תרגול ליניארית 2

שחר פרץ

11 בנובמבר 2024

תרגילי בית בימי שלישי.

(1) FIELDS

הגדרה: שדה היא קבוצה $\mathbb{F}$ ביחד עם פעולות חיבור וכפל, שנסמנם $+,\cdot$.

- סגירות: $\forall a,b\in\mathbb{F}\colon a+b, a\cdot b\in\mathbb{F}$
- קיבוציות (אסוציאטיביות): $\forall a,b,c\in\mathbb{F}.a+(b+c)=(a+b)+c,\ a\cdot(b\cdot c)=(a\cdot b)\cdot c$
- חילופיות (קומטטיביות): $\forall a,b\in\mathbb{F}.a+b=b+a,\ a\cdot b=b\cdot a$
- קיום איבר ניטרלי: $\exists 1_{\mathbb{F}}\neq 0_{\mathbb{F}}\in\mathbb{F}\colon \forall a\in\mathbb{F}\colon a\cdot 1=a,\ a+0=a$
- קיום נגדיים והוכפיים: $\forall a\in(\mathbb{F}\exists b\in\mathbb{F}\colon a+b=c)\wedge(a\neq 0\implies \exists c\in\mathbb{F}.a\cdot c=1)$
- פילוג: $\forall a,bc\in\mathbb{F}.a(b+c)=a\cdot b+a\cdot c$

דוגמאות: $\mathbb{Z}_p,\mathbb{C},\mathbb{R},\mathbb{Q}$ הם שדות. $\mathbb{Z}$ לא שדה כי אין הופכיים. גם $\mathbb{Z}_n$ לא שדה עבור n לא ראשוני כי אין הופכי לכל איבר בשדה; אם אין n לא ראשוני, אז יש $a,b>1$ כך ש־$a\cdot b=n$. אז $a\cdot b=0$ ב־$\mathbb{Z}_n$. אבל $a,b\neq 0$.

1.1 תרגילים

1.1.1 תרגיל 1

יהי $\mathbb{F}$ שדה. הוכיחו את התכונות הבאות:

1. $\forall a\in\mathbb{F}.-(-a)=a$
2. $\forall a,b\in\mathbb{F}\setminus\{0\}\colon (ab)^{-1}=a^{-1}b^{-1}$
3. $\forall a,b\in\mathbb{F}\colon ab\notin\{0,1\}.)a-aba)^{-1}=a^{-1}+(b^{-1}-a)^{-1}$ ובדקו ששני האגפים מוגדרים היטב

הוכחה (1). ננסה:

$$a+(-a)=0\to-(a+(-a))=0\to(-1)(a+(-a))=0\to(-1)a+(-1)(-a)=0,\to -a+(-(-a))=0,\to-(-a)=a$$

שיטה אחרת: מיחיודת של נגדי צ.ל. $0=a+(-a)$. מחילופיות $a+(-a)=0$, שכבר ידוע לפי הגדרה. ■

הוכחה (2). לכל $a,b\in\mathbb{F}\setminus\{0\}$:

$$(ab)^{-1}\cdot(ab)=1,\ a^{-1}a=1,\ b^{-1}b=1,\implies (ab)^{-1}(ab)=a^{-1}ab^{-1}b=a^{-1}b^{-1}(ab)\therefore$$

תזכורת: לוודא שהכל מוגדר היטב.

פתרון אחד: מיחידות של הוכפי צ.ל. $(ab)(a^{-1}b^{-1})=1$. ניעזר בחילופיות ובקביוציות ונוכי חאת הדרוש. ■

הוכחה (3). צ.ל. $(a-aba)^{-1}=a^{-1}+(b^{-1}-a)^{-1}$

$a-aba\neq 0$ כי אם $a-aba=0$ אז $a=aba$ ואז $a=ab$ וזאת סתירה. גם $b^{-1}0a\neq 0$ כי אחרת $a=b^{-1}$ ואז $ab=1$ וזו סתירה. מהיחידות של ההופכי צ.ל. $(a-aba)(a^{-1}+(b^{-1}-a)^{-1})=1$. נדע:

$$\begin{aligned}\cdots=(a-aba)a^{-1}=(a-aba)(b^{-1}-a)^{-1}=(1-ab)+(abb^{-1}-aba)(b^{-1}-a)=(1-ab)+ab(b^{-1}-a)(b^{-1}-a)^{-1}\\=(1-ab)+ab\cdot 1=1-ab+ab=1\end{aligned}$$

■

1.1.2 תרגיל 2

הוכיחו שהקבוצה $\mathbb{Q}(\sqrt{2})=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}$ הוא שדה, ביחס לפעולות החיבור והכפל של הממשיים.

