המכללה האקדמית נתניה ע"ר
רח' האוניברסיטה 1
קרית יצחק רבין
נתניה 42365

NETANYA ACADEMIC COLLEGE (R"S)
1 University St.
Kiryat Yitzhak Rabin
NETANYA 42365, ISRAEL

מבחן סוף במבנים אלגבריים למדעי המחשב-סמסטר קיץ ה'תשע"ז.

מועד א יום א,ב חשון התשע"ח 22-10-2017

- מורה: גיורא דולה, מתרגל: רענן שכטר.
- משך המבחן הוא שלש שעות.
- אפשר להשתמש רק במחשבון ובדפי העזר המצורפים.
- יש לכתוב במחברת תשובה מלאה על כל אחת מהשאלות.
- במבחן יש שלשה חלקים. בחלק א חמש שאלות מתוכן יש לבחור 4 ומשקל כל שאלה 10 נקודות. בחלק ב יש 4 שאלות ומתוכן יש לבחור 3. משקל כל שאלה בחלק ב 15 נקודות. בחלק ג שתי שאלות מתוכן יש לבחור אחת ומשקל כל שאלה 15 נקודות ס"הכ $3*15+4*10+1*15=100$
- מותר להסתמך על כל טענה שהוכחה בכתה אך יש לנסח אותה במדויק בנפרד.

בהצלחה.

טל: 8607777 (972-9) **Tel:** **פקס:** 8844439 (972-9) **Fax:**

חלק א

שאלה 1

נביט בשתי המטריצות הבאות:

$$S=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}, T=\begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix},$$

א. חשב את הקבוצה $G=\left\{S^iT^j, 0\le i,j\right\}$.

ב. חשב את הסדר של כל איבר ב-G.

ג. מצא את כל החבורות החלקיות של G.

ד. האם G אבלית?

שאלה 2

שתי תמורות על הקבוצה $\mathbb{Z}_7=\{0,1,2,3,4,5,6\}$ מוגדרות על ידי הנוסחאות הבאות (הפעולות מבוצעות ב $\mathbb{Z}_7$).

$$f=\begin{cases}\frac{x+3}{5-5x} & 1\neq x\in\mathbb{Z}_7\\ a & 1=x\in\mathbb{Z}_7\end{cases}, g=\begin{cases}\frac{2x+5}{4-5x} & 5\neq x\in\mathbb{Z}_7\\ b & 5=x\in\mathbb{Z}_7\end{cases}$$

א. מצא את a ואת b.

ב. חשב את $f^{-1}g^{-2}$.

ג. פרק את $f^{-1}g^{-2}$ למכפלה של מחזורים זרים.

ד. פרק את $f^{-1}g^{-2}$ למכפלה של חילופים.

ה. מצא את הסדר של $f^{-1}g^{-2}$.

שאלה 3

חשב את המחלק המשותף $d(x)$ הגדול ביותר של הפולינומים הבאים:
$a(x)=x^4+3x^3+3x^2+3x+3\in\mathbb{Z}_7[x],\quad b(x)=x^3+5x^2+1\in\mathbb{Z}_7[x]$. מצא פולינומים
$u(x),v(x)\in\mathbb{Z}_7[x]$ המקיימים $d(x)=\gcd(a(x),b(x))=a(x)u(x)+b(x)v(x)$.

שאלה 4

תהינה $G=(\mathbb{Z}_6,\oplus_6)$ $H=(\mathbb{Z}_2,\oplus_2)$ שתיהן עם פעולת החיבור מודולו, ונגדיר על הקבוצה $G\times H$ פעולה בינרית על ידי

$$\forall(g,h),(a,b)\in G\times H,(g,h)(a,b)=(g\oplus_6 a,h\oplus_2 b)$$

א. מצא את כל הסדרים של כל האיברים בחבורה.

ב. מצא את כל החבורות החלקיות של $G\times H$.

שאלה 5

נתונה החבורה $(\mathbb{Z}_{20}^*,\cdot)$. (כל האיברים ההפיכים עם פעולת הכפל).

א חשב את הסדר של כל האיברים ב G.

ב . חשב את 7^{137} ב- $(\mathbb{Z}_{20}^*,\cdot)$.

ב. מצא את כל החי״ח של $(\mathbb{Z}_{20}^*,\cdot)$.

ג. האם $(\mathbb{Z}_{20}^*,\cdot)$ ציקלית?

<u>חלק ב</u>

שאלה 6

הוכח משפט קיום ויחידות חלוקת פולינומים בחוג הפולינומים $S[x]$.

עבור שדה S.

שאלה 7

יהי $f:G\to H$ הומומורפיזם של חבורות: הוכח

א. תהי $K\le G$ חבורה חלקית אז $f(K)\le H$ חבורה חלקית.

ב. תהי $L \leq H$ חבורה חלקית אז $f^{-1}(L) \leq G$ חבורה חלקית.

ג. f חח"ע אם ורק אם Ker(f)={e}

.

שאלה 8

נגדיר יחס על אוסף כל החבורות: G מתיחסת ל H אם קיים איזומורפיזם של G על H . הוכח כי היחס הוא יחס שקילות.

שאלה 9

נסח והוכח את התנאי המקוצר עבור ח"ח.

<u>חלק ג</u>

שאלה 10

נתון חוג R. וקבוצה חלקית $I \subseteq R$. הקבוצה תקרא אידאל אם היא ח"ח של החבורה האבלית של R, ובנוסף מקיימת את תכונת הבליעה $x \in I, y \in R \to xy \in I$:

1. עבור $R = \mathbb{Z}$ תן דוגמא של אידאל השונה מהקבוצה המכילה רק את 0.
2. עבור R שהוא שדה תן דוגמא של אידאל השונה מהקבוצה המכילה רק את 0.
3. אידאל נקרא ראשוני אם יש לו התכונה הנוספת שאם $x \notin I, y \notin I \to xy \notin I$. מצא אידאל ראשוני בתוך החוג $R = \mathbb{Z}$. מצא גם אידאל לא ראשוני באותו חוג.

שאלה 11

נתון הומומורפיזם על של חוגים $f: R \to S$

א. אם R הוא תחום שלמות האם גם S כזה? אם כן הוכח ואם לא תן דוגמא נגדית.

ב. אם S הוא תחום שלמות האם גם R כזה? אם כן הוכח ואם לא תן דוגמא נגדית.

<u>בהצלחה</u>

תשובות:

תשובה 1

$$S^1 = S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, S^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, S^4 = I_2, T^1 = T = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, T^2 = I_2,$$

$$ST = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, S^2T = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, S^3T = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, TS = S^3T, TS^2 = S^2T, TS^3 = ST$$

ולכן G מכילה 8 איברים.

$$o(S) = 4, o(S^2) = 2, o(S^3) = 4, o(T) = 2, o(ST) = 2, o(S^2T) = 2, o(S^3T) = 2, o(I) = 1.$$

כל איבר מסדר 2 מגדיר חבורה חלקית הכוללת אותו ואת איבר היחידה ויש 5 כאלו. שני האיברים מסדר 4 מגדירים חבורה חלקית מחזורית בת 4 איברים. G איננה אבלית למשל מתקיים

$$TS = S^3T$$

תשובה 2

נחשב את f ואת g בצורה מפורשת. עבור f:

	0	1	2	3	4	5	6
	3/5	4/0	5/(−5)	6/(−10)	7/(−15)	8/(−20)	9/(−25)
	3/5	4/0	−1	6/4	0	1/1	2/3
	2	?	6	5	0	1	3

ולכן נקבל את f על ידי:

	0	1	2	3	4	5	6
$f\downarrow$	2	4	6	5	0	1	3

ובצורה דומה עבור עבור g

	0	1	2	3	4	5	6
	5/4	7/(−1)	9/(−6)	11/(−11)	13/(−16)	15/(−21)	17/(−26)
	10	0	9/1	4/3	5/5	1/0	3/2
	3	0	2	6	1	?	5

ולכן נקבל את g

על ידי:

	0	1	2	3	4	5	6
$g\downarrow$	3	0	2	6	1	4	5

וגם את g^2:

x	0	1	2	3	4	5	6
$g(x)$	3	0	2	6	1	4	5
$g^2(x)$	6	3	2	5	0	1	4

וכעת נחשב את ההפוכים:

	0	1	2	3	4	5	6
$f\downarrow$	2	4	6	5	0	1	3
$f^{-1}\downarrow$	4	5	0	6	1	3	2

x	0	1	2	3	4	5	6
$g(x)$	3	0	2	6	1	4	5
$g^2(x)$	6	3	2	5	0	1	4
$g^{-2}(x)$	4	5	2	1	6	3	0

ולבסוף נקבל את ההרכבה:

x	0	1	2	3	4	5	6
$g^{-2}(x)$	4	5	2	1	6	3	0
$f^{-1}(x)$	4	5	0	6	1	3	2
$f^{-1}g^{-2}(x)$	1	3	0	5	2	6	4

העתקה זו היא מהצורה

(0135642) ובעלת סדר 7, ונקבל אותה כמכפלת חלופים: (02)(04)(06)(05)(03)(01).

