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"ו.

מועד א יום ה,כו אלול התשע"ו 29-9-2016

- 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.

עמותה רשומה 580242451 **Fax:** (972-9) 8844439 **:פקס** **Tel:** (972-9) 8607777 **:טל**

חלק א

שאלה 1

נביט ב 4 הנקודות $(\pm1,\pm1)$ ב $\mathbb{R}^2$. הנקודות הן קדקדים של רבוע

הגדר את G כאוסף כל ההעתקות שומרות המרחק החד חד ערכיות (חח״ע) ועל של הרבוע לעצמו עם פעולת הרכבת העתקות.

א. רשום את כל איברי G.

ב. חשב את הסדר של כל אבר ב-G.

ג. כמה הומומורפיזמים חח״ע ישנם $f:\mathbb{S}_3\to G$? רשום אותם.

ד. כמה הומומורפיזמים חח״ע ישנם $f:\mathbb{S}_2\to G$? רשום אותם.

שאלה 2

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

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

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:

$a(x)=x^4+3x^3+3x^2+3x+2\in\mathbb{Z}_7[x],\ \ b(x)=x^3+5x^2+2\in\mathbb{Z}_7[x]$. מצא פולינומים $u(x),v(x)\in\mathbb{Z}_7[x]$ המקיימים $\mathrm{d(x)=gcd}(a(x),b(x))=a(x)u(x)+b(x)v(x)$.

שאלה 4

תהינה $G=(\mathbb{Z}_7,\oplus_7)$ $H=(\mathbb{Z}_2,\oplus_2)$ שתיהן עם פעולת החיבור מודולו, ונגדיר על הקבוצה $G\times H$ פעולה בינרית על ידי

$$\forall (g,h),(a,b)\in G\times H, (g,h)(a,b)=(g\oplus_7 a, h\oplus_2 b)$$

א. הוכח כי $G\times H$ עם הפעולה הזו היא חבורה.

ב. מצא את כל הסדרים של כל האיברים בחבורה.

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

שאלה 5

נתונה החבורה $(\mathbb{Z}_{30}^*,\cdot)$. (כל האיברים ההפיכים עם פעולת הכפל).

א. חשב את 7^{137} ב-$(\mathbb{Z}_{30}^*,\cdot)$.

ב. מצא את כל האיברים של $(\mathbb{Z}_{30}^*,\cdot)$ מסדר 2.

ג. האם $(\mathbb{Z}_{30}^*,\cdot)$ 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 $L\le H$ חבורה חלקית אז $f^{-1}(L)\le G$ חבורה חלקית.

ג. f חח״ע אם ורק אם Ker(f)={e}

שאלה 8

הוכח כי לכל חבורה G וחבורה חלקית H מתקיים

א. $\forall g \in G, g \in g*H$

ב. $\forall g,k \in G, k \in g*H \rightarrow k*H \subseteq g*H$

ג. $\forall g,k \in G, k \in g*H \rightarrow k*H = g*H$

ד*. $\forall g,k \in G,\ [(g*H \cap k*H \neq \emptyset) \rightarrow (g*H = k*H)]$.

ה*. $a_g : H \rightarrow g*H$ $\forall g$ היא פונקציה חד חד ערכית ועל.

ו*. $G = \bigcup_{g \in G} g*H$.

שאלה 9

יהיו $a,b \in \mathbb{Z}$ שני מספרים שלפחות אחד מהם שונה מ-0.אז קימים מספרים $x,y \in \mathbb{Z}$ כך שמתקיים $ax+by=\gcd(a,b)$.

<u>חלק ג</u>

שאלה 10

נתון חוג R. אבר $x \in R$ יקרא נילפוטנטי אם קים $n \in \mathbb{N}$ כך שמתקיים $x^n = 0$.(נשים לב כי מדובר על פעולת הכפל, כלומר $x^n = x \cdot x \cdot x \cdots x$ על ידי הכפל). $n \in \mathbb{N}$ הקטן ביותר עם התכונה הזו קרוי סדר הנילפוטנטיות של $x \in R$. אם $x \in R$ אינו נילפוטנטי אומרים כי סדר הנילפוטנטיות שלו הוא ∞ .