הוכחה. כל הכונות כמו חילופיות, אסוציאטיביות, וכו' ארוזים עם העובדה שאנחנו משתמשים בפעולות על הממשיים. נמשיך מכאן. צריך לבדוק ש־$0,1\in\mathbb{Q}(\sqrt{2})$, וסגירות לחיבור, כפל, נכדי והופכי.

בבירור $0,1\in\mathbb{Q}(\sqrt{2})$. סגירות לחיבור, כפל ונגדי נובעים מהסגירות של $\mathbb{Q}$ לפעולות האלה:

$$(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}\in\mathbb{Q}(\sqrt{2}) \tag{1}$$

$$(a+b\sqrt{2})(c+d\sqrt{2})=ac+ad\sqrt{2}+bc\sqrt{2}+bd=(ac+2bd)+(ad+bc)\sqrt{2}=(a+b\sqrt{2})=(-a)+(-b)\sqrt{2}\in\mathbb{Q}(2) \tag{2}$$

בשביל קיום הופכי, נשים לב שלכל $a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$:

$$\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\left(\frac{a}{a-2b^2}\right)+\left(\frac{b}{2b^2-a^2}\right)\in\mathbb{Q}(\sqrt{2})$$

נשים לב שזה מוגדר היטב, כי אם $a^2-2b^2=0$ אז $2=\left(\frac{a}{b}\right)^2$ $\sqrt{}=\frac{a}{b}$ וזו סתירה. ■

1.1.3 תרגיל 3

תרגילהראו שקיים שדה מגודל 4.

הוכחה. חייבים להיות $0_{\mathbb{F}},1_{\mathbb{F}}$ בשדה, נסמן את שני האיברים שנשארו a,b. יאי, תוולעות חיבור וכפל:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

שלב 1: נמצא מה הוא $1+1$.

1. אם $1+1=1$ אז $1=0$ וזו סתירה.
2. אם $1+1=a$, נתובנן ב־$a+1$
   (a) אם $1+a=1$ אז $a=0$ וזו סתירה.
   (b) אם $a+1=a$ אז $1=0$ וזו גם סתירה.
3. אם $1+a=0$, נבדוק למה $b+1$ שווה.
   (a) אם $b+1=0$, אז $a+1=0=b+1$ ואז $a=b$ וזו סתירה.
   (b) אפ $b+1=1$ אז $b=0$ וזאת סתירה.
   (c) אם $b+1=b$ אז $1=0$וזו סתירה
   (d) אם $b+1=a$ אז אז $b+1=1+1$ ואז $b=1$ וזו סתירה.

   ולכן בלתי אפשרי ש־$1+a=0$.

לכן $1+a=b$. מאותן סיבות מקבלים ש$b+1=0$.

$a^2=(1+1)^2(1+1)^2=1+1+1+1=a+1+1=b+1=0$ וזאת סתירה ולכן שאנחנו בשדה. לכן $a_a\neq a$ ואופן סימטרי $1+1\neq b$. סך הכל, קיבלנו ש־$1+1=0$.

שלב שני. נרצה להבין מה זה $a+1$

1. אם $a+1=1$ סתירה.
2. אם $a+1=a$ סתירה.
3. אם $a=1=0$ אז $a=1$ וזאת סתירה.

לכאן $a+1=b$.

שלב 3. מכאן אפשר להשלים את טבלת החיבור:

$$a+a=a\cdot(1+1)=a\cdot 0=0$$
$$b+b=b(1+1)=b\cdot 0=0$$
$$a+b=a+(a+1)-(a+a)+1=0+1=1$$
$$b+1=(a+1)+1=a+(1+1)=a+0=a$$

שלב 4. נמצא את a^2. $a^2\neq 0$ כי אנחנו בשדה. בנוסף, $a^a\neq a$ כי אחרת $a=1$. בנוסף, $a^2\neq 1$, כי אם $a^2=1$ אז $a^2-1=0 \implies 0=(a-1)(a+1)=(a+1)(a+1)$ וכך $(a+1)^2=0$ כלומר $b^2=0$ וזה לא אפשרי. לכן $a^2=b$

שלב 5.

$$ab=a(a+1)=a^2+a=b+a=1 \tag{3}$$

למעשה, לא הוכחנו שהשדה קיים, רק בנינו שדה בצורת שלילה לכל שדה אחר, אבל לא הוכחנו שהוא עובד.

השדה הלא ראשוני הקטן ביותר הבא הוא בגודל 9. תהנו בלבנות אותו.

■

1.2 טענה אקראית

קיים שדה ראשוני מגודל סופי אמ"מ גודלו היא חזקה של ראשוני. נוכיח כיוון אחד, הכיוון השני דורש כלים הרבה יותר מורכבים. אסור להשתמש באמ"מ אלא רק בכיוון אחד.