לינארית 1 פרק ראשון: שדות ומספרים מרוכבים

מבנה אלגברי: מבנה אלגברי הוא קבוצה של איברים עם פעולה או פעולות ודרישות אותן מקיימות הפעולות אלו בתוך הקבוצה.

דוגמאות לחלק מהתכונות (פעולות) שנכיר:

1. סגירות לפעולה בינארית: אומרים שקבוצה A עם פעולה $*$ סגורה לפעולה $*$ אם לכל $a,b\in A$ מתקיים $a*b\in A$.

דוגמה: נבחר את A להיות כל המספרים השלמים.

אם הפעולה $*$ היא חיבור, אז A סגורה לפעולת החיבור כי חיבור של שני מספרים שלמים ייתן מספר שלם.

אם הפעולה $*$ היא כפל, אז A לא סגורה לפעולת הכפל כי כפל של שני מספרים שלמים ייתן מספר מנה.

אם ניקח את A להיות כל המספרים המרוכבים והשלמים עם הפעולה $*$ שהיא כפל אז ניתן להגיע ש-A סגורה לכפל.

מסקנות:

1. סגירות לפעולה מושפעת הן מהקבוצה והן מהפעולה.
2. אותה קבוצה עם פעולה אחרת תיתן מבנה אלגברי אחר.

דוגמה נוספת: נבחר את A להיות קבוצת המספרים הראשוניים.

נבחר את $*$ להיות פעולת החיבור. מספרים ראשוניים לא סגורים לחיבור כי $3+5=8$ כלומר חיברנו שני ראשוניים וקיבלנו מספר לא ראשוני.

נבחר את $*$ להיות פעולת הכפל. מספרים ראשוניים לא סגורים לכפל כי $3\cdot5=15$ כלומר כפלנו שני ראשוניים וקיבלנו מספר לא ראשוני.

אם ניקח את הקבוצה A להיות מספרים פריקים, אז:

A לא סגורה לחיבור כי $4+9=13$ כלומר חיברנו שני פריקים וקיבלנו מספר ראשוני.

A סגורה לכפל כי הכפלת שני מספרים פריקים לבטח תיתן מספר פריק.

2. פעולה חילופית: אומרים שפעולה $*$ היא חילופית (או קומוטטיבית) אם לכל שני איברים a,b בקבוצה A מתקיים: $a*b=b*a$.

למשל, פעולת החיבור והכפל הן חילופיות

אבל פעולת החיסור והחילוק הן לא חילופיות:

$$5-3=2\neq3-5=2$$
$$4:2=2\neq2:4=\frac{1}{2}$$

3. פעולה קיבוצית: אומרים שפעולה $*$ היא קיבוצית (או אסוציאטיבית) אם לכל a,b,c בקבוצה A מתקיים: $(a*b)*c=a*(b*c)$.

למשל, פעולת החיבור והכפל הן קיבוציות.

אבל פעולות החיסור והחילוק הן לא קיבוציות:

$$(5-3)-7=2-7=-5$$
$$5-(3-7)=5-(-4)=9$$
$$(4:2):2=2:2=1$$
$$4:(2:2)=4:1=4$$

בקורס הזה נכיר מבנה אלגברי עם שתי פעולות שיקרא שדה.

שדות

הגדרה השדה: קבוצה F שבה מוגדרות שתי פעולות: פעולת החיבור $+$ ופעולת כפל $\cdot$ נקראת שדה ואיבריה נקראים סקלרים, אם לכל $a,b,c \in F$ מתקיימות 11 התכונות הבאות:

1. סגירות לחיבור: $a+b \in F$
2. אסוציאטיביות בחיבור: $(a+b)+c = a+(b+c)$
3. קומוטטיביות בחיבור: $a+b = b+a$
4. קיים ב- F אדיש לחיבור, המסומן 0_F, ומקיים: $a+0_F=0_F+a = a$.
5. לכל a ב- F קיים נגדי ב- F, המסומן $-a$, ומקיים: $a+(-a)=(-a)+a=0_F$.
6. סגירות לכפל: $a \cdot b \in F$
7. אסוציאטיביות בכפל: $(a\cdot b)\cdot c = a\cdot(b\cdot c)$
8. קומוטטיביות בכפל: $a\cdot b = b\cdot a$
9. קיים ב- F אדיש לכפל, המסומן 1_F, ומקיים: $a\cdot 1_F=1_F\cdot a = a$
10. לכל $a\neq 0_F$ ב- F קיים הופכי ב- F, המסומן a^{-1} ומקיים: $a\cdot a^{-1}=a^{-1}\cdot a = 1_F$
11. דיסטריביוטיביות: $a\cdot(b+c) = a\cdot b + a\cdot c$

מבין הקבוצות שהכרנו:

הקבוצה $\mathbb{N}$ היא לא שדה כי אין בה אדיש לחיבור.

הקבוצה $\mathbb{Z}$ היא לא שדה כי אין בה הופכי.

הקבוצות $\mathbb{Q}, \mathbb{R}$ הן שדות. כל 11 התכונות מתקיימות.

קבוצת המספרים האי רציונליים היא לא שדה: למשל אין בה סגירות לחיבור: $0=(-\pi)+\pi$ חיברנו שני מספרים אי רציונליים וקיבלנו מספר רציונלי.

הערות:

1. האיבר 0_F נקרא גם איבר ניטרלי.
2. האיבר 1_F נקרא גם איבר היחידה.
3. בשדה, האדיש לחיבור בהכרח שונה מהאדיש לכפל: $0_F \neq 1_F$.
4. בשדות $\mathbb{R}, \mathbb{Q}$ יש אינסוף איברים ולכן הם נקראים שדות אינסופיים.
5. בקורס נכיר גם שדות עם מספר סופי של איברים שנקראים שדות סופיים.

מאפיינים של שדה:

יהי $(F,+,\cdot)$ שדה. אזי:

א. האדיש לחיבור הוא יחיד וכך גם האדיש לכפל.

ב. הנגדי הוא יחיד וכך גם ההופכי.

ג. לכל $a\in F$ מתקיים $a\cdot 0=0$.

ד. לכל $a\in F$ מתקיים $(-1)\cdot a=-a$.

ה. $a\cdot b=0$ אם ורק אם $a=0$ או $b=0$.

הוכחה:

א. האדיש לחיבור הוא יחיד.

נניח בשלילה שקיימים שני אדישים לחיבור: e_1, e_2.

