בוחן מבנים אלגבריים הנדסה תשעז

25/1/2016כ"ז שבט

מתרגל: אחיה בר־און.

- ענה על 3 מתוך 4 שאלות.
- **על כל דף תשובה רשמו ת.ז. ואת שמכם המלא.**
- הקפידו על סדר ניקיון.
- משך הבוחן: שעה וחצי.
- מותר מחשבון פשוט בלבד.
- נמקו היטב את תשובתכם.
- השאלות לא מסודרות בהכרח לפי רמת קושי־ מומלץ להתחיל עם שאלות שאתם יודעים לפתור.
- ניקוד: ניקוד שווה של $33\frac{1}{3}$ נקודות לכל שאלה. בכל שאלה הניקוד מתחלק שווה בשווה בין הסעיפים.

המלצה: הסתכלו על כל השאלות והתחילו עם השאלות שאתם יודעים לענות.

חלקו את זמנכם בתבונה!

1	
2	
3	
4	
total	

בהצלחה!

.1

(א) תהא G חבורה חילופית. נגדיר $D=\{(g,g)\,:\,g\in G\}\subseteq G\times G$. הוכיחו כי

i. D תת חבורה של $G\times G$ ובנוסף שהיא תת חבורה נורמלית.

ii. הראו כי ${}^{G\times G}/_{D}\cong G$.

פתרון: טענה D היא תת חבורה. הוכחה $(e,e)\in D$ לפי הגדרה ולכן הנטרלי שייך ל D. אם $(g_1,g_1),(g_2,g_2)\in D$ אזי גם הכפל שלהם $(g_1g_2,g_1g_2)\in D$. אם $(g,g)\in D$ אזי גם ההפוכי שלו $\left(g^{-1},g^{-1}\right)\in D$. ולכן D תת חבורה.

טענה: היא גם נורמאלית. הוכחה: בחבורה חילופית, כל תת חבורה היא נורמלית.

כעת נגדיר

$$\phi:G\times G\to G$$

ע"י

$$(x,y)\to xy^{-1}$$

טענה זהו אפימורפיזם. הוכחה:

$$\phi\left((x,y)\,(z,w)\right)=\phi\left((xz,yw)\right)=xz\,(yw)^{-1}=xzw^{-1}y^{-1}=xy^{-1}zw^{-1}=\phi\left((x,y)\right)\phi\left((z,w)\right)$$

בנוסף לכל $g\in G$ ניקח את (g,e) כמקור. כעת נחשב את הגרעין

$$\ker\phi=\{(x,y)\in G\times G:\ \phi(x,y)=e\}=\left\{(x,y)\in G\times G:\ xy^{-1}=e\right\}=\{(x,y)\in G\times G:\ x=y\}=D$$

לפי משפט האיזו' הראשון נקבל את המבוקש.

(ב) נגדיר $G=\mathbb{C}^{\times}=\mathbb{C}\setminus\{0\}$ חבורה ביחס לכפל. $H=\{1,-1\}\leq G$ תת חבורה נורמלית שלה. הוכיחו כי ${}^{G}/_{H}\cong G$.

פתרון: נגדיר פונקציה

$$\phi:G\to G$$

ע"י $\phi(x)=x^2$ נוכיח כי זהו הומורפיזם על.

הומורפיזם: לכל $x,y\in G$ מתקיים

$$\phi(xy)=(xy)^2=x^2y^2=\phi(x)\phi(y)$$

בנוסף, לכל איבר בטווח $y\in G$ קיים $x=\sqrt{y}$ (כי אנחנו במרוכבים). בנוסף $x\neq 0$ (כי אחרת $x=0$ ואז $y=0$ אבל 0 לא בטווח) ולכן $x\in G$ ומתקיים $\phi(x)=y$.

כעת לפי משפט האיזומורפיזם הראשון מתקיים כי ${}^{G}/_{\ker\phi}\cong G$ נראה ש $\ker\phi=\{\pm1\}$ וזה יסיים את התרגיל. אכן

$$\ker\phi=\{x\in G:\phi(x)=1\}=\left\{x\in G:x^2=1\right\}=\{\pm1\}$$

2. הוכיחו כי הבאים הם חוגים. קבעו האם אלו חוגים חילופיים, האם אלו חוגים עם יחידה והאם חוגים אלו עם חילוק.

(א) $\mathbb{Z}[\sqrt{2}]=\left\{a+b\sqrt{2}\,|a,b\in\mathbb{Z}\right\}$עם חיבור וכפל של מספרים שלמים.

פתרון : נשים לב כי הקבוצה שהגדרנו היא תת קבוצה של המספרים הממשיים $\mathbb{R}$.

נתחיל עם הטענה כי $\mathbb{Z}[\sqrt{2}]$ ביחס לחיבור היא חבורה כיוון שהיא תת קבוצה של הממשיים זה שקול להוכיח כי היא תת חבורה שלהם. נשתמש בקריטריון הקצר:

לכל $a+b\sqrt{2},x+y\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ מתקיים

$$\left(a+b\sqrt{2}\right)-\left(x+y\sqrt{2}\right)=(a-x)+(b-y)\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$$

בנוסף $0\in\mathbb{Z}[\sqrt{2}]$.

