14.5.08 (1)

אלגברה לינארית 2 - תרגול 1 (36(א))

אלעד פורן Paranela@post.tau.ac.il

חדרי מחקר 10 (ליד הספריה)

אין חובת הגשה אבל ממש חשוב להגיש.

חוגים

תזכורת: חוג R הוא קבוצה עם פעולות חיבור וכפל כך ש:

$+$: מאוד נחמד (אסוציאטיבי, קומ', יש נטרלי 0, יש נגדי).

$\cdot$: טיפה נחמד (אסוציטיבי).

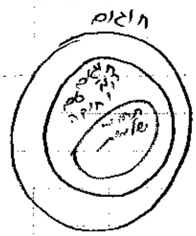
ויש קשר בין החיבור והכפל - דיסטריבוטיביות ($a(b+c)=ab+ac$)

תרגיל חימום: יהי R חוג, ויהי $a\in R$ הוכח ש $0\cdot a=0$.

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

נסמן $x=0\cdot a$ אזי $x=x+x$

$$\boxed{x=0} \Leftarrow 0=x+0 \Leftarrow -x+x=x+x-x \Leftarrow x=x+x$$



- חוג $M_n(F)$
- חוג קומוטטיבי עם יחידה.
- תחומי שלמות: חוג קומ' עם יחידה R נקרא תחום שלמות (integral domain) אם $a\cdot b=0$ אזי $a=0$ או $b=0$. דוגמאות: $\mathbb{Z}$, $K[x]$.
- שדה: שדה F הוא תחום שלמות כך שלכל $0\neq x\in F$ יש הפכי x^{-1} ($x\cdot x^{-1}=x^{-1}\cdot x=1$). למשל $\mathbb{Z}_p$, $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$.

דוגמא: חוג גאוס:

$$\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}\subseteq\mathbb{C}$$

$$(a_1+b_1i)+(a_2+b_2i)=(a_1+a_2)+(b_1+b_2)i$$

$$(a_1+b_1i)(a_2+b_2i)=(a_1a_2-b_1b_2)+(a_1b_2+b_1a_2)i$$

אזי $\mathbb{Z}[i]$ תחום שלמות. נראה של $(1+i)$ אין הופכי.
נניח בשלילה $(1+i)(a+bi)=1$ ($a,b\in\mathbb{Z}$)

$$a-b+(b+a)i=1 \Rightarrow \begin{cases} a-b=1 \\ b+a=0 \end{cases} \Rightarrow 2a=1,\ b=-a \Rightarrow \boxed{a=\tfrac{1}{2}}$$

סתירה לכך $a\in\mathbb{Z}$

14.5.08 (2)

אלגברה לינארית 2 - תרגול 1 (36/10)

<u>דוגמא:</u>

$$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b\in\mathbb{Q}\} \subseteq \mathbb{R}$$

עם החיבור והכפל הרגילים

קיימת סגירות לחיבור: $(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2})=(a_1+a_2)+(b_1+b_2)\sqrt{2}$

קיימת סגירות לכפל: $(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2})=(a_1a_2+2b_1b_2)+(a_1b_2+b_1a_2)\sqrt{2}$

יש אסוציאטיביות כי יש אסוציאטיביות במספרים הרציונליים וכנ"ל לגבי שאר התנאים של תחום השלמות.

האם $\mathbb{Q}(\sqrt{2})$ הוא שדה? צריך לבדוק האם $\frac{1}{a+b\sqrt{2}}=c+\sqrt{2}d$, $a,b,c,d\in\mathbb{Q}$

נראה כי $\mathbb{Q}(\sqrt{2})$ הוא שדה:

ניקח $a+b\sqrt{2}\in\mathbb{Q}(\sqrt{2})$ כך ש $a\neq 0$ או $b\neq 0$

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

שלמה מספר רציונלי כי ידוע ש $\mathbb{Q}$ הוא שדה ולכן הפעולות שביצעתי על a ו-b מוגדרות היטב

<u>תרגיל:</u>
נתון $R=\left\{\begin{pmatrix}a&b\\-b&a\end{pmatrix} \mid a,b\in\mathbb{Z}\right\}\subseteq M_2(\mathbb{R})$

תבדקי ש R הוא חוג ביחס לפעולות חיבור וכפל מטריצות.