תשובה 3

$$x^4+3x^3+3x^2+3x+3=(x^3+5x^2+1)(x+5)+(6x^2+2x+5)$$
$$(x^3+5x^2+1)=6x(6x^2+2x+5)+(5x+1).$$
$$6x^2+2x+5=(5x+1)(4x+1)+4,\gcd=4$$

$$4=(6x^2+2x+5)-(5x+1)(4x+1)=$$
$$=(6x^2+2x+5)-[(x^3+5x^2+1)-6x(6x^2+2x+5)](4x+1)=$$
$$=-(4x+1)(x^3+5x^2+1)+[1+6x(4x+1)](6x^2+2x+5)=$$
$$=-(4x+1)(x^3+5x^2+1)+[1+6x(4x+1)][(x^4+3x^3+3x^2+3x+3)-(x^3+5x^2+1)(x+5)]=$$
$$=[1+6x(4x+1)][(x^4+3x^3+3x^2+3x+3)+[-(4x+1)-(x+5)[1+6x(4x+1)]](x^3+5x^2+1)$$

תשובה 4

א. הסגירות נובעת רכיב רכיב, חוק הקיבוץ נובע רכיב רכיב, אבר היחידה הוא $(0,0)$ וההפכי של (x,y) הוא $(-x,-y)$ וגם הוא מוגדר רכיב רכיב.

$(0,0)^1 = 0$

$(1,0)^2 = (2,0), (1,0)^3 = (3,0), (1,0)^4 = (4,0), (1,0)^5 = (5,0), (1,0)^6 = (0,0)$

$(2,0)^2 = (4,0), (2,0)^3 = (0,0).$

$(3,0)^2 = (0,0)$

$(4,0)^2 = (2,0), (4,0)^3 = (0,0)$

$(5,0)^2 = (4,0), (5,0)^3 = (3,0), (5,0)^4 = (2,0), (5,0)^5 = (1,0), (5,0)^6 = (0,0)$

ב.

$(0,1)^2 = (0,0)$

$(1,1)^2 = (2,0), (1,1)^3 = (3,1), (1,1)^4 = (4,0), (1,1)^5 = (5,1), (1,1)^6 = (0,0)$

$(2,1)^2 = (4,0), (2,1)^3 = (0,1), (2,1)^4 = (2,0), (2,1)^5 = (4,1), (2,1)^6 = (0,0)$

$(3,1)^2 = (0,0).$

$(4,1)^2 = (2,0), (4,1)^3 = (0,1), (4,1)^4 = (4,0), (4,1)^5 = (2,1), (4,1)^6 = (0,0)$

$(5,1)^2 = (4,0), (5,1)^3 = (3,1), (5,1)^4 = (2,0), (5,1)^5 = (1,1), (5,1)^6 = (0,0)$

ג. החבורה בת 12 איברים והסדר המקסימלי של איברים הוא 6. יש 6 איברים מסדר 6. $(1,0)$ ו $(5,0)$ יוצרים את אותה ח״ח אשר איזומורפית ל $\mathbb{Z}_6$, וכמו כן $(1,1)$ ו $(5,1)$ יוצרים את אותה ח״ח אשר איזומורפית ל $\mathbb{Z}_6$, וכמו כן $(2,1)$ ו $(4,1)$ יוצרים את אותה ח״ח אשר איזומורפית ל $\mathbb{Z}_6$. כל חבורה בת 6 איברים אבלית איזומורפית ל ולכן אלו החח״ח היחידות של G מסדר 6. כל חבורה בת 3 איברים היא ציקלית ואיזומורפית ל $\mathbb{Z}_3$. יש שני איברים מסדר 3, $(2,0)$ ו $(4,0)$ היוצרים את אותה ח״ח אשר איזומורפית ל $\mathbb{Z}_3$. כל חבורה בת 2 איברים היא ציקלית ואיזומורפית ל $\mathbb{Z}_2$. יש שלשה איברים מסדר 3, $(3,0)$ ו $(0,1)$ ו $(3,1)$ היוצרים שלוש ח״ח שונות אשר איזומורפית ל $\mathbb{Z}_2$. ישנה חבורה אבלית שאיננה ציקלית בת 4 איברים אשר איזומורפית ל $\mathbb{Z}_2 \times \mathbb{Z}_2$, ונשים לב כי האיברים $(3,0)$ ו $(0,1)$ ו $(3,1)$ מתאימים לאותה חבורה (חבורת קליין). לכן קבלנו 3 ח״ח אשר איזומורפיות ל $\mathbb{Z}_6$, ח״ח אחת אשר איזומורפית ל $\mathbb{Z}_3$, ח״ח אחת אשר איזומורפית ל $\mathbb{Z}_2 \times \mathbb{Z}_2$, ולה יש 3 ח״ח אשר איזומורפיות ל $\mathbb{Z}_2$. ובנוסף החח״ח המכילה אבר יחידה בלבד ואשר היא כל G, סה״כ 10 ח״ח.