1. מהו סדר הנילפוטנטיות של 0?
2. מהו סדר הנילפוטנטיות של 1?

3. נתונים חוג מתחלף כפלית R ובו שני איברים $x \in R$ מסדר נילפוטנטיות $n \in \mathbb{N}$ ו $y \in R$ מסדר נילפוטנטיות $m \in \mathbb{N}$ האם $x + y \in R$ נילפוטנטי? הוכח או הפרך. אם נילפוטנטי מאיזה סדר נילפוטנטיות?
4. נתונים חוג מתחלף כפלית R ובו שני איברים $x \in R$ מסדר נילפוטנטיות $n \in \mathbb{N}$ ו $y \in R$ לאו דוקא נילפוטנטי. האם $xy \in R$ נילפוטנטי? הוכח או הפרך. אם נילפוטנטי מאיזה סדר נילפוטנטיות?
5. האם אוסף האיברים הנילפוטנטיים בתוך חוג מתחלף R מהווה תת חוג?

שאלה 11

תן דוגמא לחבורה G לא אבלית בת 24 איברים, ומצא שתי פונקציות שונות $f \neq g : S_3 \to G$ שכל אחת מהן היא הומומורפיזם חח״ע.

<u>בהצלחה</u>

תשובות:

תשובה 1

ברור כי כל העתקה חח״ע ועל ששומרת על המרחק צריכה לשלוח כל קדקד לקדקד אחר. נסמן את הקדקדים ב D,C,B,A ויש 8 העתקות:

$I:(A,B,C,D)\to(A,B,C,D), s:(A,B,C,D)\to(D,A,B,C), sk:(A,B,C,D)\to(C,D,A,B),$
$sh:(A,B,C,D)\to(B,C,D,A), ac:(A,B,C,D)\to(A,D,C,B), bd:(A,B,C,D)\to(C,B,A,D)$
$k1:(A,B,C,D)\to(D,C,B,A), k2:(A,B,C,D)\to(B,A,D,C)$

. הסדר של I הוא אחד, הסדרים של sk,ac,bd,k1,k2 הם 2, והסדרים של s,sh הם 4.

לא יתכן הומומורפיזם חח״ע $f:\mathbb{S}_3\to G$ כי כל אחד כזה שומר על סדר של כל אבר מהתחום, בתחום יש אברים בעלי סדר 3, ב G יש איברים רק בעלי סדר 2,4 . יתכנו הומומורפיזמים חח״ע $f:\mathbb{S}_2\to G$ כיון שגם בתחום וגם בטוח יש אברים בעלי סדר 2 ו-1 בלבד, ולכן האבר היחיד של $\mathbb{S}_2=\mathbb{Z}_2$ שהוא בעל סדר 2 , יכול ללכת ל-5 איברים שונים בG, ולכן יש 5 הומומורפיזמים חח״ע $f:\mathbb{S}_2\to G$.

תשובה 2

נחשב את f ואת g בצורה מפורשת. עבור f :

ולכן נקבל את f על ידי :

$$\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 2/5 & 3/0 & 4/(-5) & 5/(-10) & 6/(-15) & 7/(-20) & 8/(-25) \\ 2/5 & 3/0 & 4/2 & 5/4 & 6/6 & 7/1 & 8/3 \\ 6 & ? & 2 & 3 & 1 & 0 & 5 \end{array}$$

$$f \downarrow \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 1 & 0 & 5 \end{array}$$

ובצורה דומה עבור עבור g

ולכן נקבל את g על ידי :

$$\begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 3/4 & 5/(-1) & 7/(-6) & 9/(-11) & 11/(-16) & 13/(-21) & 15/(-26) \\ 3/4 & 5/6 & 7/1 & 2/3 & 4/5 & 6/0 & 1/2 \\ 6 & 2 & 0 & 3 & 5 & ? & 4 \end{array}$$

$$g \downarrow \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 0 & 3 & 5 & 1 & 4 \end{array}$$