מצד אחד e_1 אדיש לחיבור ולכן: $e_1+e_2=e_2$

מצד שני e_2 אדיש לחיבור ולכן: $e_1+e_2=e_1$

אגף שמאל שווה בשני המקרים ולכן: $e_1=e_2$ כלומר האדיש לחיבור הוא יחיד.

האדיש לכפל הוא יחיד.

נניח בשלילה שקיימים שני אדישים לכפל t_1, t_2.

מצד אחד t_1 אדיש לכפל ולכן: $t_1 \cdot t_2 = t_2$.

מצד שני t_2 אדיש לכפל ולכן: $t_1 \cdot t_2 = t_1$.

אבל שמאל שווה בשני המקרים ולכן $t_1 = t_2$ כלומר האדיש לכפל הוא יחיד.

ב. הנגדי הוא יחיד.

הנגדי של a הוא $-a$ כלומר $a+(-a)=0$.

נניח בשלילה שקיים נגדי נוסף: e, אז גם $a+e=0$

מיחידות האדיש נקבל: $a+(-a) = a+e$

נחבר $-a$ לשני האגפים ונקבל: $-a+(a+(-a)) = -a+(a+e)$

מחוק הקיבוץ נקבל: $(-a+a)+(-a) = (-a+a)+e$

מתכונות הנגדי נקבל: $0+(-a) = 0+e$

מתכונות האדיש נקבל: $-a = e$

ההופכי הוא יחיד.

ההופכי של a הוא a^{-1} כלומר $a \cdot a^{-1} = 1$

נניח בשלילה שקיים הופכי נוסף: t. אז גם $a \cdot t = 1$.

מיחידות האדיש לכפל נקבל: $a \cdot a^{-1} = a \cdot t$

נכפול את שני האגפים ב- a^{-1}: $a^{-1} \cdot (a \cdot a^{-1}) = a^{-1} \cdot (a \cdot t)$

לפי אסוציאטיביות הכפל נקבל: $(a^{-1} \cdot a) \cdot a^{-1} = (a^{-1} \cdot a) \cdot t$

מתכונות ההופכי נקבל: $1 \cdot a^{-1} = 1 \cdot t$

מתכונות האדיש לכפל נקבל: $a^{-1} = t$ כלומר ההופכי הוא יחיד.

ג. לכל $a \in F$ מתקיים $a \cdot 0 = 0$.

האיבר 0 אדיש לחיבור ולכן נכתוב:

$$a \cdot 0 = a \cdot (0+0) \underset{\text{חוק פילוג (11)}}{=} a \cdot 0 + a \cdot 0$$

קיבלנו: $a \cdot 0 = a \cdot 0 + a \cdot 0$

F סגור לכפל (לפי סעיף 6) ולכן יש ל- $a \cdot 0$ נגדי (לפי סעיף 4) שנקרא $-a \cdot 0$.

נחבר את $-a \cdot 0$ לשני האגפים ונקבל:

$$-a \cdot 0 + a \cdot 0 = -a \cdot 0 + (a \cdot 0 + a \cdot 0)$$

לפי חוק הקיבוץ נקבל:

$$-a \cdot 0 + a \cdot 0 = (-a \cdot 0 + a \cdot 0) + a \cdot 0$$

איבר ועוד הנגדי שלו נותן 0 ולכן:

$$0 = 0 + a \cdot 0$$

0 הוא אדיש לחיבור ולכן:

$$0 = a \cdot 0$$

ד. לכל $a\in F$ מתקיים: $(-1)\cdot a=-a$.

נחשב את ערכו של הביטוי $a+(-1)\cdot a$:

$$a+(-1)\cdot a = 1\cdot a+(-1)\cdot a \underset{\text{חוק חילוף בכפל}}{=} a\cdot 1+a\cdot(-1) \underset{\text{חוק הפילוג}}{=} a\cdot\left(1+(-1)\right) \underset{\text{מספר ועוד נגדי נותן 0}}{=} a\cdot 0 \underset{\text{הוכחנו בסעיף ג}}{=} 0$$

קיבלנו $a+(-1)\cdot a=0$ ולכן $(-1)\cdot a$ הוא נגדי של a

טוב אנו יודעים ש $-a$ הוא הנגדי של a ולכן מיחידות הנגדי נקבל $-a=(-1)\cdot a$.

ה. $a\cdot b=0$ אם ורק אם $a=0$ או $b=0$.

כיוון 1: נתון $a\cdot b=0$ וצריך להראות $a=0$ או $b=0$.

אם $b=0$ סיימנו (אחד מהם הוא 0)

אם $b\neq 0$ אז יש לו הופכי b^{-1}. נכפול בהופכי את שני אגפי המשוואה:

$$(a\cdot b)\cdot b^{-1} = 0\cdot b^{-1}$$

לפי חוק הקיבוץ בכפל:

$$a\cdot(b\cdot b^{-1}) = 0\cdot b^{-1}$$

איבר כפול ההופכי נותן 1 ו- 0 כפול איבר נותן 0 (לפי סעיף ג) לכן:

$$a\cdot 1 = 0$$

$$a = 0$$

לכן אם $b\neq 0$ אז $a=0$.

כיוון שני: נתון $a=0$ או $b=0$ וצריך להראות $a\cdot b=0$.

אם $b=0$ נקבל לפי סעיף ג במשפט: $a\cdot b = a\cdot 0 = 0$

אם $a=0$ נקבל לפי סעיף ג ולפי חוק החילוף בכפל: $a\cdot b=0\cdot b = b\cdot 0 = 0$.

לכן אם $b=0$ אז $a\cdot b=0$ וגם $a=0$ אז $a\cdot b=0$.

עוד מאפיינים של שדה:

משפט: יהי $(F,+,\cdot)$ שדה. אז לכל $a,b,c\in F$ מתקיים:

1. $-(a+b)=(-a)+(-b)$
2. $-(a\cdot b)=a\cdot(-b)=(-a)\cdot b$
3. $-(-a)=a$
4. $(-a)\cdot(-b)=a\cdot b$
5. $a\cdot(b-c)=a\cdot b-a\cdot c$
6. $(b+c)\cdot a=b\cdot a+c\cdot a$
7. $a\neq 0,\ (a^{-1})^{-1}=a$
8. $a,b\neq 0,\ (a\cdot b)^{-1}=a^{-1}\cdot b^{-1}$
9. אם $a+c=a+b$ אז $b=c$.
10. אם $a\cdot c=a\cdot b$ וגם $a\neq 0$ אז $b=c$.

נוכיח את 1,4,8, את השאר מוכיחים בצורה דומה.

