

בחינה סופית באלגברה ב'

לשימוש הבודק

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

מועד: ב

משך הבחינה: 2.5 שעות

המרצה: דוד בלנק

תאריך: 29.7.2004

סמסטר ב' תשס"ד

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 הטייטא 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. המטריצה A $n \times n$ הפיכה. $A \cdot B = B \cdot A = I_n$
 אם Q "מ"מ $n \times n$ אז $(\det(A) \neq 0)$ Q קווה אם ורק אם $Q = A^{-1}$.

ii. מטריצה $A = A_T^B$ מייצגת את האופרטור הליניארי $T: V \rightarrow V$ ביחס לבסיס B .
 $B = \{v^{(1)}, \dots, v^{(n)}\}$ ל- V . ρ כל וקטור $\vec{w} = \sum_{i=1}^n a_i \vec{v}^{(i)}$ $\vec{v}^{(i)}$ \vec{w} $\vec{v}^{(i)}$
 מתקיים: $A \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ כאשר $T(\vec{w}) = \sum_{i=1}^n b_i \vec{v}^{(i)}$ \vec{w} $\vec{v}^{(i)}$
 אחידות: העמודות של A הן הווקטורים $T(\vec{v}^{(1)}), \dots, T(\vec{v}^{(n)})$ $\vec{v}^{(i)}$ $T(\vec{v}^{(i)})$
 עכ"ל, הגבס B .

(ב) (5 נק') מצא/י את מטריצת המעבר $C = C_{B'}^B$ מן הבסיס $B := \{(1, 1), (-1, 2)\}$ לבסיס $B' = \{(1, -1), (2, 3)\}$ עבור \mathbb{R}^2 .

מטריצת המעבר $C_{B'}^B$ מן הבסיס B לבסיס B' היא $Q = C_{B'}^B$, וזו היא מטריצת המעבר מן הבסיס B לבסיס B' .
 $Q = \begin{pmatrix} 1 & -1 \\ 2 & 3 \end{pmatrix}$, $Q^{-1} = C_B^{B'}$ היא מטריצת המעבר מן הבסיס B' לבסיס B .
 היא $Q^{-1} = \frac{1}{5} \begin{pmatrix} 3 & -2 \\ 1 & 1 \end{pmatrix}$ וזו היא מטריצת המעבר מן הבסיס B' לבסיס B .

$$C_{B'}^B = C_{B'}^B \cdot C_B^B = \frac{1}{5} \begin{pmatrix} 3 & -2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix} = \frac{1}{5} \begin{pmatrix} 1 & -7 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{5} & -\frac{7}{5} \\ \frac{2}{5} & \frac{1}{5} \end{pmatrix}$$

כדי לבדוק: $\frac{1}{5} \begin{pmatrix} 1 & -7 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ \frac{2}{5} \end{pmatrix}$ וכן $\frac{1}{5} \begin{pmatrix} 1 & -7 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ 2 \end{pmatrix} = \begin{pmatrix} \frac{1}{5} \\ 1 \end{pmatrix}$.
 (ג) (5 נק') מצא/י את המטריצה $A = A_T^B$ המייצגת את:

$$T(x, y, z) := \begin{pmatrix} 8 & 7 & 7 \\ -5 & -6 & -9 \\ 5 & 7 & 10 \end{pmatrix} \cdot \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

ביחס לבסיס $B = \{(1, -1, 1), (0, 1, -1), (1, -2, 1)\}$

$$T(1, -1, 1) = \begin{pmatrix} 8-7+7 \\ -5+6-9 \\ 5-7+10 \end{pmatrix} = \begin{pmatrix} 8 \\ -8 \\ 8 \end{pmatrix} = 8 \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix},$$

$$T(0, 1, -1) = \begin{pmatrix} 7-7 \\ -6+9 \\ 7-10 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ -3 \end{pmatrix} = 3 \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}$$

$$T(1, -2, 1) = \begin{pmatrix} 8-14+7 \\ -5+12-9 \\ 5-14+10 \end{pmatrix} = \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ -2 \\ 1 \end{pmatrix}$$

כלומר $A = \begin{pmatrix} 8 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ כלומר A היא מטריצה כזו.

