אלגברה א' 01040066
גליון 2

יונתן אבידור - 214269565

22 בנובמבר 2025

שאלה 1

יהא $\mathbb{F}$ שדה. עבור $a,b \in \mathbb{F}$ נסמן $\frac{a}{b} = a \cdot b^{-1}$ (בהנחה כי b הפיך). הוכיחו את הזהויות הבאות באמצעות אקסיומות השדה (יש לנמק היטב).

א.

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$$

ב.

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$$

ג.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

פתרון 1

א.

נכתוב מחדש את מה שצריך להוכיח לפי הסימון שנתון לנו

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

ראשית נראה את יחידות האיבר ההופכי, על הגדרת ההופכי, לכל $l \in \mathbb{F}$, קיים נגדי l^{-1}.
נניח בשלילה שקיימים $m,n \in \mathbb{F}, m \neq n$ כך שגם m וגם m איברים נגדיים של l

$$m \underbrace{=}_{(*)} m \cdot 1 = m \cdot (l \cdot n) \underbrace{=}_{(**)} (m \cdot l) \cdot n = 1 \cdot n \implies m = n$$

כל איבר בשדה כפול איבדר היחידה שווה לאיבר $(*)$

אסוציאטיביות על כפל $(**)$

הגענו לסתירה, ולכן לכל איבר קיים הופכי בודד.
עכשיו נרצה להוכיח כי לכל $l,m \in \mathbb{F}$, מתקיים $(l \cdot m)^{-1} = l^{-1} \cdot m^{-1}$
לפי תכונות ההופכי והאקסיומה ששדה סגור תחת כפל

$$(l \cdot m)^{-1} \cdot (l \cdot m) = 1$$

על פי יחידות ההופכי שהוכחנו
אם $(l^{-1}\cdot m^{-1})\cdot(l\cdot m)=1$ אזי $(l\cdot m)^{-1}=(l^{-1}\cdot m^{-1})$

$$\left(l^{-1}\cdot m^{-1}\right)\cdot(l\cdot m)\underbrace{=}_{(*)}\left(l^{-1}\cdot l\right)\cdot\left(m^{-1}\cdot m\right)=1\cdot 1=1$$

כפל הוא אסוציאטיבי וקומוטטיבי $(*)$

ולכן $(l\cdot m)^{-1}=(l^{-1}\cdot m^{-1})$
כלומר

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

נרצה להראות ש $\left(b^{-1}\right)^{-1}=b$
על פי הגדרת ההופכי, לכל $l\in\mathbb{F}$, מתקיים $l^{-1}\cdot l=1$. נסתכל על ההופכי של l^{-1}

$$l^{-1}\cdot\left(l^{-1}\right)^{-1}=1$$

לפי יחידות האיבר ההופכי, $l=\left(l^{-1}\right)^{-1}$
כלומר

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

על פי הסימון (וזה שהכפל קומוטטיבי)

$$a^{-1}\cdot b=\frac{b}{a}$$

■

ב.
נכתוב מחדש את מה שצריך להוכיח על פי הסימון

$$\left(a\cdot b^{-1}\right)\cdot\left(c\cdot d^{-1}\right)=(a\cdot c)\cdot(b\cdot d)^{-1}$$

מכיוון שכפל הוא קומוטטיבי ואסוציאטיבי ניתן לכתוב ש

$$\left(a\cdot b^{-1}\right)\cdot\left(c\cdot d^{-1}\right)=(a\cdot c)\cdot\left(b^{-1}\cdot d^{-1}\right)$$

בסעיף הקודם הוכחנו כי לכל $l,m\in\mathbb{F}$ מתקיים $(l^{-1}\cdot m^{-1})=(l\cdot m)^{-1}$
ולכן

$$(a\cdot c)\cdot\left(b^{-1}\cdot d^{-1}\right)=(a\cdot c)\cdot(b\cdot d)^{-1}$$

על פי הסימון

$$(a \cdot c) \cdot (b \cdot d)^{-1} = \frac{a \cdot c}{b \cdot d}$$

■

ג.

