G|$.

הוכחה: יהא $G = \bigcup_{j=1}^{t} a_j H$ הפירוק של G לקוסטים זרים. אזי

$$|G| = \sum_{j=1}^{t} |a_j H| = \sum_{j=1}^{t} |H| = t\,|H|$$

■

t יקרא גם האינדקס של H ב-G, ומסמנים $t = (G : H) = \frac{|G|}{|H|}$.

דוגמאות

טבלה 1: פירוק לקוסטים של חבורות

G	H	קוסט אופייני	A בחירת איבר מכל קוסט	פירוק לקוסטים
$\mathbb{Z},+$	$n\mathbb{Z}=\{k:n\mid k\}$	$a+n\mathbb{Z}$	$\{0,1,\ldots,n-1\}$	$\bigcup_{i=0}^{n-1}(i+n\mathbb{Z})=\mathbb{Z}$
$\mathbb{Z}_{12},+$	$4\mathbb{Z}_{12}=\{0,4,8\}$	$a+4\mathbb{Z}_{12}$	$\{0,1,2,3\}$	$\bigcup_{i=0}^{3}(i+4\mathbb{Z}_{12})=\mathbb{Z}$
$\mathbb{R},+$	$\mathbb{Z}$	$a+\mathbb{Z}$	$[0,1)$	$\bigcup_{a\in[0,1)}(a+\mathbb{Z})=\mathbb{R}$
$GL_2(\mathbb{R}),\cdot$	$SL_2(\mathbb{R})$	$A\cdot SL_2(\mathbb{R})$	$\left\{\begin{bmatrix}t&0\\0&1\end{bmatrix}:t\in\mathbb{R}\right\}$	$\bigcup_{t\in\mathbb{R}^*}\begin{bmatrix}t&0\\0&1\end{bmatrix}SL_2(\mathbb{R})=GL_2(\mathbb{R})$
$\mathbb{R}^3,+$	$H=\{(x,y,z):x-y+z=0\}$	$\vec{u}+H$ הזזה של המישור	$\{a(1,-1,1):a\in\mathbb{R}\}$	$\bigcup_{a\in\mathbb{R}}(a(1,-1,1)+H)=\mathbb{R}^3$

הוכחת השורה הרביעית:
נוכיח שהקוסטים שבחרנו זרים: אם $s \neq t$ אז

$$\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix} \not\equiv \begin{bmatrix} s & 0 \\ 0 & 1 \end{bmatrix} \pmod{SL_2(\mathbb{R})}$$

מכיוון ש-

$$\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} s & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} t^{-1}s & 0 \\ 0 & 1 \end{bmatrix} \notin SL_2(\mathbb{R})$$

לכן הקוסטים $SL_2 \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}$ זרים.
נוכיח שאיחוד הקוסטים נותן את $GL_2(\mathbb{R})$:
נניח $A \in GL_2(\mathbb{R})$. לאיזה קוסט A שייך? נקח $t = \det A$ אז

$$A \in \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix} SL_2(\mathbb{R})$$

מכיוון ש-

$$\begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}^{-1} A \in SL_2(\mathbb{R})$$

$$\det \begin{bmatrix} t & 0 \\ 0 & 1 \end{bmatrix}^{-1} A = t^{-1} \cdot \det A = 1$$

3.6.1 תת חבורה נוצרת

תהי חבורה G ונסתכל על $a \in G$. מהי תת החבורה הקטנה ביותר המכילה את a?
תת החבורה הזו חייבת להכיל את 1, את a, ולכן גם את $a^{-1}, a^2, a^3, \ldots$ ואת הופכיים שלהם $a^{-2}, a^{-3}, \ldots$.
נראה שתת החבורה המבוקשת היא

$$\langle a \rangle = \{\ldots, a^{-3}, a^{-2}, a^{-1}, 1, a, a^2, a^3, \ldots\}$$

נוכיח שזוהי תת חבורה: עבור $a^k, a^l \in \langle a \rangle$

$$a^{-k}a^l = a^{l-k} \in \langle a \rangle$$

ולכן זוהי תת חבורה.
קוראים ל-$\langle a \rangle$ תת החבורה הנוצרת על ידי a.

3.6.2 סדר של איבר

הגדרה 3.20 הסדר של a, $\operatorname{Ord}(a) = \operatorname{Ord}_G(a)$ הוא המספר $0 < k$ המינימלי המקיים

$$a^k = 1$$

אם אין k כזה נסמן $\operatorname{Ord}(a) = \infty$

דוגמה $G = \mathbb{Z}_8 \quad a = 4$

$$\operatorname{Ord}(a) = 2$$

כי $4^2 = 4 + 4 = 0$

$$\operatorname{Ord}(2) = 4$$

$$\operatorname{Ord}(1) = 8$$

דוגמה נוספת $G = GL_4(\mathbb{R})$

$$\mathrm{Ord}\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} = 2$$

טענה 3,21 נניח $\infty > k = \mathrm{ord}(a)$ אזי

$$\langle a \rangle = \{1, a, \ldots, a^{k-1}\}$$

$$|\langle a \rangle| = k$$

הוכחה: על פי הגדרת $\langle a \rangle$:

$$\langle a \rangle = \left\{\ldots, a^{-2k}, a^{-(2k-1)}, \ldots, a^{-k}, a^{-(k-1)}, \ldots, a^{-1}, 1, a, \ldots, a^{k-1}, a^k, \ldots, a^{2k-1}, \ldots\right\}$$

האיברים $1, \ldots, a^{k-1}$ שונים זה מזה כי אחרת $a^i = a^j$ עבור $0 \leq i < j <\leq k-1$ ואז $a^{j-i} = 1$ אבל $0 < j - i \leq k-1$ בסתירה למינימליות k.
כל יתר האיברים שייכים לקבוצה $\{1, \ldots, a^{k-1}\}$. ניקח a^n. אז ניתן לחלק את n עם שארית ב-k: $n = qk + r$, $0 \leq r < k$. לכן

$$a^n = a^{qk}a^r = \left(a^k\right)^q a^r = 1^q a^r = a^r$$

■

מסקנה 3,22 $\langle a \rangle$ היא חבורה ציקלית מסדר k.

אם $\mathrm{ord}(a) = \infty$ אז

$$\langle a \rangle = \{\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\}$$

וכל האיברים שונים. אם היו $i < j$ כך ש-$a^i = a^j$ אז

$$a^{j-i} = 1$$

וזו סתירה לכך ש-$\mathrm{ord}(a) = \infty$.
במקרה זה $\langle a \rangle$ היא החבורה הציקלית האינסופית.

דוגמה $G = GL_2(\mathbb{R})$

$$\begin{aligned} \mathrm{ord}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} &= 1 \\ \mathrm{ord}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} &= 2 \\ A = \mathrm{ord}\begin{pmatrix} \cos\frac{2\pi}{3} & -\sin\frac{2\pi}{3} \\ \sin\frac{2\pi}{3} & \cos\frac{2\pi}{3} \end{pmatrix} &= 3 \end{aligned}$$

המטריצה A מייצגת טרנספורמציה ליניארית של סיבוב ב-$\frac{2\pi}{3}$ ולכן $A^3 = I$.

$$\mathrm{ord}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} = \infty$$

כי

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}^k = \begin{pmatrix} 1 & 0 \\ 0 & 2^k \end{pmatrix}$$

גם ב-$SL_2(\mathbb{R})$ יש מטריצה מסדר ∞:

$$A = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 2 \end{pmatrix}$$

G סופית כלשהי. לכל $a \in G$

$$\operatorname{ord}(a) < \infty$$

$$|\langle a \rangle| = \operatorname{ord}(a) < \infty$$

ממשפט לגרנז' נובע שהסדר של כל תת חבורה מחלק את החבורה, ולכן

$$\operatorname{ord}(a) \mid |G|$$

מסקנה 3.23 אם G חבורה סופית ו-$|G| = N$ אז לכל $a \in G$

$$a^N = 1$$

הוכחה: $\operatorname{ord}(a) = k$, $k \mid N$ ולכן קיים l כך ש-$kl = N$ ואז

$$a^N = a^{kl} = 1^l = 1$$

■

3.6.3 המשפט הקטן של פרמה

$G = \mathbb{Z}_p^*$ כאשר p ראשוני. נקח $a \in \mathbb{Z}_p \setminus 0$ אז

$$a^{|G|} = 1$$

כלומר

$$a^{p-1} \equiv 1 \pmod{p}$$

זוהי הוכחה אלטרנטיבית למשפט הקטן של פרמה

3.6.4 המשפט הקטן של פרמה עבור מספר לא ראשוני

$\mathbb{Z}_n^* = \{1 \le k < n : (k,n) = 1\}$. חבורת כל השאריות הזרות ל-n.

$$|\mathbb{Z}_n^*| = \phi(n) = \prod_{i=1}^{t} \left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right)$$

כאשר

$$n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$$

אז לכל $a \in \mathbb{Z}_n^*$ $(a,n) = 1$

$$a^{|\mathbb{Z}_n^*|} = 1$$

כלומר

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

3.6.5 מציאת מספרים ראשוניים ענקיים

יהי n ענק. האם n ראשוני?
נעביר את n את המבחן הבא: ניקח $1 < a < n$ ונחשב את

$$a^{n-1} \left(\mathrm{mod} n\right)$$

ניתן לבצע פעולה זו במהירות ($O\left(\log_a n\right)$) אם התוצאה לא שקולה לאחד:

$$a^{n-1} \not\equiv a^{n-1} \left(\mathrm{mod} n\right)$$

אז n איננו ראשוני.
אם n עובר את המבחן, בוחרים a אחר וחוזרים על התהליך.
אם n עבר 40 מבחנים אומרים עליו שהוא מתחזה יוצא מן הכלל לראשוני (אם לא ראשוני ממש).

3.6.6 חישובי סדר ב-$\mathbb{Z}_n$

יהא $k \in \mathbb{Z}_n$.

$$\mathrm{ord}\left(0\right) = 1$$

$$k \mid n \implies \mathrm{ord}\left(k\right) = \frac{n}{k}$$

3.6.7 תכונות סדר של איבר

אם $x^k = 1$ אז $d = \mathrm{ord}\left(x\right) \mid k$.
הוכחה: $k = qd + r$, $0 \leq r < d$ אז

$$1 = x^k = x^{qd} x^r = x^r$$

ולכן $r = 0$ ו-$d \mid k$. ■

3.6.8 סדרים של איברים ב-C_n החבורה הנוצרת ע"י איבר

$$\begin{aligned} \mathrm{ord}\left(1\right) &= 1 \\ \mathrm{ord}\left(a\right) &= n \\ \mathrm{ord}\left(a^i\right) &= ? \end{aligned}$$

טענה 3.24 $\mathrm{ord}\left(a^i\right) = \frac{n}{(n,i)}$

הוכחה: נסמן $b = \mathrm{ord}\left(a^i\right)$. נחשב את

$$\left(a^i\right)^{\frac{n}{(i,n)}} = a^{\frac{in}{(i,n)}} = \left(a^n\right)^{\frac{i}{(i,n)}}$$

מכיוון ש-$\frac{i}{(i,n)}$ הוא שלם נקבל:

$$\left(a^i\right)^{\frac{n}{(i,n)}} = 1$$

לכן

$$d \mid \frac{n}{(i,n)}$$

מצד שני

$$\left(a^i\right)^d = a^{id} = 1$$

לכן

$$n \mid id = (i,n)\,\frac{i}{(i,n)}d$$

מכיוון ש-n זר ל-$\frac{i}{(i,n)}$

$$n \mid (i,n)\,d$$

ולכן $n \leq (i,n)\,d$ ולכן

$$d \geq \frac{n}{(i,n)}$$

ואז $d = \frac{n}{(i,n)}$ ■

טענה 3,25 קבוצת האיברים ב-C_n שסדרן הוא בדיוק d $(d \mid n)$ היא

$$\left\{a^{\frac{n}{d}\cdot k}\right\}$$

כאשר $k \in \mathbb{Z}_d^*$ כלומר k זר ל-d.

הוכחה: נסמן $m = \operatorname{ord}\left(a^{\frac{n}{d}k}\right)$. ראשית $\left(a^{\frac{n}{d}\cdot k}\right)^d = a^{nk} = 1$ ולכן $\operatorname{ord}\left(a^{\frac{n}{d}k}\right) \leq d$.
נשים לב ש-$(k,d) = 1$. אז

$$a^{\frac{n}{d}km} = 1$$

ולכן

$$\begin{aligned} n &\mid \frac{n}{d}km \\ nt &= \frac{n}{d}km \\ dt &= km \end{aligned}$$

ומכיוון ש-k ו-d זרים $d \mid m$ ומכיוון ש-$m \leq d$, $d = m$.
בכיוון השני אם $\operatorname{ord}\left(a^i\right) = d$ אז

$$d = \frac{n}{(i,n)}$$

$$(i,n) = \frac{n}{d}$$

$$i = \frac{i}{(i,n)}\,(i,n) = \frac{n}{d}\frac{i}{(i,n)}$$

אבל מספר זה הוא בוודאי זר ל-d כי אחרת (i,n) היה גדול יותר. ■

דוגמה $d = n$
איברים מסדר n הם

$$\{a^k : k \in \mathbb{Z}_n^*\}$$

מספר האיברים מסדר d הוא

$$|\mathbb{Z}_d^*| = \varphi(d)$$

3.6.9 מהן תתי החבורות של C_n?
$H < C_n$, $d = |H| \mid n$.

טענה 3.26 $H = \left\langle a^{\frac{n}{d}} \right\rangle$ היא תת-החבורה היחידה של C_n מסדר d.

