בחינה סופית באלגברה ב'

פתרון

מועד: א
משך הבחינה: 2.5 שעות
המרצה: דוד בלנק
תאריך: 9.7.2004
סמסטר ב' תשס"ד

לשימוש הבודק

חלק ראשון (מתוך 61 נק')				
ש' 1	א (4)	ב (6)	ג (6)	(16)
ש' 2	א (4)	ב (6)	ג (5)	(15)
ש' 3	א (4)	ב (4)	ג (7)	(15)
ש' 4	א (4)	ב (5)	ג (6)	(15)
חלק שני (מתוך 39 נק')				
5	6	7	8	9
10	11	12	13	14
15	16	17	סה"כ:	
ציון מבחן: נק'				

הוראות לנבחנים

1. אין להשתמש בחומר עזר כלשהו, גם לא במחשבון.
2. נא לכתוב בעט כחול או שחור בלבד.
3. יש לכתוב את כל התשובות בטופס הבחינה.
4. אם הינך זקוק/ה למקום נוסף, השתמש/י בצד השני של העמוד. במקרה הצורך אפשר לכתוב את המשך התשובה בדפי הטיוטא בסוף טופס הבחינה, אך יש לציין זאת במקום המיועד לתשובה!
5. לכל שאלה בחלק הראשון מוקצות נקודות כמצויין שם; לכל שאלה בחלק השני מוקצות 3 נקודות.
6. יש לענות על כל השאלות.

חלק ראשון

יש לצטט במדויק את כל המשפטים עליהם הסתמכת בתשובתך. אין צורך להוכיחם.

שאלה 1. (א) (4 נק') הגדר/י את המושגים הבאים:

i. מטריצה $n \times k$ $A = (a_{ij})$ מייצגת את ההעתקה הלינארית $T : V \to W$ ביחס לבסיסים $\mathcal{B} = \{\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(n)}\}$ ל-V ו-$\mathcal{C} = \{\mathbf{w}^{(1)}, \ldots, \mathbf{w}^{(k)}\}$ ל-W. אם לכל וקטור $\vec{v} \in V$ כאשר נכתוב $\vec{v} = \sum_{i=1}^{n} c_i \vec{v}^{(i)}$, הוקטור $A\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} d_1 \\ \vdots \\ d_k \end{pmatrix}$ מקיים: $T(\vec{v}) = \sum_{j=1}^{k} d_j w^{(j)}$. במלים אחרות: עמודות A מייצגות את $T(v^{(1)}), \ldots, T(v^{(n)})$ בהתאמה ביחס לבסיס $\mathcal{C}$.

ii. A מטריצת המעבר מהבסיס $\mathcal{B} = \{\mathbf{u}^{(1)}, \ldots, \mathbf{u}^{(n)}\}$ לבסיס $\mathcal{C} = \{\mathbf{v}^{(1)}, \ldots, \mathbf{v}^{(n)}\}$ עבור המרחב הוקטורי $V \cong F^n$. אם A מייצגת את העתקת הזהות $Id_V : V \to V$ ביחס לבסיס $\mathcal{B}$ בתחום ול-$\mathcal{C}$ בטווח – במלים אחרות, אם העמודות של A מייצגות את $\vec{u}^{(1)}, \ldots, \vec{u}^{(n)}$ בהתאמה ביחס לבסיס $\mathcal{C}$, כך ש: $\sum_{j=1}^{n} a_{ji} \vec{v}^{(j)} = \vec{u}^{(i)}$ לכל $1 \le i \le n$.

(ב) (6 נק') מצא/י את מטריצת המעבר $A = A_C^B$ מן הבסיס $B := \{(3,1),(-1,0)\}$ לבסיס $C = \{(1,-1),(2,1)\}$ עבור $\mathbb{R}^2$.