טענה הכפל ב $\mathbb{Z}[\sqrt{2}]$ מוגדר וקיבוצי:

מוגדר: לכל $a+b\sqrt{2},x+y\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ מתקיים

$$\left(a+b\sqrt{2}\right)\left(x+y\sqrt{2}\right)=(ax+2by)+(ay+bx)\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$$

קיבוציות: נובע מקיבוציות של מספרים ממשיים

פילוג/חילופיות- גם נובע מפילוג/חילופיות של מספריים ממשיים.

בחוג $\mathbb{Z}[\sqrt{2}]$ היחידה היא $1\in\mathbb{Z}[\sqrt{2}]$

החוג $\mathbb{Z}[\sqrt{2}]$ אינו עם חילוק כי ל 2 אין הופכי. למה?

נניח בשלילה כי קיים $a+b\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$ כך ש $2(a+b\sqrt{2})=1$ זה גורר כי $2a-1=b\sqrt{2}$ בצד ימין יש מספר שלם. ולכן גם המספר בצד משאל שלם. זה קורה אמ"מ $b=0$. זה גורר $2a-1=0$ כלומר $a=\frac{1}{2}$ סתירה לכך ש $a\in\mathbb{Z}$

(ב) הקבוצה $R=\left\{\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}|\,a,b\in\mathbb{R}\right\}$ עם כפל וחיבור מטריצות.

פתרון : נתחיל עם הטענה כי R ביחס לחיבור היא חבורה כיוון שהיא תת קבוצה של המטריצות זה שקול להוכיח כי היא תת חבורה שלהם. נשתמש בקריטריון הקצר:

לכל $\begin{pmatrix}a_1 & b_1\\ 0 & 0\end{pmatrix},\begin{pmatrix}a_2 & b_2\\ 0 & 0\end{pmatrix}\in R$ מתקיים כי

$$\begin{pmatrix}a_1 & b_1\\ 0 & 0\end{pmatrix}-\begin{pmatrix}a_2 & b_2\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a_1-a_2 & b_1-b_2\\ 0 & 0\end{pmatrix}\in R$$

בנוסף $0\in R$.

טענה הכפל ב R מוגדר וקיבוצי:

מוגדר: לכל $\begin{pmatrix}a_1 & b_1\\ 0 & 0\end{pmatrix},\begin{pmatrix}a_2 & b_2\\ 0 & 0\end{pmatrix}\in R$ מתקיים כי

$$\begin{pmatrix}a_1 & b_1\\ 0 & 0\end{pmatrix}\begin{pmatrix}a_2 & b_2\\ 0 & 0\end{pmatrix}=\begin{pmatrix}a_1a_2 & a_1b_2\\ 0 & 0\end{pmatrix}\in R$$

קיבוציות: נובע מקיבוציות של מטריצות

פילוג- גם נובע מפילוג של מטריצות.

R אינו חילופי כי =

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

בחוג R אין יחידה

הוכחה: אחרת נסמן אותה ב $\left(\begin{array}{cc} a_2 & b_2 \\ 0 & 0 \end{array}\right)$. צריך להתקיים לכל $\left(\begin{array}{cc} a_1 & b_1 \\ 0 & 0 \end{array}\right)$

$$\left(\begin{array}{cc} a_1 & b_1 \\ 0 & 0 \end{array}\right)\left(\begin{array}{cc} a_2 & b_2 \\ 0 & 0 \end{array}\right)=\left(\begin{array}{cc} a_1 & b_1 \\ 0 & 0 \end{array}\right)$$

אבל

$$\left(\begin{array}{cc} a_1 & b_1 \\ 0 & 0 \end{array}\right)\left(\begin{array}{cc} a_2 & b_2 \\ 0 & 0 \end{array}\right)=\left(\begin{array}{cc} a_1a_2 & a_1b_2 \\ 0 & 0 \end{array}\right)$$

ולכן

$$\left(\begin{array}{cc} a_1a_2 & a_1b_2 \\ 0 & 0 \end{array}\right)=\left(\begin{array}{cc} a_1 & b_1 \\ 0 & 0 \end{array}\right)$$

שזה לא אפשרי (אם נבחר את $a_1 = 1$ זה גורר כי $b_2 = b_1$ אבל b_1 יכול להיות כמה אפשריות)
כיוון ש R ללא יחידה אז הוא אינו חוג עם חילוק.