הוכחה: ברור ש-H היא תת חבורה של C_n.
תהי H_1 תת חבורה מסדר d הנוצרת ע"י

$$H_1 = \left\langle a^{\frac{n}{d}k} \right\rangle$$

אז $H \ni a^{\frac{n}{d}}$ ולכן $H_1 \subset H$ אבל $|H| = |H_1| = d$ ולכן $H_1 = H$. כלומר לכל $d \mid n$ היא $\left\{a^{\frac{n}{d}i}; 0 \leq i < d\right\}$ הת"ח היחידה של C_n מסדר d. ■

מסקנה 3.27 משפט הסכום

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

דוגמה

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(6) = 1 + 1 + 2 + \varphi(2)\varphi(3) = 6$$

הוכחה: $|C_n| = n$ אבל n שווה לסכום האיברים מכל סדר שמתחלק ב-n, כלומר

$$n = \sum_{d|n} |\{k : (k, d) = 1\}| = \sum_{d|n} \varphi(d)$$

■

3.7 חבורות התמורות על $\{1, \ldots, n\}$ - S_n

$$|S_n| = n!$$

דוגמה לתמורה:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

כל תמורה ניתנת ליצוג ע"י גרף שקודקודיו הן $\{1, \ldots, n\}$ ומכיל קשת מצומת שהתמורה מעתיקה לתמונה שלה. גרף זה יכיל קשת נכנסת אחת וקשת יוצאת אחת לכל תמורה, ויהיה למעשה איחוד של מעגלים זרים.
בהנתן סדרה $(i_1, \ldots, i_k)$ של איברים מתוך $\{1, \ldots, n\}$ נבנה המתאימה את i_2 ל-i_1, את i_3 ל-i_2 וכן הלאה בצורה מעגלית, ואת כל הצמתים שאינם במעגל היא מתאימה לעצמם. תמורה כזו נקראת מחזור.

3.7.1 פירוק של תמורה למחזורים

ניתן להציג כל תמורה כמכפלת מחזורים שמופיעים בה. לדוגמה:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} = (1\,3\,5)\,(2\,4)$$

באופן כללי אם בתמורה σ מופיעים המחזורים $C_1, \ldots, C_k$ אזי

$$\sigma = C_1 \cdots C_k$$

מעניין לראות שאין חשיבות לסדר מכפלת המחזורים $C_1, \ldots, C_k$:
אם t הוא מספר המחזור המכיל את i, אז כל שאר המחזורים מתאימים את i לעצמו וגם את $C_t(i)$ לעצמו, ולכן

$$C_1 \cdots C_k(i) = C_t(i) = \sigma(i)$$

דוגמה

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 3 & 5 & 8 & 1 & 6 & 4 \end{pmatrix} = (1\,7\,6)\,(2)\,(3)\,(4\,5\,8)$$

את המחזורים באורך 1 אין צורך לרשום ולכן

$$\sigma = (1\,7\,6)\,(4\,5\,8)$$

3.7.2 פונקצית הסימן של תמורה.

הגדרה 3.28 פונקצית הסימן של תמורה σ

$$\mathrm{Sg}\sigma = (-1)^{\#(i,j):\ \begin{matrix} i<j & i>j \\ \sigma(i)>\sigma(j) & \sigma(i)<\sigma(j) \end{matrix}\ \}}$$

טענה 3.29 ניתן לחשב את הסימן על ידי

$$\mathrm{Sg}\sigma = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

הוכחה: ברור שהסימן של $\prod_{1 \le i < j \le n} \frac{\sigma(j)-\sigma(i)}{j-i}$ שווה לסימן של התמורה, ע"פ ההגדרה של סימן התמורה.
צריך להראות ש-$\left|\prod_{1 \le i < j \le n} \frac{\sigma(j)-\sigma(i)}{j-i}\right| = 1$.
אבל זה מתקיים כי כל מה שמופיע במונה מופיע במכנה ולהיפך (עוברים על כל הזוגות). ■

3.7.3 חישוב זוגיות

$$\mathrm{Sg}(id) = (-1)^0 = 1$$

$$\begin{aligned} \mathrm{Sg}((1\,2)) &= (-1)^1 = -1 \\ \mathrm{Sg}((1\,2\,3\,4)) &= (-1)^3 = -1 \\ \mathrm{Sg}((1\,2\,\cdots\,k)) &= (-1)^{k-1} \end{aligned}$$

מספר הזוגות שמחליפים יחס הוא מספר הקווים שנחתכים עם מסדרים את המספרים של התמורה בשתי שורות ומותחים קו בין כל מספר לעצמו.

טענה 3.30 לכל $\sigma, \tau \in S_n$

$$\mathrm{Sg}(\sigma\tau) = \mathrm{Sg}\sigma \cdot \mathrm{Sg}\tau$$

לפי ההגדרה

$$\begin{aligned}
\mathrm{Sg}(\sigma\tau) &= \prod_{\{i,j\}} \frac{\sigma\tau(j) - \sigma\tau(i)}{j-i} \\
&= \prod_{\{i,j\}} \frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)} \cdot \frac{\tau(j) - \tau(i)}{j-i} \\
&= \prod_{\{i,j\}} \frac{\sigma\tau(j) - \sigma\tau(i)}{\tau(j) - \tau(i)} \prod_{\{i,j\}} \frac{\tau(j) - \tau(i)}{j-i}
\end{aligned}$$

לכן זוג $\{i,j\}$ ניתן להתאים זוג יחיד $\{\tau(i), \tau(j)\}$ ולכן

$$\mathrm{Sg}\sigma\tau = \mathrm{Sg}\sigma \cdot \mathrm{Sg}\tau$$

3.7.4 לישר את התמורה

ע"י החלפת זוג איברים בשורה התחתונה של σ מנסים להגיע לתמורת הזהות. נסמן ב-(i_1, j_1) את הזוג הראשון עד (i_n, j_n) הזוג האחרון שמביא אותנו לתמורת הזהות. ניתן לעשות זאת תמיד בעזרת לכל היותר m צעדים.

טענה 3.31 הסימן של σ הוא $(-1)^m$. כלומר לא משנה בכמה צעדים מגיעים לתמורת הזהות, $(-1)^m$ יהיה הסימן של σ.

הוכחה: נראה מה הקשר בין התמורה σ לתמורה שהתקבלה לאחר חילוף אחד.

$$\begin{aligned}
\sigma_1 &= (i_1\, i_1)\,\sigma \\
\sigma_2 &= (i_2\, i_2)\,(i_1\, i_1)\,\sigma \\
&\vdots \\
\sigma_m &= (i_m\, i_m)\cdots(i_1\, i_1)\,\sigma \\
&= id
\end{aligned}$$

לכן

$$\sigma = (i_1\, i_1)\cdots(i_m\, i_m)$$

$$\mathrm{Sg}\sigma = \prod_{k=1}^{m} \mathrm{Sg}(i_k\, i_k) = (-1)^m$$

■

3.8 תת חבורות נורמליות וחבורות מנה

$H < G$ ו-G חבורה תת חבורה. קוסטים שמאליים של H ב-G הם קבוצות מהצורה

$$gH = \{gh : h \in H\}$$

נסתכל על אוסף הקוסטים $\{gH : g \in G\}$. ראינו שלמשל אם $G = \mathbb{Z}$ ו-$H = n\mathbb{Z}$ אז אוסף הקוסטים

$$\{k + n\mathbb{Z} : k = \mathbb{Z}\} = \{k + n\mathbb{Z} : 0 \leq k \leq n - 1\}$$

נסתכל על אוסף הקוסטים ונבדוק האם נוכל להגדיר עליו פעולה של חבורה.

הגדרה 3.32 אם $A, B \subset G$ נגדיר

$$A \cdot B = \{ab : a \in A, b \in B\}$$

הגדרה טבעית לפעולת כפל הקוסטים תהיה

$$g_1H \cdot g_2H = \{g_1h_1 \cdot g_2h_2 : \ h_1, h_2 \in H\}$$

מתי תוצאה זו היא קוסט לכל g_1, g_2?
נניח שכן, אז בפרט

$$H \cdot gH = g_3H$$

אבל $gH \subset H \cdot gH$ ($1 \in H$) ולכן

$$gH \subset g_3H$$

מסקנה: $g_3H = gH$.
מצד שני

$$Hg \subset HgH$$

אבל ($1 \in H$ שוב כי)

$$HgH = g_3H = gH$$

ולכן אם נכפול משמאל ב-g^{-1} נקבל

$$g^{-1}Hg \subset H \quad \forall g \in G$$

מכיוון שזה נכון לכל g זה נכון גם עבור g^{-1} ואז

$$gHg^{-1} \subset H$$

ואם נכפול משמאל ב-g^{-1} ומימין ב-g נקבל:

$$g^{-1}Hg \supset H \quad \forall g \in G$$

והמסקנה היא ש-

$$gHg^{-1} = H$$

לכל $g \in G$.

הגדרה 3.33 $H < G$ המקיימת $gHg^{-1} = H$ לכל $g \in G$ נקראת נורמלית, ואנחנו מסמנים $H \lhd G$.

טענה 3.34 נניח ש-$H \lhd G$. נגדיר פעולה על אוסף הקוסטים $\frac{G}{H} = \{gH : g \in G\}$ ע"י

$$g_1H \circ g_2H = g_1H \cdot g_2H$$

אז $\frac{G}{H}$ מהווה חבורה, הנקראת חבורת המנה, ומתקיים

$$g_1Hg_2H = g_1g_2H$$

הוכחה: ע"פ הגדרת כפל קוסטים

$$g_1Hg_2H = g_1g_2\left(g_2^{-1}Hg_2\right)H$$

אמנם יתכן שעבור איבר h מסויים יתקיים $g_2^{-1}hg_2 \neq h$ אבל כקבוצה יתקיים $g_2^{-1}Hg_2 = H$ ולכן

$$g_1Hg_2H = g_1g_2HH = g_1g_2H$$

■

נראה שמתקיימות תכונות החבורה:

1. קשירות הראנו למעלה.
2. אסוציאטיביות נכונה בגלל תכונת האסוציאטיביות בחבורה G עצמה.

$$\begin{aligned}(g_1Hg_2H)\,g_3H &= (g_1g_2H)\,g_3H = (g_1g_2)\,g_3H \\ &= g_1\,(g_2g_3)\,H = g_1H\,(g_2g_3)\,H = g_1H\,(g_2Hg_3H)\end{aligned}$$

3. איבר היחידה הוא H.

$$HgH = gH$$

4. איבר הופכי

$$(gH)^{-1} = g^{-1}H$$

כי

$$(gH)^{-1}\,gH = g^{-1}HgH = g^{-1}gH = H$$

דוגמאות

1. $G = C_6 = \{1, x, \ldots, x^5\}$, ו-$H = \{1, x^2, x^4\}$
האם $H \lhd G$? צריך לבדוק האם $\forall g : gHg^{-1} = H$. מכיוון שהחבורה הציקלית קומוטטיבית,

$$\{ghg^{-1} : h \in H\} = \{gg^{-1}h : h \in H\} = H$$

באופן כללי, אם G אבלית, אז כל חבורה חלקית היא נורמלית.
מהי חבורת המנה?

$$\frac{G}{H} = \{H, xH\}$$

הגודל של החבורה שווה לאינדקס של H ב-G:

$$\left|\frac{G}{H}\right| = (G:H) = \frac{|G|}{|H|} = 2$$

נסמן $gH = \bar{g}$.

$$\bar{x}^2 = xHxH = x^2H = \overline{x^2} = \bar{1}$$

(כי $x^2 \in H$).

2. $G = GL_2(\mathbb{R})$, $H = SL_2(\mathbb{R})$. החבורה G איננה אבלית. בכל זאת $H \lhd G$. תהא $A \in H$, ויהא $g \in G$. צריך להראות ש-

$$gAg^{-1} \in H$$

$$\begin{aligned}\det\left(gAg^{-1}\right) &= |g|\,|A|\left|g^{-1}\right| = |g|\left|g^{-1}\right|\,|A| \\ &= \det\left|gg^{-1}\right| \cdot 1 = 1\end{aligned}$$

חבורת המנה

$$\frac{GL_2(\mathbb{R})}{SL_2(\mathbb{R})} = \left\{\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} SL_2(\mathbb{R}) : x \in \mathbb{R}^*\right\}$$

ואז

$$\overline{\begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix}} = \overline{\begin{pmatrix} xy & 0 \\ 0 & 1 \end{pmatrix}}$$

אפשר לזהות חבורת מנה זו עם $(\mathbb{R}^*, \cdot)$.

