חוגים ומודולים 88-212

ד"ר ע. וישנה

מועד א', תשס"ו - **פתרון**

חלק א'. ענו על ארבע שאלות (10 נקודות לשאלה). בכל השאלות מופיעה טענה **שגויה**, ועליכם לתת לה דוגמא נגדית, שתהיה מלאה בפרטיה, ומנומקת בקיצור נמרץ. חזרה על ההגדרה אינה נחשבת נימוק.

1. **הפרך:** "אם $N \leq M$ שניהם מודולים חופשיים מעל חוג R, אז M/N חופשי".

פתרון. ניקח $R = \mathbb{Z}$, $M = R$, $N = 2R$ ($N \cong M$ כמודולים). M, N שניהם חופשיים, עם בסיסים $\{1\}, \{2\}$ בהתאמה. עם זאת, $M/N = \mathbb{Z}/2\mathbb{Z}$ אינו חופשי משום שהוא מפותל.

2. **הפרך:** "בתחום שלמות, כל אידיאל ראשוני שאינו אידיאל האפס, הוא מקסימלי".

פתרון. $R = \mathbb{Z}[x, y, z]$ הוא תחום שלמות, והאידיאל $I = \langle x \rangle$ ראשוני ואינו מקסימלי, שהרי $R/I \cong \mathbb{Z}[y, z]$ תחום שלמות שאינו שדה.

3. **הפרך:** "אם כל המקדמים (פרט לראשון) של פולינום מתוקן בעל מקדמים שלמים מתחלקים ב- 7, אז הוא אי־פריק מעל $\mathbb{Q}$". **פתרון.** $f(x) = x^2 - 49 = (x - 7)(x + 7)$ הוא דוגמא נגדית.

4. **הפרך:** "אם L אידיאל שמאלי של $\mathrm{M}_2(\mathbb{R})$ (ו- $1 \notin L$), אז $L^2 = 0$".

פתרון. $L = \begin{pmatrix} * & 0 \\ * & 0 \end{pmatrix} = \mathrm{M}_2(\mathbb{R}) \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ הוא אידיאל שמאלי אמיתי, ו- $L^2 = L \neq 0$, שהרי $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in L^2$.

5. **הפרך:** "כל אידיאל של $\mathbb{Z}[i]$, שמכיל ממש את $I = \langle i - 18 \rangle$, הוא ראשוני".

פתרון. $\mathbb{N}(i - 18) = 18^2 + 1 = 325 = 5^2 \cdot 13$, ולכן ראשוני שמחלק את $i - 18$ הוא בעל נורמה 5 או 13. כך אפשר לנחש מחלקים, ולגלות ש- $i - 18 = (2 + i)^2(3i - 2)$. כעת, $\langle (2 + i)^2 \rangle \supset \langle i - 18 \rangle$ אינו ראשוני.

חלק ב'. ענו על שלוש שאלות (20 נקודות לשאלה).

6. בחוג $R = \mathbb{Z}[x, y]$, נסמן $I_0 = \langle x, y \rangle$, $I_1 = \langle x - 1, y - 2 \rangle$ ו- $I_2 = \langle x - 2, y - 3 \rangle$.

(א) הוכח שכל שניים מבין האידיאלים הם קו־מקסימליים.

פתרון. $1 = x - (x - 1) \in I_0 + I_1$; $1 = (x - 1) - (x - 2) \in I_1 + I_2$; $1 = (y - x) - ((y - 3) - (x - 2)) \in I_0 + I_2$.

(ב) הוכח ש- $R/I_1 \cong \mathbb{Z}$ (טענה זו נכונה גם עבור I_0 ו- I_2).

פתרון. נגדיר הומומורפיזם $\phi : R \to \mathbb{Z}$ לפי $\phi(f) = f(1, 2)$. נכתוב $f(x, y) = \sum_{i,j} a_{ij}(x-1)^i(y-2)^j$, אז $\phi(f) = f(1, 2) = 0$ אם ורק אם $a_{00} = 0$, כלומר

$$f(x, y) = (y - 2) \sum_j a_{0,j+1}(y - 2)^j + (x - 1) \sum_{i,j} a_{i+1,j}(x - 1)^i(y - 2)^j.$$

לכן $\mathrm{Ker}(\phi) = I_1$, והטענה נובעת ממשפט האיזומורפיזם הראשון.

(ג) מצא איבר $f \in \mathbb{Z}[x, y]$ כך ש- $f \equiv 0 \pmod{I_0}$, $f \equiv -1 \pmod{I_1}$, $f \equiv 4 \pmod{I_2}$.

פתרון. לפי משפט השאריות הסיני קיים פתרון יחיד למערכת מודולו $I_0 \cap I_1 \cap I_2$, אלא שאת החיתוך לא קל לחשב. ננחש פתרון מהצורה $f(x, y) = a + bx + cy$, ואז התנאים הופכים למשוואות $a = 0, b + 2c = -1, 2b + 3c = 4$ שפתרונה $f = 11x - 6y$.

7. (א) צטט גרסאות נכונות ולא טריוויאליות של קריטריון אייזנשטיין ושל הלמה של גאוס.

פתרון. קריטריון אייזנשטיין: אם R שלמות ו- $P \lhd R$ אידיאל מקסימלי, אז כל פולינום $f(x) = a_n x^n + \cdots + a_0 \in R[x]$ המקיים $a_n \notin P$, $a_{n-1}, \dots, a_0 \in P$, $a_0 \notin P$, הוא אי־פריק מעל שדה השברים $F = q(R)$.

הלמה של גאוס: אם R תחום פריקות יחידה, אז גם $R[x]$ תחום פריקות יחידה.