שאלה 2. (א) (4 נק') הגדרי את המושגים הבאים:

(i) v הוא וקטור עצמי של האופרטור $T: V \rightarrow V$ עבור הערך העצמי λ . $\vec{v} \neq \vec{0}$ $\rho \in \mathbb{C}$

$$T(\vec{v}) = \lambda \cdot \vec{v} \quad \text{או} \quad T(\vec{v}) = \rho \cdot \vec{v}$$



(ii) המטריצה A סימטרית. $A^T = A$ כלומר, $a_{ij} = a_{ji}$.
 (בפ. 6) A חייב להיות $n \times n$. $1 \leq j, i \leq n$

(ב) (6 נק') האם המטריצה $A := \begin{pmatrix} 1 & 3 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ ניתנת ללכסון? אם כן, מצא/י את הערכים

העצמיים שלה, את הווקטורים העצמיים שלה, ואת המטריצה המלכסנת P .
אם לא, הסבר/י מדוע לא.

$$P_A(\lambda) = \det \begin{pmatrix} 1-\lambda & 3 & 0 \\ 0 & 1-\lambda & 0 \\ 0 & 0 & 2-\lambda \end{pmatrix} = (1-\lambda)^2(2-\lambda)$$
 : כאן נ"א, כאן נ"א, כאן נ"א
 . ש"ס, נ"א, (1, 2, 3) : כאן נ"א, כאן נ"א, כאן נ"א


108, 2 2 3 2 3 6 151 $A - I_3 = \begin{pmatrix} 0 & 3 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ 201 $\lambda = 1$ 128

הערך האפס'י \Rightarrow $(A - I \cdot I) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ בעזרת גורמים

סיכום א' פ"א מ"א נ"א המ"א ד' $\lambda = 1$. מ"א נ"א ד' ה"א נ"א

$\rho_{\lambda=1}$ הוא 1; מכיון e הייב' הסימטרי $\rho_{\lambda=2}$ שווה לסיבוי הקטעני,

[illegible]

A מ'נד ז'גרה  .

(ג) (6 נק') תהי $T: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ ההעתקה המיוצגת על-ידי המטריצה $A := \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ 1 & 0 \end{pmatrix}$.

i. נניח ש- $\mathbf{v} = (0, \frac{1}{2})$. מה יהיה $T^k(\mathbf{v})$ (עבור k שלם כלשהו)?

ii. מה יהיה הגבול של $T^k(v)$ כאשר $k \rightarrow \infty$?

$$P_A(\lambda) = \det \begin{pmatrix} \frac{1}{2} - \lambda & \frac{1}{2} \\ 1 & -\lambda \end{pmatrix} = \lambda^2 - \frac{1}{2}\lambda - \frac{1}{2} = (\lambda - 1)\left(\lambda + \frac{1}{2}\right)$$

$$\lambda = 1 - \frac{1}{2} = \frac{1}{2} \quad (1, 1) \quad p = 3r \quad p = 1, 1 \quad p = -\frac{1}{2} \quad 1 \quad p = 1 \quad \text{de } x^2, y^2 \quad (1, 1)$$

$$A^k \cdot \vec{v} = A^k \left[\frac{1}{6} \begin{pmatrix} 1 \\ 1 \end{pmatrix} - \frac{1}{6} \begin{pmatrix} 1 \\ -2 \end{pmatrix} \right] = \frac{1}{6} [A^k \begin{pmatrix} 1 \\ 1 \end{pmatrix} - A^k \begin{pmatrix} 1 \\ -2 \end{pmatrix}] = \frac{1}{6} \left[\begin{pmatrix} 1 \\ 1 \end{pmatrix} - \begin{pmatrix} 1 \\ -2 \end{pmatrix} \right] = \begin{pmatrix} \frac{1}{6} \\ \frac{1}{6} \end{pmatrix} + \begin{pmatrix} -\frac{1}{6} \\ \frac{2}{3} \end{pmatrix}$$

$$T^k(\vec{v}^2) \xrightarrow{k \rightarrow 0} = \begin{pmatrix} \frac{1}{6}, \frac{1}{6} \end{pmatrix} \quad \text{C.2.2 (ii)}$$

שאלה 3. (א) (4 נק') הגדירי את המושגים הבאים:

i. המספר השלם a מחלק את המספר השלם b (סימון: $a|b$). זכור ק"ק 1004
שלם n כך ש- $a \cdot n = b$.

ii. n מספר ראשוני. ודא ק"ק מספר שלם d $1 < d|n$

כך ש- $d|n$. [לפז'יק צווישן n ו- d יהיה חזק זה אינו ידוע]

(ב) (5 נק') הראה/י שלכל a, b, c, x, y שלמים, אם $a|b$ ו- $a|c$ אז $a|(bx + cy)$.

