פתרון תרגיל בית 11 במבנים אלגבריים
89-214 סמסטר א' תשע"ו

הוראות בהגשת הפתרון יש לרשום בכל דף שם מלא, מספר ת"ז ומספר קבוצת תרגול. הגשת התרגיל עד התאריך י"ח שבט ה'תשע"ו, 28.1.2016.

שאלה 1. א. מצאו כמה חבורות אבליות יש מסדר 2016 עד כדי איזומורפיזם.

ב. מצאו באופן מפורש חבורות מסדר 2016 עם כל אחד מן האקספוננטים הבאים: 126, 168, 1008.

פתרון. א. נשים לב כי $2016 = 2^5 \cdot 3^2 \cdot 7$. כפי שראינו בכיתה, מספר החבורות האבליות, עד כדי איזומורפיזם, תלוי בחזקות בפירוק לראשוניים. המספר הוא $\rho(5)\rho(2)\rho(1) = 7 \cdot 2 \cdot 1 = 14$. כלומר ישנן 14 חבורות אבליות מסדר 2016.

ב. נוכל לבחור חבורות אבליות מסדר 2016. אם נציג אותן בצורה קנונית, זה יקל על מציאת האקספוננט. חבורה מאקספוננט 126 תהיה $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{126}$. האם אתם יכולים להוכיח שאין חבורה אבלית אחרת מסדר 2016 עם אקספוננט 126?
חבורה מאקספוננט 168 תהיה $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_{168}$. חבורה אחרת מאקספוננט 168 היא $\mathbb{Z}_{12} \times \mathbb{Z}_{168}$. האם אתם יכולים להוכיח שאין אחרות?
חבורה מאקספוננט 1008 תהיה $\mathbb{Z}_2 \times \mathbb{Z}_{1008}$. האם אתם יכולים להוכיח שאין אחרת?

שאלה 2. תהי $G = D_5 \times U_7$.

א. מצאו את תת־חבורת הקומוטטור G'.

ב. האבליניזציה $\overline{G} = {}^{G}\!/_{G'}$ היא חבורה אבלית סופית. מצאו את הצורה הקנונית שלה, כלומר מצאו מספרים d_i כך ש-$\overline{G} \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$ כאשר $d_i | d_{i+1}$.

ג. האם $\overline{G}$ איזומורפית לחבורה כפלית של שדה כלשהו?

פתרון. א. תהינה A, B חבורות. נשים לב כי עבור $a_1, a_2 \in A$ ו-$b_1, b_2 \in B$ מתקיים ש-

$$[(a_1, b_1), (a_2, b_2)] = ([a_1, a_2], [b_1, b_2])$$

ולכן $(A \times B)' = A' \times B'$). אצלנו $B = U_7$ היא אבלית, ולכן $U_7' = \{1\}$. עבור $A = D_5$, ברור כי $D_5' \neq \{\mathrm{id}\}$ מפני ש-D_5 לא אבלית. ניקח שני איברים $\tau\sigma^i, \tau\sigma^j \in D_5$ ונחשב

$$\left[\tau\sigma^i, \tau\sigma^j\right] = \tau\sigma^i\tau\sigma^j \left(\tau\sigma^i\right)^{-1} \left(\tau\sigma^j\right)^{-1} = \tau\sigma^i\tau\sigma^j\sigma^{-i}\tau\sigma^{-j}\tau = \tau\tau\sigma^{-i}\sigma^j\sigma^{-i}\sigma^j\tau\tau = \sigma^{2j-2i}$$

אם נבחר $j = 1, i = 0$, אזי קיבלנו כי $\sigma^2 \in D_5'$. לכן $\langle\sigma^2\rangle = \langle\sigma\rangle \leq D_5'$. אפשר להראות ישירות כי אין אף שיקוף (איבר מן הצורה $\tau\sigma^i$) ב-D_5'. דרך אחרת היא לשים לב כי $\langle\sigma\rangle \lhd D_5$, ושחבורת המנה ${}^{D_5}\!/_{\langle\sigma\rangle}$ היא מסדר 2, ולכן אבלית. כלומר $D_5' \leq \langle\sigma\rangle$, ובסך הכל קיבלנו כי $D_5' = \langle\sigma\rangle$. לכן

$$G' = D_5' \times U_7' = \langle\sigma\rangle \times \{1\} \cong \mathbb{Z}_5$$

ב. הסדר של $\overline{G}$ הוא

$$\left|\overline{G}\right| = |{}^{G}\!/_{G'}| = \frac{|G|}{|G'|} = \frac{10 \cdot 6}{5} = 12$$

יש בסך הכל שתי חבורות אבליות מסדר 12: $\mathbb{Z}_{12}$ ו-$\mathbb{Z}_2 \times \mathbb{Z}_6$. האם אתם יכולים להראות כי $\overline{G} \cong \mathbb{Z}_2 \times \mathbb{Z}_6$? העזרו בכך ש-$U_7$ היא חבורה אבלית מסדר 6 ולכן $U_7 \cong \mathbb{Z}_6$ וש-$\overline{D_5} \cong \mathbb{Z}_2$.

ג. לא. החבורה הכפלית של שדה סופי היא ציקלית, ובסעיף הקודם חישבנו $\overline{G} \cong \mathbb{Z}_2 \times \mathbb{Z}_6$, שאינה חבורה ציקלית.

שאלה 3. תהי G חבורה. נגדיר באופן רקורסיבי את סדרת תת־חבורות הנגזרת שלה. תהי $G^{(0)} = G$, ועבור $n > 0$ תהי $G^{(n)} = \left[G^{(n-1)}, G^{(n-1)}\right]$. למשל $G^{(1)} = G'$.

א. חבורה נקראת פתירה אם $G^{(n)} = \{e\}$ עבור n כלשהו. הוכיחו כי חבורת הייזנברג

$$H(\mathbb{R}) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

היא פתירה.

ב. תהי G חבורה פתירה. ה-n הקטן ביותר עבורו $G^{(n)} = \{e\}$ נקרא דרגת הפתירות של G. מצאו חבורות מדרגות הפתירות הבאות: 1, 2, 3.

ג. האם S_3 פתירה? האם S_5 פתירה? מותר להעזר בטענות שהופיעו בכיתה ללא הוכחה.

פתרון. א. איבר היחידה של $H(\mathbb{R})$ הוא I_3, מטריצת היחידה בגודל 3×3. ברור כי $H(\mathbb{R})^{(0)} \neq \{I_3\}$. נחשב ישירות איבר ב-$H(\mathbb{R})'$:

$$\begin{aligned}
\left[\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \right] &= \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix}^{-1} \\
&= \begin{pmatrix} 1 & a+d & af+b+e \\ 0 & 1 & c+f \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -a-d & ac+af+df-b-e \\ 0 & 1 & -c-f \\ 0 & 0 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 & af-cd \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}
\end{aligned}$$

על ידי בחירה מתאימה של a, c, d, f אפשר להראות כי ניתן לבחור כל מספר ממשי בפינה הימנית עליונה, ולכן

$$H(\mathbb{R})' = \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{R} \right\}$$

שהיא חבורה אבלית. לכן $H(\mathbb{R})^{(2)} = (H(\mathbb{R})')' = \{I_3\}$. כלומר $H(\mathbb{R})$ פתירה.

ב. ראינו בכיתה ש-G אבלית אם ורק אם $G' = \{e\}$. אם נבחר חבורה אבלית לא טריוויאלית, כמו $\mathbb{Z}_2$, אז נקבל חבורה פתירה מדרגת פתירות 1. החבורה $H(\mathbb{R})$ היא

לא אבלית, אבל $H(\mathbb{R})^{(2)} = \{I_3\}$, ולכן מדרגת פתירות 2. עבור דרגת פתירות 3 אפשר לבחור חבורה עם מבנה דומה לזה של $H(\mathbb{R})$, אבל עבור מטריצות בגודל 4×4:

$$\left\{ \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & 1 & f \\ 0 & 0 & 0 & 1 \end{pmatrix} : a,b,c,d,e,f \in \mathbb{R} \right\}$$

דוגמה אחרת היא S_4 עבורה מתקיים $S_4^{(1)} = A_4$, $S_4^{(2)} = V_4$ (חבורת קליין, שהיא אבלית) ו-$S_4^{(3)} = \{\mathrm{id}\}$.

ג. ראינו את החישוב $S_3' = A_3$. מפני ש-A_3 אבלית, אז $A_3' = \{\mathrm{id}\}$. לכן מפני ש-$S_3^{(2)} = A_3'$, נקבל כי S_3 פתירה.
עבור S_5 ראינו בכיתה כי $S_5' = A_5$. החבורה A_5 היא פשוטה ולא אבלית, ולכן $A_5' = A_5$ (כלומר A_5 מושלמת). המשמעות היא ש-$S_5^{(n)} = A_5$ לכל $n \geq 1$, ולכן S_5 לא פתירה.

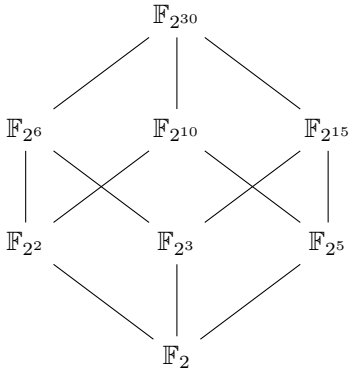
שאלה 4. הזכרו שסימנו את השדה הסופי בן q איברים ב-$\mathbb{F}_q$.

א. האם יש איזומורפיזם של שדות בין $\mathbb{Z}_8$ (עם הפעולות של חיבור וכפל מודולו 8) לבין $\mathbb{F}_8$?

ב. ציירו את סריג תת־השדות של $\mathbb{F}_{2^{30}}$.

פתרון. א. לאיזומורפיזם של שדות דרושים שדות. $\mathbb{Z}_8$ הוא בכלל לא שדה (למשל כי יש בו מחלקי אפס, $4 \cdot 2 \equiv 0 \pmod 8$), ולכן אין איזומורפיזם של שדות בינו לבין כל שדה שהוא.

ב. נעזר בטענה שראינו בכיתה לפיה עבור p ראשוני, $\mathbb{F}_{p^n}$ הוא תת־שדה של $\mathbb{F}_{p^m}$ אם ורק אם $n|m$. לכן הסריג הדרוש הוא



שאלה 5. יהי $p(x) = x^2 + 2x + 2$.

א. הוכיחו כי $p(x)$ אי פריק מעל $\mathbb{F}_7$.

ב. הוכיחו כי $p(x)$ פריק מעל $\mathbb{F}_5$.

ג. מצאו $q \neq 7$ ו-$q' \neq 5$ כך ש-$p(x)$ אי פריק מעל $\mathbb{F}_q$ ופריק מעל $\mathbb{F}_{q'}$. (רשות: נסו לבחור q, q' שאינם ראשוניים.)

פתרון. א. כדי להראות שפולינום מדרגה 2 הוא אי פריק, מספיק להראות שאין לו שורשים מעל $\mathbb{F}_7$. בדיקה עבור $\{0,\dots,6\}$ תראה כי

$$p(0)=2,\quad p(1)=5,\quad p(2)=3,\quad p(3)=3,\quad p(4)=5,\quad p(5)=2,\quad p(6)=1$$

ולכן $p(x)$ אי פריק מעל $\mathbb{F}_7$.

ב. עבור $\mathbb{F}_5$ אפשר למצוא בעזרת חישוב ישיר את השורשים $1,2$. לכן

$$p(x)=(x-2)(x-1)$$

ג. אם p פריק מעל $\mathbb{F}_5$, אז הוא ישר פריק מעל כל הרחבה של $\mathbb{F}_5$, כמו למשל $\mathbb{F}_{25}$. אפשר גם לראות שעבור שדות ממאפיין 2 מתקיים $p(x)=x\cdot x$, ולכן בחירת $q'=2^k$ לכל $k\in\mathbb{N}$ תתאים.
אפשר לבדוק ישירות שאין ל-$p(x)$ שורשים מעל $\mathbb{F}_3$ (וגם מעל $\mathbb{F}_{11}$), ולכן הוא אי פריק שם. באופן יותר כללי נשים לב שאם המאפיין שונה מ-2, אז $x=0$ אינו שורש של $p(x)$. כמו כן אם $x^2+2x+2=0$, אזי $(x+1)^2=-1$. בחבורה הכפלית $\mathbb{F}_q$ נבדוק מתי קיים שורש y של -1. כלומר $y^2=-1$, ולכן $y^4=1$. באילו שדות יש איבר מסדר 4 בחבורה הכפלית? יש לדרוש ש-$\left|\mathbb{F}_q^*\right|=q-1$ זה קורה כאשר $q\equiv 1 \pmod 4$, ולמשל עבור $q=7$ או $q=27$ זה לא נכון, ולכן שם $p(x)$ אי פריק.

בהצלחה!