חוגים ומודולים 88-212

פרופ' ס. שניידר, ד"ר ע. וישנה

מועד א', תשס"ד

ענה על חמש מתוך שבע השאלות. לכל השאלות ניקוד שווה. משך המבחן: שעתיים וחצי.

1. יהי $R = \mathrm{Hom}(V)$ החוג של העתקות ליניאריות ממרחב וקטורי V לעצמו, ויהיו $U, W \subseteq V$ תת-מרחבים. נסמן $L = \{T \in R : U \subseteq \mathrm{Ker}(T)\}$ ו- $N = \{T \in R : \mathrm{Im}(T) \subseteq W\}$.

   א. הוכח ש- L אידיאל שמאלי של R, ו- N אידיאל ימני.

   ב. חשב את המכפלה LN כאשר $W \subseteq U$.

   ג. נניח ש- $V = \mathbb{R}^2$ (כך ש- $R = M_2(\mathbb{R})$), ו- $U = \mathrm{span}\{\begin{pmatrix} 1 \\ 0 \end{pmatrix}\}$, $W = \mathrm{span}\{\begin{pmatrix} 0 \\ 1 \end{pmatrix}\}$. הוכח: $\mathrm{Id} \in LN$.

2. R חוג קומוטטיבי.

   א. הוכח ש- $I \lhd R$ אידיאל ראשוני אם ורק אם R/I תחום שלמות.

   ב. נניח ש- R תחום ראשי, ו- a מתפרק למכפלה של ראשוניים $a = p_1^{t_1} \cdots {p_s}^{t_s}$. הוכח שהאי-דיאלים הראשוניים המכילים את Ra הם Rp_i, $i = 1, ..., s$.

3. א. מצא את המחלק המשותף המקסימלי של $a = 4 - 2i$ ושל $b = 5 + 3i$ בחוג $\mathbb{Z}[i]$.

   ב. פרק את $5 + 3i$ לגורמים ראשוניים בחוג זה.

4. קבע אילו מתת-החבורות (החיבוריות) הבאות של החוג $R = M_2(\mathbb{Z})$ הן אידיאלים ימניים, שמאליים או דו-צדדיים. הצדק תשובתך.

$$N_1 = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : 3|2a + b\},$$

$$N_2 = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : 3|2a + b,\ 3|2c + d\},$$

$$N_3 = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : 3|2a + b, 3|2c + d, 3|a + c, 3|b - d\}.$$

5. א. מהם האידיאלים הראשוניים של $\mathbb{Z}_{60} = \mathbb{Z}/60\mathbb{Z}$? (אין קשר בין הסעיפים בשאלה זו)

   ב. מצא אידיאלים $I, J \lhd \mathbb{Z}$ כך ש- $I \cdot J \neq I \cap J$.

   ג. הוכח שהאידיאל הנוצר על-ידי 3 ו- $x + 2$ בחוג $\mathbb{Z}[x]$ אינו ראשי.

6. א. נסמן $\rho = e^{2\pi i/3}$. הוכח ש- $\mathbb{Q}[x]/\langle x^2 + x + 1\rangle \cong \mathbb{Q}[\rho]$.

   ב. הוכח או הפרך: $\mathbb{Q}[\sqrt{-3}] \cong \mathbb{Q}[x]/\langle x^2 + x + 1\rangle$.

7. חשב את הסדר ואת האקספוננט של החבורה האבלית

$$G = \left\langle a, b, c \;\middle|\; \begin{array}{c} 4a + 16b + 5c = 0 \\ 20a - 6b + 7c = 0 \\ 14b + 3c = 0 \end{array} \right\rangle.$$

חוגים ומודולים 88-212
פרופ' ס. שניידר, ד"ר ע. וישנה
מועד ב', תשס"ד

ענה על חמש מתוך שבע השאלות. לכל השאלות ניקוד שווה. משך המבחן: שעתיים וחצי.

1. יהי R חוג קומוטטיבי. אם $I \lhd R$ אידיאל, מגדירים $\sqrt{I} = \{a \in R | \exists n : a^n \in I\}$.
   (א) הוכח ש- $\sqrt{I}$ אידיאל של R (הדרכה: אם $a^n, b^m \in I$, חשוב על $(a+b)^{n+m}$).
   (ב) הוכח שאם $I \subseteq J$ אז $\sqrt{I} \subseteq \sqrt{J}$, וש- $\sqrt{\sqrt{I}} = \sqrt{I}$.
   (ג) הראה ש- $\sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{I+J}$.