לפי ההנחה $a|b$ ו- $a|c$, ולכן לפי ההגדרה ק"ק a מסביר שלם m כך ש- $am = b$, $an = c$.

$$bx + cy = (am)x + (an)y = a(mx + ny)$$

לפי חוק הפילוס, ואילו m ו- n הם שלמים, אז $mx + ny$ הוא שלם, ו-

$$az = bx + cy \text{ שם, ואז היינו } z = mx + ny$$

כלומר $a|bx + cy$, לפי ההנחה.



(ג) (6 נק') האם ניתן להצפין את המספר $x = 10$ בשיטת RSA במפתח הגלוי $(n, e) = (35, 5)$?
 אם כן, עשה/י זאת. אם לא, הסבר/י מדוע לא, מצא/י מפתח ציבורי אחר (n', e') שבעזרתו
 ניתן להצפינו, ועשה/י זאת.

שיטת ה-RSA דורשת שנבחר x כזה ש $x \not\equiv 0 \pmod{n}$ ו- $y \equiv x^e \pmod{n}$
 אולם לפעם כך נבחר e כך $(x, n) = 1$, כי אז $\phi(n)$ מתחלק את e , כלומר
 נבחר d כך $d \equiv e^{-1} \pmod{\phi(n)}$ ו- $d \cdot e \equiv 1 \pmod{\phi(n)}$ (במקרה שלנו: $n=35$ ו- $\phi(n)=24$)
 כאן, $\phi(n)=4 \cdot 6=24$, $d=5$ כי $5 \cdot 5=25 \equiv 1 \pmod{24}$ אזו נבחר $d=5$
 כמעט אף פעם לא נבחר d כזה: $y^d \equiv (x^e)^d = x^{k\phi(n)+1} = (x^{\phi(n)})^k \cdot x \equiv x \pmod{n}$ (כי $(x, n)=1$)
 נסתמך על העובדה $x^{\phi(n)} \equiv 1 \pmod{n}$ - בתנאי $(x, n)=1$!
 ואכן במקרה שלנו $x=10$: $10^2 \equiv -5 \pmod{35}$, $10^4 \equiv -10 \pmod{35}$ וכן $10^5 \equiv -50 \equiv -15 \pmod{35}$
 ו- $10^5 \equiv -15 \pmod{35}$ ו- $(-15)^2 \equiv 225 \equiv 15 \pmod{35}$ ו- $(-15)^4 \equiv 15^2 \equiv 15 \pmod{35}$ ו- $(-15)^5 \equiv -225 \equiv -15 \pmod{35}$ ו- $10^5 \equiv -15 \pmod{35}$

אולם נבחר $(n, e) = (21, 5)$ ו- $(10, 21) = 1$ ואז $\phi(n) = 2 \cdot 6 = 12 \leq n = 21$
 ו- $d=5$ שכן d הוא הפכי e (כי $e=5$ ו- 5 אי-זוגי, 12 זוגי)
 $y \equiv x^e \pmod{n}$
 $= 10^5 \pmod{21}$
 ונחשבו: $10^2 \equiv 100 \equiv 16 \pmod{21}$, $10^4 \equiv (-5)^2 \equiv 25 \equiv 4 \pmod{21}$, $10^5 \equiv 40 \equiv 19 \pmod{21}$ (כי $40 \equiv 19 \pmod{21}$)
 ו- $10^5 \equiv 19 \pmod{21}$ ו- $10^5 \equiv (-2)^5 \equiv -32 \equiv 10 \pmod{21}$
 כלומר $y=19$ ו- $y=10$ (כי $19 \equiv 10 \pmod{21}$)

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

i. R חוג חילופי עם יחידה. $(R, +)$ תבורה אבלית (בתור חבורה) שם 0 הוא איבר היחידה.
 פתרון: כי-א-ר R חבורה אבלית (בתור חבורה) שם 0 הוא איבר היחידה.
 $a(b+c) = (a \cdot b) + (a \cdot c)$ ו- $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$, ו- $1 \cdot a = a \cdot 1 = a$: R הוא חוג.
 ii. d הוא המרחק המזערי בקוד C כלומר,
 $d = \min_{\vec{u} \neq \vec{v} \in C} \{d_H(\vec{u}, \vec{v})\}$
 כאשר d_H הוא המרחק המניימן בין שני וקטורים $\vec{u}, \vec{v} \in F^n$ (מרחב וקטורי F)
 שם $d_H(\vec{u}, \vec{v}) := \#\{i \in [n] \mid u_i \neq v_i\}$.