3. החבורה הדיהידרלית D_n.

$$D_3 = \{id, (12), (13), (23), (123), (132)\}$$

$$H = \{id, (12)\}$$

$H < G$. האם היא נורמלית? נראה שהיא לא נורמלית:
נקח את $S = (12)$ ואת $R = (123)$ אז

$$RSR^{-1} = SR^{-1} \cdot R^{-1} = SR^{-2} \notin H$$

נסתכל על תת חבורת הסיבובים

$$N = \left\{I, R, R^2\right\}$$

צ"ל

$$gNg^{-1} \subset N$$

ברור ש-

$$R^i N R^{-i} = N$$

מכיוון ש-N היא חבורת סיבובים ולכן היא ציקלית.

$$SR^iS^{-1} = SR^iS = R^{-i} \in N$$

4. $G = S_n$, $H = A_n$ היא חבורת התמורות הזוגיות.
H נורמלית כי

$$\mathrm{Sg}\left(\tau\sigma\tau^{-1}\right) = \mathrm{Sg}\left(\tau\right)\mathrm{Sg}\left(\sigma\right)\mathrm{Sg}\left(\tau^{-1}\right) = \mathrm{Sg}\left(\sigma\right) = 1$$

$$\frac{S_n}{A_n} = \{A_n, (12)\,A_n\}$$

$$(S_n : A_n) = 2$$

נראה שכל איבר שמקיים $\mathrm{Sg}\left(\sigma\right) = -1$ שייך ל-$(12)\,A_n$:

$$\begin{aligned} \mathrm{Sg}\left((12)\,\sigma\right) &= -1 \cdot -1 = 1 \\ (12)\,\sigma &\in A_n \\ \sigma &\in (12)\,A_n \end{aligned}$$

3.9 הומומורפיזם

הומומורפיזם בין החבורות G ל-H היא העתקה $\phi : G \to H$ המקיימת

$$\phi\left(xy\right) = \phi\left(x\right)\phi\left(y\right) \quad \forall x, y \in G$$

מסקנות:

1. $\phi\left(1\right) = 1$ כי

$$\begin{aligned} \phi\left(1\right) &= \phi\left(1 \cdot 1\right) = \phi\left(1\right)\phi\left(1\right) \\ 1 &= \phi\left(1\right) \end{aligned}$$

2. $\phi\left(x^{-1}\right) = \left(\phi\left(x\right)\right)^{-1}$ כי

$$\phi\left(x\right)\phi\left(x^{-1}\right) = \phi\left(xx^{-1}\right) = \phi\left(1\right) = 1$$

דוגמאות

1. $\phi : G \to H$, $\phi\left(x\right) = 1$
זוהי הומומורפיזם כי

$$1 = \phi\left(xy\right) = 1 \cdot 1 = \phi\left(x\right)\phi\left(y\right)$$

2. $\phi : \mathbb{Z} \to \mathbb{Z}$, $\phi\left(x\right) = x$, וזוהי הומומורפיזם כי

$$\phi\left(xy\right) = xy = \phi\left(x\right)\phi\left(y\right)$$

3. $\phi(x) = 5x$, החבורה היא $\mathbb{Z}$ עם פעולת החיבור.

$$\phi(x+y) = 5(x+y) = 5x + 5y = \phi(x) + \phi(y)$$

4. $\phi : S_n \to \{\pm 1\}$

$$\begin{aligned} \phi(\sigma) &= \operatorname{Sg}(\sigma) \\ \phi(\sigma\tau) &= \operatorname{Sg}(\sigma\tau) = \operatorname{Sg}(\sigma)\operatorname{Sg}(\tau) = \phi(\sigma)\phi(\tau) \end{aligned}$$

5. $\phi(A) = \det A$, $\phi : GL_n(\mathbb{R}) \to \mathbb{R}^*$

$$\det AB = \det A \det B$$

6. $G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, c \neq 0 \right\}$, $H = (R^* \times R^*, \cdot)$ (כאשר $(x,y)\cdot(x',y') = (xx', yy')$).

$$\phi : G \to H$$

$$\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = (a, c)$$

נבדוק האם זהו הומומורפיזם:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix} = \begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}$$

$$\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right)\phi\left(\begin{pmatrix} a' & b' \\ 0 & c' \end{pmatrix}\right) = (a,c)(a',c') = (aa', cc') = \phi\left(\begin{pmatrix} aa' & ab' + bc' \\ 0 & cc' \end{pmatrix}\right)$$

ולכן זוהי הומומורפיזם.

7. $\phi(x) = x^2$, $\phi : \mathbb{Z} \to \mathbb{Z}$. זוהי איננה הומומורפיזם כי בדרך כלל $(x+y)^2 \neq x^2 + y^2$.

3.9.1 סיווג הומומורפיזם

$\phi : G \to H$ הומו' תקרא

1. מונומורפיזם אם ϕ חח"ע.
2. איזומורפיזם אם ϕ חח"ע ועל.

אם קיים איזומורפיזם $\phi : G \to H$ נסמן $G \cong H$

דוגמה החבורה מודולו n היא איזומורפית לחבורה הציקלית מסדר n.

$$\mathbb{Z}_n \cong C_n = \langle x \rangle$$

ע"י ההעתקה

$$\phi(k) = x^k$$

מכיוון ש-

$$\phi(k+l) = x^{k+l} = x^k x^l = \phi(k)\phi(l)$$

3.9.2 תכונות הומומורפיזם

$\phi : G \to H$
נסמן את התמונה של G

$$\phi(G) = \{\phi(g) : g \in G\}$$

טענה 3.35 $\phi(G) < H$. התמונה של G היא תת חבורה של H

הוכחה: צ"ל לכל $y, z \in \phi(G)$ $yz^{-1} \in \phi(G)$.

$$yz^{-1} = \phi(g_1)\phi(g_2)^{-1} = \phi(g_1)\phi\left(g_2^{-1}\right) = \phi\left(g_1 g^{-1}\right) \in \phi(G)$$

■

3.9.3 גרעין של הומומורפיזם

$$\ker\phi = \{g \in G : \phi(g) = 1\}$$

טענה 3.36 $\ker\phi \lhd G$

הוכחה: יהיו $g_1, g_2 \in \ker\phi$, וצריך להוכיח ש-$g_1 g_2^{-1} \in \ker\phi$:

$$\phi\left(g_1 g_2^{-1}\right) = \phi(g_1)\phi(g_2)^{-1} = 1 \cdot 1 = 1$$

■

נורמליות: צ"ל אם $g \in \ker\phi$ ו-$x \in G$ כלשהו, אז $xgx^{-1} \ni \ker\phi$.
הוכחה:

$$\phi\left(xgx^{-1}\right) = \phi(x)\phi(g)\phi(x)^{-1} = \phi(x)\phi(x)^{-1} = 1$$

■

מכיוון שהגרעין של ϕ נורמלי ב-G ניתן ליצור את חבורת המנה $\frac{G}{\ker\phi}$.

3.9.4 משפט האיזומורפיזם הראשון

משפט 3.37 נניח ש-$\phi : G \to H$ היא על. אזי $\frac{G}{\ker\phi} \cong H$, כלומר חבורת המנה של הגרעין של ϕ ב-G היא איזומורפית לחבורת היעד של ההומומורפיזם.
באופן כללי יותר, לכל $\phi : G \to H$ (גם אם היא איננה על) מתקיים

$$\frac{G}{\ker\phi} \cong \phi(G)$$

בפרט אם G סופית $|\phi(G)| = \left|\frac{G}{\ker\phi}\right|$, ו-$|G| = |\ker\phi|\,|\phi(G)|$.

הוכחה: נגדיר ההעתקה מחבורת המנה לתמונה של G ב-H:

$$\ker\phi = N \lhd G \qquad \tilde{\phi} : \frac{G}{\ker\phi} \to \phi(G)$$

$$\tilde{\phi}(gN) = \phi(g)$$

נראה ש-$\tilde{\phi}$ מוגדרת היטב, כלומר שאם $gN = g'N$ מתקיים $\phi(g') = \phi(g)$, כלומר ההתאמה לא תלויה במייצג של הקוסט.
אם $gN = g'N$ אז $g' \in gN$ כלומר קיים n כך ש-$g' = gn$ ואז

$$\phi(g') = \phi(gn) = \phi(g)\phi(n) = \phi(g) \cdot 1 = \phi(g)$$

נראה ש-$\tilde{\phi}$ היא הומומורפיזם:
יהיו g_1N ו-g_2N איברים בחבורת המנה $\frac{G}{N}$, ונוכיח ש-

$$\tilde{\phi}(g_1N \cdot g_2N) = \tilde{\phi}(g_1N)\,\tilde{\phi}(g_2N)$$

אבל

$$\tilde{\phi}(g_1N \cdot g_2N) = \tilde{\phi}(g_1g_2N) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \tilde{\phi}(g_1N)\,\tilde{\phi}(g_2N)$$

נראה ש-$\tilde{\phi}$ היא על:
יהי $x = \phi(g)$ אז $x = \tilde{\phi}(gN)$, כלומר $\tilde{\phi}$ היא על.
נראה ש-$\tilde{\phi}$ חח"ע:
נניח ש-$g_1N \neq g_2N$ ונוכיח ש-$\tilde{\phi}(g_1N) \neq \tilde{\phi}(g_2N)$, כלומר $\phi(g_1) \neq \phi(g_2)$.
נניח בשלילה שעבור $g_1N \neq g_2N$ מתקיים $\phi(g_1) = \phi(g_2)$. אז

$$\phi\left(g_1^{-1}g_2\right) = \phi(g_1)^{-1}\phi(g_2) = 1$$

כלומר $g_1^{-1}g_2 \in \ker\phi = N$ ואז $g_1N = g_2N$. ■

טבלה 2: דוגמאות לשימוש במשפט האיזומורפיזם הראשון

G	H	ϕ	$\ker\phi$	$\frac{G}{\ker\phi}$	$\phi(G)$
G	H˜	$\phi(g) = 1$	G	$\frac{G}{G}$	$\{1\}$
$\mathbb{Z}$	$\mathbb{Z}$	$\phi(n) = 3n$	$\{0\}$	$\frac{\mathbb{Z}}{\{0\}} = \mathbb{Z}$	$3\mathbb{Z}$
$\mathbb{Z}_{10}$	$\mathbb{Z}_5$	$\phi(x) = x \pmod 5$	$\{0,5\}$	$\frac{\mathbb{Z}_{10}}{\{0,5\}}$	$\mathbb{Z}_5$
$GL_n(\mathbb{R})$	$\mathbb{R}^*$	$\phi(x) = \det x$	$SL_n(\mathbb{R})$	$\frac{GL_n(\mathbb{R})}{SL_n(\mathbb{R})}$	$\mathbb{R}^*$
S_n	$\{\pm 1\}$	$\phi(\sigma) = \mathrm{Sg}(\sigma)$	A_n	$\frac{S_n}{A_n}$	$\{\pm 1\}$
$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : ac \neq 0$	$\mathbb{R}^* \times \mathbb{R}^*$	$\phi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = (a,c)$	$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R}$	$\frac{G}{\ker\phi}$	$\mathbb{R}^* \times \mathbb{R}^*$
$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{R}$	$(\mathbb{R},+)$	$\phi\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = b$	$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	G	$(\mathbb{R},+)$

צריך להראות שהשורה האחרונה בכלל מתארת הומומורפיזם:

$$\phi\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix}\right) = \phi\left(\begin{pmatrix} 1 & bb' \\ 0 & 1 \end{pmatrix}\right) = bb' = \phi\left(\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}\right)\phi\left(\begin{pmatrix} 1 & b' \\ 0 & 1 \end{pmatrix}\right)$$

שימוש

טענה 3.38 G חבורה אבלית ו-$p \mid |G|$ אז G מכילה איבר מסדר p.

הוכחה: אינדוקציה על $|G|$.
עבור $|G| = 1$ הטענה נכונה כי G מכילה את 1.
עבור $|G| > 1$ נבחר $G \ni x \neq 1$. אם הסדר של x מתחלק ב-p אז

$$\operatorname{ord}(x) = kp$$

אז

$$\operatorname{ord}\left(x^k\right) = p$$

וסיימנו.
אחרת $|\langle x\rangle| = \operatorname{ord}(x) = m$ ו-p איננו מחלק את m ($p \not| m$).
מן האבליות נובע ש-

$$N = \langle x\rangle \lhd G$$

ונוכל להתבונן בחבורת המנה $\frac{G}{N} = H$.

$$|H| = \frac{|G|}{|N|}$$

אבל $(|N|, p) = 1$ ו-$p \mid |G|$ ולכן $p \mid |H|$.
$|H| < |G|$ כי $|N|$ איננו אחד (בחרנו איבר x שאיננו איבר היחידה). לכן על פי הנחת האינדוקציה קיים איבר ב-$z \in H$ שסדרו בדיוק p.
$z = yN$ קוסט כלשהו בחבורת המנה ($y \in G$).

$$\begin{aligned}
\operatorname{ord}(z) &= p \\
z^p &= 1 = N \\
(yN)^p &= N \\
y^p N &= N \\
y^p &\in N
\end{aligned}$$

ממשפט לגרנז' נובע

$$\begin{aligned}
(y^p)^{|N|} &= 1 \\
\left(y^{|N|}\right)^p &= 1
\end{aligned}$$

יש להראות ש-$y^{|N|} \neq 1$: נניח בשלילה ש-$y^{|N|} = 1$, אז

$$z^{|N|} = y^{|N|}N = 1N$$

כלומר הסדר של z מחלק את $|N|$. אבל בחרנו את z כך ש-$\operatorname{ord}(z) = p$ ואז $p \mid |N|$ וזו סתירה.

$$\operatorname{ord}\left(y^{|N|}\right) = p$$

ומצאנו איבר מסדר p ב-G. ■

3.9.5 אוטומורפיזם

הגדרה 3.39 איזומוריפזם $\phi : G \to G$ נקראת אוטומופריזם.

3.10 משפט קיילי

משפט 3.40 לכל חבורה סופית G מסדר n קיימת תת חבורה H של S_n כך ש-G איזומורפית ל-H.

דוגמה עבור $G = C_4$ קיימת $C_4 \cong H < S_4$. נבחר למשל את $H = \langle (1,2,3,4) \rangle$.
הוכחה: נגדיר $\phi : G \to S_n$ באופן הבא:
אם $G = \{g_1, \ldots, g_n\}$ נחשוב על S_n כעל חבורת התמורות על איברי G.

$$G \ni g \quad \phi(g) = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ gg_1 & gg_2 & \cdots & gg_n \end{pmatrix}$$

זוהי תמורה, כי אם $gg_i = gg_j$ היינו מקבלים $g_i = g_j$ וזו סתירה.
ניתן להסתכל על התמורה $\phi(g)$ כפונקציה על G שמעתיקה את g' ל-gg'

$$\phi(g)(g') = gg'$$

נוכיח ש-ϕ הומומורפיזם - $\phi(gh) = \phi(g)\phi(h)$

$$g' \in G \quad \phi(gh)(g') = (gh)g' = g(hg') = \phi(g)(hg') = \phi(g)(\phi(h)(g')) = (\phi(g) \cdot \phi(h))(g')$$

ולכן $\phi(gh) = \phi(g)\phi(h)$ וההעתקה ϕ היא הומומורפיזם.
נראה ש-ϕ חח"ע. ממשפט האיזומורפיזם הראשון נובע ש-

$$\frac{G}{\ker \phi} \cong \phi(G) \subset S_n$$

ולכן מספיק להראות ש-$\ker \phi = \{1\}$ (ואז $G \cong \phi(G)$).
נקח $g \neq 1$ ונראה ש-$\phi(g) \neq id$ איננו תמורת הזהות.

$$\phi(g)(1) = g \neq 1$$

ולכן $\phi(g)$ איננה תמורת הזהות. לכן $\ker \phi = \{1\}$. ו-$G \cong \phi(G)$. ■

3.10.1 שימושים למשפט קיילי

תהא $H < G$ תת חבורה כלשהי. נסתכל באוסף הקוסטים $\{gH : g \in G\}$, אז

$$|\{gH : g \in G\}| = (G : H) = m$$

נגדיר העתקה

$$\phi : G \to S_m$$

מהחבורה G לחבורת התמורות מעל הקוסטים $\{gH\}$.

$$\phi(g)(g'H) = gg'H$$

ϕ היא הומו' בדומה להוכחת משפט קיילי כי

$$\phi(gh)(g'H) = ghg'H = (\phi(g) \cdot \phi(h))(g'H)$$

נתבונן בגרעין של ϕ:

- $\ker \phi \lhd G$
- אם $\phi(g) = id$ אז

$$\phi(g)(H) = gH = id(H) = H$$

ולכן

$$g \in H$$

כלומר הגרעין של ϕ מוכל ב-H.

