



מבחן סוף במבנים אלגבריים למדעי המחשב-סמסטר קיץ

ה'תשע"ח.

מועד ב יום ב כ חשון התשע"ט 29-10-2018

- מורה: גיורא דולה, מתרגל: רענן שכטר.
- משך המבחן הוא שלש שעות.
- אפשר להשתמש רק במחשבון ובדפי העזר המצורפים.
- יש לכתוב במחברת תשובה מלאה עבור כל אחת מהשאלות.
- במבחן יש ארבעה חלקים. בחלק א שתי שאלות ומשקל כל שאלה 10 נקודות. בחלק ב יש 2 שאלות ומשקל כל שאלה 15 נקודות. אפשר לענות על כמה שאלות שרותים מחלקים א ו ב. בחלק ג יש 4 שאלות ומשקל כל שאלה 15 נקודות. ומתוכן יש לבחור 3. בחלק ד יש שאלה אחת ומשקלה 5 נקודות.
- $2*10+2*15+3*15+1*5=100$
- מותר להסתמך על כל טענה שהוכחה בכתה אך יש לנסח אותה במדויק בנפרד.

בהצלחה.

חלק א

שאלה 1

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).

$$f = \begin{cases} \frac{1}{x} - 2 & 0 \neq x \in \mathbb{Z}_7 \\ a & 0 = x \in \mathbb{Z}_7 \end{cases}, g = (1, 2, 6)(5, 4, 3)$$

- א. מצא את a .
- ב. חשב את $f^2 g^{-1}$.
- ג. פרק את $f^2 g^{-1}$ למכפלה של מחזורים זרים.
- ד. פרק את $f^2 g^{-1}$ למכפלה של חילופים.
- ה. מצא את הסדר של $f^2 g^{-1}$.

שאלה 2

חשב את המחלק המשותף $d(x)$ הגדול ביותר של הפולינומים הבאים:
מצא פולינומים $a(x) = x^4 + x^2 + 1 \in \mathbb{Z}_5[x]$, $b(x) = x^3 + 1 \in \mathbb{Z}_5[x]$
 $d(x) = \gcd(a(x), b(x)) = a(x)u(x) + b(x)v(x)$ המקיימים $u(x), v(x) \in \mathbb{Z}_5[x]$.

חלק ב

שאלה 3

נביט בשתי המטריצות הבאות:

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

- א. חשב את הסדרים של כל האיברים מהצורה $\{S^i T^j, 0 \leq i, j\}$
- ב. מצא שתי ח"ח שונות של $\{S^i T^j, 0 \leq i, j\}$ אשר כל אחת איזומורפית

ל \mathbb{Z}_6 .

שאלה 4

- נתונה החבורה $G = (\mathbb{Z}_{48}^*, \cdot)$. (כל האיברים ההפיכים עם פעולת הכפל).
- א רשום את כל האיברים ב G .
- ב. חשב את 5^{122} ב- G .
- ג. מצא את כל הסדרים של אברי החבורה.
- ד. מצא ב G שלוש תת חבורות שונות בנות ארבעה איברים.

חלק ג

שאלה 5

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

שאלה 6

- יהי $f: G \rightarrow H$ הומומורפיזם של חבורות : הוכח
- א. תהי $K \leq G$ חבורה חלקית אז $f(K) \leq H$ חבורה חלקית.
- ב. תהי $L \leq H$ חבורה חלקית אז $f^{-1}(L) \leq G$ חבורה חלקית.
- ג. $\text{Ker}(f) = \{e\}$ אם ורק אם f חח"ע אם ורק אם $\{e\}$.

שאלה 7

- נסח והוכח את התנאי המקוצר עבור ח"ח.

שאלה 8

הוכח בחוג הפולינומים $S[x]$. עבור שדה S , לכל שני פולינומים

$p(x), q(x)$ קימים פולינומים $a(x), b(x)$ כך שמתקיים השוויון

$$a(x)p(x) + b(x)q(x) = \gcd(p(x), q(x))$$

חלק ד

שאלה 9

מצא הומומורפיזם חח"ע $f: \mathbb{S}_3 \rightarrow GL(3, \mathbb{Z})$

בהצלחה

תשובה 1

נחשב את f ואת g בצורה מפורשת. עבור f :

	0	1	2	3	4	5	6	
$1/0-2$								
$1/1-2$								
$1/2-2$								
$1/3-2$								
$1/4-2$								
$1/5-2$								
$1/6-2$								
a	6	2	3	0	1	4		
5	6	2	3	0	1	4		
x	0	1	2	3	4	5	6	
$f(x)$	5	6	2	3	0	1	4	את f^2
$f^2(x)$	1	4	2	3	5	6	0	

ולכן נקבל את f וגם

ונקבל את g על ידי:

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

וכעת נחשב את ההרכבה:

	x	0	1	2	3	4	5	6
	$g^{-1}(x)$	0	6	1	4	5	3	2
(01)(246)(35) העתקה זו היא מהצורה	$f^2(x)$	1	4	2	3	5	6	0
	$f^2 g^{-1}(x)$	1	0	4	5	6	3	2