2. כידוע, $1001 = 7 \cdot 11 \cdot 13$ ו- $1001 - 1000 = 1$. מצא $|x| < 10000$ כך ש- $x \equiv 28 \pmod{100}$ ו- $x \equiv 30 \pmod{91}$.

3. (א) הוכח שאם R חוג קומוטטיבי, $I \lhd R$ הוא אידיאל מקסימלי אם ורק אם R/I שדה.
   יהי $I = \langle a, f(x) \rangle \lhd \mathbb{Z}[x]$, כאשר $a \in \mathbb{Z}$, $f(x) \in \mathbb{Z}[x]$ פולינום מתוקן עם $deg(f) \geq 1$.
   (ב) הוכח שקיים הומומורפיזם חד-חד-ערכי $\varphi : \mathbb{Z}/\mathbb{Z} \cap I \to \mathbb{Z}[x]/I$.
   (ג) אם I אידיאל מקסימלי של $\mathbb{Z}[x]$, הוכח ש- $\mathbb{Z} \cap I$ מקסימלי ב- $\mathbb{Z}$ והסק ש- a ראשוני.

4. הוכח ש- 5 אי-פריק בחוג $\mathbb{Z}[\sqrt{2}]$. הדרכה: אם $5 = (a+b\sqrt{2})(c+d\sqrt{2})$ אז גם $5 = (a-b\sqrt{2})(c-d\sqrt{2})$ (מדוע?) ולכן $25 = (a^2-2b^2)(c^2-2d^2)$ ב- $\mathbb{Z}$.

5. יהי R חוג קומוטטיבי, ו- I אידיאל של $M_2(R)$. נגדיר $J = \{a \in R : \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \in I\}$. הוכח ש- $J \lhd R$, וש- $I = M_2(J)$.

6. (א) הוכח שהפולינום $g(x) = x^5 - 6$ אי-פריק מעל $\mathbb{Q}$.
   (ב) הוכח ש- $f(x) = x^4 + x^3 + x^2 + x + 1$ אי-פריק מעל $\mathbb{Z}$ (הדרכה: הוכח ש -$f(x+1)$ אי-פריק).
   (ג) יהי ρ שורש של $f(x)$. הוכח ש- $\rho^5 = 1$.
   (ד) חשב את המימד של $\mathbb{Q}[\rho, \sqrt[5]{6}]$ מעל $\mathbb{Q}$.

7. תהי $T : \mathbb{C}^4 \to \mathbb{C}^4$ העתקה לינארית. מגדירים את $V = \mathbb{C}^4$ להיות מודול מעל $\mathbb{C}[x]$ לפי הפעולה $f(x) \cdot v = f(T)(v)$, וקיים איזומורפיזם של מודולים, $V \cong \mathbb{C}[x]/\langle x^4 + 2x^2 + 1 \rangle$. מצא את צורת ז'ורדן של T, והסבר.

חוגים ומודולים 88-212
פרופ' ס. שניידר, ד"ר ע. וישנה
מועד ב', תשס"ד
פתרון

1. יהי R חוג קומוטטיבי. אם $I \lhd R$ אידיאל, מגדירים $\sqrt{I} = \{a \in R | \exists n : a^n \in I\}$.

(א) הוכח ש- $\sqrt{I}$ אידיאל של R (הדרכה: אם $a^n, b^m \in I$, חשוב על $(a+b)^{n+m}$).

פתרון. אם $a, b \in I$ אז קיימים n, m כך ש- $a^n, b^m \in I$, ואז $(a+b)^{n+m} = \sum_{k+s=n+m}^{\binom{n+m}{k}} a^k b^s \in I$ מכיוון שלכל k, s כך ש- $k+s = n+m$, או ש- $n \leq k$ (ואז $a^k \in I$), או $m \leq s$ (ואז $b^s \in I$). לפי ההגדרה $a+b \in \sqrt{I}$. בנוסף צריך להוכיח ש- $-a \in \sqrt{I}$, אבל $(-a)^n = \pm a^n \in I$. לבסוף, אם $r \in R$ אז $(ra)^n = r^n a^n \in I$ כי $a^n \in I$, ולכן $ra \in \sqrt{I}$.