<u>הוכיחי</u> $R\cong\mathbb{Z}[i]$ (R איזומורפי ל $\mathbb{Z}[i]$)

<u>תזכורת:</u> אם R,S חוגים:

<u>הומומורפיזם</u> זו העתקה $\varphi:R\to S$ ששומרת על הפעולות.

<u>איזומורפיזם</u> זה הומומורפיזם חח"ע ועל.

למשל, ההעתקה $\varphi:\mathbb{R}[x]\to\mathbb{R}$ המוגדרת $\varphi(\sum a_ix^i)=a_0$, היא בבירור הומומורפיזם, אבל לא איזומורפיזם כי $\varphi(a_0+a_1x)=a_0$ וכן $\varphi(a_0+a_1'x)=a_0$.

<u>פתרון:</u> נגדיר $\varphi:\mathbb{Z}[i]\to R$ ע"י $\varphi(a+bi)=\begin{pmatrix}a&b\\-b&a\end{pmatrix}$

זו העתקה הפיכה: $\varphi^{-1}:\begin{pmatrix}a&b\\-b&a\end{pmatrix}\longrightarrow a+bi$ לכן φ חח"ע ועל.

נבדוק ש φ שומרת על הפעולות:

$$\left.\begin{aligned}\varphi((a+bi)(c+di))&=\varphi(ac-bd+(ad+bc)i)=\begin{pmatrix}ac-bd&ad+bc\\-(ad+bc)&ac-bd\end{pmatrix}\\ \varphi(a+bi)\varphi(c+di)&=\begin{pmatrix}a&b\\-b&a\end{pmatrix}\begin{pmatrix}c&d\\-d&c\end{pmatrix}=\begin{pmatrix}ac-bd&ad+bc\\-(ad+bc)&ac-bd\end{pmatrix}\end{aligned}\right\}\Rightarrow \varphi\text{ שומרת על כפל}$$

⊛ נותר לבדוק ש φ שומרת על חיבור.

לכן φ איזומורפיזם.

☒ מש"ל.

הגדרה: א"ס $\varphi: R\to R$ נקרא אוטומורפיזם.

דוגמא: $\varphi: \mathbb{Z}[i]\to\mathbb{Z}[i]$

$$\varphi(a+bi)=a-bi$$

בדקו ש φ אוטומורפיזם של $\mathbb{Z}[i]$.

* במובן אוטומורפיזם זה מושג נדיר וקשה, לכן מבנה בעל הרבה אוטומורפיזמים הוא כנראה מבנה מאוד סימטרי.

מחלק משותף מקסימלי

הגדרה: אם $n,m\in\mathbb{Z}$ אזי הממ"מ של m,n הוא המספר הטבעי הגדול ביותר שמחלק את שניהם. מסמנים אותו $gcd(m,n)$.

דוגמאות: $gcd(15,6)=3$ (כי את 6 מחלקים 1,2,3,6 ואת 15 1,3,5,15 ו-3 הם המשותף)

$gcd(75,25)=25$

$gcd(144,100)=2^2=4$ (כי $144=16\cdot 9=2^4\cdot 3^2$ וגם $100=2^2\cdot 5^2$)

הבעיה היא שמספרים גדולים קשים לפירוק לגורמים ולכן משתמשים בשיטה הבאה:

אלגוריתם אוקלידס

נניח ש $a,b\in\mathbb{Z}$, $0<b<a$. $a=q\cdot b+r;\ 0\le r<b$

$$gcd(a,b)=gcd(b,r)$$

* הסבר לכך הוא שאם נמצא מספר שמחלק את b וגם את r אז הוא בהכרח מחלק גם את a. את ההוכחה לכתוב בבית.