מסקנות

1. p ראשוני ו-$|G| = p$ ולכן $G \cong C_p$ כי נקח $x \neq 1 \in G$ אז $\operatorname{ord}(x) = k$. $1 < k \mid p$ ולכן $k = p$.
2. $|G| = p^2$, $G = C_{p^2}$.

$$C_p \times C_p = \left\{ \left(x^i, x^j \right) : 0 \leq i, j \leq p-1 \right\}$$

טענה 3.41 אם $|G| = p^2$ אז G אבלית.

הוכחה: נבחר $1 \neq x \in G$. אם $\operatorname{ord}(x) = p^2$ אז $G = C_{p^2}$ וסיימנו.
נניח בה"כ שלכל $1 \neq x \in G$ $\operatorname{ord}(x) = p$. נסתכל בחבורה הציקלית H הנוצרת ע"י x כלשהו, אז $|H| = p$.
נסתכל בהעתקה

$$\phi : G \to S_{(G:H)} = S_p$$

העתקה מ-G לאוסף הקוסטים gH. ידוע לנו ממשפט האיזומורפיזם הראשון ש-

$$\frac{G}{\ker \phi} \cong K \subset S_p$$

וכמו כן $\ker \phi \subset H$. בגלל שהסדר של H הוא ראשוני יש רק שתי אפשרויות לגרעין: ■

1. $\ker \phi = \{1\}$
2. $\ker \phi = H$

האפשרות הראשונה לא תתכן כי אחרת היה מתקבל $G \cong K < S_p$ ואז $|S_p| = p! \mid |K| = |G| = p^2$ ולא יתכן ש-$p^2 \mid p!$.
לכן $H = \langle x \rangle \lhd G \quad \forall x \in G$.
נקח $x, y \in G$ ונראה ש-$xy = yx$.
אם $\langle y \rangle = \langle x \rangle$ אז ברור ש-$xy = yx$ (שניהם איברים באותה תת חבורה ציקלית ואבלית).
אחרת $\langle y \rangle \cap \langle x \rangle = \{1\}$ כי הסדר של $\langle x \rangle$ ושל $\langle y \rangle$ הוא ראשוני והסדר של כל תת חבורה שלהם צריכה לחלק את p.

$$x \left(yx^{-1}y^{-1} \right) = \left(xyx^{-1} \right) y^{-1}$$

$\langle y \rangle$ נורמלית ב-G ולכן $xyx^{-1} \in \langle y \rangle$ ו-$\langle x \rangle$ נורמלית ב-G ולכן $\left(yx^{-1}y^{-1} \right) \in \langle x \rangle$. אבל האיבר היחידה שמשותף לשתי החבורות הוא 1 ולכן

$$\begin{aligned} xyx^{-1}y^{-1} &= 1 \\ xy &= yx \end{aligned}$$

ו-G אבלית.

3.11 חבורות p

- חבורת p היא חבורה מסדר p^n כאשר p ראשוני.
- חבורות מסדר p^2: $\mathbb{Z}_{p^2}$ ו-$\mathbb{Z}_p \times \mathbb{Z}_p$.
- חבורות מסדר p^3: $\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$.

כל הדוגמאות למעלה הן חבורות אבליות.
דוגמה לחבורה לא אבלית מסדר p^3 היא חבורת Heisenberg:

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z}_p \right\}$$

עם פעולת כפל מטריצות:

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & y+az+b \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{pmatrix}$$

G סגורה לכפל והיא תת קבוצה של חבורת המטריצות ההפיכות לכן היא חבורה.
אבל

$$\begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+a & b+xc+y \\ 0 & 1 & z+c \\ 0 & 0 & 1 \end{pmatrix}$$

ולכן G איננה אבלית.
נמצא את ההפכי של מטריצה A:

$$\begin{cases} a+x &= 0 \\ b+cx+y &= 0 \\ c+z &= 0 \end{cases} \Rightarrow \begin{cases} x &= -a \\ z &= -c \\ y &= ac-b \end{cases}$$

$$A^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

נחשב את $Z(G)$ המרכז של G:

$$\forall X \in G \qquad AX = XA \Leftrightarrow A \in Z(G)$$

$$\begin{aligned} b+xc+y &= y+az+b \\ xc &= az \end{aligned}$$

אם נבחר $x = z = 1$ נקבל $c = a$, ואם נבחר $x = 0$, $z = 1$ נקבל $a = 0$, לכן המרכז כולל מטריצות מהצורה

$$A = \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

נותר להראות של מטריצה A מהצורה הזו היא במרכז. קל לבדוק ש-A מתחלפת עם כל $X \in G$.

$$Z(G) = \left\langle \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \right\rangle$$

הרכז הוא תת חבורה ציקלית איזומורפי ל-$\mathbb{Z}_p$. נשים לב שהרכז איננו טריוויאלי. $Z(G) \lhd G$ תת חבורה נורמלית ב-G.

טענה 3.42 G חבורה כלשהי, ונניח $G/Z(G)$ ציקלית, אז G אבלית.

הוכחה: $G/Z(G)$ ציקלית, ולכן היא נוצרת ע"י קוסט מסויים

$$G/Z(G)=\langle gZ(G)\rangle$$

כל איבר $x\in G$ נמצא באחד הקוסטים, ולכן

$$x\in g^kZ(G)$$

$$x=g^kz$$

עבור $z\in Z(G)$ כלשהו.
נקח שני איברי G:

$$x=g^{k_1}z_1,\ y=g^{k_2}z_2$$

$$xy=g^{k_1}z_1g^{k_2}z_2=g^{k_1+k_2}z_1z_2=g^{k_1+k_2}z_1z_2=g^{k_2}z_2g^{k_1}z_1=yx$$

לכן G אבלית. ■

עבור הדוגמה שלנו, $G/Z(G)$ אבלית, ולכן היא איזומורפית ל-$\mathbb{Z}_p\times\mathbb{Z}_p$ ולא ל-$\mathbb{Z}_{p^2}$.
נחשב סדרים של איברים ב-G:

$$A^2=\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}^2=\begin{pmatrix}1&2a&2b+ac\\0&1&2c\\0&0&1\end{pmatrix}$$
$$A^3=\begin{pmatrix}1&a&b\\0&1&c\\0&0&1\end{pmatrix}^3=\begin{pmatrix}1&3a&3b+3ac\\0&1&3c\\0&0&1\end{pmatrix}$$

אם $p=2$, החבורה מסדר $|G|=p^3=8$, $|Z(G)|=2$, $|G/Z(G)|=4$. כל איבר בריבוע הוא במרכז.
אם $p=3$ כל איבר ב-G_3 הוא מסדר 3.

3.12 צמידות

הגדרה 3.43 $a,b\in G$, b נקרא צמוד של a אם קיים $c\in G$ כך ש-$b=cac^{-1}$.

טענה 3.44 G חבורה, היחס על G - $a\sim b\Leftrightarrow b$ צמוד ל-a הוא יחס שקילות.

מחלקות השקילות נקראות מחלקות צמידות.

$$C(a)=\{x\in G\mid x\sim a\}$$

G איחוד זר של מחלקות הצמידות.

$$G=\bigcup C(a)$$

$$|G|=\sum|C(a)|$$

דוגמאות

1. G חבורה ו-$a \in Z(G)$.

$$\begin{aligned} C(a) &= \{x \in G \mid x = cac^{-1}, c \in G\} \\ &= \{x \in G \mid x = a\} = \{a\} \end{aligned}$$

2. G חבורת היזנברג.

$$\begin{aligned} A &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \\ X &= \begin{pmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{pmatrix} \\ XAX^{-1} &= \begin{pmatrix} 1 & a & b+xc-az \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

אם a או c שונים מאפס אז למשוואה

$$d = b + xc - az$$

יש פתרון (x, z נעלמים). לכן

$$C(A) = \left\{ \begin{pmatrix} 1 & a & d \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid d \in \mathbb{Z}_p \right\}$$

אם $a = c = 0$ אז $A \in Z(G)$ ואז $C(A) = \{A\}$ כפי שראינו.
מכאן נובע שיש p מחלקות צמידות בגודל 1 ו-$p^2 - 1$ מחלקות צמידות בגודל p.

בחבורה G אבלית אם x, y צמודים אז

$$y = gxg^{-1} = gg^{-1}x = x$$

לכן אם x צמוד ל-y אז $x = y$.
בחבורה $G = S_n$ מתי $\sigma, \tau \in S_n$ צמודות?

טענה 3,45 σ, τ צמודות $\Leftrightarrow$ יש להן בדיוק אותו מבנה מחזורים.

ע"פ למת ההצמדה.

בעיה תהי

$$\sigma = (12)(34)\cdots(n-1\ n)$$

מה מספר התמורות הצמודות ל-σ?
מספר התמורות עם $\frac{n}{2}$ מעגלים באורך 2

$$\frac{n!}{2^{\frac{n}{2}}\left(\frac{n}{2}\right)!}$$

מושג הצמידות מופיע גם במטריצות. אם $A, B \in GL_2(\mathbb{R})$, A, B צמודות אם יש

$$C \in GL_n(\mathbb{R})$$

כך ש-

$$CAC^{-1} = B$$

למטריצות צמודות אותם ערכים עצמיים.

3.12.1 רכז/מנרמל של חבורה

הגדרה 3.46 G חבורה, $a \in G$. רכז (מנרמל/**Normalizer**) של a הוא

$$N(a) = \left\{ y \in G \mid yay^{-1} = a \right\}$$

הרכז הוא תת חבורה של G.

למשל

$$C_G(1) = G$$

$$\bigcap_{x \in G} C_G(x) = \{ y : xy = yx \ \forall x \} = Z(G)$$

חשוב לציין שרכז של איבר היא תת חבורה. אם $y, z \in C_G(x)$ אז

$$\left(yz^{-1}\right) x = yxz^{-1} = xyz^{-1} = x\left(yz^{-1}\right)$$

ולכן גם $yz^{-1} \in C_G(x)$.

דוגמאות G אבלית אז $C_G(x) = G$ לכל x וגם $Z(G) = G$
עבור $G = S_3$, $Z(S_3) = \{1\}$.
עבור $G = S_n$, מהו הרכז של $\sigma \in S_n$?
כל התמורות π שמקיימות

$$\sigma\pi = \pi\sigma$$

כלומר

$$\pi^{-1}\sigma\pi = \sigma$$

כל π שמצמיד את σ לעצמה יהיה ברכז. ולכן אם ל-σ יש a_1 מחזורים באורך 1, ... , עד a_n מחזורים באורך n, (כמובן שמתקיים $\sum_{i=1}^{n} i a_i = n$) אז גודל הרכז של σ הוא

$$|C_G(\sigma)| = a_1! a_2! \cdots a_n! 1^{a_1} 2^{a_2} \cdots n^{a_n}$$

משפט 3.47 G חבורה, $a \in G$. אם $C(a)$ מחלקת הצמידות של a, ו-$N(a)$ רכז של a אז

$$|C(a)| = [G : N(a)] = \frac{|G|}{|N(a)|}$$

הוכחה: $C(a) = \left\{ a, g_1 a g^{-1}, g_2 a g_2^{-1}, \dots \right\}$
ויש את אוסף הקוסטים

$$G/N(a) = \{ N(a), g_1 N(a), g_2 N(a), \dots \}$$

נראה שיש התאמה חח"ע ועל בין $C(a)$ לבין $G/N(a)$.
אם x ו-y נציגים של אותו קוסט,

$$xN(a) = yN(a)$$

אז קיים $b \in N(a)$ כך ש-$x = yb$. b ברכז של a ולכן

$$xax^{-1} = yba(yb)^{-1} = ybab^{-1}y^{-1} = yay^{-1}$$

לכן אם x ו-y נציגי אותו קוסט, אז הם נציגי אותו איבר במחלקת הצמידות.
אם x, y אינם מאותו קוסט, וננית בשלילה כי $yay^{-1} = xax^{-1}$, אז

$$x^{-1}ya = ax^{-1}y$$

ואז

$$x^{-1}y \in N(a)$$

ו-

$$xN(a) = yN(a)$$

בסתירה להנחה. הוכחנו שההתאמה חח"ע ועל ולכן

$$|C(a)| = |G/N(a)|$$

■

מסקנה 3.48 נוסחת המחלקות:

$$|G| = \sum |C(a)| = \sum \frac{|G|}{|N(a)|}$$

משפט 3.49 תהי G חבורה, $|G| = p^n$ עם p ראשוני. אזי $Z(G) \neq \{e\}$.