(ב) הוכח שאם $I \subseteq J$ אז $\sqrt{I} \subseteq \sqrt{J}$, וש- $\sqrt{\sqrt{I}} = \sqrt{I}$.

פתרון. יהי $a \in \sqrt{I}$, אז קיים n כך ש- $a^n \in I$ ומכיוון ש- $I \subseteq J$, $a^n \in J$. לפי ההגדרה $a \in \sqrt{J}$.

באשר לשוויון $\sqrt{\sqrt{I}} = \sqrt{I}$, ההכלה $\sqsubseteq$ ברורה (שכן $K \sqsubseteq \sqrt{K}$ לכל אידיאל K: בוחרים $n=1$). יהי $a \in \sqrt{\sqrt{I}}$, אז לפי ההגדרה קיים n כך ש- $a^n \in \sqrt{I}$, ושוב לפי ההגדרה קיים m כך ש- $(a^n)^m \in I$. אבל אז $a^{nm} \in I$ ולפי ההגדרה $a \in \sqrt{I}$.

(ג) הראה ש- $\sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{I+J}$.

פתרון. מכיוון ש- $I, J \subseteq I+J$, מתקיים $\sqrt{I}, \sqrt{J} \subseteq \sqrt{I+J}$ ולכן גם $I+J \subseteq \sqrt{I} + \sqrt{J} \subseteq \sqrt{I+J}$. מכאן ש- $\sqrt{\sqrt{I+J}} \subseteq \sqrt{\sqrt{I} + \sqrt{J}} \subseteq \sqrt{I+J}$נ$\sqrt{I+J}$.

2. כידוע, $1001 = 7 \cdot 11 \cdot 13$ ו- $1001 - 1000 = 1$. מצא $|x| < 10000$ כך ש- $x \equiv 28 \pmod{100}$ ו- $x \equiv 30 \pmod{91}$.

פתרון. בשאלה כתובים ש- $a = -1000$, $b = 1001$ מקיימים $\{ a \equiv 0 \pmod{100} a \equiv 1 \pmod{91} \}$ ו- $\{ b \equiv 1 \pmod{100} b \equiv 0 \pmod{91} \}$. לכן $x = 28b + 30a = 28028 - 30000 = -1972$ פותר את שתי המשוואות.

3. (א) הוכח שאם R חוג קומוטטיבי, $I \lhd R$ הוא אידיאל מקסימלי אם ורק אם R/I שדה.

פתרון (משפט שהוכח בכתה). אם I מקסימלי אז לכל $a + I \in R/I$ שאינו אפס (כלומר $a \in I$), $I + Ra$ מכיל ממש את I, לכן שווה ל- R ולכן מכיל את 1. מכאן שקיים b כך ש- $ab \in 1 + I$ ו- $b + I$ ההופכי של $a + I$ ב- R/I. לכן R/I שדה. בכיוון ההפוך, אם R/I שדה ו- $I \subset J \lhd R$, יהי $a \in J - I$, אז $a + I \neq 0 + I$ ולכן $a + I$ הפיך; כלומר, קיים $b \in R$ כך ש- $(a+I)(b+I) = ab + I = 1 + I$ ואז $1 \in I + Ra \subseteq J$, כלומר $J = R$ (מכאן ש- I מקסימלי).

יהי $I = \langle a, f(x) \rangle \lhd \mathbb{Z}[x]$, כאשר $a \in \mathbb{Z}$, $f(x) \in \mathbb{Z}[x]$ פולינום מתוקן עם $deg(f) \geq 1$.

(ב) הוכח שקיים הומומורפיזם חד-חד-ערכי $\varphi : \mathbb{Z}/\mathbb{Z} \cap I \to \mathbb{Z}[x]/I$. פתרון. השיכון $\rho : \mathbb{Z} \to \mathbb{Z}[x]$ לפי $\rho(a) = a$ וההטלה $\theta : [x] \to \mathbb{Z}[x]/I$ הם בוודאי הומומורפיזמים, ולכן ההרכבה שלהם $\varphi = \theta \circ \rho$ $(\varphi : \mathbb{Z} \to \mathbb{Z}[x]/I)$ המוגדרת לפי $(\varphi(a) = a + I)$ הומומורפיזם. הגרעין כולל כל $a \in \mathbb{Z}$ כך ש- $a + I = 0 + I$ כלומר $a \in I$; מכאן ש- $\mathrm{Ker}(\varphi) = \mathbb{Z} \cap I$. לפי משפט האיזומורפיזם הראשון, $\varphi : \mathbb{Z}/\mathrm{Ker}(\varphi) \to [x]/I$ הוא חד-חד-ערכי.

