

פתרון מבנים אלגבריים להנדסה, 83-218, בוחן 2 תשע"ט

י"ג סיון ה'תשע"ט, 16.6.19

מרצה: פרופ' נתן קלר.

מתרגל: אריאל ויצמן.

- מבנה הבוחן וניקוד: בחרו **3 מתוך 4** השאלות. כל שאלה שווה 34 נקודות.
- הקפידו על סדר וניקיון.
- משך הבוחן: שעה וחצי.
- ללא חומר עזר. גם לא מחשבון.
- נמקו היטב את תשובותיכם!

המלצה: הסתכלו על כל השאלות והתחילו עם השאלות שעליהן אתם יודעים לענות.

חלקו את זמנכם בתבונה!

בהצלחה!

(א) קבוצת השלמים של גאוס היא הקבוצה הבאה: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ (כאשר $i = \sqrt{-1}$). הוכיחו שקבוצה זו עם פעולות חיבור וכפל כמו במרוכבים היא חוג חילופי עם יחידה. (17 נק')

(ב) יהי R חוג. נניח שקיימים $a, b \in R$ כך ש- $ab = a, ba = b$. הוכיחו: $a^2 = a, b^2 = b$. (17 נק')

פתרון:

א. כיון ש- $\mathbb{Z}[i] \subseteq \mathbb{C}$ נוכל להשתמש בקריטריון המקוצר:

סגירות לחיבור: לכל $a + bi, c + di \in \mathbb{Z}[i]$ אכן מתקיים: $(a + bi) - (c + di) = (a - c) + (b - d)i \in \mathbb{Z}[i]$ (כ) $(a - c, b - d \in \mathbb{Z})$.

סגירות לכפל: לכל $a + bi, c + di \in \mathbb{Z}[i]$ אכן מתקיים: $(a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i]$ (כ) $(ac - bd, ad + bc \in \mathbb{Z})$.

חילופיות בירושה מ- \mathbb{C} .

עם יחידה: כיון ש- $1_{\mathbb{C}} = 1 + 0i \in \mathbb{Z}[i]$, זו גם היחידה של החוג שלנו.

ב. מתקיים:

$$a^2 = a \cdot a \stackrel{*}{=} (ab)a \stackrel{**}{=} a(ba) \stackrel{*}{=} ab \stackrel{*}{=} a$$

כאשר שיוויון * נובע מהנתונים, וביוויון ** מקיבוץ. בדומה מאד:

$$b^2 = bb = (ba)b = b(ab) = ba = b$$

2. יהא R חוג חילופי עם יחידה. איבר $a \in R$ יקרא מחלק אפס אם קיים $b \in R$ כך ש $ab = 0$. הוכיחו או הפירוכו:

(א) אם $a \in R$ הפיך אז a אינו מחלק אפס. (17 נק')

(ב) אם $a \in R$ אינו מחלק אפס אז a הפיך. (17 נק')

פתרון:

א. הוכחה: נניח בשלילה כי a מחלק אפס אזי קיים $b \neq 0$ כך ש $ab = 0$. נכפול את השוואה ב a^{-1} ונקבל

$$b = 1 \cdot b = a^{-1}ab = a^{-1}0 = 0$$

סתירה.

ב. הפרכה: למשל $3 \in \mathbb{Z}$ אינו מחלק אפס כי לכל $b \neq 0$ מתקיים $3b \neq 0$ אבל 3 אינו הפיך.

3. תזכורת: פולינום $p(x) \in \mathbb{F}[x]$ נקרא ראשוני אם לכל $a(x), b(x) \in \mathbb{F}[x]$ מתקיים: $p(x) \mid a(x)b(x) \Rightarrow p(x) \mid a(x) \vee p(x) \mid b(x)$.

(א) הוכיחו כי אם $p(x) \in \mathbb{F}[x]$ פולינום (מדרגה גדולה ממש מאפס) אי פריק אזי הוא ראשוני. (17 נק')

(ב) הראו שיש בדיוק פולינום אי-פריק אחד ממעלה שנייה ב $\mathbb{Z}_2[x]$. (17 נק')

פתרון:

א. נתון $p(x)$ אי פריק. צ"ל p ראשוני.