הוכחה: אם $N(a) = G$ אז $Z(G) \ni a$
אם $a \notin Z(g)$ אז $|N(a)| < |G|$
נסמן

$$|N(a)| = p^{n_a} < p^n$$

ע"פ נוסחת המחלקות

$$|G| = \sum \frac{|G|}{|N(a)|} = |Z(G)| + \sum_{a \notin Z(G)} \frac{|G|}{|N(A)|}$$

$$p^n = |Z(G)| + \sum_{n_a < n} \frac{p^n}{p^{n_a}}$$

$$|Z(G)| = p^n - \sum_{n_a < n} \frac{p^n}{p^{n_a}}$$

מכאן נובע ש-$p \mid |Z(G)|$. $|Z(G)| \geq 1$ ולכן

$$p \geq |Z(G)|$$

ולכן $Z(G)$ איננו טריוויאלי. ■

4 חוגים

4.1 הגדרה

4.1.1 אקסיומות החוג

1. $(R, +)$ חבורה חיבורית אבלית.
2. תכונות הכפל:
   (א) אסוציאטיביות - $a(bc) = (ab)c$
   (ב) סגירות
3. קשר בין כפל לחיבור - דיסטריביוטיביות $(a+b)c = ab + ac$; $c(a+b) = ca + cb$

דוגמאות $(\mathbb{Z},+,\cdot)$, $\mathbb{R}$, $\mathbb{Z}_n$, $M_n(\mathbb{R})$ מטריצות $n\times n$.
$\mathbb{R}\times\mathbb{R}=\{(a,b)\,;\ a,b\in\mathbb{R}\}$ עם חיבור רגיל וכפל $(a,b)(c,d)=(ac,bd)$ רכיב רכיב.
הכפל הוא אסוציאטיבי ודיסטריביוטיבי מכיוון שהוא מתבצע רכיב רכיב. תכונות אלו נובעות מהתכונות המתאימות ב-$\mathbb{R}$.
$C[0,1]$ כל הפונקציות הרציפות $f:[0,1]\to\mathbb{R}$. עם הפעולות

$$\begin{aligned}(f+g)(x) &= f(x)+g(x)\\ (fg)(x) &= f(x)\,g(x)\end{aligned}$$

חיבור ומכפלה נקודתיים.
מכיוון שהפעולות מתבצעות בנפרד לכל נק' x, תכונות הכפל והחיבור הנדרשות נובעות מהתכונות המתאימות ב-$\mathbb{R}$. צריך להראות קשירות. זה נובע מכך שסכום מכפלת פונקציות רציפות גם הוא פונקציה רציפה.

טענה 4.1 S חוג, $a\in S$ ו-$0\in S$ האדיש לחיבור, אז $0\cdot a=0$

הוכחה: מן הדיסטריביוטיביות נובע כי

$$\begin{aligned}0\cdot a &= (0+0)\,a=0a+0a\\ 0 &= 0a\end{aligned}$$

■

4.1.2 חוגים עם תכונות מיוחדות

1. החוג קומוטטיבי אם $xy=yx$ לכל $x,y\in R$.
2. חוג עם יחידה - קיים איבר $1\neq 0$ כך ש-

$$1x=x1=x$$

לכל $x\in R$.

3. $x\neq 0$ יקרא מחלק אפס אם קיים $y\neq 0$ כך ש-$xy=0$.
4. חוג קומוטטיבי עם יחידה יקרא תחום שלמות אם אין בו מחלקי אפס.
5. R שדה אם R תחום שלמות ולכל $x\neq 0$ קיים הפכי כפלי y כלומר $xy=1$.

טבלה 3: דוגמאות לחוגים

חוג	קומוטטיבי	בעל יחידה	תחום שלמות	שדה
$\mathbb{Z}$	כן	כן	כן	לא
$\mathbb{R}$	כן	כן	כן	כן
$\mathbb{Z}_n$	כן	כן	רק אם n ראשוני	רק אם n ראשוני
$M_n(\mathbb{R})$	לא	כן	$\begin{pmatrix}0&1\\0&0\end{pmatrix}^2=0$	לא
$\mathbb{R}\times\mathbb{R}$	כן	כן	$(1,0)(0,1)=0$	לא
$C[0,1]$	כן	כן	לא	לא

טענה 4.2 $\mathbb{Z}_n$ חוג קומוטטיבי עם יחידה. ב-$\mathbb{Z}_n$ יש מחלק אפס $\Leftrightarrow$ n פריק.

הוכחה: כיוון ראשון. נניח $n = ab$, $1 < a, b < n$.

$$ab \equiv 0 \pmod{n}$$

כיוון שני. נניח $ab \equiv 0$, עבור $0 \neq a, b \in \mathbb{Z}_n$. אזי $n \mid ab$. אם n היה ראשוני אז או ש-$n \mid a$ או ש-$n \mid b$.
$n \mid a \Leftarrow a = 0$. a $n \mid b \Leftarrow b = 0$. וזו סתירה. ■

טענה 4.3 אם R תחום שלמות סופי, R שדה.

הוכחה: צ"ל שלכל $0 \neq r \in R$ קיים הפכי s כך ש-$rs = 1$.
נסמן $|R| = n$. $R \setminus \{0\} = \{r_1, \ldots, r_{n-1}\}$. נעיין בקבוצה

$$A = \{rr_1, rr_2, \ldots, rr_{n-1}\}$$

ב-A יש $n-1$ אברים שונים, כי אם נניח שעבור $i < j$

$$\begin{aligned} rr_i &= rr_j \\ rr_i - rr_j &= 0 \\ r(r_i - r_j) &= 0 \end{aligned}$$

אבל $r \neq 0$ ו-$r_i \neq r_j$ אז קיבלנו מחלק אפס וזו סתירה.
$|A| = n-1$ ו-$0 \notin A$, ולכן $1 \in A$, כלומר קיים r_iכך ש-$rr_i = 1$. ■

4.2 תתי חוגים ואידיאלים

4.2.1 תת חוג

$(R, +, \cdot)$ חוג.
$S \subset R$ יקרא תת חוג אם $(S, +, \cdot)$חוג.
$(S, +, \cdot)$ תת חוג אם

1. $(S, +)$ תת חבורה של $(R, +)$.
2. S קשירה ביחס לכפל.

דוגמאות

1. $\mathbb{Z} < \mathbb{Q} < \mathbb{R}$
2. $M_n(\mathbb{Z}) < M_n(\mathbb{R})$.

4.2.2 אידיאל

R חוג. $I \subset R$ יקרא אידיאל אם:

1. $(I, +)$ תת חבורה של $(\mathbb{R}, +)$.
2. תכונת הבליעה - לכל $a \in I$, $r \in R$: $ar \in I$.

דוגמאות

4.2.3 פעולות על אידיאלים

$I_1, I_2 < R$ אידיאלים ב-R.

$$I_1 + I_2 = \{a_1 + a_2;\ a_1 \in I_1, a_2 \in I_2\}$$

טענה 4.4 $I_1 + I_2$ אידיאל

הוכחה: ראשית נראה שזוהי תת חבורה חיבורית:

$$(a_1 + a_2) + (a_1' + a_2') = \underbrace{(a_1 + a_1')}_{\in I_1} + \underbrace{(a_2 + a_2')}_{\in I_2} \in I_1 + I_2$$

תכונת הבליעה:

$$r\,(a_1 + a_2) = ra_1 + ra_2 \in I_1 + I_2$$

■

טענה 4.5 $I_1 \cap I_2$ אידיאל.

הוכחה: הטענה לגבי תת חבורות כבר הוכחה. נוכיח את תכונת הבליעה:

$$\begin{aligned} ra &\in I_1 \\ ra &\in I_2 \end{aligned}$$

ולכן $ra \in I_1 \cap I_2$ וזהו אידיאל. ■

4.2.4 האידיאלים של $\mathbb{Z}$

$\mathbb{Z}, \{0\}$ האידיאלים הטריוויאלים.
$n\mathbb{Z}\ n \geq 1$ אידיאל כי לכל $nk \in n\mathbb{Z}$, $r \in \mathbb{Z}$.

$$(nk)\,r = n\,(kr) \in n\mathbb{Z}$$

מכיוון שכל תת חבורה של $\mathbb{Z}$ היא מהצורה $n\mathbb{Z}$ אלו כל האידיאלים של $\mathbb{Z}$.

טענה 4.6 $n\mathbb{Z} + m\mathbb{Z} = (n, m)\,\mathbb{Z}$

הוכחה: ידוע שאם $k \mid l$ אז $k\mathbb{Z} \supset l\mathbb{Z}$. ולכן $(n, m) \mid n, m$

$$n\mathbb{Z}, m\mathbb{Z} \subset (n, m)\,\mathbb{Z}$$

$(n, m)\,\mathbb{Z}$ הוא אידיאל, ולכן

$$n\mathbb{Z} + m\mathbb{Z} \subset (n, m)\,\mathbb{Z}$$

מצד שני, יהיו $x, y \in \mathbb{Z}$ כך ש-$xn + ym = (n, m)$. לכן

$$(n, m) \in m\mathbb{Z} + m\mathbb{Z}$$

$$\begin{aligned} (n, m)\,\mathbb{Z} &\subset m\mathbb{Z} + m\mathbb{Z} \\ (n, m)\,\mathbb{Z} &= m\mathbb{Z} + m\mathbb{Z} \end{aligned}$$

■

בצורה דומה מוכיחים ש-$m\mathbb{Z} \cap m\mathbb{Z} = [n, m]\,\mathbb{Z}$.

הערה 4.7 אם $1 \in I$ אז $I = R$.

מסקנה 4.8 אם R שדה אז אין ב-R אידיאלים פרט לאידיאלים הטריוויאליים. אם $0 \neq x \in I$ אז מתכונת הבליעה נובע ש-$x^{-1}x \in I$ כלומר $1 \in I$ ואז $R = I$.

4.2.5 האידיאלים של $\mathbb{R} \times \mathbb{R}$

1. $I_1 = \{0\} \times \mathbb{R}$
2. $I_2 = \mathbb{R} \times \{0\}$
3. $I_1 + I_2 = \mathbb{R} \times \mathbb{R}$
4. $I_1 \cap I_2 = \{0\}$

טענה 4.9 כל אידיאל ב-$S = \mathbb{R} \times \mathbb{R}$ הוא אחד מהארבעה.

הוכחה: יהי I שונה מהנ"ל. כך ש-$(x, y) \in I$ $x, y \neq 0$. אבל אז

$$\left(x^{-1}, y^{-1}\right)(x, y) = (1, 1) \in I$$

ולכן $I = S$. ■

4.3 הומומורפיזם בין חוגים

הגדרה 4.10 העתקה $\phi : R \to S$ המקיימת

$$\begin{aligned} \phi(x + y) &= \phi(x) + \phi(y) \\ \phi(xy) &= \phi(x)\,\phi(y) \end{aligned}$$

טענה 4.11 הגרעין של ϕ, $\ker\phi$ הוא אידיאל ב-R.

$$\ker\phi = \{a \in R : \phi(a) = 0\}$$

תכונת הבליעה מתקיימת: אם $a \in \ker\phi$

$$\phi(ra) = \phi(r)\,\phi(a) = \phi(r)\,0 = 0$$

לכן

$$ra \in \ker\phi$$

דוגמאות נוספות

1. $C[0,1]$ - חוג הפונקציות הרציפות על $[0,1]$. העתקה $\phi : C[0,1] \to \mathbb{R}$, $\phi(f) = f\left(\frac{3}{4}\right)$ היא הומומורפיזם. הגרעין שלה הוא קבוצת הפונקציות שמתאפסות ב-$\frac{3}{4}$ וזהו אידיאל.
2. $\mathbb{Z} \subset \mathbb{R}$ נסתכל על החוג

$$\mathbb{Z}\left[\sqrt{5}\right] = \left\{a + b\sqrt{5} : a, b \in \mathbb{Z}\right\}$$

$\mathbb{Z}\left[\sqrt{5}\right]$ הוא תת חוג של $\mathbb{R}$.

$$\left(a + b\sqrt{5}\right) + \left(a' + b'\sqrt{5}\right) = (a + a') + (b + b')\sqrt{5}$$

$$\left(a + b\sqrt{5}\right)\left(a' + b'\sqrt{5}\right) = (aa' + 5bb') + (ab' + ba')\sqrt{5}$$

3. נגדיר העתקה $\phi : \mathbb{Z}\left[\sqrt{5}\right] \to \mathbb{Z}\left[\sqrt{5}\right]$

$$\phi\left(a+b\sqrt{5}\right) = a - b\sqrt{5}$$

העתקה זו היא הומומורפיזם חיבורי:

$$\phi\left(x+y\right) = \phi\left(x\right) + \phi\left(y\right)$$

נבדוק את הכפל:

$$\begin{aligned}
\phi\left(\left(a+b\sqrt{5}\right)\left(a'+b'\sqrt{5}\right)\right) &= \phi\left(\left(aa'+5bb'\right)+\left(ab'+ba'\right)\sqrt{5}\right) = \left(aa'+5bb'\right)-\left(ab'+ba'\right)\sqrt{5} \\
\phi\left(\left(a+b\sqrt{5}\right)\right)\phi\left(\left(a'+b'\sqrt{5}\right)\right) &= \left(a-b\sqrt{5}\right)\left(a'-b'\sqrt{5}\right) = \left(aa'+5bb'\right)-\left(ab'+ba'\right)\sqrt{5}
\end{aligned}$$

מסקנה: ϕ היא הומומורפיזם של חוגים.
הגרעין של ϕ הוא 0.

4. $\mathbb{Z} \subset \mathbb{C}$. נסתכל ב-$\mathbb{Z}\left[i\right]$.

$$\mathbb{Z}\left[i\right] = \left\{a+bi : a,b \in \mathbb{Z}\right\}$$

$$\begin{aligned}
\left(a+bi\right)\left(a'+b'i\right) &= aa'-bb'+\left(ab'+a'b\right)i \\
\left(a+bi\right)+\left(a'+b'i\right) &= \left(a+a'\right)+\left(b+b'\right)i
\end{aligned}$$

חוג זה נקרא השלמים של גאוס.

$$\phi : \mathbb{Z}\left[i\right] \to M_2\left(\mathbb{R}\right)$$

$$\phi\left(a+bi\right) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

קל לראות שזהו הומומורפיזם חיבורי. ניתן להראות שגם הכפל נשמר בהעתקה. הגרעין של ההעתקה הוא 0.

5. R_1, R_2 חוגים. נגדיר את חוג המכפלה $R = R_1 \times R_2$, עם כפל וחיבור רכיב רכיב.

$$\left(r_1, r_2\right) \dot{+} \left(r_1', r_2'\right) = \left(r_1 \dot{+} r_1', r_2 \dot{+} r_2'\right)$$

בצורה דומה מגדירים חוג מכפלה עבור k חוגים.
נניח $m_1, \ldots m_k$ מספרים טבעיים זרים בזוגות $\left(m_i, m_j\right) = 1$. $N = m_1 \cdots m_j$.

$$\phi : \mathbb{Z} \to \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$$

$$x \to \left(x \bmod m_1, \ldots, x \bmod m_k\right)$$

זהו איזומורפיזם של חוגים, ע"פ משפט השאריות הסיני.

4.4 חוג המנה

I אידיאל ב-R, נגדיר את חוג המנה. I הוא אידיאל ב-R, ולכן תת חבורה חיבורית של R. R קומוטטיבי בחיבור, ולכן $I \lhd R$ ו

$$R/I = \{r + I : r \in R\}$$

היא חבורה חיבורית.
נגדיר כפל ב-R/I ע"י

$$(r + I)(r' + I) = rr' + I$$

נבדוק שההגדרה אינה תלויה במיצגים של הקוסטים:
נניח $r + I = s + I$, $r' + I = s' + I$. צ"ל $(r + I)(r' + I) = (s + I)(s' + I)$.

$$\begin{aligned} r - s &= i \in I \\ r' - s' &= i' \in I \end{aligned}$$

$$\begin{aligned} rr' &= (s + i)(s' + i') = ss' + is' + si' + ii' \\ rr' - ss' &= is' + si' + ii' \end{aligned}$$

ביטוי זה שייך ל-I כי I אידיאל. (תכונת הבליעה). $rr' - ss' \in I$ ולכן $rr' + I = ss' + I$.

4.5 משפט האיזומורפיזם

נסתכל על $\phi : R \to S$ הומומורפיזם של חוגים. $\phi(R) \subset S$ הוא תת חוג של S.

$$R/\ker\phi \cong \phi(R)$$

הוכחה: נגדיר $\tilde{\phi} : R/\ker\phi \to \phi(R)$ ע"י

$$\tilde{\phi}(r + I) = \phi(r)$$

כאשר $I = \ker\phi$.

$$\begin{aligned} \tilde{\phi}(r + I \dot{+} r' + I) &= \tilde{\phi}(r \dot{+} r' + I) = \phi(r \dot{+} r') = \phi(r) \dot{+} \phi(r') \\ &= \tilde{\phi}(r + I) \dot{+} \tilde{\phi}(r' + I) \end{aligned}$$

$\tilde{\phi}$ על וחח"ע כי אם $r' + I = r + I$ אז

$$\phi(r') = \tilde{\phi}(r' + I) = \tilde{\phi}(r + I) = \phi(r)$$

ואם $\phi(r) = \phi(r')$ אז

$$\begin{aligned} \phi(r - r') &= \phi(r) - \phi(r') = 0 \\ r - r' &\in I \\ r + I &= r' + I \end{aligned}$$

■

4.6 חוג הפולינומים במשתנה אחד מעל שדה $\mathbb{F}$

$$\mathbb{F}[x] = \{a_0 + a_1 x + \cdots + a_n x^n : a_0, \ldots a_n \in \mathbb{F}\} \quad n \geq 0$$

כאשר x סמל.
חיבור מתבצע רכיב רכיב:

$$(a_0 + \cdots + a_n x^n) + (b_0 + \cdots + b_n x^n) = (a_0 + b_0) + \cdots + (a_n + b_n) x^n$$

הכפל הוא

$$\begin{aligned}\left(\sum_{k=0}^{n} a_k x^k\right)\left(\sum_{l=0}^{m} b_l x^l\right) &= a_0 b_0 + (a_1 b_0 + a_0 b_1) x + \cdots \\ &= \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j\right) x^k\end{aligned}$$

בחוג קיימת יחידה, הפולינום 1. החוג קומוטטיבי, בגלל קומוטטיביות השדה.
$0 \neq f(x) \in \mathbb{F}[x]$, נכתוב

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

אז הדרגה של f היא n - החזקה הגבוהה ביותר של f שאיננה אפס, ומסומנת $\deg f$.

$$\begin{aligned}\deg(f \cdot g) &= \deg f + \deg g \\ \deg(f + g) &\leq \max\{\deg f, \deg g\}\end{aligned}$$

$\mathbb{F}[x]$ הוא תחום שלמות. אם ניקח שני פולינומים שונים מאפס, אז דרגת המכפלה תהיה גדולה מדרגתם ולכן גם הוא יהיה שונה מאפס.

4.6.1 חוג אוקלידי - הקשר בין $\mathbb{F}[x]$ ל-$\mathbb{Z}$

ננסה להעביר מושגים מהחוג $\mathbb{Z}$ לחוג $\mathbb{F}[x]$.

4.6.2 מושג החלוקה

ניתן לדבר על חלוקה של פולינומים. יהיו $f(x), g(x) \in \mathbb{F}[x]$. נגדיר $f(x) \mid g(x)$ אם קיים $h(x)$ כך ש-

$$f(x) h(x) = g(x)$$

לדוגמה $x - 1 \mid x^3 - 1$ אבל $x - 1 \not| x^3 - 2$. לא קיים $h(x)$ כך ש-

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

כי אם היה, והיינו מציבים $x = 1$ אז

$$h(1) \cdot 0 = -1$$

וזה לא יתכן.

4.6.3 חלוקה עם שארית

בחלוקת מספרים שלמים עם שארית מצאנו מספר קטן מהמחלק שהוא השארית. במקרה של פולינומים נשווה את דרגת השארית לדרגת המחלק.
$f(x), g(x) \in \mathbb{F}[x]$, $g \neq 0$.

טענה 4.12 קיימים $Q(x), R(x)$ יחידים המקיימים

$$\begin{aligned} f(x) &= Q(x)\,g(x) + R(x) \\ \deg R(x) &< \deg g(x) \end{aligned}$$

הוכחה: יחידות: נניח שקיימים Q, Q_1 כך ש

$$f(x) = Qg + R = Q_1 g + R_1$$

אז

$$\begin{aligned} Qg - Q_1 g &= R_1 - R \\ (Q - Q_1)\,g &= R_1 - R \end{aligned}$$

$$\begin{aligned} \deg(Q - Q_1)\,g &= \deg(R_1 - R) < \deg g \\ \deg(Q - Q_1)\,g &= \deg(Q - Q_1) + \deg g \end{aligned}$$

לכן $Q = Q_1$ ואז $R_1 = R$.
קיום: הוכחה באינדוקציה על $n = \deg f$.
אם $\deg g > \deg f$ נקח $Q = 0$ ו-$R = f$.
אחרת,

$$\deg f \geq \deg g$$

$$\begin{aligned} f &= \sum_{i=0}^{n} a_n x^i \qquad a_n \neq 0 \\ g &= \sum_{i=0}^{m} b_n x^i \qquad b_n \neq 0 \end{aligned}$$

נסתכל על

$$\begin{aligned} \tilde{f}(x) &= f(x) - \frac{a_n}{b_m} x^{n-m} g(x) \\ &= (a_0 + \cdots + a_n x^n) - \frac{a_n}{b_m} x^{n-m} (b_0 + \cdots + b_m x^m) \end{aligned}$$

האיבר האחרון בפולינום הוא $a_n x^n - \frac{a_n}{b_m} x^{n-m} b_m x^m = 0$ ולכן

$$\deg \tilde{f} \leq n - 1$$

ולפי הנחת האינדוקציה

$$\tilde{f} = \tilde{Q} g + \tilde{R}$$

ולכן

$$\begin{aligned} f - \frac{a_n}{b_m} x^{n-m} g &= \tilde{Q} g + \tilde{R} \\ f &= \left(\frac{a_n}{b_m} x^{n-m} + \tilde{Q} \right) + \tilde{R} \end{aligned}$$

$$\deg \tilde{R} < \deg g$$

ומצאנו $R = \tilde{R}$ ו-$Q = \frac{a_n}{b_m} x^{n-m} + \tilde{Q}$. ■

4.6.4 מחלק משותף גדול ביותר

עבור $f(x), g(x) \in \mathbb{F}[x]$. המחלק המשותף המקסימלי של f, g הוא הפולינום בעל הדרגה המקסימלית כך ש-$h \mid f, g$.
אלגוריתם אוקלידס למציאת (f, g): נחלק עם שארית $f(x) = Qg + R$, $\deg R < \deg g$.

טענה 4.13 הממג"ב של f, g שווה לזה של R ו-g.

$$(f, g) = (R, g)$$

הוכחה: בדיוק כמו עם מספרים. צ"ל

$$(g, f) = (f - Qg, g)$$

אם $h \mid g, f \Leftarrow h \mid g, f - Qg$
אם $h \mid g, f - Qg \Leftarrow h \mid f, g$
לכן $(g, f) = (f - Qg, g)$. ■

דוגמה:

$$\begin{aligned} f &= x^5 + x^3 + 2 \\ g &= x^2 - 1 \end{aligned}$$

$$\begin{array}{rl} x^5 + x^3 + 2 & : \quad x^2 - 1 = x^3 + 2x \\ \underline{x^5 - x^3} & \\ 2x^3 + 2 & \\ \underline{2x^3 - 2x} & \\ 2x - 2 & \end{array}$$

כלומר

$$f = \left(x^3 + 2x\right) g + 2x - 2$$

$$\left(x^2 - 1, x^5 + x^3 + 2\right) = \left(2x - 2, x^2 - 1\right)$$

$$x^2 - 1 \quad : \quad 2x - 2 = \frac{1}{2}(x + 1)$$

ולכן

$$\left(2x-2,x^2-1\right)=\left(0,2x-2\right)$$

כלומר

$$\left(f,g\right)=2x-2$$

טענה 4.14 קיימים פולינומים $A\left(x\right),B\left(x\right)$ כך ש-

$$A\left(x\right)f\left(x\right)+B\left(x\right)g\left(x\right)=\left(f,g\right)$$

הוכחה: כמו עם מספרים, נשתמש באלגוריתם אוקלידס על מנת למצוא את הפולינומים המתאימים. נניח בה"כ ש-$\deg f\geq\deg g$, אז ניתן לחלק את f ב-g עם שארית ולקבל

$$f\left(x\right)=Q\left(x\right)g\left(x\right)+R\left(x\right)$$

אז $\left(f,g\right)\mid g\left(x\right)$ ו-$\left(f,g\right)\mid f\left(x\right)$ לכן $\left(f,g\right)\mid R\left(x\right)=f\left(x\right)-Q\left(x\right)g\left(x\right)$. לכן

$$\left(f,g\right)=\left(g,R\right)=\left(g,f-Qg\right)$$

נוכיח באינדוקציה על דרגת $g\left(x\right)$ את קיומם של הפולינומים $A\left(x\right)$ ו-$B\left(x\right)$.
אם $\deg g\left(x\right)=0$, אז בכל שדה $f\left(x\right)\mid g\left(x\right)$ ולכן $\left(f,g\right)=g\left(x\right)$, כלומר $A\left(x\right)=0$, $B\left(x\right)=1$.
נניח שהטענה נכונה לכל $\deg g\left(x\right)<n$ ונוכיח עבור $\deg g\left(x\right)=n$.
$R\left(x\right)$ היא השארית של $f\left(x\right)$ בחלוקה ל-$g\left(x\right)$, ולכן $\deg R\left(x\right)<\deg g\left(x\right)=n$ ומכאן נובע שע"פ הנחת האינדוקציה קיימים $\tilde{A},\tilde{B}$ כך ש-

$$\left(g,R\right)=\tilde{A}g\left(x\right)+\tilde{B}R\left(x\right)$$

אבל $\left(g,R\right)=\left(f,g\right)$ ו-$R\left(x\right)=f\left(x\right)-Q\left(x\right)g\left(x\right)$ ולכן

$$\left(f,g\right)=\left(g,R\right)=\tilde{A}\left(x\right)g\left(x\right)+\tilde{B}\left(x\right)\left(f\left(x\right)-Q\left(x\right)g\left(x\right)\right)=\tilde{B}\left(x\right)f\left(x\right)+\left(\tilde{A}\left(x\right)-\tilde{B}\left(x\right)Q\left(x\right)\right)g\left(x\right)$$

$$\begin{aligned}A\left(x\right)&=\tilde{B}\left(x\right)\\B\left(x\right)&=\tilde{A}\left(x\right)-\tilde{B}\left(x\right)Q\left(x\right)\end{aligned}$$

■

טבלה 4: מציאת ממג"ב של פולינום

g	f	Q	B	A
x^2-1	x^5+x^3+2	x^3+2x	$-\left(x^3-2x\right)$	1
$2x+2$	x^2-1	$\frac{x+1}{2}$	1	0
0	$2x+2$		0	1

4.7 אידיאלים ראשיים

הגדרה 4.15 R חוג קומוטטיבי, $a \in R$. האידיאל הראשי הנוצר על ידי a הוא הקבוצה

$$aR = \{ar \ : \ r \in R\}$$

כלומר aR הם כל איברי R המתחלקים ב-a.

זהו אידיאל כי

$$ar_1 + ar_2 = a\left(r_1 + r_2\right)$$

ולכן יש סגירות לחיבור

$$r\left(ar_1\right) = a\left(rr_1\right) \in aR$$

ולכן מתקיימת תכונת הבליעה.

דוגמה $R = \mathbb{R}\left[x\right]$, $a = 3$.

$$3\mathbb{R}\left[x\right] = \mathbb{R}\left[x\right]$$

כי כל פולינום ניתן לחלוקה ב-3.
$a = x + 2$

$$\left(x+2\right)\mathbb{R}\left[x\right]$$

היא קבוצת כל הפולינומים $f\left(x\right)$ כך שקיים $g\left(x\right)$ ו-$g\left(x\right)\left(x+2\right) = f\left(x\right)$. במלים אחרות אלו כל הפולינום ש-(-2) הוא שורש שלהם.

הגדרה 4.16 חוג R קומוטטיבי יקרא ראשי אם כל אידיאל I של R הוא אידיאל ראשי.

טענה 4.17 $\mathbb{F}\left[x\right]$ ($\mathbb{F}$ שדה) הוא חוג ראשי.