(ב) (6 נק') הראה/י ש- \mathbb{Z}/n (חוג השלמים מודולו n) הוא שדה אם ורק אם n ראשוני.

מכיוון ש- \mathbb{Z} חוג חיסובי עם יחידה, כך גם חוג המנה $\mathbb{Z}/n := \mathbb{Z}/n\mathbb{Z}$ (כאשר $n\mathbb{Z} := \{a \in \mathbb{Z} \mid a \in n\mathbb{Z}\}$). אם n אינו ראשוני, נאמי
 על $\eta = a \cdot b$ ו- $\bar{a}, \bar{b} \neq \bar{0} = \bar{0} = \bar{a} \cdot \bar{b}$ עבור $\bar{a}, \bar{b} \in \mathbb{Z}/n$ - כלומר \mathbb{Z}/n אינו שדה.
 י"ח מילר, אבס, ולסון, הוצגו אינו שדה.
 מאידך, אם n ראשוני, אז האיזומורפיזם $\mathbb{Z} \rightarrow \mathbb{Z}/n$ (כ) $a \mapsto \bar{a}$ הוא איזומורפיזם חבורות.
 מכאן $(a, n) = 1$ ולכן $\exists x, y \in \mathbb{Z}$ כך ש- $ax + ny = 1$ ולכן $\bar{a}\bar{x} = \bar{1}$ ולכן \bar{a} הפיך.
 האיזומורפיזם $\langle a, n \rangle$ הנוצר ע"י הוספת a ל- \mathbb{Z} מכיל את 1 , והוא כל החוג
 \mathbb{Z} (אילו) - ולכן לכל משפט שאותו בכיתה, \mathbb{Z}/n הוא שדה.

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

חשבו/י את הפיענוח בעל השגיאה המזערית עבור 01011 , ומצא/י את המשקל המזערי של הקוד.

(i) מילות הקוד הן: $C = \{00000, 10101, 01010, 11100, 01101, 10100, 01011, 10101\}$

(ii) אנו רואים ש- 01010 אינו ב- C , ואכן יש ב- C שני מילים הנבדלות

מ- 01010 בקוארציה אחת בלבד: 01010 ו- 11101 .

(iii) מילת הסוף הקוצק רואים שתי המילים \nearrow \nwarrow נבדלות בשתי קוארציות.

בלבד - ואכן המילים: 01010 ו- 10101 בעלות משקל האינסוף 2.

מכיוון שאין אף מילה $\neq 0$ ב- C בעלת משקל האינסוף 1, היינו

שהמשקל המזערי ב- C הוא בז"ק [2].



חלק שני

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

שאלה 5. קיימת מטריצה P כך ש- $P^{-1} \begin{pmatrix} 12 & -7 & 89 \\ -7 & -2 & 3 \\ 89 & 3 & 45 \end{pmatrix} P = D$ אלכסונית. (כן/לא).

נימוק: המטריצה סימטרית, ולכן ניתנת לכסוסן.

שאלה 6. לשתי מטריצות המייצגות את $T: V \rightarrow W$ (ביחס לבסיסים שונים) יש אותה דרגה. (כן/לא).

נימוק: הדרגה היא המימד של התמונה של T .
 $\text{Im}(T) = \{ T(\vec{v}) \in W \mid \vec{v} \in V \}$, וזו אינה תלויה בבחירת הבסיסים.

שאלה 7. אם למטריצה A $n \times n$ יש ערך עצמי יחיד λ (עם ריבוי אלגברי n), אז A אינה ניתנת לליכסוסן. (כן/לא).

נימוק: נסתכל ב- $A = I_n$ יש ערך עצמי יחיד $\lambda = 1$ עם ריבוי n , ו- A עצמה כבר אלכסונית.