.3

(א) נגדיר: $b(x) = x^3 + x^2 \in \mathbb{R}[x]$, $a(x) = 7x^7 + 6x^6 + 5x^5 + 4x^4 + 3x^3 + 2x^2 + x$ מצאו $d = \gcd(a, b)$
ומצאו $p, q \in \mathbb{R}[x]$ כך ש $ap + qb = d$.
פתרון : נחשב

$$\begin{aligned} a(x) &= b(x)\cdot\left(7x^4 - x^3 + 6x^2 - 2x + 5\right) + (-3x^2 + x) \\ b(x) &= (-3x^2 + x)\left(-\frac{x}{3} - \frac{4}{9}\right) + \left(\frac{4}{9}x\right) \\ (-3x^2 + x) &= \left(\frac{4}{9}x\right)\cdot\left(-\frac{27}{4}x + \frac{9}{4}\right) + 0 \end{aligned}$$

ולכן

$$\begin{aligned} \frac{4}{9}x &= b(x) - (-3x^2 + x)\left(-\frac{x}{3} - \frac{4}{9}\right) \\ &= b(x) - \left[a(x) - b(x)\cdot\left(7x^4 - x^3 + 6x^2 - 2x + 5\right)\right]\left(-\frac{x}{3} - \frac{4}{9}\right) \\ &= b(x)\left[1 + \left(7x^4 - x^3 + 6x^2 - 2x + 5\right)\left(-\frac{x}{3} - \frac{4}{9}\right)\right] + a(x)\left(\frac{x}{3} + \frac{4}{9}\right) \end{aligned}$$

ומכאן ש

$$x = b(x)\frac{\left[1 + \left(7x^4 - x^3 + 6x^2 - 2x + 5\right)\left(-\frac{x}{3} - \frac{4}{9}\right)\right]}{4/9} + a(x)\frac{\left(\frac{x}{3} + \frac{4}{9}\right)}{4/9}$$

ולכן (אם ניקח פולינום מתוקן) $\gcd(a, b) = x$ כאשר $q(x) = \frac{9}{4}\left[1 + \left(7x^4 - x^3 + 6x^2 - 2x + 5\right)\left(-\frac{x}{3} - \frac{4}{9}\right)\right]$, $p(x) = \frac{9}{4}\left(\frac{x}{3} + \frac{4}{9}\right)$

(ב) יהיו $a(x),b(x),c(x)\in\mathbb{F}[x]$ שלושה פולינומים הוכיחו כי אם $\gcd(a(x),c(x))=\gcd(b(x),c(x))=1$ אזי

$$\gcd(a(x)b(x),c(x))=1$$

פתרון : לפי המפשט קיימים פולינומים $t_1(x),s_1(x),t_2(x),s_2(x)$ כך ש

$$t_1(x)a(x)+s_1(x)c(x)=1$$

$$t_2(x)b(x)+s_2(x)c(x)=1$$

נכפיל ונקבל כי

$$[t_1(x)a(x)+s_1(x)c(x)]\,[t_2(x)b(x)+s_2(x)c(x)]=1$$

אחרי פתיחת סוגריים נקבל

$$t(x)a(x)b(x)+s(x)c(x)=1$$

[כאשר $t(x)=t_1(x)t_2(x), s(x)=t_1(x)a(x)s_2(x)+s_1(x)t_2(x)b(x)+s_1(x)c(x)s_2(x)$].
טענה: $\gcd(a(x)b(x),c(x))=1$. ברור כי 1 מחלק את $c(x),a(x)b(x)$. נניח $d(x)|c(x),a(x)b(x)$ אזי $d(x)$ מחלק גם את הצירוף $t(x)a(x)b(x)+s(x)c(x)=1$ ולכן $d(x)|1$ ולכן $d(x)\in\mathbb{F}$ בפרט

$$\deg(d)=0\leq\deg(1)$$

וסיימנו.

4. מצאו $x\in\mathbb{Z}$ המקיים:

$$x \equiv 57 \mod 137$$

$$x \equiv 22 \mod 131$$

שימו לב כי $131,137$ הינם מספרים ראשוניים.
פתרון : נמצא e_1,e_2 המקיימים

$$e_1 \equiv 1 \mod 137$$

$$e_1 \equiv 0 \mod 131$$

$$e_2 \equiv 0 \mod 137$$

$$e_2 \equiv 1 \mod 131$$

ע"י הצגת $\gcd(131,137)=1$ כצירוף לינארי שלהם:

$$\begin{aligned} 137 &= 1\cdot 131+6 \\ 131 &= 21\cdot 6+5 \\ 6 &= 1\cdot 5+1 \end{aligned}$$

לכן

$$\begin{aligned} 1 &= 6-1\cdot 5 = 6-1\cdot(131-21\cdot 6) = 22\cdot 6-1\cdot 131 \\ &= 22\cdot(137-1\cdot 131)-1\cdot 131 = -23\cdot 131+22\cdot 137 \end{aligned}$$

ולכן $e_2 = 1+23\cdot 131 = 22\cdot 137$ שקול ל 0 מוד 137 ושקול ל 1 מוד 131
לכן $e_1 = 1-22\cdot 137 = -23\cdot 131$ שקול ל0 מוד 131 ושקול ל 1 מוד 137 .
נגדיר $x = 57e_1+22e_2$ ואז

$$x \equiv 57e_1 \equiv 57 \mod 137$$

$$x \equiv 22e_2 \equiv 22 \mod 131$$

חישוב במחשבון יתן $x=-105433$