

## פתרון תרגיל בית 10 בשדות ותורת גלואה 88-311 סמסטר א' תשע"ט

**שאלה 1.** מצאו כמה פולינומים מתוקנים אי פריקים יש ממעלה 4 מעל  $\mathbb{F}_3$ .

פתרון. מכפלת הפולינומים האי פריקים ממעלה שמחלקת את 4, לפי טענה מהכיתה, היא

$$x^{3^4} - x = \Pi_1 \Pi_2 \Pi_4$$

כאשר  $\Pi_i$  היא מכפלת כל הפולינומים המתוקנים האי פריקים ממעלה  $i$ . את  $\Pi_1 = x^3 - x$  קל לפרק, והפולינומים ממעלה 1 הם  $x, x-1, x-2$ . כלומר יש 3 כאלו. מכפלת הפולינומים ממעלה שמחלקת את 2 היא  $\Pi_2 = x^2 - x$ , ולכן  $\Pi_2$  היא ממעלה  $3^2 - 3^1 = 6$ . כלומר יש  $\frac{6}{2} = 3$  פולינומים אי פריקים ממעלה 2. באותו אופן, המעלה של  $\Pi_4$  היא  $72 = 3^4 - 3 \cdot 2 - 3 \cdot 1 = 72$  (למעשה במקרה זה קצת יותר מהיר לחשב  $3^4 - 3^2 = 72$ ). לכן יש  $\frac{72}{4} = 18$  פולינומים מתוקנים אי פריקים ממעלה 4.

**שאלה 2.** הזכרנו שהנורמה כפלית והעקבה חיבורית (זה נובע מכך שאיברי חבורת גלואה הם הומומורפיזמים של חוגים). כעת תוכיחו שהן גם טרנזיטיביות. תהי  $F \subseteq L \subseteq K$  שרשרת שדות כך שכל ההרחבות הן גלואה. הוכיחו

$$N_{K/F} = N_{L/F} \circ N_{K/L} \quad \text{Tr}_{K/F} = \text{Tr}_{L/F} \circ \text{Tr}_{K/L}$$

פתרון. נסמן  $G = \text{Gal}(K/F)$  ו- $H = \text{Gal}(K/L)$ . מכיוון שלפי ההנחה גם  $K/F$  גלואה, אז לפי התאמת גלואה  $\text{Gal}(L/F) \cong G/H$ . כעת, לכל  $x \in K$  מתקיים

$$\begin{aligned} N_{L/F} N_{K/L}(x) &= N_{L/F} \left( \prod_{\sigma \in H} \sigma(x) \right) = \prod_{\sigma \in H} \sigma(N_{L/F}(x)) \\ &= \prod_{\sigma \in H} \sigma \left( \prod_{\tau \in G/H} \tau(x) \right) = \prod_{g \in G} g(x) = N_{K/F}(x) \end{aligned}$$

ובאופן דומה (סכום במקום מכפלה) עבור העקבה. זה יותר מסובך להוכיח את הטרנזיטיביות של הנורמה כאשר ההרחבה אינה גלואה.

**שאלה 3.** יהי  $K = \mathbb{Q}[\sqrt[3]{5}]$ .

א. שכנו את השדה  $K$  בחוג  $\text{End}_{\mathbb{Q}}(K) \cong M_3(\mathbb{Q})$  לפי הזיהוי שראינו.

ב. מצאו את הנורמה והעקבה של כל איבר  $\alpha = a + b\sqrt[3]{5} + c\sqrt[3]{25} \in K$ .

ג. הוכיחו כי  $\sqrt[3]{3} \notin K$ . רמז: מצאו עקבות.

פתרון. איך פותרים את שני הסעיפים הראשונים עם מערכת התוכנה המתמטית SageMath:

```

sage: K.<theta> = NumberField(x^3-5)
sage: OK = K.ring_of_integers()
sage: R.<a,b,c> = OK[]
sage: A = [m.matrix() for m in OK.basis()]
sage: A
[
[1 0 0] [0 1 0] [0 0 1]
[0 1 0] [0 0 1] [5 0 0]
[0 0 1], [5 0 0], [0 5 0]
]
sage: M = a*A[0] + b*A[1] + c*A[2]
sage: M
[ a  b  c]
[5*c a  b]
[5*b 5*c a]
sage: M.trace()
3*a
sage: M.det()
a^3 + 5*b^3 - 15*a*b*c + 25*c^3

```

א. נבחר בסיס  $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$  של  $K$  מעל  $\mathbb{Q}$ . למעשה צריך לראות לאן כפל משמאל באיבר כללי  $\alpha = a + b\sqrt[3]{5} + c\sqrt[3]{25} \in K$  שולח כל אחד מאיברי הבסיס

$$\begin{aligned} \alpha \cdot 1 &= a + b\sqrt[3]{5} + c\sqrt[3]{25} \\ \alpha \cdot \sqrt[3]{5} &= 5c + a\sqrt[3]{5} + b\sqrt[3]{25} \\ \alpha \cdot \sqrt[3]{25} &= 5b + 5c\sqrt[3]{5} + a\sqrt[3]{25} \end{aligned}$$