נכתוב מחדש את מה שצריך להוכיח על פי הסימון

$$\left(a \cdot b^{-1}\right) + \left(c \cdot d^{-1}\right) = ((a \cdot d) + (b \cdot c)) \cdot (b \cdot d)^{-1}$$

על פי אקסיומות השדה, 1 הוא אדיש כפלית ולכן אפשר להכפיל כל ביטוי ב1, בנוסף $d^{-1} \cdot d = 1$

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

נכתוב מחדש את הביטוי

$$\left(d \cdot d^{-1}\right) \cdot (a \cdot b^{-1}) + \left(c \cdot d^{-1}\right)$$

על פי קומוטוטיביות ואסוציאטיביות הכפל, אפשר לכתוב $(d \cdot d^{-1}) \cdot (a \cdot b^{-1}) = (a \cdot d) \cdot (b^{-1} \cdot d^{-1})$

בצורה דומה

$$\left(c \cdot d^{-1}\right) = \left(b \cdot b^{-1}\right) \cdot \left(c \cdot d^{-1}\right) = (b \cdot c) \cdot \left(b^{-1} \cdot d^{-1}\right)$$

נכתוב מחדש את הביטוי

$$(a \cdot d) \cdot \left(b^{-1} \cdot d^{-1}\right) + (b \cdot c) \cdot \left(b^{-1} \cdot d^{-1}\right)$$

על פי אקסיומות השדה, הכפל דיסטריביוטיבי על החיבור ולכן

$$(a \cdot d) \cdot \left(b^{-1} \cdot d^{-1}\right) + (b \cdot c) \cdot \left(b^{-1} \cdot d^{-1}\right) = ((a \cdot d) + (b \cdot c)) \cdot \left(b^{-1} \cdot d^{-1}\right)$$

■

שאלה 2

א.

יהא $d \in \mathbb{Z}$ כלשהו. נתבונן בתת-קבוצה הבאה של $\mathbb{C}$:

$$L = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\right\}$$

הוכיחו כי L תת-שדה של $\mathbb{C}$.

ב.

הוכיחו כי כל תת-שדה של $\mathbb{C}$ בהכרח מכיל את $\mathbb{Q}$.

פתרון 2

ידוע כי על מנת להוכיח שתת-קבוצה תחת שדה היא תת-שדה צריך להוכיח שלושה דברים: קיום איבר שאינו איבר ה0, סגירות לכפל וחיבור, והמצאות האיבר הופכי והאיבר נגדי בתת-קבוצה. לכן אלו הדברים שנרצה להוכיח
על מנת להוכיח שקיים איבר השונה מ0, ניתן לראות כי $1+2\sqrt{d}$ נמצא בL ואינו איבר ה0.
על מנת להראות שL סגורה לחיבור, נראה שלכל $m,n \in L$, מתקיים $m+n \in L$
נגדיר את m,n

$$\begin{aligned} m &:= a+b\sqrt{d} \quad a,b \in \mathbb{Q} \\ n &:= c+e\sqrt{d} \;\; c,e \in \mathbb{Q} \end{aligned}$$

נסתכל על החיבור שלהם

$$m+n = a+b\sqrt{d}+c+e\sqrt{d} = \underbrace{a+c}_{\in\mathbb{Q}}+\underbrace{(b+e)}_{\in\mathbb{Q}}\sqrt{d}$$

$a+c \in \mathbb{Q}$ כי $\mathbb{Q}$ סגורה לחיבור, אותו דבר לגבי $b+e \in \mathbb{Q}$
$m+n \in L$ ולכן L סגורה לחיבור.
נסתכל עכשיו על $m \cdot n$

$$\begin{aligned} m \cdot n = \left(a+b\sqrt{d}\right) \cdot \left(c+e\sqrt{d}\right) &= \left(a+b\sqrt{d}\right) \cdot c + \left(a+b\sqrt{d}\right) \cdot e\sqrt{d} \\ &= c \cdot a + c \cdot b\sqrt{d} + e\sqrt{d} \cdot a + e\sqrt{d} \cdot b\sqrt{d} \\ &= \underbrace{c \cdot a}_{\in\mathbb{Q}} + \underbrace{(c \cdot b + e \cdot a + e \cdot b)}_{\in\mathbb{Q}}\sqrt{d} \end{aligned}$$