כעת יהיו a, b פולינומים כך ש $p \mid ab$ נוכיח כי $p \mid b$ או $p \mid a$. נסמן $d = \gcd(a, p)$

אזי בפרט $d \mid p$ ולכן קיים q כך ש $p = dq$ כיוון ש p אי פריק חייב להיות כי הדרגה של d או q שווה ל p ושל הפולינום השני היא 0.

אם $\deg(d) = \deg(p)$ אז $\deg(q) = 0$ ולכן $q \in \mathbb{F}$ פולינום קבוע ואז $p(x) = d(x)q$. כיוון ש $q \neq 0$ נקבל כי $d(x) = p(x) \cdot q^{-1}$ ובפרט $d(x) \mid a(x) \wedge d(x) \mid p(x)$ ולכן $p(x) \mid a(x)$ וסיימנו.

אחרת $\deg(d(x)) = 0$ ואז $d(x) = 1$.

באותו אופן נסמן $d'(x) = \gcd(b(x), p(x))$ ואז אם $\deg(d'(x)) = \deg(p(x))$ אז $p(x) \mid b(x)$ וסיימנו.

אחרת $d'(x) = 1$ ואז $\gcd(a, p) = \gcd(b, p) = 1$ ולפי תרגיל בית 1 $\gcd(ab, p) = 1$ אבל $p|ab, p$ ולכן $\deg(p) \leq 0$
 $\deg(1) = 0$ כלומר p פולינום קבוע כלומר מדרגה 0. סתירה.

ב. פולינום מדרגה לכל היותר 2 הוא מהצורה $p(x) = ax^2 + bx + c$ כאשר $a, b, c \in \mathbb{Z}_2$. אם הפולינום הוא אי פריק בפרט אין לו שורשים ולכן $p(0) \neq 0$ שזה גורר כי $c \neq 0$ וגם $p(1) \neq 0$ מה שגורר כי $a + b + c \neq 0$. כיוון שמדובר ב \mathbb{Z}_2 אזי שונה מאפס אומר שווה ל-1 ולכן

$$\begin{aligned} c &= 1 \\ a + b + c &= 1 \end{aligned}$$

וביחד

$$\begin{aligned} c &= 1 \\ a &= b \end{aligned}$$

כיוון שרוצים דרגה בדיוק 2 אזי $a \neq 0$ ולכן $a = 1$ ובס"ה נקבל כי $p(x) = x^2 + x + 1$. הוא אכן לא פריק כי אם הוא היה פריק היה לו שורש (לפי תרגיל קודם) אבל $p(1) \neq 0$ וגם $p(0) \neq 0$ ואלו השורשים היחידים האפשריים בשדה שלנו.

4. נסמן: $f(x) = x^5 + x^2, g(x) = x^4 + x^3 \in \mathbb{R}[x]$.

(א) מצאו את $\gcd(f(x), g(x))$. (17 נק')

(ב) מצאו פולינומים $a(x), b(x) \in \mathbb{R}[x]$ כך ש- $\gcd(f(x), g(x)) = a(x) \cdot f(x) + b(x) \cdot g(x)$. (17 נק')

פתרון:

א. נבצע חילוק פולינומים:

$x - 1$	
$x^5 + x^2$	$x^4 + x^3$
$x^5 + x^4$	
↓	
$-x^4 + x^2$	
$-x^4 - x^3$	
↓	
$x^3 + x^2$	

נמשיך עם $g(x)$ והשארית $r(x) = x^3 + x^2$: קל לראות ש- $x^4 + x^3 = x(x^3 + x^2)$ (אפשר כמובן לעשות חילוק פולינומים של g ב- r ולקבל שארית 0) מה שאומר ש- $r(x)|g(x)$, ולכן נקבל $\gcd(g, f) = \gcd(r, g) = r(x)$.
 ב. נקלף אחורה ונקבל:

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

ולכן:

$$\gcd(f, g) = x^3 + x^2 = (x^5 + x^2) - (x - 1)(x^4 + x^3) = f(x) + (-x + 1)g(x)$$

כלומר

$$a(x) = 1, b(x) = -x + 1$$