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

בעצם הכוונה הוא שהנגדי של $a+b$ הוא הנגדי של a + הנגדי של b.

$$(a+b)+(-a)+(-b) \underset{\text{חילוף}}{=} (a+b)+(-b)+(-a) \underset{\text{קיבוץ}}{=} a+\left(b+(-b)\right)+(-a) \underset{\text{נגדי}}{=} a+0+(-a) \underset{\text{קיבוץ}}{=} (a+0)+(-a) \underset{\text{אדיש לחיבור}}{=} a+(-a) \underset{\text{נגדי}}{=} 0$$

לכן הנגדי של $a+b$, כלומר $-(a+b)$ הוא $(-a)+(-b)$.

(4) $(-a)\cdot(-b) = a\cdot b$

פירוש הכתוב במילים הוא "מינוס כפול מינוס שווה לפלוס".

נוכיח מאגף שמאל עד שנגיע לאגף ימין:

$$(-a)\cdot(-b) \underset{\text{סעיף ד}}{=} (-1)\cdot a\cdot(-1)\cdot b \underset{\text{חילוף}}{=} (-1)\cdot(-1)\cdot a\cdot b \underset{\text{סעיף ג}}{=} -(-1)\cdot a\cdot b \underset{\text{לפי סעיף ב במשפט זה}}{=} 1\cdot a\cdot b \underset{\text{אדיש}}{=} a\cdot b$$

(8) $a,b\neq 0,\ (a\cdot b)^{-1} = a^{-1}\cdot b^{-1}$

פירוש הכתוב במילים הוא שההופכי של $a\cdot b$ הוא $a^{-1}\cdot b^{-1}$.

לכן כדי להוכיח שזה נכון עלינו לכפול אותם ולקבל 1.

$$(a\cdot b)\cdot a^{-1}\cdot b^{-1} \underset{\text{חילוף}}{=} (a\cdot b)\cdot b^{-1}\cdot a^{-1} \underset{\text{קיבוץ}}{=} a\cdot(b\cdot b^{-1})\cdot a^{-1} \underset{\text{הופכי}}{=} a\cdot(1)\cdot(a)^{-1} \underset{\text{קיבוץ}}{=} (a\cdot 1)\cdot a^{-1} \underset{\text{אדיש}}{=} a\cdot a^{-1} \underset{\text{הופכי}}{=} 1$$

לכן ההופכי של $a\cdot b$ כלומר $(a\cdot b)^{-1}$ הוא $a^{-1}\cdot b^{-1}$ או בשפה מתמטית $(a\cdot b)^{-1} = a^{-1}\cdot b^{-1}$.

שדות סופיים:

שדה סופי הוא שדה שיש בו מספר סופי של איברים. בכל שדה יש לפחות שני איברים 0 ו-1.

נבנה שדה סופי עם שני האיברים 0 ו-1. נרשום טבלה של חיבור וטבלה של כפל:

+	0	1
0	0	1
1	1	0

x	0	1
0	0	0
1	0	1

כדי להוכיח ש-$F=\{0,1\}$ עם פעולות החיבור והכפל שהגדרנו הוא שדה נצטרך לבדוק את כל 11 התכונות.

1. $a+b\in F$: כל תוצאות החיבור הן ב-F.
2. $(a+b)+c = a+(b+c)$ יש 8 שלשות לבדוק. נבדוק 2 לדוגמה:

$$\begin{cases}(1+1)+1 = 0+1 = 1\\ 1+(1+1) = 1+0 = 1\end{cases} \qquad \begin{cases}(1+0)+1 = 1+1 = 0\\ 1+(0+1) = 1+1 = 0\end{cases}$$

3. $a+b=b+a$: קיים סימטריות בטבלת החיבור ולכן $a+b=b+a$
4. אדיש לחיבור: $a+0=0+a=a$: השורה והעמודה של 0 זהות לכותרת.
5. קיום נגדי: $a+(-a)=(-a)+a=0$: הנגדי של 0 זה 0 והנגדי של 1 זה אחד.
6. $a\cdot b\in F$: כל התוצאות הן ב-F.
7. $(a\cdot b)\cdot c = a\cdot(b\cdot c)$ יש 8 שלשות לבדוק. נבדוק 2 לדוגמה:

$$\begin{cases}(1\cdot 1)\cdot 1 = 1\cdot 1 = 1\\ 1\cdot(1\cdot 1) = 1\cdot 1 = 1\end{cases} \qquad \begin{cases}(1\cdot 0)\cdot 1 = 0\cdot 1 = 0\\ 1\cdot(0\cdot 1) = 1\cdot 0 = 0\end{cases}$$

8. $a\cdot b = b\cdot a$: קיים סימטריות בטבלת הכפל.
9. קיים אדיש לכפל: $a\cdot 1 = 1\cdot a = a$: השורה והעמודה של 1 זהות לכותרת.
10. הופכי ל-1: $1\cdot 1 = 1\cdot 1 = 1$. ההופכי של 1 הוא 1.
11. $a\cdot(b+c) = a\cdot b + a\cdot c$: יש 8 שלשות לבדוק. נבדוק 2 לדוגמה

$$\begin{cases}1\cdot(1+1) = 1\cdot 0 = 0\\ 1\cdot 1+1\cdot 1 = 1+1 = 0\end{cases} \qquad \begin{cases}1\cdot(0+1) = 1\cdot 1 = 1\\ 1\cdot 0+1\cdot 1 = 0+1 = 1\end{cases}$$

כל 11 התכונות התקיימו בטבלאות ולכן קיבלנו שדה עם 2 איברים וזה השדה הקטן ביותר שניתן לקבל.

חשבון מודולו n :

הקבוצה : $\mathbb{Z}_n=\{0,1,2,\dots,n-1\}$, $n>1$.

האם ניתן להגדיר בקבוצה $\mathbb{Z}_n$ חיבור וכפל, לקבלת שדה סופי עם n איברים?
ברור לנו שחיבור וכפל רגילים לא יתאימו, כי אז לא נקבל סגירות.
נבצע את החשבון הרגיל ונרשום את השארית שמתקבלת מחילוק התוצאה ב- n.
שארית החלוקה ב- n תמיד תהיה בין 0 לבין $n-1$ ולכן הסגירות מובטחת. חשבון זה נקרא חשבון מודולו n.

דוגמה: $\mathbb{Z}_3=\{0,1,2\}$. נכתוב את לוח החיבור מודולו n ואת לוח הכפל מודולו n.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

דוגמה לשימוש בפעולות: נחשב את הביטוי $2+2\times(1+1)$

$$2+2\times(1+1)=2+2\times2=2+(2\times2)=2+1=0$$

נהוג לסמן פעולות חשבון במודולו כך: $a(\bmod n)$ או $\oplus,\odot$.