שאלה 8. אם A מטריצה 2×2 עם ערכים עצמיים $\{1, -1\}$, אז A^6 ניתנת לליכסוסן. (כן/לא).

נימוק: אם \vec{v} ו- \vec{u} הוקמו ב- A עבור $\lambda = 1, -1$ בהתאמה, הם בתיים (כי העצמים שונים), ולכן באמצעותם נבנה נוקבע $A^k \vec{u} = (-1)^k \vec{u}$ ו- $A^k \vec{v} = 1^k \vec{v}$, כלומר \vec{u} ו- \vec{v} הם עבור הערך העצמי ± 1 של A^6 . המטריצה A^6 .

שאלה 9. $11^{24} \equiv 121 \pmod{23}$. (כן/לא).

נימוק: ע"פ משפט פרימא, מכיוון $\gcd(11, 23) = 1$, מתקיים $11^{22} \equiv 1 \pmod{23}$ ולכן $11^{24} = 11^{22} \cdot 11^2 \equiv 1 \cdot 121 \equiv 121 \pmod{23}$.

שאלה 10. פונקציית ϕ של אולר מקיימת: $\phi(n) = \phi(2n)$ לכל n טבעי. (כן/לא).

נימוק: זה נכון רק אם n אי-זוגי; אלוס $n=2$ נכון $\phi(2) = 1$ ו- $\phi(4) = 2$.
 $\phi(2) = 2 - 1 = 1$ ו- $\phi(2^2) = 2^2 - 2^1 = 2$.

שאלה 11. בשדה F יש לכל היותר שני פתרונות שונים למשוואה $x^2 = 1$.
 נימוק: כן/לא.

כדי פתרון כזה הוא אפס של הפולינום $f(x) = x^2 - 1$,
 וכדי אפס λ של f ניתן לומר $f(x) = (x - \lambda)g(x)$ עבור $g(x) = x + \lambda$.
 מכיון ש f היא 2 , יכולים להיות לכל היותר שני אפסים שונים.

שאלה 12. $a^{n-1} \equiv 1 \pmod{n}$ עבור $(a, n) = 1$ אם ורק אם n ראשוני.
 נימוק: כן/לא.

נניח, a אינו ראשוני, $a^{n-1} \equiv 1 \pmod{n}$ עבור $(a, n) = 1$.
 נבחר $a = 2$, $n = 341$. $2^{340} \equiv 1 \pmod{341}$ אבל $341 = 11 \cdot 31$ אינו ראשוני.

שאלה 13. לכל n שלם חיובי ישנה חבורה G עם בדיוק n איברים.
 נימוק: כן/לא.

כן. \mathbb{Z}/n יש בדיוק n איברים, והוא חבורה.
 $\{0, 1, \dots, n-1\}$

שאלה 14. אם I אידיאל ראשי בחוג חילופי עם יחידה R אז R/I שדה.
 נימוק: כן/לא.

כן. $R = \mathbb{Z}$ אידיאל ראשי הוא 0 או $p\mathbb{Z}$, p ראשוני.
 $I = 4\mathbb{Z}$ אינו ראשוני (לפיטגורס), ולכן $\mathbb{Z}/4\mathbb{Z}$ אינו שדה.

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

כן. פולינום ממעלה חיובית אין לו פתרון ב- $F[x]$.

שאלה 16. בקוד לינארי C בעל משקל מזערי d אפשר לזהות כל שגיאה ממשקל $d - 1$.
 נימוק: כן/לא.

אם $\vec{v} \in F^n$ שגיאה ממעלה קוד \vec{w} מסתירה \vec{v} ב- C .
 הוא $d - 1$ אינה יכולה להיות אף היא ב- C .

שאלה 17. בקוד לינארי, המרחק המזערי בין מילות קוד שונות שווה למשקל המזערי של מילים שונות מאפס.
 נימוק: כן/לא.

המשקל המזערי הוא d .

$$d_H(\vec{v}, \vec{u}) = w_H(\vec{v} - \vec{u})$$

מכיון C לינארי, אם $\vec{v}, \vec{u} \in C$ אז $\vec{v} - \vec{u} \in C$.

מאחר $w_H(\vec{v}) = d_H(\vec{v}, \vec{0})$, $w_H(\vec{v}) = d_H(\vec{v}, \vec{u})$ עבור $\vec{u} = \vec{0}$.

בהצלחה: