

אלגברה מופשטת 3 – תרגיל 8 – פתרון

בכל השאלות החישוביות עליכם להצדיק את תשובתכם (כלומר, להוכיח שזו התשובה). תשובה ללא הצדקה לא תזכה בנקודות.

שאלה 1

נסמן ב- \mathbb{F}_q את השדה הסופי בגודל q .

1. בנו באופן מפורש את \mathbb{F}_{32} .
2. כמה גורמים אי פריקים יש ל- $x^{64} - x$ מעל \mathbb{F}_2 ? (אין צורך למצוא את הגורמים)
3. כמה גורמים אי פריקים יש ל- $x^{64} - x$ מעל \mathbb{F}_4 ? (אין צורך למצוא את הגורמים)

פיתרון

סעיף 1: נמצא פולינום ממעלה 5 מעל \mathbb{F}_2 . הפולינומים $x, x+1, x^2+x+1$ הם הפולינומים היחידים ממעלה 2 או פחות מעל \mathbb{F}_2 (בדקו!). נגדיר $f(x) = x^2(x+1)(x^2+x+1) + 1 = x^5 + x^2 + 1$ (אזי $x^2(x^3+1) + 1 = x^5 + x^2 + 1$). לא מתחלק באף אחד מהפולינומים $x, x+1, x^2+x+1$ ולכן אי פריק (אחרת הוא היה צריך להתחלק בראשוני ממעלה 2 או פחות). מכאן נובע ש- $E = \mathbb{F}_2[x]/\langle x^5 + x^2 + 1 \rangle$ הוא שדה ממימד 5 מעל \mathbb{F}_2 ולכן $|E| = 2^{[E:\mathbb{F}_2]} = 2^5 = 32$. סיימו.

הערה: פתרונות נכונים נוספים: $\mathbb{F}_2[x]/\langle x^5 + x^4 + x^2 + x + 1 \rangle, \mathbb{F}_2[x]/\langle x^5 + x^3 + 1 \rangle, \mathbb{F}_2[x]/\langle x^5 + x^4 + x^3 + x + 1 \rangle, \mathbb{F}_2[x]/\langle x^5 + x^4 + x^3 + x^2 + 1 \rangle, \mathbb{F}_2[x]/\langle x^5 + x^3 + x^2 + x + 1 \rangle$ (למה אין עוד פתרונות?)

סעיפים 2 ו-3: נסמן ב- $n_q(k)$ את מספר הפולינומים האי פריקים ממעלה k מעל \mathbb{F}_q . לפי משפט מכפלת כל הפולינומים האי פריקים המתוקנים ממעלה שמחלקת את k היא $x^{q^k} - x$, לכן $q^k = \sum_{d|k} dn_q(d)$ ובנוסף, מספר הגורמים האי פריקים של $x^{q^k} - x$ הוא $\sum_{d|k} n_q(d)$.

מתקיים $n_2(1) = 2$ (ברור).

$$n_2(2) = \frac{2^2-2}{2} = 1 \text{ ולכן } 2^2 = n_2(1) + 2n_2(2) = 2 + 2n_2(2)$$

$$n_2(3) = \frac{2^3-2}{3} = 2 \text{ ולכן } 2^3 = n_2(1) + 3n_2(3) = 2 + 3n_2(3)$$

$$n_2(6) = \frac{2^6-2}{6} = 9 \text{ ולכן } 2^6 = n_2(1) + 2n_2(2) + 3n_2(3) + 6n_2(6) = 2 + 2 + 6 + 6n_2(6)$$

לכן, מספר הגורמים של $x^{64} - x$ מעל \mathbb{F}_2 הוא

$$n_2(1) + n_2(2) + n_2(3) + n_2(6) = 2 + 1 + 2 + 9 = 14$$

מתקיים $n_4(1) = 4$ (ברור).

$$n_4(3) = \frac{4^3-4}{3} = 20 \text{ ולכן } 2^4 = n_4(1) + 3n_4(3) = 4 + 3n_4(3)$$

לכן, מספר הגורמים של $x^{64} - x$ מעל \mathbb{F}_4 הוא $n_4(1) + n_4(3) = 4 + 20 = 24$

שאלה 2

יהי ρ_n שורש יחידה n -פרמיטיבי ויהי ψ_n הפולינום המינימלי שלו (הפולינום הציקלוטומי).

1. חשבו את $\psi_{15}, \psi_{16}, \psi_{18}$ (התשובה צריכה להיות פולינום מפורש מעל \mathbb{Q}).

2. פרקו את ψ_{18} מעל $\mathbb{Q}[\rho_3]$ באשר ρ_3 שורש יחידה 3-פרימיטיבי.

פיתרון

סעיף 1: בהרצאה הוכחנו ש- $\psi_d = x^n - 1$ ו- $\deg \psi_n = \varphi(n)$. בנוסף, הראינו גם ש- $\psi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1$ עבור כל ראשוני p .

חישוב ψ_{15} : לפי הנוסחה $\prod_{d|n} \psi_d = x^n - 1$ מתקיים

$$\psi_{15} = \frac{x^{15}-1}{\psi_5\psi_3\psi_1} = \frac{x^{15}-1}{(x^5-1)\psi_3} = \frac{x^{10}+x^5+1}{\psi_3} = \frac{x^{10}+x^5+1}{x^2+x+1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

(השווין האדום חושב בעזרת חילוק ארוך של פולינומים.)

חישוב ψ_{16} : מתקיים $x^{16} - 1 = (x^8 + 1)(x^8 - 1)$. השורשים של ψ_{16} הם שורשי יחידה 16-פרימיטיביים ולכן אף אחד מהם לא מאפס את $x^8 - 1$. לכן $\gcd(x^8 - 1, \psi_{16}) = 1$ היות ו- $\psi_{16} | x^{16} - 1$ נובע שבהכרח $\psi_{16} | x^8 + 1$. ידוע ש- $\deg \psi_{16} = \varphi(16) = 16 \left(1 - \frac{1}{2}\right) = 8$ ולכן $\psi_{16} = x^8 + 1$.

חישוב ψ_{18} : מתקיים $\deg \psi_{18} = \varphi(18) = 18 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 6$ ולכן $\psi_{18} | x^{18} - 1$. בנוסף, $x^{18} - 1 = (x^9 - 1)(x^9 + 1) = (x^9 - 1)(x^3 + 1)(x^6 - x^3 + 1)$. שורשי ψ_{18} הם שורשי יחידה 18 פרימיטיביים ולכן לא מאפסים את $x^9 - 1$ ו- $x^3 + 1$ (כי $x^3 + 1 | x^6 - 1$). לכן בהכרח $\psi_{18} | x^6 - x^3 + 1$. אבל $\deg \psi_{18} = 6$ ולכן $\psi_{18} = x^6 - x^3 + 1$.

סעיף 2: נסמן $\rho_n = \exp\left(\frac{2\pi i}{n}\right) \in \mathbb{C}$. מתקיים $\rho_6 = \rho_3 + 1 \in \mathbb{Q}[\rho_3]$ (נובע ישירות מההגדרה). אם ρ הוא שורש יחידה 18-פרימיטיבי, אז ρ^3 הוא שורש יחידה 6-פרימיטיבי. יש רק שני שורשי יחידה 6-פרימיטיביים (כי $\varphi(6) = 2$) והם ρ_6, ρ_6^5 . לכן בהכרח $\rho^3 - \rho_6 = 0$ או $\rho^3 - \rho_6^5 = 0$. זה אומר שכל שורשי הפולינום $\psi_{18}(x) = x^6 - x^3 + 1$ הם שורשים של $(x^3 - \rho_6)(x^3 - \rho_6^5)$. לכן, מעל $\mathbb{Q}[\rho_3]$ מתקיים $\psi_{18}(x) = (x^3 - \rho_6)(x^3 - \rho_6^5)$. גמרנו אם נראה ש- $x^3 - \rho_6, x^3 - \rho_6^5$ אי פריקים מעל $\mathbb{Q}[\rho_3]$.

באמת, מתקיים $3 = \frac{\varphi(18)}{\varphi(3)} = \frac{[\mathbb{Q}[\rho_{18}]:\mathbb{Q}]}{[\mathbb{Q}[\rho_3]:\mathbb{Q}]} = [\mathbb{Q}[\rho_{18}]:\mathbb{Q}[\rho_3]]$. לכן, מעלת הפולינום המינימלי של ρ_{18} מעל $\mathbb{Q}[\rho_3]$ היא 3. אבל שורש של $x^3 - \rho_6 \in \mathbb{Q}[\rho_3][x]$ ולכן הפולינום המינימלי של ρ_{18} מעל $\mathbb{Q}[\rho_3]$ הוא $x^3 - \rho_6$. בפרט, נובע ש- $x^3 - \rho_6$ אי פריק מעל $\mathbb{Q}[\rho_3]$. אותו טיעון עם ρ_{18}^{-1} במקום ρ_{18} ו- $x^3 - \rho_6^5$ במקום $x^3 - \rho_6$ יראה ש- $x^3 - \rho_6^5$ גם אי פריק מעל $\mathbb{Q}[\rho_3]$.

לסיכום, הפירוק לגורמים של ψ_{18} מעל $\mathbb{Q}[\rho_3]$ הוא $(x^3 - \rho_6)(x^3 - \rho_6^5) = (x^3 - (1 + \rho_3))(x^3 - (1 + \rho_3^{-1}))$.

שאלה 3

יהי F שדה ו- $f \in F[x]$ פולינום ספרבילי אי פריק ממעלה 5. יהי E שדה הפיצול של f מעל F ויהיו $\alpha_1, \dots, \alpha_5$ השורשים של f ב- E . נניח כי $|Gal(E/F)| = 120$.

1. חשבו את $[F[\alpha_1 + \alpha_2 + \alpha_3]:F]$. מצאו קבוצת יוצרים* של $Gal(E/F[\alpha_1 + \alpha_2 + \alpha_3])$. אילו מהשורשים $\alpha_1, \dots, \alpha_5$ נמצאים ב- $F[\alpha_1 + \alpha_2 + \alpha_3]$?

2. חשבו את $[F[\alpha_1 + \alpha_2^2]: F]$. מצאו קבוצת יוצרים* של $Gal(E/F[\alpha_1 + \alpha_2^2])$. אילו מהשורשים $\alpha_1, \dots, \alpha_5$ נמצאים ב- $F[\alpha_1 + \alpha_2^2]$?

(*) יצגו את אברי חבורת גלואה כתמורות ב- S_5 (=תמורות על השורשים $\alpha_1, \dots, \alpha_5$).

פיתרון

תהי $G = Gal(E/F)$. קיים שיכון חבורות של G ב- S_5 שנתון על ידי שליחת איבר $\sigma \in G$ לתמורה $\hat{\sigma} \in S_5$ שהוא משרה על השורשים $\alpha_1, \dots, \alpha_5$ ($\sigma \alpha_i = \alpha_{\hat{\sigma}(i)}$). נתון ש- $|S_5| = 120 = |G|$ ולכן השיכון הנ"ל הוא איזומורפיזם חבורות (כלומר, $G \cong S_5$). עבור $\pi \in S_5$ נסמן ב- $\tilde{\pi}$ את האיבר המתאים לו ב- G ($\tilde{\pi}(\alpha_i) = \alpha_{\pi(i)}$).

בנוסף, באותו אופן כמו שהוכחנו בכיתה, הקבוצה $B = \{\alpha_1^i \alpha_2^j \alpha_3^k \alpha_4^l \mid 0 \leq i < 5, 0 \leq j < 4, 0 \leq k < 3, 0 \leq l < 2\}$ היא בסיס ל- E כמרחב וקטורי מעל F . אנו נשתמש בזה כדי להראות שאיברים מסויימים ב- E שונים מאיברים אחרים.

הסבר קצר למי שפספס את השיעור: נגדיר $K_i = F[\alpha_1, \dots, \alpha_i]$ ($K_0 = F$). אזי $K_{i-1} \subseteq K_i$ ומתקיים ש- $[K_i: K_{i-1}]$ שווה למעלת הפולינום המינימלי של α_i מעל K_{i-1} שהיא לכל היותר $6 - i$ כי α_i שורש של הפולינום $\frac{f(x)}{(x-\alpha_1)\dots(x-\alpha_{i-1})} \in K_{i-1}[x]$. כלומר, $d_i := [K_i: K_{i-1}] \leq 6 - i$. אבל מתקיים $d_5 d_4 \dots d_1 = [K_5: K_4][K_4: K_3] \dots [K_1: K_0] = [K_5: K_0] = [E: F] = |G| = 120$ ולכן בהכרח $d_i = 6 - i$ כי אחרת נקבל $d_5 d_4 \dots d_1 < 120$. למעשה, $d_5 = 1$ ו- $K_4 = E$. זה אומר שהקבוצה $B_i = \{\alpha_i^j \mid 0 \leq j < 6 - i\}$ היא בסיס ל- K_i כמרחב וקטורי מעל K_{i-1} . לכן, ה"מכפלה" $B_1 B_2 B_3 B_4$ היא בסיס ל- E מעל $K_4 = E$. קל לבדוק שהקבוצה הזו שווה ל- B .

סעיף 1: $[F[\alpha_1 + \alpha_2 + \alpha_3]: F]$ שווה למספר ה"צמודים" השונים (ביחס ל- G) של $\alpha_1 + \alpha_2 + \alpha_3$. לכל $\pi \in S_5$ מתקיים $\tilde{\pi}(\alpha_1 + \alpha_2 + \alpha_3) = \alpha_{\pi(1)} + \alpha_{\pi(2)} + \alpha_{\pi(3)}$. יש 10 π ש- $\alpha_1 + \alpha_2 + \alpha_3 \neq \alpha_{\pi(1)} + \alpha_{\pi(2)} + \alpha_{\pi(3)}$ (שלושת $\{\pi(1), \pi(2), \pi(3)\}$ אפשריות ולכן ל- $\alpha_1 + \alpha_2 + \alpha_3$ לכל היותר עשרה צמודים. נוכיח שהם שונים. בלי הגבלת כלליות מספיק לבדוק רק ש- $\alpha_1 + \alpha_2 + \alpha_3 \neq \alpha_2 + \alpha_3 + \alpha_4$ ו- $\alpha_1 + \alpha_2 + \alpha_3 \neq \alpha_3 + \alpha_4 + \alpha_5$. כל שאר המקרים שקולים לאחד מאלה בגלל הסימטריה בין השורשים. באמת, $\alpha_1 + \alpha_2 + \alpha_3 \neq \alpha_2 + \alpha_3 + \alpha_4$ אם $\alpha_1 \neq \alpha_4$ וזה נכון כי f ספרבילי. $\alpha_1 + \alpha_2 + \alpha_3 \neq \alpha_3 + \alpha_4 + \alpha_5$ אם $\alpha_1 \neq \alpha_4$ וזה נכון כי בשני האגפים יש צ"ל שונים של אברי הבסיס B . לכן, ל- $\alpha_1 + \alpha_2 + \alpha_3$ עשרה צמודים שונים, כלומר $[F[\alpha_1 + \alpha_2 + \alpha_3]: F] = 10$.

תהי $\pi \in S_5$ אזי $H := Gal(E/F[\alpha_1 + \alpha_2 + \alpha_3])$ אם $\tilde{\pi}$ אם $\pi(\{1,2,3\}) = \{1,2,3\}$ אם $\alpha_{\pi(1)} + \alpha_{\pi(2)} + \alpha_{\pi(3)} = \alpha_1 + \alpha_2 + \alpha_3$ אחרת $\alpha_{\pi(1)} + \alpha_{\pi(2)} + \alpha_{\pi(3)} \neq \alpha_1 + \alpha_2 + \alpha_3$. חבורת התמורות $\pi \in S_5$ המקיימות $\pi(\{1,2,3\}) = \{1,2,3\}$ נוצרת ע"י $(1,2,3), (1,2), (4,5)$. (הסבר: החבורה היא בגודל 12 (מדוע?). $(1,2), (4,5)$ יוצרות חבורה בגודל 4 ו- $(1,2,3)$ יוצרת חבורה בגודל 3. לכן שלושת האיברים האלה יוצרים חבורה בגודל שמתחלק ב-12= $\gcd(3,4)$ לכן, החבורה $Gal(E/F[\alpha_1 + \alpha_2 + \alpha_3])$ נוצרת ע"י האוטומורפיזמים המתאימים לתמורות $(1, 2, 3), (1, 2), (4, 5)$.

$E/F[\alpha_1 + \alpha_2 + \alpha_3]$ הרחבת גלואה עם חבורה H ולכן, לפי משפט $E^H = F[\alpha_1 + \alpha_2 + \alpha_3]$. לכן, $\alpha_i \in H$ אם $\sigma \in H$ מתקיים $\sigma \alpha_i = \alpha_i$. מתקיים $\alpha_1 \in H$, $(1,2)\alpha_2 = \alpha_1$, $(1,2)\alpha_3 = \alpha_1$, $(4,5)\alpha_4 = \alpha_5$, $(4,5)\alpha_5 = \alpha_4$ ולכן לכל $1 \leq i \leq 5$ קיים $\sigma \in H$ כך ש- $\sigma \alpha_i \neq \alpha_i$. לכן, אף לא אחד מהשורשים $\alpha_1, \dots, \alpha_5$ נמצא ב- $F[\alpha_1 + \alpha_2 + \alpha_3]$.

הערה: לסעיף 1 יש "קיצור דרך" אם שמים לב ש- $F[\alpha_1 + \alpha_2 + \alpha_3] = F[\alpha_4 + \alpha_5]$ מפני ש- $\alpha_1 + \dots + \alpha_5 \in F$.

סעיף 2: $[F[\alpha_1 + \alpha_2^2]: F]$ שווה למספר ה"צמודים" השונים (ביחס ל- G) של $\alpha_1 + \alpha_2^2$. לכל $\pi \in S_5$ מתקיים $\tilde{\pi}(\alpha_1 + \alpha_2^2) = \alpha_{\pi(1)} + \alpha_{\pi(2)}^2$. יש $4 \cdot 5 = 20$ זוגות סדורים מהצורה $(\pi(1), \pi(2))$ ולכן ל- $\alpha_1 + \alpha_2^2$ לכל היותר 20 צמודים. נוכיח שהם שונים. בלי הגבלת כלליות מספיק לבדוק רק את המקרים הבאים:

1. $\alpha_1 + \alpha_2^2 \neq \alpha_4 + \alpha_3^2$. זה נכון כי אלו שני צירופים לינאריים שונים של אברי הבסיס B .
2. $\alpha_1 + \alpha_2^2 \neq \alpha_1 + \alpha_3^2$. זה נכון כי אלו שני צירופים לינאריים שונים של אברי הבסיס B .
3. $\alpha_1 + \alpha_2^2 \neq \alpha_3 + \alpha_2^2$. זה נכון כי אלו שני צירופים לינאריים שונים של אברי הבסיס B .
4. $\alpha_1 + \alpha_2^2 \neq \alpha_3 + \alpha_1^2$. זה נכון כי אלו שני צירופים לינאריים שונים של אברי הבסיס B .
5. $\alpha_1 + \alpha_2^2 \neq \alpha_2 + \alpha_1^2$. זה נכון כי אלו שני צירופים לינאריים שונים של אברי הבסיס B .

כל שאר המקרים שקולים לאחד מאלה בגלל הסימטריה בין השורשים. לכן, ל- $\alpha_1 + \alpha_2^2$ 20 צמודים שונים, כלומר $[F[\alpha_1 + \alpha_2^2]: F] = 20$.

תהי $\pi \in S_5$, אזי $H := Gal(E/F[\alpha_1 + \alpha_2^2]) \in H$ אם"ם $\alpha_{\pi(1)} + \alpha_{\pi(2)}^2 = \alpha_1 + \alpha_2^2$ (אחרת $\pi(1) = 1, \pi(2) = 2$ אם"ם $\alpha_{\pi(1)} + \alpha_{\pi(2)}^2 = \alpha_1 + \alpha_2^2$). חבורת התמורות המקיימות זאת נוצרת ע"י $(3,4), (3,4,5)$. לכן H נוצרת ע"י $(3,4), (\overline{3,4,5})$.

$E^H = F[\alpha_1 + \alpha_2^2]$ לפי משפט $\alpha_i \in H$, לכן, $\sigma \alpha_i = \alpha_i$ מתקיים $\sigma \in \{(\overline{3,4}), (\overline{3,4,5})\}$ (מספיק לבדוק על קבוצת יוצרים של H !).

מתקיים $(\overline{3,4,5})\alpha_2 = \alpha_2, (\overline{3,4})\alpha_2 = \alpha_2, (\overline{3,4,5})\alpha_1 = \alpha_1, (\overline{3,4})\alpha_1 = \alpha_1$ מצד שני, $F[\alpha_1 + \alpha_2^2]$ $\alpha_3, \alpha_4, \alpha_5 \notin F[\alpha_1 + \alpha_2^2]$ ולכן $(\overline{3,4,5})\alpha_3 = \alpha_3, (\overline{3,4,5})\alpha_4 = \alpha_5, (\overline{3,4,5})\alpha_5 = \alpha_4$.