דוגמאות:

$$30(\bmod 7)=2\ ,\qquad 3\oplus_7 4\odot_7 5=3\oplus_7 6=_7 2$$

נשאלת השאלה האם $\{\mathbb{Z}_n,\oplus_n,\oplus_n\}$ היא שדה?

בדוגמה של $\mathbb{Z}_3$ רואים את חוק הפילוג, קיום אדיש לחיבור ולחיסור, קיום הופכי ונגדי.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

האם זה יעבוד תמיד? לכל n שנבחר? חוק הפילוג בחיבור וכפל קיים כאן כי הוא קיים בסכום ובמכפלה רגילים ולכן השארית חלוקה ב- n לא משתנה.
למשל שארית החלוקה ב- n של $7+5$ או $5+7$ היא אותו הדבר.

נגדי תמיד קיים: אם $a=0$ הנגדי הוא 0.
לכל: $0\neq a_n\in\mathbb{Z}_n$ נבחר את הנגדי של a להיות $n-a$.
מאחר ו- $0<n-a<n$ לכן $n-a\in\mathbb{Z}_n$ ובנוסף: $a+(n-a)=a+n-a=n=0\ (\bmod n)$

חוק הקיבוץ וחוק הפילוג: נוכיח משפט שיראה שאלו מתקיימים לכל n.

משפט: יהיו $a,b\in\mathbb{Z}$ ו- $n\in\mathbb{N}$ אזי:

$$(1)\quad (a+b)(\bmod n)=\big(a(\bmod n)+b(\bmod n)\big)(\bmod n)$$

$$(2)\quad a\cdot b\,(\bmod n)=\big(a(\bmod n)\cdot b(\bmod n)\big)\,(\bmod n)$$

נוכיח את (1)

יהיו $a,b\in\mathbb{Z}$ ו- $n\in\mathbb{N}$ נחלק את a ואת b ב- n:

$$a = nq_1 + r_1 \Rightarrow a = r_1 \pmod n$$
$$b = nq_2 + r_2 \Rightarrow b = r_2 \pmod n$$
$$\Downarrow$$
$$a+b \pmod n = (nq_1+r_1)+(nq_2+r_2) = n(q_1+q_2)+(r_1+r_2) = r_1+r_2 \pmod n = \big(a \pmod n + b \pmod n\big) \pmod n$$

את הכפל אפשר להוכיח בצורה דומה.

ומה לגבי קיום הופכי?

ראינו כי: $4\cdot 2 =_8 0$.

נניח כי ל-4 יש הופכי, נכפול בו את שני האגפים ונקבל $2 =_8 0$ וזו סתירה.

בנוסף, זה בסתירה למשפט: בשדה $ab=0$ אםם $a=0$ או $b=0$ וכאן $a=4$ ו-$b=2$ אבל $ab =_8 0$.

סתירה זו מתקיימת לכל n פריק.

לכן כדי ש-$\mathbb{Z}_n$ יהיה שדה n צריך להיות ראשוני.

משפט: הקבוצה $\mathbb{Z}_n$ הוא שדה אם ורק אם n ראשוני.

הוכחה:

כיוון ראשון: $\mathbb{Z}_n$ הוא שדה וצריך להוכיח n מספר ראשוני.

נניח בשלילה ש-n לא ראשוני. במקרה זה קיימים $a,b \in \mathbb{Z}_n$ כך ש: $a\cdot b = n = 0 \pmod n$.

וזו סתירה לתכונות השדה שאם $a\cdot b=0$ אז $a=0$ או $b=0$. לכן n הוא מספר ראשוני.

כיוון שני: נניח ש-n מספר ראשוני וצריך להוכיח $\mathbb{Z}_n$ הוא שדה.

כבר ראינו שכל התכונות מתקיימות לכל n פרט לקיום הופכי. לכן נותר להוכיח רק את קיום ההופכי לכל $a\neq 0$ ב-$\mathbb{Z}_n$.

יהי $a \neq 0$ ב-$\mathbb{Z}_n$ נראה שקיים $b\neq 0$ ב-$\mathbb{Z}_n$ כך שמתקיים $ab=1$

נסתכל על הקבוצה $A=\{a\cdot 1, a\cdot 2, \dots, a\cdot(n-1)\}$.

ונראה ש- $1 \in A$ ולכן ל-a יש הופכי.

שלב 1: $0 \notin A$. אחרת נקבל $a\cdot b = 0 \pmod n$ עבור a,b שקטנים מ-n. כלומר: $a\cdot b = 0 = n \pmod n$

וזה אומר או ש-n לא ראשוני כי הוא מכפלה של שני מספרים קטנים מ-n או ש-$b=1$ ואז $a=0$ בסתירה לנתון על a.

שלב 2: בקבוצה $A=\{a\cdot 1, a\cdot 2, \dots, a\cdot(n-1)\}$ יש בדיוק $n-1$ איברים והם כולם שונים זה מזה.

ב-A יש $n-1$ איברים כי לקחנו את a וכפלנו אותו ב-1, ב-2, ב-3 וכולי עד $n-1$.

נניח ש $n-1$ המספרים ב-A לא שונים זה מזה,

כלומר קיימים $0<b_1<b_2<n$ כך ש $a\cdot b_1 = a\cdot b_2$:

$$a\cdot b_2 - a\cdot b_1 = 0 \pmod n$$
$$a(b_2-b_1) = 0 \pmod n$$

כלומר המכפלה מתחלקת ב-n וזה סותר את הנתון ש-n מספר ראשוני.

לכן קיבלנו ש-A מכילה $n-1$ איברים שונים זה מזה של $\mathbb{Z}_n$ ולא מכילה את 0.

ולכן בהכרח אחד מהם הוא 1. כלומר קיים מספר b בין 1 לבין $n-1$ כך ש-$ab=1$ כלומר ל-a יש הופכי.

תרגילים מעל שדות סופיים:

תרגיל 1: פתרו את המשוואות הנתונות מעל $\mathbb{Z}_7$.

א. $3+x=1$

נוסיף לשני האגפים את הנגדי של 3, כלומר את $-3\equiv_7 4$ ונקבל: $x\equiv_7 5$.