$c \cdot a \in \mathbb{Q}$ כי $\mathbb{Q}$ סגורה לכפל. $c \cdot b + e \cdot a + e \cdot b \in \mathbb{Q}$ כי $\mathbb{Q}$ סגורה לכפל ולחיבור.
$m \cdot n \in L$ ולכן L סגורה לכפל.
נשאר רק להוכיח את האיבר ההופכי והנגדי
ראשית נוכיח כי $a \in \mathbb{F} \implies -a \in \mathbb{F}$
נסתכל על הנגדי של m, ונוכיח שהוא ב L

$$-m = \underbrace{(-a)}_{\in\mathbb{Q}}+\underbrace{(-b)}_{\in\mathbb{Q}}\sqrt{d}$$

$-a \in \mathbb{Q}$ כי $-1 \in \mathbb{Q}$ ו$\mathbb{Q}$ סגורה לכפל. אותו דבר לגבי $-b \in \mathbb{Q}$
נסתכל על ההופכי של m ונוכיח שהוא בL

$$m^{-1} = \frac{1}{a+b\sqrt{d}} = \frac{1}{a+b\sqrt{d}} \cdot \frac{a-b\sqrt{d}}{a-b\sqrt{d}}$$
$$= \frac{a-b\sqrt{d}}{\left(a+b\sqrt{d}\right)\left(a-b\sqrt{d}\right)} = \left(a-b\sqrt{d}\right) \cdot \underbrace{\frac{1}{a^2-b^2d}}_{\mathbb{Q}}$$
$$= \underbrace{\left(\frac{a}{a^2-b^2d}\right)}_{\in\mathbb{Q}} + \underbrace{\left(-\frac{b}{a-b^2d}\right)}_{\in\mathbb{Q}} \sqrt{d} \in L$$

L מקיים את כל התכונות של תת-שדה של $\mathbb{C}$ ולכן תת שדה של $\mathbb{C}$.
■
ב.
יהי $F \subseteq \mathbb{C}$ להיות תת שדה של $\mathbb{C}$.
על מנת להוכיח ש$F \subseteq \mathbb{Q}$ נרצה להוכיח שלכל $a, b \in \mathbb{Z}$ $b \neq 0,$ מתקיים $a \cdot b^{-1} \in F$
נוכיח קודם ש$F \subseteq \mathbb{Z}$ ותת שדה של F.
ידוע ש $\mathbb{Z}$ שדה ולכן צריך רק להוכיח ש$F \subseteq \mathbb{Z}$
על מנת לעשות זאת צריך להראות שכל$a \in \mathbb{Z}$ מקיים $a \in F$
נפרק למקרים.
$a = 0$ נמצא כי $0 \in F$ על פי ההגדרה של F כתת שדה של $\mathbb{C}$.
$a > 0$, ניתן לכתוב כ$a = \underbrace{1+1+1+\ldots+1}_{a \text{ פעמים}}$. נשים לב ש$1 \in F$ על פי ההגדרה של F כתת שדה של $\mathbb{C}$.
$a < 0$, ניתן לכתוב כ$a = 0 + \underbrace{(-1)+(-1)+(-1)+\ldots+(-1)}_{a \text{ פעמים}}$. נשים לב ש$-1 \in F$ כי -1 הוא הנגדי של 1.
הוכחנו כי $F \subseteq \mathbb{Z}$, מה שאומר שלכל $a, b \in \mathbb{Z}, b \neq 0$ מתקיים$a \cdot b^{-1} \in F$ כי F סגור להופכיים ולכפל.
על פי ההגדרה של $\mathbb{Q} = \{a \cdot b^{-1} \mid a, b \in \mathbb{Z}, b \neq 0\}$
אפשר לראות כי $F \subseteq \mathbb{Q}$.
מכיוון שF הוגדר לכל תת-שדה של $\mathbb{C}$. כל תת שדה של $\mathbb{C}$ בהכרח מכיל את $\mathbb{Q}$.
■

שאלה 3

א.
יהא $\mathbb{F}$ שדה סופי עם מספר זוגי של איברים. הראו כי מתקיים $1+1=0$
ב.
באמצעות סעיף א', הסיקו כי לא קיים שדה עם שישה איברים