$$gcd(144,100)\underset{1\cdot 100+44}{=}gcd(100,44)\underset{2\cdot 44+12}{=}gcd(44,12)=gcd(12,8)\underset{1\cdot 8+4}{=}gcd(8,4)\underset{2\cdot 4+0}{=}gcd(4,0)=\underline{4}$$

($3\cdot 12+8$)

תרגיל: מצא מחלק משותף מקסימלי של הפולינומים $\underbrace{x^4+x^3+x}_{g}$, $\underbrace{x^5+x^3+x^2+x+1}_{f}$

* תחילה נחלק את הפולינומים:

① $(x^5+x^3+x^2+x+1) : (x^4+x^3+x) = x-1$

$$x^5+x^3+x^2+x+1$$
$$-(x^5+x^4+x^2)$$
$$-x^4+x^3+x+1$$
$$-(-x^4-x^3-x)$$
$$2x^3+2x+1$$

קיבלנו,

$$x^5+x^3+x^2+x+1=(x-1)(x^4+x^3+x)=2x^3+2x+1$$

② $(x^4+x^3+x) : (2x^3+2x+1) = \frac{1}{2}x+\frac{1}{2}$

$$x^4+x^3+x$$
$$-(x^4+x^2+\tfrac{1}{2}x)$$
$$x^3-x^2+\tfrac{1}{2}x$$
$$-(x^3+x+\tfrac{1}{2})$$
$$\boxed{-x^2-\tfrac{1}{2}x-\tfrac{1}{2}}$$

③ $(2x^3+2x+1) : (-x^2-\frac{1}{2}x-\frac{1}{2}) = -2x+1$

$$2x^3+2x+1$$
$$-(2x^3+x^2+x)$$
$$-x^2+x+1$$
$$-(-x^2-\tfrac{1}{2}x-\tfrac{1}{2})$$

כלומר,

$$gcd(f,g)=gcd(x^4+x^3+x,\ 2x^3+2x+1)$$

② לפי $= gcd(2x^3+2x+1,\ -x^2-\frac{1}{2}x-\frac{1}{2})$

③ לפי $= gcd(-x^2-\frac{1}{2}x-\frac{1}{2},\ \frac{3}{2}x+\frac{3}{2})$

④ לפי $= gcd(\frac{3}{2}x+\frac{3}{2},\ -1)=1$

אלגברה לינארית 2 - תרגול 1 (המשך)

(4)
$$\begin{array}{r|l} -x^2-\frac{1}{2}x-\frac{1}{2} & \frac{3}{2}x+\frac{3}{2} \\ \hline -x^2-x & -\frac{2}{3}x+\frac{1}{3} \\ \hline \frac{1}{2}x-\frac{1}{2} & \\ \frac{1}{2}x+\frac{1}{2} & \\ \hline \boxed{-1} & \end{array}$$

<u>הגדרה:</u> אם $f,g \in k[x]$ אז הממ"מ שלהם היא הפולינום המתוקן מהמעלה המקסימלית שמחלק את שניהם.

<u>דוגמא:</u> נסתכל על הפולינומים $(2x+1)(2x+3)$, $(2x+1)(2x+1)$
נוח להגיד ש $2x+1$ מחלק הגדול ביותר אך גם $4x+2$ מחלק את שניהם
(כי $(2x+1)(2x+1)=(4x+2)(x+\frac{1}{2})$) לכן, ניקח את המתוקן, כלומר את $x+\frac{1}{2}$.

<u>הגדרה:</u> פולינום נקרא מתוקן אם המקדם המוביל שלו הוא 1.

<u>הערה לש.ב.</u> - יש שאלה 5 למצוא gcd מתוקן ש "לכתוב בצורה מפורשת" אפשר להתעלם.