ב. $3x=4$

נכפול את שני האגפים בהופכי של 3, כלומר ב- $3^{-1}\equiv_7 5$ ונקבל: $5\cdot 3x\equiv_7 5\cdot 4 \Rightarrow x\equiv_7 20\equiv_7 6$

תרגיל 2:

פתרו את המשוואה $3x+6=11$ מעל $\mathbb{Z}_7$ ומעל $\mathbb{Z}_3$:

מעל $\mathbb{Z}_7$:

$$3x+6\equiv_7 4$$

נוסיף לשני האגפים את הנגדי של 6 כלומר את $-6\equiv_7 1$ ונקבל: $3x+6+1\equiv_7 4+1$

$$3x\equiv_7 5$$

נכפול את שני האגפים בהופכי של 3 שהוא $3^{-1}\equiv_7 5$ ונקבל: $x\equiv_7 25\equiv_7 4$

מעל $\mathbb{Z}_3$:

$$3x+6\equiv_3 2$$

$$0\cdot x+0\equiv_3 2$$

מעל $\mathbb{Z}_3$ למשוואה אין פתרון.

תרגיל 3: פתרו את המשוואה $x+y=1$ מעל $\mathbb{Z}_3$.

פתרון: ננסה לבודד מ-x ונוסיף ל-2 האגפים את הנגדי של x ב- $\mathbb{Z}_3$ כלומר את $2x$:

$$2x+x+y\equiv_3 1+2x$$

$$0+y\equiv_3 1+2x$$

$$y\equiv_3 1+2x$$

הפתרונות הם כל הזוגות מהצורה $(x,1+2x)$

ב- $\mathbb{Z}_3$ יש רק 3 פתרונות שהם: $x,y=(0,1),(1,0),(2,2)$

תרגיל: שדה חדש

נגדיר: $F=\{(x,y)\mid x,y\in\mathbb{R}\}$ זוגות סדורים של מספרים ממשיים.

אילו פעולות חיבור וכפל אנו יכולים להגדיר על F כך שנקבל שדה?

ניסיון 1:

נגדיר חיבור: $(x,y)+(z,t)=(x+z,y+t)$

נגדיר כפל: $(x,y)\cdot(z,t)=(xz,yt)$

נבדוק את כל 11 התכונות ונראה אם F שדה?

1. סגירות לחיבור:

$$(x+y)+(z,t)=(x+z,y+t)\in F$$

2. חוק החילוף לחיבור:

$$(x,y)+(z,t)=(x+z,y+t)=(z+x,t+y)=(z,t)+(x,y)$$

3. חוק הקיבוץ לחיבור:

$$\big((x,y)+(z,t)\big)+(e,f)=(x+z,y+t)+(e,f)=\big((x+z)+e,(y+t)+f\big)=\big(x+(z+e),y+(t+f)\big)=(x,y)+(z+e,t+f)=$$
$$=(x,y)+\big((z+t)+(e+f)\big)$$

4. אדיש לחיבור: $(x,y)+(0,0)=(x+0,y+0)=(x,y)$

לכן האדיש לחיבור הוא $(0,0)$.

5. נגדי לחיבור: $(x,y)+(-x,-y)=(x-x,y-y)=(0,0)$

לכן הנגדי לחיבור הוא: $(-x,-y)$.

באופן דומה מתקיים גם סגירות, חוק החילוף וחוק הקיבוץ גם לכפל.

6. סגירות לכפל: $(x,y)\cdot(z,t)=(xz,yt)\in \mathbb{F}$

7. חוק החילוף בכפל: $(x,y)\cdot(z,t)=(xz,yt)=(zx,ty)=(z,t)\cdot(x,y)$

8. חוק הקיבוץ לכפל:

$$\big((x,y)\cdot(z,t)\big)\cdot(e,f)=\big((xz)\cdot e,(yt)\cdot f\big)=\big(x\cdot(ze),y\cdot(tf)\big)=(x,y)\cdot\big((z\cdot t),(e\cdot f)\big)=(x,y)\cdot\big((z,t)\cdot(e,f)\big)$$

9. אדיש לכפל:

$$(x,y)\cdot(1,1)=(x,y)$$

ולכן $(1,1)$ הוא אדיש לכפל.

10. קיום הופכי? לא קיים הופכי לכל איבר ב-F. למשל לאיבר $(0,1)$ לא קיים הופכי כי לכל x ממשי:

$$(1,0)\cdot(x,y)=(1\cdot x,0\cdot y)=(x,0)\neq(1,1)$$

לא הצלחנו להגיע לשדה. F לא יהיה שדה עם פעולת הכפל שהוגדרה בניסיון 1.

נעשה עוד ניסיון. נשאיר את החיבור אותו דבר אבל נגדיר כפל חדש

ניסיון 2:

$$(x,y)+(z,t)=(x+z,y+t)$$
$$(x,y)\cdot(z,t)=(xz-yt,xt+yz)$$

נבדוק את תכונות הכפל החדש שהגדרנו:

6. סגירות לכפל: $(x,y)\cdot(z,t)=(xz-yt,xt+yz)\in F$

7. חוק החילוף לכפל:

$$(x,y)\cdot(z,t)=(xz-yt,xt+yz)=(zx-ty,tx+zy)=(z,t)\cdot(x,y)$$

8. חוק הקיבוץ לכפל:

$$\big((x,y)\cdot(z,t)\big)\cdot(e,f)=(xz-yt,xt+yz)\cdot(e,f)=\big((xz-yt)e-(xt+yz)f,(xz-yt)f+(xt+yz)e\big)$$

$$=\big(x(ze-tf)-y(te+zf),x(zf+te)+y(-tf+ze)\big)=(x,y)\cdot(ze-tf,te+zf)=(x,y)\cdot\big((z,t)\cdot(e,f)\big)$$

9. איבר היחידה (אדיש לכפל) הוא $(1,0)$ כי:

$$(x,y)\cdot(1,0)=(x\cdot1-y\cdot0,x\cdot0+y\cdot1)=(x,y)$$

10. הופכי לכפל הוא: $\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right)$ כי:

$$(x,y)\cdot\left(\frac{x}{x^2+y^2},\frac{-y}{x^2+y^2}\right)=\left(x\cdot\frac{x}{x^2+y^2}-y\cdot\frac{(-y)}{x^2+y^2},x\cdot\frac{(-y)}{x^2+y^2}+y\cdot\frac{x}{x^2+y^2}\right)$$

$$=\left(\frac{x^2+y^2}{x^2+y^2},\frac{(-xy+yx)}{x^2+y^2}\right)=(1,0)$$

11. חוק הפילוג:

$$(x,y)\cdot\big((z,t)+(e,f)\big)=(x,y)\cdot(z+e,t+f)=\big(x(z+e)-y(t+f),x(t+f)+y(z+e)\big)=(xz-yt+xe-yf,xt+yz+xf+ye)$$

$$=(xz-yt,xt+yz)+(xe-yf,xf+ye)=(x,y)\cdot(z,t)+(x,y)\cdot(e,f)$$

כל 11 התכונות מתקיימות ולכן F שדה.

