פתרון מבחן תשע"ט מועד א

29 ביוני 2020

.1

(א) יהי $f: S_3 \to \mathbb{Z}_{5779}$ הומ'. הוכיחו שלכל $\pi \in S_n$ מתקיים $f(\pi) = 0$.
פתרון: תהי $\pi \in S_n$ תמורה. ונניח $f(\pi) = a$ ולכן:

$$0 = f(id) = f(\pi^6) = 6a$$

לכן $6a = k \cdot 5779$ וכיון ש־ $\frac{5779}{6} \notin \mathbb{N}$ אז נקבל $a = k' \cdot 5779 \equiv 0 (\bmod 5779)$.

(ב) תהי G קומוטטיבית, H חבורה, $f: G \to H$ הומ' לא טריוויאלי. האם H קומוטטיבית?
פתרון: לאו דוקא. למשל נוכל להגדיר $f: \mathbb{Z}_2 \to S_3$ ע"י $f(0) = id, f(1) = (1, 2)$.

.2

(א) תהי G חבורה עם $|G| = 84$. ותהיינה $H_1, H_2 \leq G$ ת"ח. הוכיחו כי אם $|H_1| = 28, |H_2| = 12$ אז $H_1 \cap H_2$ קומוטטיבית.
פתרון: נשים לב ש־ $H_1 \cap H_2 \leq H_1, H_2$ ולכן אם נסמן $|H_1 \cap H_2| = k$ אז $k|12, 28 \Rightarrow k|\gcd(12, 28) = 4$, ולכן $k \in \{1, 2, 4\}$. אם $k = 1$ זו החבורה הטריוויאלית שכמובן חילופית. אם $k = 2$ אז זו חבורה מסדר ראשוני ולכן ציקלית ולכן חילופית. אם $k = 4$ ראינו שבמקרה זה החבורה תמיד חילופית (או שהיא ציקלית או שכולם (חוץ מהיחידה) מסדר 2 ואז לפי תרגיל בית חילופית).

(ב) תנו דוג' לחבורה אינסופית G כך שלכל n טבעי יש לה ת"ח מסדר n.
פתרון: נתבונן בחבורה G של אוסף הפונקציות ההפיכות מהטבעיים לעצמם עם פעולת ההרכבה. לכל n תת החבורה $H = \langle (1, 2, \ldots, n) \rangle$ היא מגודל n (אנחנו רגילים להסתכל עליה כת"ח של S_n, אבל היא גם ת"ח של G שלגבי כל טבעי גדול מ־n שולחת אותו לעצמו).

.3

(א) עושים $\gcd(x^7-1,x^6-1)$, ואז מקלפים אחורה כדי למצוא את הצירוף הנ"ל.

(ב) ראשית, אתקן את הטעות מהתרגול: אסור לבחור אידיאלים, כי אם A,B אידיאלים, אז נקבל:

$$(a+b)+(a'+b')=(a+a')+(b+b')\in A+B$$

$$(a+b)(a'+b')=\underbrace{aa'+ab'+ba'}_{\in A}+bb'\in A+B$$

איזה תתי חוגי יש שאינם אידיאלים? ראשית, ניתן לקחת את השדה עצמו. כלומר החוג הוא $\mathbb{R}[x]$ אז $\mathbb{R}$ הוא תת־חוג. בנוסף $\mathbb{Q}[x]\leq\mathbb{R}[x]$ (באופן כללי, אם $S\leq R$ תת־חוג אז $S[x]\leq R[x]$ תת־חוג של חוג הפולינומים). כלומר, לקחנו $A=\mathbb{R},B=\mathbb{Q}[x]$. כעת נשים לב שאין סגירות לכפל, כי למשל:

$$\underbrace{(\sqrt{2}+x)}_{\in\mathbb{R}+\mathbb{Q}[x]}\cdot\underbrace{(\sqrt{3}+x)}_{\in\mathbb{R}+\mathbb{Q}[x]}=\sqrt{6}+x(\sqrt{2}+\sqrt{3})+x^2\notin\mathbb{R}+\mathbb{Q}[x]$$

4. מתרגיל בית.

5.

(א) $\mathbb{F}$ שדה סופי בו $1+1=0$. הוכיחו שכל איבר הוא ריבוע. כלומר לכל x קיים y כך ש־ $x=y^2$.

פתרון: הנתון אומר שזהו שדה שנבנה מעל $\mathbb{Z}_2$, כלומר, שדה עם 2^n איברים.

גם כאן אתקן טעות מהתרגול: פתרתי בעזרת טענה: הפונקציה $f:\mathbb{F}\to\mathbb{F}$ המוגדרת ע"י $f(a)=a^2$ היא איזו':

הומ': כי $f(ab)=(ab)^2=a^2b^2=f(a)f(b)$. עד כאן נכון (גם הטענה נכונה)

חח"ע: צריך להוכיח שאם $f(a)=f(b)$ אז $a=b$. אכן, כי אם $a^2=b^2$ אז $a=\pm b$ כפי שנשאלתי המעבר הזה לא נכון בשדות סופיים אוטומטית.

לכן, נפתור בעזרת תרגיל שעשינו בכיתה: בשדה סופי עם p^n איברים מתקיים שלכל איבר a בשדה:

$$a^{p^n}=a$$

ולכן נקבל אצלנו עבור $p=2$ שמתקיים:

$$\left(a^{2^{n-1}}\right)^2=a^{2^n}=a$$

ו־ $a^{2^{n-1}}$ ה"מקור" של a.

(ב) תנו דוגמא לשדה עם יותר משני איברים בו מתקיים התנאי של סעיף א:

פתרון: ניקח את הפולינום x^2+x+1 שאי־פריק מעל $\mathbb{Z}_2$. זה שדה עם 4 איברים, והתנאי אכן עובד.