תשובה 5

קודם כל נחשב את כל האיברים שיש להם ממם (gcd) 1 עם 20 והללו הם $1,3,7,9,11,13,17,19$, כלומר החבורה הזו היא בת 8 איברים. כעת נחשב את הסדר של כל איבר:

$$1^1 = 1$$

$$3^2 = 9 = 9, 3^3 = 27 = 7, 3^4 = 81 = 1$$

$$7^2 = 49 = 9, 7^3 = 9 \cdot 7 = 63 = 3, 7^4 = 3 \cdot 7 = 21 = 1,$$

$$9^2 = 81 = 1,$$

$$11^2 = 121 = 1,$$

$$13^2 = 169 = 9, 13^3 = 9 \cdot 13 = 117 = 17, 13^4 = 17 \cdot 13 = 221 = 1,$$

$$17^2 = 289 = 9, 17^3 = 9 \cdot 17 = 153 = 13, 17^4 = 17 \cdot 13 = 221 = 1,$$

$$19^2 = 361 = 1$$

לכן החבורה איננה ציקלית כיון שאין לה איבר מסדר 8. בנוסף $137 = 136 + 1 = 4 \cdot 34 + 1$ ולכן $7^{137} = 7^{4 \cdot 34 + 1} = (7^4)^{34} 7 = 1 \cdot 7 = 7$ כדרוש.

יש 4 איברים מסדר 4 והם יוצרים 2 ח״ח מסדר 4 אשר איזומורפיות ל $\mathbb{Z}_4$ האחת מכילה את 3 ו 7, השניה את 13 ואת 17. יש 3 איברים מסדר 2 והללו יוצרים 3 ח״ח בנות שני איברים אשר איזומורפיות ל $\mathbb{Z}_2$, ובנוסף 3 האברים מסדר 2 יוצרים ח״ח בת ארבעה איברים אשר איזומורפית לחבורת קליין $\mathbb{Z}_2 \times \mathbb{Z}_2$, ואשר כוללת את 3 החבורות החלקיות האיזומורפיות ל $\mathbb{Z}_2$ כחבורות חלקיות. לכן יש $1+3+2$ חבורות חלקיות אמיתיות, ובנוסף החבורות החלקיות הטריוויאליות בנות אבר אחד וכל G, סה״כ 8 חבורות חלקיות.

תשובה 10

א. עבור $R = \mathbb{Z}$ קבוצת המספרים המתחלקים ב6 היא ח״ח של החבורה של R, ומכפלת כל מספר שלם במספר המתחלק ב-6 היא מספר המתחלק ב-6 ולכן קיימת תכונת הבליעה

ב. אם R שדה ומכיל אבר השונה מ-0 a, אז לפי הגדרה הוא מכיל גם את $aa^{-1} = 1$ ולכן עבור כל $r \in R$ מתקיים $1r \in I$ כ כלומר $I = R$

ג. קבוצת המספרים המתחלקים ב 2 היא אידאל ראשוני כי קבוצת המשלימים שהיא כל המספרים האי זוגיים סגורה לכפל

ד. שדה תן דוגמא של אידאל השונה מהקבוצה המכילה רק את 0.

ה. אידאל נקרא ראשוני אם יש לו התכונה הנוספת שאם $x \in I, y \in R \to xy \in I$. מצא אידאל ראשוני בתוך החוג $R = \mathbb{Z}$.
מצא גם אידאל לא ראשוני באותו חוג.

תשובה 11

א. דוגמא נגדית $R = \mathbb{Z}, S = \mathbb{Z}_4, f : \mathbb{Z} \to \mathbb{Z}_4, f(x) = x\%4$. זהו הומומורפיזם של חוגים כיון ש
$(x+y)\%4 = (x\%4 + y\%4)\%4, (xy)\%4 = (x\%4 y\%4)\%4$ על לפי ההגדרה
חוג השלמים הוא תחום שלמות אך ב $\mathbb{Z}_4$ יש מחלקי 0 למשל
$2 \cdot 2 = 0 \in \mathbb{Z}_4$.

ב. דוגמא נגדית $R = \mathbb{Z}_4, S = \mathbb{Z}_2, f : \mathbb{Z}_4 \to \mathbb{Z}_2, f(x) = x\%2$. זהו הומומורפיזם של חוגים כיון ש
$(x+y)\%2 = (x\%2 + y\%2)\%2, (xy)\%2 = (x\%2 y\%2)\%2$ על לפי ההגדרה
$\mathbb{Z}_2$ הוא שדה ולכן תחום שלמות אך ב $\mathbb{Z}_4$ יש מחלקי 0 למשל
$2 \cdot 2 = 0 \in \mathbb{Z}_4$