מספרים מרוכבים

למשוואה $x^2+1=0$ אין פתרון ממשי. "נמציא" פתרון למשוואה ונקרא לו i, כלומר $(i)^2+1=0$ כלומר $i^2=-1$.

הגדרה: מספר מהצורה $z=a+ib$ כאשר $a,b\in\mathbb{R}$ וגם $i=\sqrt{-1}$ נקרא מספר מרוכב, ונתייחס לו בתור "דבר האלגברי" שלו.

דוגמאות: $7-4i$, $8i$, 10, $-\frac{2}{13}+6\sqrt{3}\,i$ הם כולם מספרים מרוכבים.

אוסף כל המספרים המרוכבים מסומן $\mathbb{C}$.

יהי $z=a+ib$ מספר מרוכב, כלומר $a,b\in\mathbb{R}$ וגם $i=\sqrt{-1}$, אזי:

א. a נקרא החלק הממשי של z ומסומן $Re(z)$.

ב. b נקרא החלק המדומה של z ומסומן $Im(z)$.

נשים לב שהחלק הממשי וגם החלק המדומה הם מספרים ממשיים כלומר $a,b\in\mathbb{R}$.

ג. הצמוד של z מסומן $\bar{z}$ ושווה ל: $\bar{z}=a-ib$ כלומר $Re(\bar{z})=Re(z)$, $Im(\bar{z})=-Im(z)$

דוגמאות:

נתון: $z=-4-7i$ אזי: $Re(z)=-4$, $Im(z)=-7$, $\bar{z}=-4+7i$

נתון: $z=3i$ אזי: $Re(z)=0$ $Im(z)=3$ $\bar{z}=-3i$

נתון: $z=-9$ אזי: $Re(z)=-9$ $Im(z)=0$ $\bar{z}=-9$

ד. z נקרא ממשי אם $Im(z)=0$

ה. z נקרא מדומה טהור אם $Re(z)=0$.

חזקות של i:

$$i=\sqrt{-1}$$
$$i^2=(\sqrt{-1})^2=-1$$
$$i^3=i^2\cdot i=-1\cdot i=-i$$
$$i^4=i^3\cdot i=(-i)\cdot(-i)=-i^2=-(-1)=1$$
$$i^5=i^4\cdot i=1\cdot i=i$$
$$i^6=i^5\cdot i=i\cdot i=-1$$

המקרה הכללי i^k עבור k טבעי:

נכתוב $k=4q+r$ כאשר $r=0,1,2,3$ אזי נקבל:

$$i^k=i^{4q+r}=i^{4q}\cdot i^r=(i^4)^q\cdot i^r=1^q\cdot i^r=i^r$$

המסקנה היא שרק השארית של החלוקה של החזקה ב-4 קובעת את ערך הביטוי:

$$i^k=i^{4q+r}=i^r=\begin{cases}1 & r=0\\ i & r=1\\ -1 & r=2\\ -i & r=3\end{cases}$$

דוגמא:

$$i^{323}=i^{4\cdot 80+3}=i^3=-i$$

דוגמא: נבט על המשוואה הריבועית $x^2-4x+13=0$ ונפתור אותה לפי נוסחת השורשים:

$$x_{1,2}=\frac{4\pm\sqrt{4^2-4\cdot 13}}{2}=\frac{4\pm\sqrt{-36}}{2}=\frac{4\pm 6\sqrt{-1}}{2}=2\pm 3i$$

פעולות חשבון עם מספרים מרוכבים:

יהי z,w שני מספרים מרוכבים. נסמן: $z=a+ib$, $w=x+iy$

נאמר כי z שווה ל- w ונסמן $z=w$ אם $Re(z)=Re(w)$ וגם $Im(z)=Im(w)$.

1. חיבור: $z+w=(a+ib)+(x+iy)=(a+x)+(b+y)i$
2. חיסור: $z+w=(a+ib)-(x+iy)=(a-x)+(b-y)i$
3. כפל: $z\cdot w=(a+ib)\cdot(x+iy)=(ax-by)+(ay+bx)i$
4. חילוק: יהיו z,w שני מספרים מרוכבים, כך ש- $w\neq 0$.
   נגדיר חילוק $\frac{z}{w}$ כך שבסוף החשבון מקבלים מספר מרוכב. $\frac{z}{w}=\frac{z}{w}\cdot\frac{\bar{w}}{\bar{w}}$

משפטים:

משפט 1: יהי $z=a+ib$ מספר מרוכב. הראו ש- z ממשי אם ורק אם $z=\bar{z}$.

הוכחה:

כיוון ראשון: נתון $z=a+ib$ ממשי, נוכיח $z=\bar{z}$.

נתון ש- z ממשי, כלומר $z=a+0i$ ולכן $\bar{z}=a-0i$ ולכן $z=\bar{z}$.

כיוון שני: נתון $z=\bar{z}$ נוכיח z ממשי.

נתון: $a+ib=a-ib$ ולכן $2bi=0$ כלומר $b=0$ ולכן $z=a+0i$ כלומר z ממשי.

משפט 2: יהי $z=a+bi$ מספר מרוכב. הראו ש- z מדומה טהור אמ"מ $\bar{z}=-z$.

כיוון ראשון: נתון ש- z מדומה טהור, כלומר $z=0+bi$ ולכן $\bar{z}=0-bi$ כלומר $\bar{z}=-z$.

כיוון שני: נתון $\bar{z}=-z$ כלומר $a-bi=-(a+bi)$ לכן $2a=0$ כלומר $a=0$ ולכן $z=0+bi$ כלומר z מדומה טהור.

הצגה גיאומטרית של מספר מרוכב:

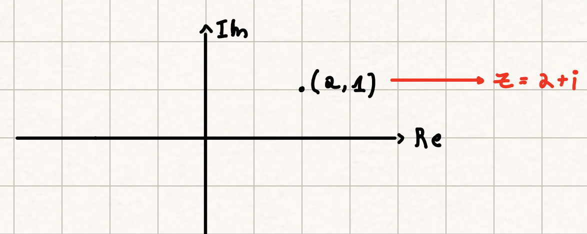
יהי z מספר מרוכב: $z=a+ib$. הזוג הסדור (a,b) נקרא "ייצוג גיאומטרי של המספר המרוכב z".

נזכיר כי לכל מספר z יש זוג סדור יחיד (a,b) ולכל זוג סדור (a,b) יש מספר מרוכב z יחיד.

לדוגמה, למספר $z=4-3i$ מתאים הזוג הסדור $(4,-3)$. ולזוג הסדור $(-2,-7)$ מתאים המספר: $z=-2-7i$.

תיאור גיאומטרי של מספר מרוכב:

כלומר, נוכל להציג מספרים מרוכבים באמצעות מערכת צירים שנקראת "המישור המרוכב".



על ציר ה- x נמצאים המספרים הממשיים (Re) ועל ציר ה- y נמצאים המספרים המדומים טהורים (Im).

המספרים הממשיים מוכלים במספרים המרוכבים ונמצאים על הציר הממשי.

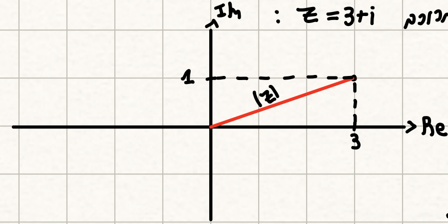
המספר 0 הוא גם ממשי וגם מדומה טהור, והוא היחיד בעל תכונה זו.

במספרים המרוכבים אין סדר כי הם מפוזרים על כל המישור ולכן הסימנים $>,<$ לא רלוונטיים בקבוצה זו.

גודל של מספר מרוכב (ערך מוחלט):

אם מתייחסים אל מספר מרוכב כזוג סדור במישור המרוכב, נוכל להגדיר מרחק של מספר מרוכב מהראשית וזה יהיה הערך המוחלט שלו (הגודל שלו), כפי שאנחנו מכירים במספרים הממשיים.

דוגמה: נצייר על המישור את המספר המרוכב $z=3+i$:



$$|z|=\sqrt{a^2+b^2}=\sqrt{3^2+1^2}=\sqrt{10}$$

לפי משפט פיתגורס $|z|=\sqrt{10}$

נשים לב שיש אינסוף מספרים מרוכבים

בעלי אורך ערך מוחלט (מעגל שכזה גדול).

הגדרה: $z=a+ib$ הוא מספר מרוכב. הערך המוחלט של z או המודול של z מסומן $|z|$ ושווה ל: $|z|=\sqrt{a^2+b^2}$

משפטים:

יהי z מספר מרוכב: $z=a+ib$ כאשר $a,b\in\mathbb{R}$. אזי:

1. $z\cdot\bar{z}=|z|^2$.
2. $|z|=0$ אמ"מ $z=0$.

הוכחה:

1. צ"ל $z\cdot\bar{z}=|z|^2$

נציב $z=a+ib$ בצורה אלגברית ונחשב:

$$z\cdot\bar{z}=(a+ib)(a-ib)=a^2+b^2=|z|^2$$

2. צ"ל $|z|=0$ אמ"מ $z=0$.

כיוון ראשון: $|z|=0$ צ"ל $z=0$.

נתון $|z|=0$, נעלה בריבוע: $|z|^2=0^2$:

$$0^2=0=|z|^2=\left(\sqrt{a^2+b^2}\right)^2=a^2+b^2$$

$$0=a^2+b^2$$

סכום ריבועים ממשיים הוא 0 ולכן $a=0,b=0$ ולכן $z=0+0i=0$.

כיוון שני: $z=0$ צ"ל $|z|=0$.

$$|z|=|0|=|0+0i|=\sqrt{0^2+0^2}=\sqrt{0}=0$$

תזכורת:

1. יהיו $z,w\in\mathbb{C}$. להגדרת החילוק $\frac{z}{w}$ כאשר $w\neq0$ יש צורך להרחיב את השבר כך שבמכנה נקבל מספר ממשי.
2. כאמור יש שמתקיים $w\cdot\bar{w}=|w|^2$, כלומר כפל של מספר מרוכב בצמוד שלו מבטיח שהתוצאה היא מספר ממשי חיובי.

הגדרת החילוק של שני מספרים מרוכבים:

יהיו z,w שני מספרים מרוכבים, כך ש- $w\neq0$. נגדיר $\frac{z}{w}$, ע"י: $\frac{z}{w}=\frac{z\cdot\bar{w}}{w\cdot\bar{w}}=\frac{z\cdot\bar{w}}{|w|^2}$

דוגמה:

1. $$\frac{5-4i}{2i-1}=\frac{5-4i}{2i-1}\cdot\frac{\overline{2i-1}}{\overline{2i-1}}=\frac{(5-4i)(-2i-1)}{|-2i+1|^2}=\frac{-13-6i}{5}=-\frac{13}{5}-\frac{6}{5}i$$

2. $$\frac{-3+2i}{2i}=\frac{-3+2i}{2i}\cdot\frac{\overline{2i}}{\overline{2i}}=\frac{(-3+2i)(-2i)}{|2i|^2}=\frac{6i+4}{4}=1+\frac{3}{2}i$$

תכונות פעולות של מספרים מרוכבים:

יהי z, z_1, z_2, z_3 מספרים מרוכבים, אזי מתקיים:

1. $z_1+z_2=z_2+z_1$
2. $z_1+(z_2+z_3)=(z_1+z_2)+z_3$
3. $z_1\cdot z_2=z_2\cdot z_1$
4. $z_1\cdot(z_2\cdot z_3)=(z_1\cdot z_2)\cdot z_3$
5. $z_1\cdot(z_2+z_3)=z_1\cdot z_2+z_1\cdot z_3$
6. $z+\bar{z}=2Re(z)$
7. $z-\bar{z}=2i\,Im(z)$
8. $\overline{z_1\pm z_2}=\bar{z}_1\pm \bar{z}_2$
9. $\overline{z_1\cdot z_2}=\bar{z}_1\cdot \bar{z}_2$
10. $\overline{z^n}=(\bar{z})^n,\ n\in\mathbb{N}$
11. $|\bar{z}|=|z|=|\bar{z}|$
12. $z\cdot\bar{z}=|z|^2$
13. $|z_1\cdot z_2|=|z_1|\cdot|z_2|$
14. $|z^n|=|z|^n,\ n\in\mathbb{N}$
15. $\overline{\left(\frac{z_1}{z_2}\right)}=\frac{\bar{z}_1}{\bar{z}_2}\quad z_2\neq 0$
16. $\left|\frac{z_1}{z_2}\right|=\frac{|z_1|}{|z_2|},\ z_2\neq 0$
17. $Re(z)\leq|z|$
18. $|z_1+z_2|\leq|z_1|+|z_2|$