$D = \begin{pmatrix}3 & -1\\ 1 & 0\end{pmatrix}$ היא מטריצת המעבר מ-B לבסיס הסטנדרטי $\{\vec{e}_1,\vec{e}_2\}$ ב-$\mathbb{R}^2$

ואילו $E = \begin{pmatrix}1 & 2\\ -1 & 1\end{pmatrix}$ היא מטריצת המעבר מ-C לבסיס הסטנדרטי ב-$\mathbb{R}^2$,

לכן $E^{-1} = \frac{1}{3}\begin{pmatrix}1 & -2\\ 1 & 1\end{pmatrix}$ מטריצת המעבר מהבסיס הסטנדרטי ל-C,

ובסה"כ מטריצת המעבר המבוקשת היא

$$A_C^B = E^{-1}\cdot D = \begin{pmatrix}\frac13 & -\frac23\\ \frac13 & \frac13\end{pmatrix}\begin{pmatrix}3 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}\frac13 & -\frac13\\ \frac43 & -\frac13\end{pmatrix}$$

בדיקה: (i) $\frac13\begin{pmatrix}1 & -1\\ 4 & -1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}\frac13\\ \frac43\end{pmatrix}$ ומתקיים: $\frac13(1,-1)+\frac43(2,1)=(3,1)$

(ii) $\frac13\begin{pmatrix}1 & -1\\ 4 & -1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}-\frac13\\ -\frac13\end{pmatrix}$ ומתקיים: $-\frac13(1,-1)-\frac13(2,1)=(-1,0)$

(ג) (6 נק') אם ההעתקה הלינארית $T:\mathbb{R}^3\to\mathbb{R}^2$ מוגדרת $T(x,y,z) := (x,y)$, מצא/י את המטריצה A המייצגת את T ביחס לבסיסים $B = \{(1,0,1),(1,1,0),(0,1,0)\}$ בתחום ו-$C = \{(2,1),(-3,-1)\}$ בטווח.

$P = \begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 0 & 0\end{pmatrix}$ היא מטריצת המעבר מ-B לבסיס הסטנדרטי ב-$\mathbb{R}^3$.

$\hat{A} = \begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}$ מייצגת את T ביחס לבסיסים הסטנדרטיים בתחום ובטווח (כי $\hat{A}\begin{pmatrix}1\\0\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$, $\hat{A}\begin{pmatrix}0\\1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$, $\hat{A}\begin{pmatrix}0\\0\\1\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$

ואלה אכן ההטלות של וקטורי הבסיס הסטנדרטי ב-$\mathbb{R}^3$ על שתי הקואורדינטות הראשונות).

$Q = \begin{pmatrix}2 & -3\\ 1 & -1\end{pmatrix}$ היא מטריצת המעבר מ-C לבסיס הסטנדרטי ב-$\mathbb{R}^2$,

לכן $Q^{-1} = \begin{pmatrix}-1 & 3\\ -1 & 2\end{pmatrix}$ היא מטריצת המעבר מהבסיס הסטנדרטי ב-$\mathbb{R}^2$ ל-C, ובסה"כ:

$$A = Q^{-1}\cdot\hat{A}\cdot P = \begin{pmatrix}-1 & 3\\ -1 & 2\end{pmatrix}\begin{pmatrix}1 & 0 & 0\\ 0 & 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 0 & 0\end{pmatrix} = \begin{pmatrix}-1 & 3 & 0\\ -1 & 2 & 0\end{pmatrix}\begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 1\\ 1 & 0 & 0\end{pmatrix} = \begin{pmatrix}-1 & 2 & 3\\ -1 & 1 & 2\end{pmatrix}$$

היא המייצגת המבוקשת.

בדיקה: $(-1)(2,1)-1(-3,-1)=(1,0)=T(1,0,1)$, $2(2,1)+1(-3,-1)=(1,1)=T(1,1,0)$,

$3(2,1)+2(-3,-1)=(0,1)=T(0,1,0)$

שאלה 2. (א) (4 נק') הגדר/י את המושגים הבאים:

(i) המטריצה P מלכסנת את המטריצה A. אם $D := P^{-1}AP$ היא מטריצה אלכסונית, כלומר $D=(d_{ij}) \Leftarrow d_{ij}=0$ עבור $i \neq j$.

(ii) $p_A(\lambda)$ הפולינום האופייני של המטריצה A.

$$P_A(\lambda) = \det(A - \lambda I_n)$$

(ב) (6 נק') האם המטריצה:

$$A := \begin{pmatrix} 3 & -1 & -1 \\ -2 & 3 & 2 \\ 4 & -1 & -2 \end{pmatrix}$$

ניתנת ללכסון? אם כן, מצא/י את הערכים העצמיים שלה, את הוקטורים העצמיים שלה, את המטריצה המלכסנת P, ואת הצורה האלכסונית D שלה. אם לא, הסבר/י מדוע לא.