הוכחה: ההוכחה דומה להוכחה המתאימה עבור $\mathbb{Z}$.
יהא $I \neq \{0\}$ אידיאל כלשהו ב-$\mathbb{F}\left[x\right]$. יהא $f\left(x\right) \neq 0$ אחד הפולינומים עם הדרגה הקטנה היותר ב-I.
נראה ש-$f\left(x\right)$ הוא היוצר של I, כלומר $I = f\left(x\right)\mathbb{F}\left[x\right]$.
כיוון אחד: $f\left(x\right)h\left(x\right) \in I$ לכל $h\left(x\right) \in \mathbb{F}\left[x\right]$ כי I אידיאל, ולכן $f\left(x\right)\mathbb{F}\left[x\right] \subset I$.
כיוון שני: יהי $g\left(x\right) \in I$. נחלק אותו עם שארית ב-$f\left(x\right)$:

$$g\left(x\right) = Q\left(x\right)f\left(x\right) + R\left(x\right)$$

$$\deg R < \deg f$$

$$R\left(x\right) = g\left(x\right) - Q\left(x\right)f\left(x\right) \in I$$

אם $R \neq 0$ והדרגה שלו קטנה מ-f קיבלנו סתירה למינימליות f. לכן $R = 0$, ו-$g\left(x\right) = Q\left(x\right)f\left(x\right)$. לכן $g\left(x\right) \in f\left(x\right)\mathbb{F}\left[x\right]$ ו-$I = f\left(x\right)\mathbb{F}\left[x\right]$. ■

תכונות האידיאלים הראשיים

$$\begin{aligned} f\mathbb{F}[x] + g\mathbb{F}[x] &= \gcd(f,g)\,\mathbb{F}[x] \\ f\mathbb{F}[x] \cap g\mathbb{F}[x] &= \operatorname{lcm}(f,g)\,\mathbb{F}[x] \end{aligned}$$

$f(x)\,\mathbb{F}[x]\,,\ h(x)\,\mathbb{F}[x]$. נסמן $(f) = f(x)\,\mathbb{F}[x]$.

טענה 4.18 $f \mid g \Leftrightarrow (g) \subset (f)$

הוכחה: $\Rightarrow$ נניח $f \mid g$. קיים h כך ש $fh = g$.

$$g \in (f)$$

ולכן

$$(g) \subset (f)$$

$\Leftarrow$ נניח $(g) \subset (f)$, בפרט $g \in (f)$ ולכן קיים h כך ש-$g = fh$ ומכאן $f \mid g$. ■

4.7.1 מספרים ופולינומים ראשוניים

$2 \leq n \in \mathbb{Z}$ ראשוני אם אין הצגה $n = ab$ עבור $1 \leq a, b$.

הגדרה 4.19 נגדיר בצורה אנלוגית פולינום **אי-פריק** $f(x) \in \mathbb{F}[x]$ (אפשר לומר ראשוני). $f(x)$ אי פריק אם אין הצגה

$$f(x) = g(x)\,h(x)$$

כך ש-$\deg f > \deg g, \deg h$.

טענה 4.20 כל פולינום ניתן להצגה יחידה

$$f = f_1 \cdots f_k$$

כאשר $f_1 \dots f_k$ אי פריקים.

דוגמאות

- $\mathbb{F} = \mathbb{R}$

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

ולכן f פריק.

- לעומת זאת $f(x) = x^2 + 1$, אם היה פריק, היה צריך להיות אפשרי לכתוב

$$f(x) = (x-\alpha)(x-\beta)$$

כאשר $\alpha, \beta \in \mathbb{R}$. α צריך להיות $\sqrt{-1}$ אבל אנו יודעים שאין α כזה ב-$\mathbb{R}$.

- $\mathbb{F} = \mathbb{Q}$.

$$f(x) = x^3 - 1 = (x-1)\left(1 + x + x^2\right)$$

לכן f פריק, אבל $x^3 - 2$ איננו פריק, כי אם הוא היה פריק, והוא מדרגה 3 אז הוא היה צריך להיות מהצורה

$$f(x) = x^3 - 2 = (x-\alpha)\,g(x)$$

עבור $\alpha \in \mathbb{Q}$ המקיים $\alpha^3 = 2$ אבל אין α כזה.

- $\mathbb{F}=\mathbb{Z}_2$. $f(x)=1+x+x^2$ אם f היה פריק אז

$$f(x)=(x-\alpha)(x-\beta)$$

ואז $\alpha\in\mathbb{Z}_2$ כך ש-α שורש של $1+x+x^2$. אפשר לבדוק על 2 האפשרויות ולראות ש-f איננו פריק.

טענה 4,21 אם $\alpha_1\ldots,\alpha_k\in\mathbb{F}$ שורשים שונים של $f(x)\in\mathbb{F}[x]$ אז $(x-\alpha_1)\cdots(x-\alpha_k\ )\mid f(x)$

הוכחה: אינדוקציה על k.
$k=1$. נחלק עם שארית

$$f(x)=Q(x)(x-\alpha_1)+R(x)$$

$$\deg R<\deg(x-\alpha_1)=1$$

$$R(x)=r\in\mathbb{F}$$

$$f(x)=Q(x)(x-\alpha_1)+r$$

נציב $x=\alpha_1$

$$f(\alpha_1)=r=0$$

לכן

$$f(x)=Q(x)(x-\alpha_1)$$

צעד האינדוקציה. לפי הנחת האינדוקציה

$$f(x)=Q(x)(x-\alpha_1)\cdots(x-\alpha_{k-1})$$

נציב $x=\alpha_k$

$$f(\alpha_k)=0=Q(x)(\alpha_k-\alpha_1)\cdots(\alpha_k-\alpha_{k-1})$$

לכן מכך ש-$Q(x)=0$ נובע לפי הנחת האינדוקציה

$$Q(x)=(x-\alpha_k)P(x)$$

לכן

$$f(x)=P(x)(\alpha_k-\alpha_1)\cdots(\alpha_k-\alpha_k)$$

הוכחה אחרת:

$$\begin{array}{rcl}x-\alpha_1 & \mid & f(x)\\ & \vdots & \\ x-\alpha_k & \mid & f(x)\end{array}$$

$x-\alpha_1,\ldots,x-\alpha_k$ זרים, ולכן

$$(\alpha_k-\alpha_1)\cdots(\alpha_k-\alpha_k)\mid f(x)$$

■

4.7.2 בדיקת אי פריקות

טענה 4.22 יהא פולינום $f(x) \in F[x]$ ונניח $2 \leq \deg f \leq 3$ אז f אי פריק $\Leftrightarrow$ אין לו שורש ב-F.

הוכחה: אם f פריק אז הדרגה של אחד הגורמים שלו צריכה להיות 1 ואז יש לו שורש. ■

4.8 חוג המנה

בחוג השלמים, חוג המנה $\mathbb{Z}/n\mathbb{Z}$ שווה ל-$\mathbb{Z}_n$. ראינו ש-$\mathbb{Z}_n$ שדה רק אם n ראשוני.

הגדרה 4.23 R חוג קומוטטיבי עם 1. אידיאל $I < R$ יקרא מקסימלי, אם:

1. $I \neq R$
2. האידיאל היחיד J המקיים $I \subsetneq J \subset R$ הוא R עצמו.

דוגמאות

1. $4\mathbb{Z} \subsetneq 2\mathbb{Z} \neq \mathbb{Z}$. לכן $4\mathbb{Z}$ איננו מקסימלי. מצד שני $2\mathbb{Z}$ מקסימלי.

טענה 4.24 $n\mathbb{Z}$ מקסימלי אסם n ראשוני.

הוכחה: אם $n = ab$ אז $n\mathbb{Z} \subset a\mathbb{Z}$, ולכן $n\mathbb{Z}$ לא מקסימלי, ולהיפך. ■

טענה 4.25 $I = (f(x))$ אידיאל מקסימלי בחוג $\mathbb{F}[x]$ אסם $f(x)$ אי פריק.

הוכחה: אם $f = gh$, $\deg f > \deg h, \deg g$ אז

$$(f) \subsetneq (g) \subsetneq \mathbb{F}[x]$$

((g) שונה מ-$\mathbb{F}[x]$ כי $0 < \deg g$).
לכן (f) איננו מקסימלי.
כיוון שני: אם (f) איננו אידיאל מקסימלי, אז קיים g כך ש-

$$(f) \subsetneq (g) \subsetneq \mathbb{F}[x]$$

ואז $g \mid f$ ו-f איננו פריק. ■

טענה 4.26 בחוג קומוטטיבי עם 1 R, $I < R$ אידיאל מקסימלי $\Leftrightarrow R/I$ שדה.

מסקנה 4.27 בחוג הפולינומים $\mathbb{F}[x]$, $\mathbb{F}[x]/(f)$ הוא שדה אסם (f) אידיאל מקסימלי, אסם $f(x)$ אי פריק.
(בדומה למה שהוכחנו ב-$\mathbb{Z}$).

הוכחה: אם I אידיאל מקסימלי, צ"ל R/I שדה.
מבניית חוג המנה אנו יודעים כי R/I הוא חוג קומוטטיבי עם 1. לאיבר $r \in R$ מתאים קוסט $\bar{r} = r + I \in R/I$. היחידה של R/I היא $\bar{1} = 1 + I$.
צ"ל שלכל $\bar{r} \neq \bar{0}$ יש הפכי.
$r \notin I$ כי $\bar{r} \neq \bar{0}$. נעיין באידיאל $J = I + rR$.

$$I \subsetneq J \subset R$$

כי $r \in rR$ ולכן $r \in J$ אבל $r \notin I$.
ממקסימליות I נובע ש-$J = R$.

$$I + rR = R$$

$$1 \in R$$

ולכן קיימים $i \in I$, $s \in R$ כך ש-

$$1 = i + rs$$

$$\bar{1} = \overline{i + rs} = \bar{i} + \bar{r}\bar{s}$$

$$\bar{i} = \bar{0}$$

ולכן

$$\bar{1} = \bar{r}\bar{s}$$

ו-$\bar{s}$ הוא ההפכי של $\bar{r}$.
כיוון שני: אם R/I שדה, צ"ל ש-I אידיאל מקסימלי.
יהי J אידיאל שמכיל את I ושונה ממנו.
נבחר $r \in J \setminus I$.

$$0 \neq \bar{r} \in R/I$$

(כי $r \notin I$).
לפיכך יש ל-$\bar{r}$ הפכי ב-R/I כלומר קיים $\bar{s}$ כך ש-$\bar{1} = \bar{r}\bar{s} = \overline{rs}$. לכן

$$rs + I = 1 + I$$

$$rs - 1 \in I$$

קיים $i \in I$ כך ש-

$$rs - 1 = i$$

$r \in J$ ו-J אידיאל ולכן $rs \in J$. $i \in I \subsetneq J$ ולכן

$$1 = rs - i \in J$$

J אידיאל המכיל את 1 ולכן $J = R$. ■

דוגמאות $\mathbb{F} = \mathbb{R}$. לא לכל משוואה יש פתרון. למשל למשוואה $f(x) = x^2 + 1$ אין פתרון ממשי.
בעיה: מצא שדה המכיל את $\mathbb{F}$ ומכיל גם פתרון למשוואה $f(x) = 0$.
אפשר להניח ש-$f(x)$ אי פריק, כי אם הוא היה פריק, היה אפשר לטפל בגורמים שלו בנפרד.
פתרון: השדה $\mathbb{K} = \mathbb{F}[x]/(f)$.
$\mathbb{K}$ שדה ע"פ הטענה.
$f(x) = a_0 + a_1 x + \cdots + a_n x^n$ כאשר $a_i \in \mathbb{F}$.
$\mathbb{F} \subset \mathbb{K}$ כי לכל $a \in \mathbb{F}$ הפולינום $a + (f)$ נמצא ב-$\mathbb{K}$. הפולינומים שונים זה מזה.

טענה 4,28 למשוואה $\bar{f}(T) = \bar{a_0} + \bar{a_1}T + \bar{a_2}T^2 + \cdots + \bar{a_n}T^n$ יש פתרון ב-$\mathbb{K}$.

הוכחה: נקח $T = \bar{x} = x + (f)$.

$$\begin{aligned} \bar{f}(\bar{x}) &= \bar{a_0} + \bar{a_1}\bar{x} + \bar{a_2}\bar{x}^2 + \cdots + \bar{a_n}\bar{x}^n \\ &= \overline{a_0 + a_1 x + \cdots + a_n x^n} = \overline{f(x)} = 0 \end{aligned}$$

כי $\overline{f(x)} \in (f)$ ■

4.9 שדה הרחבה

טענה 4.29 R חוג קומוטטיבי עם 1, $I \lhd R$, I מקסימלי אסם R/I שדה.

$\mathbb{F}$ שדה. $F[x]$ חוג הפולינומים במשתנה x מקדמים ב-F. $F[x]$ חוג ראשי, כלומר כל אידיאל הוא מהצורה $I = (f)$ ($(f) = f(x) F[x]$).

טענה 4.30 $f(x) F[x]$ אי פריק אסם (f) מקסימלי אסם $F[x]/(f)$ שדה.

הגדרה 4.31 שדה הרחבה של F הוא שדה $F \subset K$ (פעולות F הן פעולות K).

למשל $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.

4.9.1 דרגת ההרחבה

K הוא בפרט מרחב וקטורי מעל F: יש בו חיבור וכפל בסקלר מ-F. דרגת ההרחבה מוגדרת להיות המימד של K כמרחב וקטורי מעל F ומסומן $(K : F) = \dim_F K$.
לדוגמה: $F = R \subset C = K$.

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)\,i \\ \lambda(a+bi) &= \lambda a + \lambda b i\end{aligned}$$

1 ו-i הוא בסיס של $\mathbb{R}^{\mathbb{C}}$, ולכן $2 = \dim_{\mathbb{R}} \mathbb{C}$.

בעיה יהא $f(x) \in F[x]$ אי פריק. מצא שדה הרחבה $F \subset K$ כך שקיים $\lambda \in K$ המקיים $f(\lambda) = 0$.