פתרון 3

נניח בשלילה כי לכל איבר $0 \neq a \in \mathbb{F}$ בשדה הסופי$\mathbb{F}$ שבו יש כמות זוגית של איברים מתקיים $a + a \neq 0$ כלומר $a \neq -a$
זה אומר שעל כל איבר קיים גם ההופכי שלו. כלומר כמות האיברים בשדה היא מספר זוגי + 1 (כי ל0 אין הופכי). כלומר כמות האיברים היא אי-זוגית, הגענו לסתירה.
■
ב.
נניח בשלילה כי קיים שדה $\mathbb{F}$ בעל שישה איברים.
נגדיר את איבריו:
ארבעת האיברים הראשונים זהים לשדה בעל ארבעת האיברים $\{0,1,a,b\}$ כאשר $a \neq b$
נבחר כך ש$a \neq b+1$, $b \neq a+1$, בשביל שישה איברים נצטרך להוסיף עוד שניים.
מכיוון ש$\mathbb{F}$ סגור תחת חיבור, גם $a+1$ נמצא ב$\mathbb{F}$, וגם $b+1$.
נתבונן ב$a+b$, מכיוון ש$\mathbb{F}$ סגור תחת חיבור. $a+b$ צריך להיות שווה לאיבר אחר ב$\mathbb{F}$.
נבדוק לכל אחד מהאיברים, אם נראה ש$a+b$ לא שווה לאף איבר אחר ב$\mathbb{F}$, נגיע לסתירה

$$\begin{cases} a+b=0 \implies a=-b \overbrace{\implies}^{(*)} a=b \ (**) \\ a+b=1 \implies a+b+b=a+1 \implies a=a+1 \ (**) \\ a+b=a \implies b=0 \ (**) \\ a+b=b \implies a=1 \ (**) \\ a+b=a+1 \implies b=1 \ (**) \\ a+b=b+1 \implies a=1 \ (**) \end{cases}$$

(*) כפי שהוכחנו בסעיף הקודם, בשדה בעל כמות זוגית של איברים, כל איבר שווה להופכי של עצמו
(**) על פי הגדרת $\mathbb{F}$, $0 \neq 1 \neq a \neq a+1 \neq b \neq b+1$
הגענו לסתירה
■

שאלה 4

יהא $\mathbb{F}$ שדה. תהא $f:\mathbb{F}\to\mathbb{F}$ פונקציה המקיימת את התכונות הבאות:

$$f(x+y)=f(x)+f(y)$$
$$f(x\cdot y)=f(x)\cdot f(y)$$

נסמן

$$Ker(f)=\{x\in\mathbb{F}:f(x)=0\}$$

הוכיחו כי $Ker(f)=\{0\}$ או $Ker(f)=\mathbb{F}$

פתרון 4

צריך להוכיח בעצם שאם ישנו איבר $x\in\mathbb{F}$ אחד שמקיים$f(x)\neq 0$, אזי זה נכון לכל האיברים מלבד 0 עצמו.
נניח בשלילה שקיים לפחות $0\neq x\in\mathbb{F}$ אחד אבל לא כולם
נגדיר$a:=f(1)$, $a\in\mathbb{F}$ כי הפלט שלf תמיד ב$\mathbb{F}$, בנוסף נגדיר $a\neq 0$, זה אפשרי כי קבענו שיש לפחות איבר אחד שעבורו $f(x)\neq 0$
נסתכל על $f(x\cdot x^{-1})$

$$f\left(x\cdot x^{-1}\right)=0\cdot f\left(x^{-1}\right)=0$$

אבל אפשר גם לכתוב

$$f\left(x\cdot x^{-1}\right)=f(1)=a$$

כלומר $a=0$, סתירה.
■

שאלה 5

א.
מצאו את שארית החלוקה של2^{81} ב17
ב.
הוכיחו $2\cdot 3^n+5\cdot 14^n+4\cdot 25^n$ מתחלק ב11 לכל מספר טבעי וחיובי n.
ג.
אולי אחר כך

פתרון 5

א.
על מנת למצוא את שארית החלוקה של 2^{81} ב17
צריך למצוא את הערך של $(2^{81})\,\mathrm{mod}17$.
נשים לב ש$2^4 = 16 \equiv_{17} -1$.

$$2^{81} = 2^{(4\cdot 20)+1} \equiv_{17} (-1)^{20} \cdot 2 = 1 \cdot 2 = \boxed{2}$$

ב.
נפעיל$\bmod 11$ על הביטוי, אם התוצאה היא 0 אזי הביטוי מתחלק ב11

$$2 \cdot 3^n + 5 \cdot 14^n + 4 \cdot 25^n = 2 \cdot 3^n + 5 \cdot 3^n - 7 \cdot 3^n = (2+5-7) \cdot 3^n = 0 \cdot 3^n = 0$$

■