(1) נחשב:

$$P_A(\lambda) = \det\begin{pmatrix} 3-\lambda & -1 & -1 \\ -2 & 3-\lambda & 2 \\ 4 & -1 & -2-\lambda \end{pmatrix} = (3-\lambda)\left[(3-\lambda)(-2-\lambda)+2\right] - (-1)\left[-2(-2-\lambda)-8\right] + (-1)\left[2-4(3-\lambda)\right]$$

$$= (3-\lambda)\left[\lambda^2-\lambda-6+2\right] + \left[2\lambda+4-8\right] - \left[4\lambda-12+2\right]$$

$$= (3-\lambda)\left[\lambda^2-\lambda-4\right] - 2\lambda+6 = (3-\lambda)\left[\lambda^2-\lambda-4+2\right] = (3-\lambda)\left[\lambda^2-\lambda-2\right]$$

$$= (3-\lambda)(\lambda+1)(\lambda-2)$$

ולכן שלושת הערכים העצמיים של P הם $2, 3$ ו- -1.

---

(2) עבור $\lambda_1 = 3$ (ריבוי אלגברי 1) נפתור את מערכת המשוואות:

$$\begin{pmatrix} 0 & -1 & -1 \\ -2 & 0 & 2 \\ 4 & -1 & -5 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 1 \\ 4 & -1 & -5 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \begin{cases} x-z=0 \\ y+z=0 \end{cases}$$

אנו רואים שדרגת המטריצה הנ"ל היא 2, ולכן מרחב הפתרונות ממימד 1 והוא $(t,-t,t)$, ואפשר לבחור $\vec{v} = (1,-1,1)$

(3) עבור $\lambda_2 = 2$ נפתור:

$$\begin{pmatrix} 1 & -1 & -1 \\ -2 & 1 & 2 \\ 4 & -1 & -4 \end{pmatrix}\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & -1 & -1 \\ 0 & -2 & 0 \\ 0 & 3 & 0 \end{pmatrix} \Rightarrow \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \Rightarrow (t,0,t), \quad \vec{v} = (1,0,1)$$

(4) עבור $\lambda_2 = -1$ נפתור:

$$\begin{pmatrix} 4 & -1 & -1 \\ -2 & 4 & 2 \\ 4 & -1 & -1 \end{pmatrix} \Rightarrow \begin{pmatrix} 4 & -1 & -1 \\ 0 & 7 & 3 \\ 0 & 0 & 0 \end{pmatrix} \Rightarrow \vec{v} = (1,-3,7)$$

והמטריצה המלכסנת $P = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & -3 \\ 1 & 1 & 7 \end{pmatrix}$, צורה אלכסונית: $D = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & -1 \end{pmatrix}$ ..4/

(ג) (5 נק') תהי $T:\mathbb{R}^2\to\mathbb{R}^2$ ההעתקה המיוצגת על-ידי המטריצה $A:=\begin{pmatrix}0.9 & 0.2\\ 0.1 & 0.8\end{pmatrix}$.

i. נניח ש-$\mathbf{v}=(3,3)$. מה יהיה $T^k(\mathbf{v})$ (עבור k שלם כלשהו)?

ii. מה יהיה הגבול של $T^k(\mathbf{v})$ כאשר $k\to\infty$?

(i) $P_A(\lambda)=\det\begin{pmatrix}0.9-\lambda & 0.2\\ 0.1 & 0.8-\lambda\end{pmatrix}=\lambda^2-1.7\lambda+0.72-0.2=\lambda^2-1.7\lambda+0.7=(\lambda-1)(\lambda-0.7)$

ולכן הערכים העצמיים הם 1, 0.7.

הוקטורים העצמיים הם $\vec{v}_1=(2,1)$ ו-$\vec{v}_2=(1,-1)$ בהתאמה.

ולכן $\vec{v}=x(2,1)+y(1,-1)=(3,3)$ כלומר $\begin{cases}2x+y=3\\ x-y=3\end{cases}\Leftarrow$ $x=2$, $y=-1$

אכן $(3,3)=2(2,1)-(1,-1)$, ולכן

$T^k(\vec{v})=T^k\left(2\cdot(2,1)+(-1)(1,-1)\right)$
$=2\cdot T^k(2,1)+(-1)\cdot T^k(1,-1)=2\cdot 1^k(2,1)+(-1)\cdot(0.7)^k(1,-1)=2\,(2,1)-(0.7)^k(1,-1)$
$=\left(4-(0.7)^k,\ 2+(0.7)^k\right)$

(ii) כאשר $k\to\infty$ נקבל $(0.7)^k\to 0$ ולכן $T^k(\vec{v})\xrightarrow[k\to\infty]{}(4,2)$

שאלה 3. (א) (4 נק') הגדר/י את המושגים הבאים:

i. $d=(a,b)$ <u>המחלק המשותף המירבי</u> של a ו-b. הוא המספר (החיובי) המירבי המחלק גם את a וגם את b - כלומר, כך שקיימים מספרים שלמים c ו-e כך ש- $dc=a$, $de=b$.

ii. שני המספרים a ו-b <u>שקולים מודולו</u> n. אם $b-a$ מתחלק ב-n

(ב) (4 נק') הראה/י שלכל a, b, k, ו-n חיוביים, אם $a\equiv b \pmod n$ אז $a^k\equiv b^k \pmod n$.

נראה שכללית אם $a\equiv b \pmod n$ - כלומר, קיים x שלם כך ש- $a-b=xn$ - וגם $c\equiv d \pmod n$ - כלומר, קיים y שלם כך ש- $c-d=yn$ - אז $ac-bd=ac-ad+ad-bd=ayn+dxn=n(ay+dx)$

ולכן באינדוקציה על k נקבל $a^{k-1}\equiv b^{k-1} \pmod n$ ו- $a\equiv b \pmod n$ $\Leftarrow$ $a\cdot a^{k-1}=a^k\equiv b^k=b\cdot b^{k-1} \pmod n$.

לחילופין, אפשר לכתוב $a^k-b^k=(a-b)(a^{k-1}+a^{k-2}b+\dots ab^{k-2}+b^{k-1})$

ולכן $(a-b)\mid a^k-b^k$ ומכיוון ש- $n\mid a-b$ אז בוודאי $n\mid a^k-b^k$.

(ג) (7 נק') i. הצפן/י את המספר $x = 9$ בשיטת RSA במפתח הגלוי $(n, e) = (35, 5)$.

ii. מצא/י את מפתח הפיענוח $d \equiv e^{-1} \pmod{\varphi(n)}$ בעזרת האלגוריתם של אוקלידס.

iii. בדוק/י את תשובתך על-ידי פיענוח.

(i) $y \equiv x^e \pmod{n} \Rightarrow y \equiv 9^5 \pmod{35}$

נחשב $9^2 = 81 \equiv 11 \pmod{35}$ לכן $9^4 \equiv (11)^2 = 121 \equiv 16 \pmod{35}$ לכן $9^5 \equiv (16)(9) \equiv 144 \equiv 4 \pmod{35}$

כלומר $\boxed{y=4}$.

(ii) $n = 5 \cdot 7$ לכן $\varphi(n) = 4 \cdot 6 = 24$ ונחפש d כך ש: $d \cdot 5 \equiv 1 \pmod{24}$

וזהו $\boxed{d=5}$: ביתר פירוט נחשב את $(5,24)$ בעזרת האלגוריתם:

$$\begin{aligned} 24 &= 4 \cdot 5 + 4 \Rightarrow (24,5) = (5,4) \\ 5 &= 1 \cdot 4 + 1 \Rightarrow (5,4) = (4,1) \\ 4 &= 4 \cdot 1 + 0 \Rightarrow (4,1) = 1 \end{aligned}$$

$$\begin{aligned} 1 &= 1 \cdot 4 + (-3) \cdot 1 \\ 1 &= 1 \cdot 4 + (-3)(5 - 1 \cdot 4) \\ &= 4 \cdot 4 - 3 \cdot 5 \\ 1 &= 4 \cdot (24 - 4 \cdot 5) - 3 \cdot 5 = 4 \cdot 24 - 19 \cdot 5 \end{aligned}$$

לכן $1 = 4 \cdot 24 - 19 \cdot 5$ כלומר $-19 \cdot 5 \equiv 1 \pmod{24}$ ולכן $d \equiv -19 \equiv 5 \pmod{24}$

הוא הערך.

(iii) נפענח: $4^5 = 1024 = 1015 + 9 \equiv 9 \pmod{35}$

שאלה 4. (א) (4 נק') הגדר/י את המושגים הבאים:

i. R <u>תחום שלמות</u>. אם R חוג חילופי עם יחידה ללא מחלקי אפס (כלומר, $ab=b\cdot a$ לכל $a,b\in R$, ואם $ab=0$, אז $a=0$ או $b=0$).

ii. C <u>קוד לינארי</u> מעל שדה F בעל <u>משקל מזערי</u> d. C תת-מרחב לינארי של מרחב וקטורי $V=F^n$ מעל F, ולכל $\vec{v}\neq\vec{0}$ ב-C, מספר הקואורדינטות השונות מ-0 ב-$\vec{v}$ הוא לפחות d (ויש אחד שמשקלו מזערי זה $=d$).

(ב) (5 נק') הראה/י ש-$\mathbb{Z}/n$ (חוג השלמים מודולו n) הוא תחום שלמות אם ורק אם n ראשוני.

אם n ראשוני, אפשר לייצג כל $\bar{a},\bar{b}$ שאינם 0 ב-$\mathbb{Z}/n$ ע"י מספרים a,b בין 1 ל-$(n-1)$ [כולל], ואם $\bar{a}\cdot\bar{b}=0$ ב-$\mathbb{Z}/n$ אז $ab\equiv 0 \pmod{n}$ כלומר $n|ab$, וזה לא יתכן אם $1\le a,b<n$.

לכן $\mathbb{Z}/n$ תחום שלמות.

מאידך, אם n אינו ראשוני, אז $n=a\cdot b$ עבור $1<a,b<n$

לכן $\bar{a}\cdot\bar{b}=0$ ב-$\mathbb{Z}/n$ למרות ש-$\bar{a}\neq 0\neq\bar{b}$ ב-$\mathbb{Z}/n$.

(ג) (6 נק') i. מצא/י את מילות הקוד ואת מטריצת הבדיקה של הקוד הלינארי הבינארי בעל מטריצה יוצרת
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

זהו קוד ממימד 3 מעל $\mathbb{F}_2$, ולכן יש בו 2^3 מילים - כל שורות המטריצה והוקטור ה-0. המילים הן לכן:

$C=\{000000, 100011, 011001, 001110, 111010, 101101, 010111, 110100\}$

מטריצת הבדיקה מתקבלת מתוך משוואות הבדיקה:

$v_4=v_2+v_3$

$v_5=v_1+v_2+v_3$

$v_6=v_1+v_2$

כלומר
$$H=\begin{pmatrix} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

חלק שני

בחלק זה עליך לסמן האם הטענה הרשומה נכונה או לא, ולנמק בקצרה את תשובתך!

שאלה 5. קיימת מטריצה ממשית 3×3 G כך ש- $G\begin{pmatrix}1&2&3\\4&5&6\\5&7&9\end{pmatrix}=\begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}$. כן/לא.

נימוק: למטריצה $A=\begin{pmatrix}1&2&3\\4&5&6\\5&7&9\end{pmatrix}$ השורה השלישית היא סכום השתיים הראשונות, ולכן $\det A=0$ כלומר A אינה הפיכה.

שאלה 6. אם A ו-E מטריצות $n\times n$, ו-E הפיכה, אז ל-A ול-$B:=E^{-1}AE$ יש אותם ערכים עצמיים. כן/לא.

נימוק: $A\vec v=\lambda\vec v$ עם $\vec v\neq\vec 0$ $\Longleftrightarrow$ $E^{-1}\vec v\neq\vec 0$ וגם $AE(E^{-1}\vec v)=\lambda E(E^{-1}v)$

$\Longleftrightarrow$ $E^{-1}AE(E^{-1}v)=\lambda(E^{-1}v)$ כלומר λ ע"ע של B.

שאלה 7. אם $A=A^T$ מטריצה סימטרית $n\times n$, יש ל-$\mathbb{R}^n$ בסיס המורכב מווקטורים עצמיים של A. כן/לא.

נימוק: כל מטריצה סימטרית ניתנת ללכסון

שאלה 8. אם A מטריצה 2×2 עם ערכים עצמיים $\{1,-1\}$ ו-$B^2=A$, אז B ניתנת ללכסון מעל $\mathbb{R}$. כן/לא.

נימוק: אילו B היתה ניתנת ללכסון מעל $\mathbb{R}$, עם ערכים עצמיים $\lambda_1,\lambda_2\in\mathbb{R}$, אז ל-$A=B^2$ היו ערכים עצמיים λ_1^2,λ_2^2

ואז $\lambda_1^2=1$, $\lambda_2^2=-1$ – וזה לא יתכן אם $\lambda_2\in\mathbb{R}$

שאלה 9. אם $c|ab$ אז c מחלק את מכפלת שני המספרים $d_1:=(a,c)$ ו-$d_2:=(b,c)$. כן/לא.

נימוק: נכתוב $\bar c d_1=c$, $\bar a d_1=a$ עבור $(\bar a,\bar c)=1$ ואז $\bar c d_1|\bar a d_1 b$

כלומר $\bar c|\bar a b$ אך $(\bar a,\bar c)=1$ ולכן $\bar c|b$ ובהכרח $\bar c|(b,c)=d_2$

(כי גם $\bar c|c$) לכן $c=d_1\bar c|d_1d_2$.

שאלה 10. אם a, b, c ו-n חיוביים, $(a,b)=1$, ו-$ab=c^n$ אז יש d, e שלמים כך ש- $a=d^n$ ו-$b=e^n$. כן/לא.

נימוק: אם נפרק את a ו-b לגורמים ראשוניים אז $a=p_1^{e_1}\cdots p_k^{e_k}$

ו- $b=q_1^{f_1}\cdots q_l^{f_l}$ כאשר היחידות $\{p_1,\dots,p_k\}$ ו-$\{q_1,\dots,q_l\}$ זרות.

מכיוון ש-$ab=c^n$, כל ראשוני בפירוק של ab מופיע בחזקה n, ולכן $n|e_1,\dots,e_k$

וגם $n|f_1,\dots,f_l$

שאלה 11. אם $a^2 \equiv b^2 \pmod{n}$ אז $a \equiv \pm b \pmod{n}$. כן/לא.

נימוק:

לדוגמה $2^2 \equiv 0^2 \pmod 4$ אך $2 \not\equiv 0 \pmod 4$

שאלה 12. $(a+b)^p \equiv a^p + b^p$ מודולו p לכל p ראשוני ו-a ו-b שלמים. כן/לא.

נימוק:

$(a+b)^p = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}$

אך $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ שלם, p מחלק את המונה, ולא את המכנה, ולכן $p \mid \binom{p}{i}$ לכל $1 \le i < p$.

שאלה 13. בכל חבורה אבלית $\langle G,+\rangle$ ולכל איבר $G \ni g_0$ (קבוע), הפונקציה $\phi : G \to G$ המוגדרת $\phi(x) := g_0 + x$ לכל $G \ni x$ היא הומומורפיזם של חבורות. כן/לא.

נימוק:

$\phi(0) = g_0$, אבל בהומומורפיזם צריך להתקיים $\phi(0) = 0$.

שאלה 14. אם I אידאל מירבי בחוג חילופי עם יחידה R אז R/I שדה. כן/לא.

נימוק: אם $0 \neq \bar{x} \in R/I$ מיוצג ע"י $x \notin I$, אז $R = \langle I, x \rangle$, ולכן קיים $y \in R$ כך ש- $i + xy = 1$ עבור i כלשהו ב-I - כלומר, $\bar{x}\bar{y} \equiv 1 \pmod I$, ולכן $\bar{x}$ הפיך.

שאלה 15. חוג הפולינומים $F[x]$ מעל שדה F הוא תחום שלמות. כן/לא.

נימוק: אם נכפול שני פולינומים $0 \neq a_n x^n + \dots + a_0$ ו- $0 \neq b_k x^k + \dots + b_0$ נקבל מקדם עליון $a_n b_k x^{n+k}$, ולכן המכפלה שונה מאפס.

שאלה 16. בקוד לינארי C בעל משקל מזערי d אפשר לתקן שגיאה e אם ורק אם משקלה הוא $w_H(\mathbf{e}) = \lfloor \frac{d-1}{2} \rfloor$. כן/לא.

נימוק: לפעמים אפשר לתקן גם שגיאות ממשקל גבוה יותר, אם הקוד אינו מושלם.

שאלה 17. בשיטת הסינדרומים אפשר לתקן שגיאה e אם ורק אם היא מוביל מחלקה. כן/לא.

נימוק: השיטה מתקנת כל $\vec{v}$ שאינו ב-C ע"י זיהוי המחלקה של $\vec{v}$ ב-V/C, ותיקון $\vec{v}$ ל-$\vec{v} - \vec{e} \in C$ כאשר $\vec{e}$ הוא בדיוק מוביל המחלקה.

בהצלחה!