וגם את g^2 :

$$\begin{array}{cccccccc} x & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ g(x) & 6 & 2 & 0 & 3 & 5 & 1 & 4 \\ g^2(x) & 4 & 0 & 6 & 3 & 1 & 2 & 5 \end{array}$$

וכעת נחשב את ההפוכים :

$$f \downarrow \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 1 & 0 & 5 \end{array}$$

$$f^{-1} \downarrow \begin{array}{ccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 2 & 3 & 1 & 6 & 0 \end{array}$$

$$\begin{array}{cccccccc} x & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ g(x) & 6 & 2 & 0 & 3 & 5 & 1 & 4 \\ g^2(x) & 4 & 0 & 6 & 3 & 1 & 2 & 5 \\ g^{-2}(x) & 1 & 4 & 5 & 3 & 0 & 6 & 2 \end{array}$$

ולבסוף נקבל את ההרכבה :

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

העתקה זו היא מהצורה $(041)(265)$ ובעלת סדר 3,

ונקבל אותה כמכפלת חלופים: $(25)(26)(01)(04)$.

תשובה 3

$$x^4+3x^3+3x^2+3x+2=(x^3+5x^2+2)(x+5)+(6x^2+x+6)$$
$$(x^3+5x+2)=(6x+6)(6x^2+x+6)+5x+1.$$
$$6x^2+x+6=(4x+5)(5x+1)+1$$
$$5x+1=1(5x+1)+0,\mathrm{gcd}=1$$

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

תשובה 4

תהינה $G=(\mathbb{Z}_7,\oplus_7)$ $H=(\mathbb{Z}_2,\oplus_2)$ שתיהן עם פעולת החיבור מודולו, ונגדיר על הקבוצה $G\times H$ פעולה בינרית על ידי

$$\forall(g,h),(a,b)\in G\times H,(g,h)(a,b)=(g\oplus_7 a,h\oplus_2 b)$$

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.

$(0,0)^1 = 0$

$(1,0)^2 = (2,0), (1,0)^3 = (3,0), (1,0)^4 = (4,0), (1,0)^5 = (5,0), (1,0)^6 = (6,0), (1,0)^7 = (0,0)$

$(2,0)^2 = (4,0), (2,0)^3 = (6,0), (2,0)^4 = (1,0), (2,0)^5 = (3,0), (2,0)^6 = (5,0), (2,0)^7 = (0,0)$

$(3,0)^2 = (6,0), (3,0)^3 = (2,0), (3,0)^4 = (5,0), (3,0)^5 = (1,0), (3,0)^6 = (4,0), (3,0)^7 = (0,0)$

ב. $(4,0)^2 = (1,0), (4,0)^3 = (5,0), (4,0)^4 = (2,0), (4,0)^5 = (6,0), (4,0)^6 = (3,0), (4,0)^7 = (0,0)$

$(5,0)^2 = (3,0), (5,0)^3 = (1,0), (5,0)^4 = (6,0), (5,0)^5 = (4,0), (5,0)^6 = (2,0), (5,0)^7 = (0,0)$

$(6,0)^2 = (5,0), (6,0)^3 = (4,0), (6,0)^4 = (3,0), (6,0)^5 = (2,0), (6,0)^6 = (1,0), (6,0)^7 = (0,0)$

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

$(1,1)^2 = (2,0), (1,1)^3 = (3,1), (1,1)^4 = (4,0), (1,1)^5 = (5,1), (1,1)^6 = (6,0), (1,1)^7 = (0,1), (1,1)^8 = (1,0),$

$(1,1)^9 = (2,1), (1,1)^{10} = (3,0), (1,1)^{11} = (4,1), (1,1)^{12} = (5,0), (1,1)^{13} = (6,1), (1,1)^{14} = (0,0)$

ברגע שנמצא אבר מסדר 14 בחבורה בת14 איברים אז אפשר להבין כי הסדר של כל איבר הוא מכפלת הסדרים של רכיביו, ולכן כל האיברים $(1,1),(2,1),(3,1),(4,1),(5,1),(6,1)$ יהיו בעלי סדר 14.