ובעלת סדר 10, ונקבל אותה כמכפלת חלופים : (01)(24)(26)(35)

תשובה 2

$$a(x) = x^4 + x^2 + 1 \in \mathbb{Z}_5[x], \quad b(x) = x^3 + 1 \in \mathbb{Z}_5[x]$$

$$x^4 + x^2 + 1 = (x^3 + 1)x + (x^2 + 4x + 1)$$

$$(x^3 + 1) = (x^2 + 4x + 1)(x + 1) + 0.$$

$$\gcd = x^2 + 4x + 1$$

$$\gcd = x^2 + 4x + 1 = x^4 + x^2 + 1 - (x^3 + 1)x = a(x) - xb(x)$$

תשובה 3

$$S = \begin{pmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, T = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, S^1 = S, S^2 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, S^3 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, S^4 = I_3, T^1 = T,$$

$$T^2 = I, ST = \begin{pmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, (ST)^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & -1 \\ -1 & 0 & 0 \end{pmatrix}, (ST)^3 = -I, o(ST) = 6.$$

$$S^2T = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}, (S^2T)^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}, o(S^2T) = 4,$$

$$S^3T = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, (S^3T)^2 = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 0 & 0 \end{pmatrix}, (S^3T)^3 = -I, o(S^3T) = 6,$$

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

סעיף ב החי"ח הנוצרת על ידי ST, S^3T מהאיברים כל אחד מהאיברים

תשובה 4

קודם כל נחשב את כל האיברים שיש להם מממ (gcd) עם 48 והללו הם 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47. כעת נחשב את הסדר של כל האיברים:

1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47

$$o(1) = 1,$$

$$5^2 = 25, 5^3 = 125 = 29, 5^4 = 29 \cdot 5 = 145 = 1, o(5) = 4$$

$$7^2 = 49 = 1, o(7) = 1$$

$$11^2 = 121 = 25, 11^3 = 25 \cdot 11 = 275 = 35, 11^4 = 35 \cdot 11 = 385 = 1, o(11) = 4$$

$$13^2 = 169 = 25, 13^3 = 25 \cdot 13 = 325 = 37, 13^4 = 37 \cdot 13 = 481 = 1, o(13) = 4$$

$$17^2 = 289 = 1, o(17) = 2$$

$$19^2 = 361 = 25, 19^3 = 25 \cdot 19 = 475 = 43, 19^4 = 43 \cdot 19 = 817 = 1, o(19) = 4$$

$$23^2 = 529 = 1, o(23) = 2$$

$$25^2 = 625 = 1, o(25) = 2$$

$$29^2 = 841 = 25, 29^3 = 25 \cdot 29 = 725 = 5, 29^4 = 5 \cdot 29 = 145 = 1, o(29) = 4$$

$$31^2 = 961 = 1, o(31) = 2$$

$$35^2 = 1225 = 25, 35^3 = 25 \cdot 35 = 875 = 11, 35^4 = 35 \cdot 11 = 385 = 1, o(35) = 4$$

$$37^2 = 1369 = 25, 37^3 = 25 \cdot 37 = 925 = 13, 37^4 = 13 \cdot 37 = 481 = 1, o(37) = 4$$

$$41^2 = 1681 = 1, o(41) = 2$$

$$43^2 = 1849 = 25, 43^3 = 25 \cdot 43 = 1075 = 19, 43^4 = 43 \cdot 19 = 817 = 1, o(43) = 4$$

$$47^2 = 2029 = 1, o(47) = 2$$

$$5^{122} = 5^{4 \cdot 30 + 2} = (5^4)^{30} 5^2 = (1)^{30} 5^2 = 1 \cdot 25 = 25$$

$$H = \{5, 25, 29, 1\}, H = \{11, 25, 35, 1\}, H = \{13, 25, 37, 1\}, H = \{19, 25, 43, 1\}$$

תשובה 9

א. נשים לב כי על ידי האיברים $R, A \in \mathbb{S}_3$, ניתן לבטא את שאר

איברי \mathbb{S}_3 , כיון שמתקיים $R^2 = L, R^3 = I, RA = B, R^2 A = C, R^3 A = A$

כלומר $\mathbb{S}_3 = \{R^i A^j, 0 \leq i, j, R^3 = A^2 = I\}$ כמו כן נשים לב כי מתקיים

היחס $RA = AR^2 = B$. לכן מספיק שנעתיק את R לאיבר מסדר 3

ואת A לאיבר מסדר 2 ב $GL(3, \mathbb{Z})$, והללו יקימו את הקשר

יש כמה איברים כאלו ונבחר $f(R)f(A) = f(A)f(R)^2$

$$S = f(A) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, T = f(R) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, S^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, T^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, T^3 = I,$$

$$TS = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = ST^2$$