בוחן 3 מבנים אלגבריים הנדסה תשעח

14.1.2018

מתרגל: אחיה בר־און.

- ענו על 3 מתוך 4 שאלות.
- **כתבו בדף הראשון של המחברת את הת.ז. שלכם בצורה ברורה.**
- הקפידו על סדר ניקיון.
- משך הבוחן: שעה וחצי.
- חומר עזר: מחשבון פשוט.
- נמקו כל תשובה.
- כל שאלה 34 נקודות.
- השאלות לא מסודרות בהכרח לפי רמת קושי־ מומלץ להתחיל עם שאלות אותן אתם יודעים לפתור.

המלצה: הסתכלו על כל השאלות והתחילו עם השאלות עליהן אתם יודעים לענות.

חלקו את זמנכם בתבונה!

1	
2	
3	
4	
total	

בהצלחה!

1. יהא $a \in \mathbb{Z}$. הוכיחו: אם $\gcd(a,n) \neq 1$ אז $[a] \notin U_n$. (כאשר $[a] = a + n\mathbb{Z}$ היא מחלקת השקילות של a).
תזכורת: U_n היא חבורת ההפיכים של $\mathbb{Z}/n\mathbb{Z}$, כלומר הקבוצה $\{[x] \in \mathbb{Z}/n\mathbb{Z} | \exists [y] \in \mathbb{Z}/n\mathbb{Z} : [x][y] = [1] = [y][x]\}$ עם פעולת הכפל $[x][y] = [xy]$.
פתרון : נניח $\gcd(a,n) \neq 1$ צ"ל $a \notin U_n$. נגדיר $b = \frac{n}{\gcd(a,n)}$ מהנתון $0 < b < n$. בנוסף

$$ab = a\frac{n}{\gcd(a,n)} = \frac{a}{\gcd(a,n)} \cdot n \equiv 0 \mod n$$

לכן $[a][b] = [0]$ ב $\mathbb{Z}_n$ ו $[b] \neq [0]$ (כי $0 < b < n$ ולכן בפרט n לא מחלק את b). קיבלנו כי $[a]$ מחלק אפס ב $\mathbb{Z}_n$ ולכן לא הפיך. כלומר $[a] \notin U_n$

2. 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 משפט 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.

3. יהא $(R, +, \cdot)$ חוג. יהיו I, J אידיאלים של R כך ש $I \cap J = \{0\}$. הוכיחו כי לכל $x \in I$ ולכל $y \in J$ מתקיים כי $x \cdot y = 0$.
פתרון : יהא $x \in I$ ו $y \in J$ מתקיים כי $xy \in I$ כי Iבולע מימין ו $xy \in J$ כי J בולע משמאל. לכן $xy \in I \cap J$ כיוון ש $I \cap J = \{0\}$ נקבל כי $xy = 0$.

4.

(א) יהא $n \in \mathbb{N}$. נגדיר $m = n^2 + 4n + 1$. הוכיחו כי $\gcd(m,n) = 1$.
פתרון : מתקיים כי $1 = m - (n+4)n$. נניח בשלילה $1 < d = \gcd(m,n)$ אזי dמחלק את n ו m ולכן גם את 1 (כי הוא צירוף שלהם). סתירה.

(ב) נגדיר $n = 1011$ ו $m = \frac{n^2+4n+1}{2} = \frac{1026166}{2} = 513083$. מצאו $x \in \mathbb{Z}$ המקיים

$$x \equiv 0 \mod n$$
$$x \equiv 1 \mod m$$

(שימו לב ש x יכול להיות שלילי).

פתרון : מתקיים כי $n\left(n+4\right)-2m=1$. ולכן $n\left(n+4\right)-=1-2m$ בפרט אם נגדיר $x=1-2m=$ -1026165 נקבל כי

$$\begin{aligned} x=-\left(n+4\right)n\equiv&0 \mod n \\ x=1-2m\equiv&1 \mod m \end{aligned}$$

.