ג. לחבורה יש ח״ח יחידה מסדר 14 וזו היא עצמה, יש לה ח״ח בת 7 איברים המורכבת ונוצרת על ידי האיברים מהצורה $(1,0),(2,0),(3,0),(4,0),(5,0),(6,0)$ ויש לה ח״ח בת 2 איברים הנוצרת על ידי $(1,0)$ מצא את כל החבורות החלקיות של $G \times H$.

תשובה 5

קודם כל נחשב את כל האיברים שיש להם מממ (gcd) 1 עם 30 והללו הם 1,7,9,11,13,17,19,23,29 כלומר החבורה הזו היא בת 8 איברים. כעת נחשב את הסדר של כל איבר:

$1^1 = 1$

$7^2 = 49 = 19, 7^3 = 19 \cdot 7 = 133 = 13, 7^4 = 13 \cdot 7 = 91 = 1,$

$11^2 = 121 = 1$

$13^2 = 169 = 19, 13^3 = 19 \cdot 13 = 247 = 7, 13^4 = 7 \cdot 13 = 91 = 1$

מכיון שלמשל $17 = -13 (\mathrm{mod}\, 30)$ נובע כי המינוס בחזקה זוגית נעלם, ולכן לכל איבר יש סדר כמו למינוס שלו. 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.

תשובה 10

כיון שמתקיים $0^1=0$ נובע כי סדר הנילפוטנטיות של 0 הוא 1.
כיון שמתקיים $1^n=1$ נובע כי אף חזקה של 1 איננה שוה 0, 1 איננו נילפוטנטי ולכן סדר הנילפוטנטיות של 1 הוא ∞. נביט בנוסחא הידועה עבור חוג מתחלף $(x+y)^k = x^k + \binom{k}{1}x^{k-1}y+\cdots = \sum_{j=0}^{k}\binom{k}{j}x^{k-j}y^j$,

המקדמים $\binom{k}{j}$ קרויים המקדמים הבינומיים של ניוטון ואין צורך לדעת מהו ערכם המדויק כדי לשים לב לכך שעבור $k>n+m$ מתקיים אחד מהשניים $(j>m)\vee(k-j>n)$ ומכאן נובע כי $(y^j=0)\vee(x^{k-j}=0)$ ולכן כל מחובר הוא 0 ולכן הסכום הוא 0 ולכן אכן $x+y$ נילפוטנטי מסדר $m+n$. שוב בחוג מתחלף $(xy)^k=x^ky^k$ ולכן נובע כי $(xy)^n=x^ny^n=0y^n=0$ כלומר אכן xy הוא נילפוטנטי מסדר n. לכן אוסף האיברים הנילפוטנטיים של R איננו תת חוג של R. הוא אמנם סגור לחיבור וכפל אבל אינו מכיל את אבר היחידה.

תשובה 11

ראינו כי אוסף כל הפונקציות החח״ע ועל של קדקדי משולש שוה צלעות לעצמן מהווה חבורה S_3 בת $3!=6$ איברים ולכן אוסף כל ההעתקות חח״ע ועל של פירמידה סימטרית לעצמה הוא חבורה S_4 בת 24 איברים. נסמן את קבוצת קדקדי הפירמידה ב $A=\{0,1,2,3\}$ אז יש 6 העתקות חח״ע ועל של הקבוצה החלקית $B=\{0,1,2\}$ ואם נוסיף להן את הדרישה כי כל העתקה כזו מעתיקה את הקדקד 3 לעצמו, נקבל חבורה חלקית לא אבלית של S_4, ולכן גם S_4 איננה אבלית. בצורה דומה יש 6 העתקות חח״ע ועל של הקבוצה החלקית $C=\{1,2,3\}$ ואם נוסיף להן את הדרישה כי כל העתקה כזו מעתיקה את הקדקד 0 לעצמו, נקבל חבורה חלקית אחרת לא אבלית של S_4, שתי החבורות החלקיות הללו איזומורפיות ל S_3