(ג) אם I אידיאל מקסימלי של $\mathbb{Z}[x]$, הוכח ש- $\mathbb{Z} \cap I$ מקסימלי ב- $\mathbb{Z}$ והסק ש- a ראשוני.

פתרון. אם I אידיאל מקסימלי אז $\mathbb{Z}[x]/I$ שדה לפי סעיף א', I $\mathbb{Z}/\mathbb{Z} \cap$ שאיזומורפי לתת-חוג שלו מוכרח להיות תחום (ככל תת-חוג של שדה), ולכן $\mathbb{Z} \cap I$ אידיאל ראשוני של $\mathbb{Z}$. אבל כל אידיאל ראשוני של $\mathbb{Z}$ הוא גם מקסימלי. כעת נניח ש- f מתוקן. אז $I \cap \mathbb{Z} = (\mathbb{Z}[x] \cdot f(x) + \mathbb{Z}[x] \cdot a) \cap \mathbb{Z} = \mathbb{Z}a$ משיקולי דרגה, והיוצר a ראשוני.

4. הוכח ש- 5 אי-פריק בחוג $\mathbb{Z}[\sqrt{2}]$. הדרכה: אם $5 = (a+b\sqrt{2})(c+d\sqrt{2})$ אז גם $5 = (a-b\sqrt{2})(c-d\sqrt{2})$ (מדוע?) ולכן $25 = (a^2 - 2b^2)(c^2 - 2d^2)$ ב- $\mathbb{Z}$.

פתרון. המשוואה השניה נובעת מן הראשונה על-ידי הצמדה; או מכיוון שהכתיב של כל איבר ב- $[\sqrt{2}]$ בצורה $n + m\sqrt{2}$ $(n, m \in)$ הוא יחיד, ושתי המשוואות שקולות ל- $ac - 2bd = 5$ ו-

$ad+bc=0$. על-ידי הכפלתן מקבלים את המשוואה השלישית. הפירוקים האפשריים של 25 ב- הם כמובן $25=(\pm1)(\pm25)=(\pm5)(\pm5)$. אם $a^2-2b^2=\pm1$ אז $a+b\sqrt{2}$ הפיך, ואפשר מלכתחילה להניח שזה לא המצב. לכן $a^2-2b^2=\pm5$. זה גורר $a^2\equiv 2b^2 \pmod 5$ ולכן או $a\equiv b\equiv 0 \pmod 5$ (מכאן נובע $5|5^2$, סתירה), או ש- $(a/b)^2=2$ בשדה $\mathbb{Z}/5\mathbb{Z}$. אבל 2 אינו ריבוע בשדה הזה. לכן אין למשוואה פתרון; לא קיימים איברים עם נורמה ±5 ב- $\mathbb{Z}[\sqrt{2}]$, ו- 5 איפריק.

5. יהי R חוג קומוטטיבי, ו- I אידיאל של $M_2(R)$. נגדיר $J=\{a\in R : \begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}\in I\}$. הוכח ש- $J\lhd R$, וש- $I=M_2(J)$. יהי פתרון. יהיו $a,b\in J$, אז לפי הגדרת J, $\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix} b & 0\\ 0 & 0\end{pmatrix}\in I$, לכן גם $\begin{pmatrix} a-b & 0\\ 0 & 0\end{pmatrix}\in I$ ו- $a-b\in J$. כעת יהי $r\in R$, אז $\begin{pmatrix} r & 0\\ 0 & r\end{pmatrix}\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}=\begin{pmatrix} ra & 0\\ 0 & 0\end{pmatrix}\in I$ כי I אידיאל, ושוב לפי ההגדרה $ra\in J$.

האיבר הכללי של $M_2(J)$ הוא $x=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$ עבור $a,b,c,d\in J$. יהיו a,b,c,d כנ"ל; צריך להוכיח ש- $x\in I$. לפי ההגדרה $\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix} b & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix} c & 0\\ 0 & 0\end{pmatrix}, \begin{pmatrix} d & 0\\ 0 & 0\end{pmatrix}\in I$, לכן

$$\begin{pmatrix} a & b\\ c & d\end{pmatrix}=\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}+\begin{pmatrix} b & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix} 0 & 1\\ 0 & 0\end{pmatrix}+\begin{pmatrix} 0 & 0\\ 1 & 0\end{pmatrix}\begin{pmatrix} c & 0\\ 0 & 0\end{pmatrix}+\begin{pmatrix} 0 & 0\\ 1 & 0\end{pmatrix}\begin{pmatrix} d & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix} 0 & 1\\ 0 & 0\end{pmatrix}\in I.$$

בכיוון ההפוך, אם $x=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in I$, אז לכל i,j המטריצה $e_{1i}xe_{j1}=\begin{pmatrix} x_{ij} & 0\\ 0 & 0\end{pmatrix}\in I$, ו- $a,b,c,d\in J$.

6. (א) הוכח שהפולינום $g(x)=x^5-6$ אי-פריק מעל $\mathbb{Q}$.

פתרון. קריטריון אייזנשטיין עם $p=5$ מראה שהפולינום איפריק מעל $\mathbb{Z}$, ולכן (גאוס) מעל Q.

(ב) הוכח ש- $f(x)=x^4+x^3+x^2+x+1$ אי-פריק מעל $\mathbb{Z}$ (הדרכה: הוכח ש $f(x+1)$- אי-פריק).

פתרון. $f(x+1)=x^4+5x^3+10x^2+10x+5$ אי-פריק שוב לפי אייזנשטיין עם $p=5$, והרי פירוק $f(x)=g(x)h(x)$ משרה פירוק $f(x+1)=g(x+1)h(x+1)$. לכן f איפריק.

(ג) יהי ρ שורש של $f(x)$. הוכח ש- $\rho^5=1$.

פתרון. $\rho^5-1=(\rho-1)(\rho^4+\rho^3+\rho^2+\rho+1)=(\rho-1)f(\rho)=0$ ולכן ρ^5=1.

(ד) חשב את המימד של $\mathbb{Q}[\rho,\sqrt[5]{6}]$ מעל $\mathbb{Q}$.

פתרון. לפי סעיפים א' וב', $[\mathbb{Q}[\sqrt[5]{6}:\mathbb{Q}]=5$ ו- $[\mathbb{Q}[\rho]:\mathbb{Q}]=4$. המימדים זרים, ולכן $[\mathbb{Q}[\rho,\sqrt[5]{6}]]=4\cdot5=20$.

7. תהי $T:\mathbb{C}^4\to\mathbb{C}^4$ העתקה לינארית. מגדירים את $V=\mathbb{C}^4$ להיות מודול מעל $\mathbb{C}[x]$ לפי הפעולה $f(x)\cdot v=f(T)(v)$, וקיים איזומורפיזם של מודולים, $V\cong\mathbb{C}[x]/\langle x^4+2x^2+1\rangle$. מצא את צורת ז'ורדן של T, והסבר.

פתרון. הפולינום המינימלי של x ב- $[x]/\langle x^4+2x^2+1\rangle$ הוא $x^4+2x^2+1=(x+i)^2(x-i)^2$, לכן זהו הפולינום המינימלי של T וצורת ז'ורדן שלה כוללת בלוקים בגודל 2×2 בכל ערך עצמי. כלומר, $T\approx\begin{pmatrix} i & 1 & 0 & 0\\ 0 & i & 0 & 0\\ 0 & 0 & -i & 1\\ 0 & 0 & 0 & -i\end{pmatrix}$.

חוגים ומודולים 88-212
פרופ' ס. שניידר, ד"ר ע. וישנה
מועד ב', תשס"ד
פתרו-NOT

להלן תשובות מקוריות ושגויות בתכלית לשאלות (כולן לקוחות ממחברות בחינה). בידקו את עצמכם: האם אתם יכולים למצוא, במהירות, את הסיבה לכך שהתשובות אינן נכונות?

1. יהי R חוג קומוטטיבי. אם $I \lhd R$ אידיאל, מגדירים $\sqrt{I} = \{a \in R | \exists n : a^n \in I\}$.

(א) הוכח ש- $\sqrt{I}$ אידיאל של R (הדרכה: אם $a^n, b^m \in I$, חשוב על $(a+b)^{n+m}$).
"פתרונות". ⋆ $(a+b)^{n+m} = a^{n+m} + 2a^{n+m}b^{n+m} + b^{n+m}$.
⋆ $I \ni a \cdot a^{n-1} = a^n \in I$ גורר ש- $a \in I$ וגם $a^{n-1} \in I$.

(ב) הוכח שאם $I \subseteq J$ אז $\sqrt{I} \subseteq \sqrt{J}$, וש- $\sqrt{\sqrt{I}} = \sqrt{I}$.
"פתרונות". ⋆ אם $a \in \sqrt{I}$ אז $a^n \in \sqrt{I}$ וגם $a^{2n} \in \sqrt{\sqrt{I}}$. אבל כידוע $a^n = a^{2n}$ ולכן $\sqrt{I} = \sqrt{\sqrt{I}}$.

(ג) הראה ש- $\sqrt{\sqrt{I} + \sqrt{J}} = \sqrt{I + J}$.
"פתרונות". ⋆ בסעיף ב' הוכחנו $\sqrt{\sqrt{I}} = \sqrt{I}$, ולכן $\sqrt{I} = I$ ו- $I^2 = I$. לכן מספיק להוכיח $\sqrt{I} + \sqrt{J} = I + J$, כלומר $I + J + 2\sqrt{IJ} = I^2 + J^2 + 2IJ$. נצמצם $I = I^2$ ו- $J = J^2$ ונשאר $\sqrt{IJ} = IJ$, מש"ל.
⋆ $a^{nm} \in I + J$ אם ורק אם $a^{nm} \in I$ או $a^{nm} \in J$.

2. כידוע, $1001 = 7 \cdot 11 \cdot 13$ ו- $1 = 1001 - 1000$. מצא $|x| < 10000$ כך ש- $x \equiv 28 \pmod{100}$ ו- $x \equiv 30 \pmod{91}$.

3. (א) הוכח שאם R חוג קומוטטיבי, $I \lhd R$ הוא אידיאל מקסימלי אם ורק אם R/I שדה.
יהי $I = \langle a, f(x) \rangle \lhd \mathbb{Z}[x]$, כאשר $a \in \mathbb{Z}$, $f(x) \in \mathbb{Z}[x]$ פולינום מתוקן עם $deg(f) \geq 1$.
"פתרונות". ⋆ I אידיאל מקסימלי אם ורק אם הוא ראשוני, אם ורק אם R/I תחום שלמות, אם ורק אם הוא שדה.
⋆ I אידיאל מקסימלי, לכן הוא פולינום אי-פריק, מתוקן, מהמעלה הכי נמוכה שאפשר, ולכן R/I שדה.
יהי $I = \langle a, f(x) \rangle \lhd \mathbb{Z}[x]$, כאשר $a \in \mathbb{Z}$, $f(x) \in \mathbb{Z}[x]$ פולינום מתוקן עם $deg(f) \geq 1$.

(ב) הוכח שקיים הומומורפיזם חד-חד-ערכי $\varphi : \mathbb{Z}/\mathbb{Z} \cap I \to \mathbb{Z}[x]/I$.
⋆ $\varphi(c) = f(c)$ מגדיר הומומורפיזם $\mathbb{Z}/\mathbb{Z} \cap I \to \mathbb{Z}[x]$ לפי תכונות של פולינומים.

(ג) אם I אידיאל מקסימלי של $\mathbb{Z}[x]$, הוכח ש- $\mathbb{Z} \cap I$ מקסימלי ב- $\mathbb{Z}$ והסק ש- a ראשוני.