(ב) הוכח שהפולינום $f(x)=x^4-x^3-4x^2+3x+9$ אי־פריק מעל $\mathbb{Q}$ (הדרכה: העזר בהצבה $f(x+t)=x^4+(4t-1)x^3+(6t^2-3t-4)x^2+\dots$).

פתרון. נחשב $f(x+t)=x^4+(4t-1)x^3+(6t^2-3t-4)x^2+(4t^3-3t^2-8t+3)x+(t^4-t^3-4t^2+3t+9)$. נחפש $t\in\mathbb{Z}$ וראשוני p כך ש־

$$4t-1, 6t^2-3t-4, 4t^3-3t^2-8t+3, t^4-t^3-4t^2+3t+9\equiv 0 \pmod{p}.$$

מן המשוואה הראשונה נובע ש־ $t\equiv 4^{-1}$, ומן השניה ש־ $6t^2-3t-4=6\cdot 4^{-2}-3\cdot 4^{-1}-4=(6-12-64)\cdot 4^{-2}=35\cdot 8^{-1}\equiv 0$. לכן $35\equiv 0$ ו־ $p\in\{5,7\}$. אם $p=5$ אז $t\equiv 4^{-1}\equiv -1$, ואם $p=7$ אז $t\equiv 4^{-1}\equiv 2$. נציב זאת במקדם הבא: נסמן $h(t)=4t^3-3t^2-8t+3$, אז $h(-1)=4$, $h(2)=7$. כלומר, $f(4^{-1})\not\equiv 0 \pmod 5$, $f(4^{-1})\equiv 0 \pmod 7$. כך פסלנו את $p=5$, ונשאר לבחור $p=7$ עם $t=2$. נציב: $f(x+2)=x^4+7x^3+14x^2+7x+7$, איפריק מעל $\mathbb{Q}$ לפי קריטריון אייזנשטיין ($p=7$, כאמור). לכן גם $f(x)$ איפריק.

8. (א) בתחום ראשי, איבר a הוא ראשוני אם ורק אם האידיאל Ra מקסימלי.

פתרון. אם האידיאל Ra מקסימלי אז הוא ראשוני ולכן גם a ראשוני. נניח ש־ a ראשוני, ונניח $Ra\subseteq I\subset R$. מכיוון שהחוג ראשי, $I=Rs$ עבור $s\in R$ מתאים, שאינו הפיך. אז $s\mid a$. אבל a איפריק, ולכן s חבר של a ו־ $I=Rs=Ra$.

(ב) חשב את חוג המנה $\mathbb{Z}[i]/\langle 1+2i\rangle$.

פתרון. $N(1+2i)=(1+2i)(1-2i)=5$, שהוא ראשוני ב־ $\mathbb{Z}$. לכן $1+2i$ איפריק ב־ $\mathbb{Z}[i]$, ומכיוון שזהו חוג אוקלידי, הוא ראשוני ולפי סעיף א' האידיאל $\langle 1+2i\rangle$ מקסימלי. בשדה זה $5=0$, ולכן השדה מכיל את $\mathbb{Z}/5\mathbb{Z}$, שבו $2^2=-1$. מצד שני, ההעתקה $\mathbb{Z}[i]{\rightarrow}\mathbb{Z}/5\mathbb{Z}$ המוגדרת לפי $a+bi\mapsto a+2b$ היא אפימורפיזם ש־ $1+2i$ בגרעין שלו. לכן חוג המנה הוא השדה $\mathbb{Z}/5\mathbb{Z}$.

9. מצא את הצורה הקנונית של המטריצה $A=\begin{pmatrix}1+t^4 & 1+t^2\\ 1+t & 1+t^3\end{pmatrix}$ מעל לחוג (האוקלידי) $R=\mathbb{Z}_2[t]$. חשב את המימד של R^2/AR^2 כמרחב־וקטורי מעל $\mathbb{Z}_2$.

פתרון. בעזרת כמה פעולות אלמנטריות נגלה ש־

$$\begin{aligned}\begin{pmatrix}1+t^4 & 1+t^2\\ 1+t & 1+t^3\end{pmatrix} &\sim \begin{pmatrix}1+t^4-(t^3+t^2+t+1)(1+t) & 1+t^2-(t^3+t^2+t+1)(1+t^3)\\ 1+t & 1+t^3\end{pmatrix}\\ &= \begin{pmatrix}0 & t+t^4+t^5+t^6\\ 1+t & 1+t^3\end{pmatrix}\\ &\sim \begin{pmatrix}0 & t+t^4+t^5+t^6\\ 1+t & 0\end{pmatrix}\\ &\sim \begin{pmatrix}1+t & 0\\ 0 & t(1+t)^2(t^3+t^2+1)\end{pmatrix}\end{aligned}$$

כאשר הצעד האחרון הוא החלפת שורות ועמודות, וזה שלפניו נובע מכך ש־ $(1+t)\mid(1+t^3)$.

מכאן ש־ $R^2/AR^2\cong R/(1+t)R\oplus R/(t+t^4+t^5+t^6)R$, סכום ישר של שני מודולים ציקליים מפותלים. המימד של R/fR הוא $\deg(f)$, ולכן המימדים של שני המרכיבים הם $1,6$ בהתאמה, ו־ $\dim(R^2/AR^2)=\deg(\det(A))=7$. למעשה מכיוון ש־ $t+t^4+t^5+t^6=t(1+t)^2(t^3+t^2+1)$, אפשר לפרק גם בצורה $R^2/AR^2\cong R/tR\oplus R/(1+t)R\oplus R/(1+t)^2R\oplus R/(1+t^2+t^3)R$.