פתרון

$$K = F[x]/(f)$$

נסתכל על ההעתקה הקנונית

$$\begin{aligned}F[x] &\to F[x]/(f) \\ g &\to \bar{g} = g + (f)\end{aligned}$$

קבוצת הקוסטים של איברי F היא

$$\tilde{F} = \{\bar{a} = a + (f);\ a \in F\} \subset K$$

אז $\tilde{F} \cong F$ הוא שדה חלקי של K.
נראה ש-f באמת פריק ב-K.
$\tilde{f}(t) \in K[t]$ יוגדר להיות:

$$f(t) = \sum_{i=0}^{n} a_i x^i$$

$$\tilde{f}(t) = \sum_{i=0}^{n} \bar{a_i} t^i$$

טענה 4.32 $\bar{x} = x + (f)$ הוא שורש ב-K של $\tilde{f}(t)$.

הוכחה: בשדה K:

$$\tilde{f}(\bar{x}) = \sum_{i=0}^{n} \bar{a_i}\bar{x}^i = \sum_{i=0}^{n} \overline{a_i x^i} = \overline{\sum_{i=0}^{n} a_i x^i} = \overline{f(x)} = f(x) + (f) = 0 + (f) = \bar{0}$$

■

דוגמה $F=\mathbb{R}$. $f(x)=x^2+1$.

$$K=\mathbb{R}[x]/\left(x^2+1\right)$$

איברי השדה K נראים מהצורה

$$\lambda_0+\lambda_1 x+\cdots+\lambda_n x^n$$

הסכם: נזהה את $\tilde{F}$ עם F. לא נכתוב $\bar{g}$ אלא g עבור סקלרים.
נסמן $w=\bar{x}\in K$.

$$K=\{a+bw : a,b\in\mathbb{R}\}$$

זאת מכיוון שהוכחנו ש-$w^2=-1$ ולכן $w^3=w$, $w^4=1$ וכן הלאה. לכן מספיק לקחת פולינום ממעלה 1 בשביל לקבל את כל איברי K.
פעולת החיבור ב-K:

$$(a_1+b_1w)+(a_2+b_2w)=(a_1+a_2)+(b_1+b_2)\,w$$

פעולת הכפל ב-K:

$$(a_1+b_1w)(a_2+b_2w)=a_1a_2+(a_1b_2+b_1a_2)\,w+b_1b_2w^2$$

מכיוון ש-$w^2=-1$

$$(a_1+b_1w)(a_2+b_2w)=a_1a_2-b_1b_2w^2+(a_1b_2+b_1a_2)\,w$$

4.9.2 אריתמטיקה של $K=F[x]/(f)$

נסמן $w=\bar{x}=x+(f)$. אם $f(x)=\sum_{i=0}^n a_ix^i$ אז

$$\sum_{i=0}^n a_iw^i=f(w)=0$$

טענה 4.33 $K=\left\{\sum_{i=0}^{n-1}\lambda_iw^i;\ \lambda_i\in F\right\}$

הוכחה: כל איבר ב-K הוא מהצורה

$$\theta_i\in F\qquad\sum_{i=0}^{N}\theta_iw^i$$

לכן די להראות ש-$w^m\in\mathrm{Span}\left\{1,w,\ldots,w^{n-1}\right\}$. עבור $0\le m\le n-1$ ברור. אם $m=n$ אז

$$a_nw^n+a_{n-1}w^{n-1}+\cdots+a_0=0$$

$$w^n=-\left(\frac{a_{n-1}}{a_n}w^{n-1}+\cdots+\frac{a_0}{a_n}w^0\right)\in\mathrm{Span}\left\{1,\ldots,w^{n-1}\right\}$$

עבור $w^{n+1}=ww^n$

$$ww^n\quad\in\quad w\mathrm{Span}\left\{1,\ldots,w^{n-1}\right\}=\mathrm{Span}\left\{w,\ldots,w^n\right\}\subset\mathrm{Span}\left\{1,\ldots,w^{n-1}\right\}$$

וניתן להמשיך באינדוקציה.

$\{1, \ldots, w^{n-1}\}$ מהווים בסיס של F^K. הם ב"ת כי אם

$$\overline{\sum_{i=0}^{n-1} \theta_i x^i} = \sum_{i=0}^{n-1} \theta_i w^i = \bar{0}$$

כלומר

$$\sum_{i=0}^{n-1} \theta_i x^i \in (f)$$

אז היינו מקבלים ש-$f \mid \sum_{i=0}^{n-1} \theta_i x^i$ אבל אז $\theta_0 = \cdots = \theta_{n-1} = 0$ כי f איננו פריק. ■

כפל

$$\left(\sum_{i=0}^{n-1} \lambda_i w^i\right)\left(\sum_{i=j}^{n-1} \beta_j w^i\right) \quad = \quad \sum_{i=0}^{n-1}\left(\sum_{i=j}^{n-1} \lambda_i \beta_j\right) w^{i+j}$$

אבל אנחנו רוצים להציג את הפולינום עם חזקות קטנות מ-n של w. נציג אם כן את כל חזקות w כצירוף של $1, \ldots, w^{n-1}$ ומפשטים.

דוגמה $F = \mathbb{Q}$. $f(x) = x^2 - x - 1$ א"פ.

$$K = \mathbb{Q}[x] / \left(x^2 - x - 1\right)$$

$$K = \{a + bw;\ a, b \in \mathbb{Q}\}$$

נבנה את לוח הכפל של w:

טבלה 5: לוח הכפל של $\mathbb{Q}[x] / \left(x^2 - x - 1\right)$

	1	w
1	1	w
w	w	$w+1$

$$w^2 - w - 1 = 0 \implies w^2 = w + 1$$

לכן פעולת הכפל תהיה

$$\begin{aligned}(a + bw)(c + dw) &= ab + (ad + bc)w + (bd)(w + 1) \\ &= (ab + bd) + (ad + b(c + d))w\end{aligned}$$

מציאת הפכי:

$$\begin{aligned}1 &= (a + bw)(c + dw) \\ &= (ab + bd) + (ad + bc + bd)w\end{aligned}$$

$$\begin{cases} ab + bd &= 1 \\ ad + b(c + d) &= 0 \end{cases}$$

5 שדות סופיים

לכל p ראשוני $\mathbb{Z}_p$ הוא שדה. האם יש שדות סופיים אחרים ואיך לבנותם?

הגדרה 5.1 F שדה כלשהו. $1 \in F$. $\bar{n} = \overbrace{1+\cdots+1}^{n}$.
המציין של F, $\mathrm{char}F$ הוא ה-n המינימלי כך ש-

$$\bar{n} = 0$$

בשדה אינסופי, אם אין n כזה, מסמנים $\mathrm{char}F = 0$.

טענה 5.2 אם $p = \mathrm{char}F \neq 0$ אז p ראשוני.

הוכחה: נניח $\mathrm{char}F = kl$, אז

$$0 = \overline{kl} = \underbrace{1+\cdots+1}_{kl} = \underbrace{(1+\cdots+1)}_{k}\underbrace{(1+\cdots+1)}_{l}$$

מכיוון שזהו שדה, אחד מן הגורמים צריך להיות 0, אבל זו סתירה למינימליות המציין. ■

מסקנה 5.3 יהי F שדה סופי, ויהי $p = \mathrm{char}F$. אז $|F| = p^k$. כל השדות הסופיים הם מסדר שהוא חזקה של ראשוני.

הוכחה: נתבונן ב-$\mathbb{Z}_p = \{0, 1, \ldots, p-1\} \subset F$. נתיחס ל-$F$ כמרחב וקטורי מעל $\mathbb{Z}_p$. נקח $v_1, \ldots, v_k$ להיות בסיס של F מעל $\mathbb{Z}_p$.

$$F = \sum_{i=1}^{k} \lambda_i v_i \quad \lambda_i \in \mathbb{Z}_p$$

לכן

$$|F| = p^k$$

■

5.1 בניית שדה סופי מסדר p^k

מוצאים פולינום $\mathbb{Z}_p[x] \ni f(x) = \sum_{i=0}^{k} a_i x^i$ שהוא אי פריק.
השדה $K = \mathbb{Z}_p/(f)$ הוא מסדר p^k כי כבר ראינו ש-

$$K = \left\{ \sum_{i=0}^{k-1} \lambda_i w^i;\ \lambda_i \in \mathbb{Z}_p, w = \bar{x} \right\}$$

$$(K : \mathbb{Z}_p) = \dim_{\mathbb{Z}_p} K = k$$

$$|K| = p^k$$

דוגמה $p=2$. מצא שדה עם 8 איברים. עלינו למצוא פולינום אי פריק מדרגה 3, ב-$\mathbb{Z}_2[x]$:

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

הוא אי פריק.

$$K=\mathbb{Z}_2/\left(1+x^2+x^3\right)$$

$$K=\left\{\lambda_0+\lambda_1 w+\lambda_2 w^2;\ \lambda_i\in\mathbb{Z}_2\right\}$$

חבור וקטורי:

$$\begin{aligned}&\lambda_0+\lambda_1 w+\lambda_2 w^2\\ &+\lambda_0'+\lambda_1' w+\lambda_2' w^2\\ &=(\lambda_0+\lambda_0')+(\lambda_1+\lambda_1')\,w+(\lambda_2+\lambda_2')\,w^2\end{aligned}$$

לחישוב כפל נחשב את לוח הכפל:

$$\begin{aligned}1+w^2+w^3 &= 0\\ w^3 &= w^2+1\\ w^4 &= w^3+w=w^2+w+1\end{aligned}$$

טבלה 6: לוח הכפל של $\mathbb{Z}_2[x]/\left(1+x^2+x^3\right)$

	1	w	w^2
1	1	w	w^2
w	w	w^2	w^2+1
w^2	w^2	w^2+1	w^2+w+1

לכן

$$\begin{aligned}\left(\lambda_0+\lambda_1 w+\lambda_2 w^2\right)\left(\lambda_0'+\lambda_1' w+\lambda_2' w^2\right) &= \lambda_0\lambda_0'+w\left(\lambda_0\lambda_1'+\lambda_1\lambda_0'\right)+w^2\left(\lambda_0\lambda_2'+\lambda_1\lambda_1'+\lambda_0'\lambda_2\right)\\ &\quad +w^3\left(\lambda_1\lambda_2'+\lambda_1'\lambda_2\right)+w^4\left(\lambda_2\lambda_2'\right)\\ &= \left(\lambda_0\lambda_0'+\lambda_1\lambda_2'+\lambda_1'\lambda_2+\lambda_2\lambda_2'\right)+w\left(\lambda_0\lambda_1'+\lambda_1\lambda_0'+\lambda_2\lambda_2'\right)\\ &\quad +w^2\left(\lambda_0\lambda_2'+\lambda_1\lambda_1'+\lambda_0'\lambda_2+\lambda_1\lambda_2'+\lambda_1'\lambda_2+\lambda_2\lambda_2'\right)\end{aligned}$$

5.2 שדות הרחבה ומטריצות

F שדה כללי. $A\in M_n(F)$.

$$F[A]=\left\{\sum_{i=0}^{m}\lambda_i A^i;\ \lambda_i\in F\right\}$$

$F[A]$ הוא תת חוג של $M_n(F)$.
נגדיר הומומורפיזם $\varphi: F[x]\to F[A]$

$$\begin{aligned}\varphi(x) &= A\\ \varphi\left(\sum\lambda_i x^i\right) &= \sum\lambda_i A^i\end{aligned}$$

אנו יודעים ש-

$$F[x]/\ker\varphi \cong F[A]$$

$$\ker\varphi = \{p(x) \in F[x]\,;\, p(A) = 0\}$$

$\ker\varphi$ הוא אידיאל ב-$F[x]$ ולכן הוא חייב להיות מהצורה

$$\ker\varphi = g(x)\,F[x]$$

כאשר $g(x)$ הוא הפולינום המינימלי של A. כלומר הפולינום מהדרגה המינימלית שכאשר מציבים בו את A מקבלים את מטריצת האפס.
ע"פ משפט קיילי המינגטון, הפולינום האופייני של מטריצה $\det(xI - A)$ מאפס את המטריצה, ולכן הפולינום המינימלי מחלק את הפולינום האופייני.

דוגמה $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. במקרה זה הפולינום המינימלי של A הוא הפולינום האופייני שלה

$$g(x) = x^2 + 1$$

כי

$$A^2 + I = 0$$

כעת

$$\mathbb{R}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \cong \mathbb{R}[x]/\left(x^2+1\right) \cong \mathbb{C}$$

דוגמה 2 ננסה לייצג את השדה $GF(8)$ ע"י חוג מטריצות. אנו מחפשים מטריצה $A \in M_3(\mathbb{Z}_2)$, שהפולינום המינימלי שלה הוא $1 + x^2 + x^3 \in \mathbb{Z}_2[x]$.

$$A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$$

ובאופן כללי עבור $f(x) = \gamma_0 + \gamma_1 x + \cdots + \gamma_{n-1}x^{n-1} + x^n$ המטריצה תהיה

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & -\gamma_1 \\ 1 & 0 & 0 & & & -\gamma_2 \\ 0 & 1 & 0 & & & \vdots \\ \vdots & & 1 & 0 & & \\ 0 & & & \ddots & \ddots & \\ 0 & 0 & \cdots & 0 & 1 & -\gamma_{n-1} \end{bmatrix}$$

$$GF(8) \cong \left\{ \lambda_0 I + \lambda_1 \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix};\ \lambda_i \in \mathbb{Z}_2 \right\}$$

כעת קל יותר לחשב את ההפכי של $(\lambda_0 + \lambda_1 w + \lambda w^2)$. נמצא את $(\lambda_0 + \lambda_1 A + \lambda_2 A^2)^{-1}$. את ההפכי של מטריצה אנחנו יודעים לחשב. העמודה השמאלית בתוצאה היא תמיד המקדמים של הפולינום.

5.3 עובדות נוספות

F שדה סופי אז $F^* = F \setminus \{0\}$ חבורה כפלית.

טענה 5.4 F^* ציקלית.
בשדה ממציין p לכל a, b

$$\begin{aligned} (a+b)^p &= a^p + b^p \\ (a+b)^{p^k} &= a^{p^k} + b^{p^k} \end{aligned}$$

הוכחה: ניתן להוכיח על ידי התבוננות בפיתוח הבינום של ניוטון. ■