תכונות 5-1 הן חוקים רגילים של חיבור (קומוטטיביות), קיבוץ (אסוציאטיביות) ופילוג (דיסטריבוטיביות).
תכונה 6 אומרת שאם נחבר מספר והצמוד שלו, נקבל מספר ממשי.
תכונה 7 אומרת שאם נחסר מספר והצמוד שלו, נקבל מספר מדומה טהור.
תכונה 9-8 הן חוקים לחיבור, חיסור וכפל של צמוד.
את תכונה 10 ניתן להוכיח על n באינדוקציה על תכונה 9.
את תכונה 14 מוכיחים באינדוקציה על n ע"י הצבת $z_1=z_2=z$ בתכונה 13.
תכונה 18 נקראת אי שוויון המשולש ונוכיח אותו בהמשך בשתי דרכים.

נוכיח את כל התכונות המסומנות באדום:

1. $z_1+z_2=z_2+z_1$

נניח: $z_1=a_1+ib_1,\ z_2=a_2+ib_2$

$$z_1+z_2=(a_1+a_2)+i(b_1+b_2)=(a_2+a_1)+i(b_2+b_1)=z_2+z_1$$

6. $z+\bar{z}=2Re(z)$

נניח $z=a+ib\ ,\ \bar{z}=a-ib$

$$z+\bar{z}=a+ib+(a-ib)=2a=2Re(z)$$

7. $z-\bar{z}=2i\,Im(z)$

נניח $z=a+ib\ ,\ \bar{z}=a-ib$

$$z-\bar{z}=a+ib-(a-ib)=2ib=2i\,Im(z)$$

9. $\overline{z_1\cdot z_2}=\overline{z_1}\cdot\overline{z_2}$

נסמן $z_1=a_1+ib_1$, $z_2=a_2+ib_2$.

$$\overline{z_1\cdot z_2}=\overline{(a_1+ib_1)(a_2+ib_2)}=\overline{(a_1a_2-b_1b_2)+i(a_1b_2+a_2b_1)}=(a_1a_2-b_1b_2)-i(a_1b_2+a_2b_1)$$

$$\overline{z_1}\cdot\overline{z_2}=(a_1-ib_1)\cdot(a_2-ib_2)=a_1a_2-a_1ib_2-ib_1a_2+i^2b_1b_2=(a_1a_2-b_1b_2)-i(a_1b_2+a_2b_1)$$

13. $|z_1\cdot z_2|=|z_1|\cdot|z_2|$

נסמן: $z_1=a_1+ib_1$, $z_2=a_2+ib_2$.

אגף שמאל:

$$|z_1\cdot z_2|=\left|(a_1+ib_1)(a_2+ib_2)\right|=\left|(a_1a_2-b_1b_2)+i(a_1b_2+a_2b_1)\right|=\sqrt{(a_1a_2-b_1b_2)^2+(a_1b_2+a_2b_1)^2}$$

$$=\sqrt{a_1^2a_2^2-2a_1a_2b_1b_2+b_1^2b_2^2+a_1^2b_2^2+2a_1b_2a_2b_1+a_2^2b_1^2}$$

$$=\sqrt{a_1^2a_2^2+b_1^2b_2^2+a_1^2b_2^2+a_2^2b_1^2}$$

אגף ימין:

$$|z_1|\cdot|z_2|=|a_1+ib_1|\cdot|a_2+ib_2|=\sqrt{a_1^2+b_1^2}\cdot\sqrt{a_2^2+b_2^2}=\sqrt{(a_1^2+b_1^2)\cdot(a_2^2+b_2^2)}$$

$$=\sqrt{a_1^2a_2^2+b_1^2b_2^2+a_1^2b_2^2+a_2^2b_1^2}$$

14. $|z^n|=|z|^n,\ n\in\mathbb{N}$

נוכיח באינדוקציה על n:

בסיס האינדוקציה: $n=1$: $|z^1|=|z|=|z|^1$

לא ממש הוכחנו משהו לכן נראה גם עבור $n=2$:

$$|z^2|=|z\cdot z|\underset{\text{תכונה 13}}{=}|z|\cdot|z|=|z|^2$$

הנחת האינדוקציה: נניח כי מתקיים $|z^n|=|z|^n$ ונרצה להוכיח $|z^{n+1}|=|z|^{n+1}$

$$|z^{n+1}|=|z^n\cdot z|\underset{\text{תכונה 13}}{=}\underbrace{|z^n|}_{\text{הנחת אינדוקציה}}\cdot|z|=|z|^n\cdot|z|=|z|^{n+1}$$

מתכונות 9 ו- 13 אפשר להוכיח באופן דומה שעבור כל כמות סופית $k\in\mathbb{N}$ של מספרים מרוכבים מתקיים:

(a) $\overline{z_1\cdot z_2\cdot\ldots\cdot z_k}=\overline{z_1}\cdot\overline{z_2}\cdot\ldots\cdot\overline{z_k}$

(b) $|z_1\cdot z_2\cdot\ldots\cdot z_k|=|z_1|\cdot|z_2|\cdot\ldots\cdot|z_k|$

15. $\overline{\left(\frac{z_1}{z_2}\right)}=\frac{\overline{z_1}}{\overline{z_2}}$ $z_2\neq0$

$$\overline{\left(\frac{z_1}{z_2}\right)}\underset{\text{הגדרת חילוק}}{=}\overline{\left(\frac{z_1\cdot\overline{z_2}}{|z_2|^2}\right)}=\overline{\left(z_1\cdot\overline{z_2}\cdot\frac{1}{|z_2|^2}\right)}\underset{\text{לפי a}}{=}\overline{z_1}\cdot\overline{\overline{z_2}}\cdot\overline{\left(\frac{1}{|z_2|^2}\right)}=\overline{z_1}\cdot z_2\cdot\frac{1}{|z|^2}=\frac{\overline{z_1}\cdot z_2}{|z_2|^2}=\frac{\overline{z_1}\cdot z_2}{z_2\cdot\overline{z_2}}=\frac{\overline{z_1}}{\overline{z_2}}$$

17. $Re(z) \le |z|$

נניח $z = a+ib$ ונקבל:

$$|z| = \sqrt{a^2+b^2} \ge \sqrt{a^2} = |a| \ge a = Re(z)$$

18. אי שוויון המשלש.