4. הוכח ש- 5 אי-פריק בחוג $\mathbb{Z}[\sqrt{2}]$. הדרכה: אם $5 = (a+b\sqrt{2})(c+d\sqrt{2})$ אז גם $5 = (a-b\sqrt{2})(c-d\sqrt{2})$ (מדוע?) ולכן $25 = (a^2-2b^2)(c^2-2d^2)$ ב- $\mathbb{Z}$.
"פתרונות". ⋆ הנורמה של $a + b\sqrt{2}$ בחוג $\mathbb{Z}[\sqrt{2}]$ היא $a^2 + 2b^2$.
⋆ הסיבה לגרירה הראשונה ("מדוע?") היא שב- $\mathbb{Z}[\sqrt{2}]$, $bc\sqrt{2} = -bc\sqrt{2}$ ו- $ad\sqrt{2} = -ad\sqrt{2}$.
⋆ מחפשים פתרונות ל- $5 = a^2 - 2b^2$ עבור $a, b \in$. מכיוון ש- $a = 3, b = \sqrt{2}$ מהווה פתרון שאינו ב- $\mathbb{Z}$, והפתרון צריך להיות יחיד, לא קיים פתרון ב- $\mathbb{Z}$.
⋆ $5 = (1+2i)(1-2i)$ הוא הפירוק היחיד של 5 ב- $\mathbb{Z}[i]$. אבל $2i \in \mathbb{Z}[\sqrt{2}]$, לכן אין פירוק שם.
⋆ אין פירוק כי למשוואה $5 = a^2 - 2b^2$ אין פתרון בשלמים.
⋆ אם שני איברים מחלקים את 5, אז גם המכפלה שלהם מחלקת את 5.
⋆ $5 = a^2 - 2b^2$ גורר $a^2 - \sqrt{2}b^2 = \sqrt{5}$, ולזה אין פתרון בשלמים.
⋆ כדי להוכיח ש- 5 אי-פריק, מספיק להוכיח שאין לו שורש בחוג.
⋆ $5 = (a+b\sqrt{2})(c+d\sqrt{2})$ גורר ש- 5 מחלק את $a + b\sqrt{2}$.
⋆ הוכחה של- $a^2 - 2b^2 = 5$ אין פתרון בשלמים: אם $a = 0$ אז $b = \sqrt{-5/2}$, ואם $b = 0$ אז $a = \sqrt{5}$. בשני המקרים הפתרון אינו ב-$\mathbb{Z}$.

5. יהי R חוג קומוטטיבי, ו- I אידיאל של $M_2(R)$. נגדיר $J=\{a\in R:\begin{pmatrix} a & 0\\ 0 & 0\end{pmatrix}\in I\}$. הוכח ש- $J\lhd R$, וש- $I=M_2(J)$.

6. (א) הוכח שהפולינום $g(x)=x^5-6$ אי-פריק מעל $\mathbb{Q}$.

"פתרונות". * המועמדים הרציונליים היחידים הם $\pm1,\pm1/2,\pm1/3,\pm1/6$. לפי בדיקה הם אינם שורשים, ולכן הפולינום אי-פריק.

* $x^5-6=(x^{5/2}-\sqrt{6})(x^{5/2}+\sqrt{6})$, אבל $\sqrt{6}\notin\mathbb{Q}$ ולכן זה אינו פירוק מעל $\mathbb{Q}$.
* השורש $x=6^{1/5}$ כידוע אי-פריק מעל $\mathbb{Q}$, ולכן הפולינום אי-פריק מעל $\mathbb{Q}$.
* הוכחה לזה ש- $\sqrt[5]{6}\notin\mathbb{Q}$: $\sqrt[5]{2}\notin\mathbb{Q}$ וגם $\sqrt[5]{3}\notin\mathbb{Q}$.

(ב) הוכח ש- $f(x)=x^4+x^3+x^2+x+1$ אי-פריק מעל $\mathbb{Z}$ (הדרכה: הוכח ש -$f(x+1)$ אי-פריק). "פתרונות". * השורש של הפולינום הוא $\sqrt[5]{1}>0$.

(ג) יהי ρ שורש של $f(x)$. הוכח ש- $\rho^5=1$.

(ד) חשב את המימד של $\mathbb{Q}[\rho,\sqrt[5]{6}]$ מעל $\mathbb{Q}$.

"פתרונות". * המימד של $\mathbb{Q}[\rho]$ מעל $\mathbb{Q}$ הוא 5 לפי סעיף ג'.

המימד של $\mathbb{Q}[\rho]$ מעל $\mathbb{Q}$ הוא 1 לפי הפולינום $x-\rho$.

* מכיוון ש- 5 ראשוני, המימד של $\mathbb{Z}[\rho,\sqrt[5]{6}]$ מעל $\mathbb{Q}$ הוא 5.
* המימד של $\sqrt[5]{6}$ הוא 5, ושל ρ הוא 4. לכן המימד המשותף הוא $\max\{5,4\}=5$.

7. תהי $T:\mathbb{C}^4\to\mathbb{C}^4$ העתקה לינארית. מגדירים את $V=\mathbb{C}^4$ להיות מודול מעל $\mathbb{C}[x]$ לפי הפעולה $f(x)\cdot v=f(T)(v)$, וקיים איזומורפיזם של מודולים, $V\cong\mathbb{C}[x]/\langle x^4+2x^2+1\rangle$. מצא את צורת ז'ורדן של T, והסבר.