ולכן השיכון (בבחירה הזו של הבסיס) ישלח את  $\alpha$  למטריצה (או לשיחלוף)

$$\begin{pmatrix} a & b & c \\ 5c & a & b \\ 5b & 5c & a \end{pmatrix} \in M_3(\mathbb{Q})$$

ב. העקבה  $\text{Tr}_{K/\mathbb{Q}}(\alpha)$  היא העקבה של המטריצה בשיכון מהסעיף הקודם, שהיא  $3a$ . הנורמה  $N_{K/\mathbb{Q}}(\alpha)$  היא הדטרמיננטה של המטריצה הזו, והיא  $a^3 + 5b^3 - 15abc + 25c^3$ .

ג. ניסיון ראשון לפתרון הבעיה יהיה להניח בשלילה כי  $\sqrt[3]{3} = a + b\sqrt[3]{5} + c\sqrt[3]{25}$  עבור  $a, b, c \in \mathbb{Q}$ , להעלות את המשוואה בשלישית ולהתחיל להשוות מקדמים. החישובים יוצאים נוראיים ומסובכים להכללה.

דרך יותר מוצלחת היא להעזר ברמז ובלינאריות של העקבה. שוב נניח בשלילה כי

$$\sqrt[3]{3} = a + b\sqrt[3]{5} + c\sqrt[3]{25} \in K \quad (1)$$

מפני שהפולינום המינימלי של  $\sqrt[3]{3}$  הוא ממעלה 3, אז בהכרח  $K = \mathbb{Q}[\sqrt[3]{3}]$ . מכאן נוכל למצוא שני בסיסים שונים של  $K$  מעל  $\mathbb{Q}$ : הראשון הוא  $\{1, \sqrt[3]{5}, \sqrt[3]{25}\}$  כמו בסעיפים הקודמים, והשני הוא  $\{1, \sqrt[3]{3}, \sqrt[3]{9}\}$ . לפי הבסיס הראשון, העקבות של  $\sqrt[3]{5}$

ו- $\sqrt[3]{25}$  לפי הבסיס הראשון הן

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{5}) &= \mathrm{Tr} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 5 & 0 & 0 \end{pmatrix} = 0 \\ \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{25}) &= \mathrm{Tr} \begin{pmatrix} 0 & 0 & 1 \\ 5 & 0 & 0 \\ 0 & 5 & 0 \end{pmatrix} = 0\end{aligned}$$

ומחישוב דומה  $\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{3}) = 0$  לפי הבסיס השני. על משוואה (1) נפעיל את  $\mathrm{Tr}_{K/\mathbb{Q}}$  ונקבל

$$\begin{aligned}\sqrt[3]{3} &= a + b\sqrt[3]{5} + c\sqrt[3]{25} \\ \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{3}) &= \mathrm{Tr}_{K/\mathbb{Q}}(a + b\sqrt[3]{5} + c\sqrt[3]{25}) \\ &= a \mathrm{Tr}_{K/\mathbb{Q}}(1) + b \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{5}) + c \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{25}) \\ &= 3a\end{aligned}$$

כלומר  $a = 0$ . נכפיל את משוואה (1) ב- $\sqrt[3]{5}$  ונקבל

$$\sqrt[3]{3}\sqrt[3]{5} = \sqrt[3]{15} = a\sqrt[3]{5} + b\sqrt[3]{25} + 5c$$

גם למספר  $\sqrt[3]{15} \in K$  יש פולינום מינימלי ממעלה 3. בסיס שלישי  $\{1, \sqrt[3]{15}, \sqrt[3]{225}\}$  של  $K$  מעל  $\mathbb{Q}$  יעזור לחשב ש- $\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{15}) = 0$  ונסיק כמו מקודם כי  $15c = 0$ , כלומר  $c = 0$ . נציב חזרה במשוואה (1) ונקבל  $\sqrt[3]{3} = b\sqrt[3]{5}$ . כלומר  $\frac{3}{5} = b^3$ , אבל אז בוודאי ש- $b$  אינו רציונלי. זו סתירה, ולכן  $\sqrt[3]{3} \notin K$ .

**שאלה 4.** יהי  $\alpha \in \mathbb{F}_{p^n}$ . חשבו את  $\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha)$  ואת  $N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha)$ .

פתרון. החבורה  $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$  היא ציקלית ונוצרת על ידי אוטומורפיזם פרובניוס. כלומר האוטומורפיזמים הם העלאת  $\alpha$  בחזקת  $p^i$  עבור  $0 \leq i < n$ . לכן

$$\mathrm{Tr}_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{n-1}}$$

וגם

$$N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(\alpha) = \alpha \alpha^p \dots \alpha^{p^{n-1}} = \alpha^{(p^n-1)/(p-1)}$$

**שאלה 5.** יהי  $f(x) \in \mathbb{F}_3[x]$  פולינום אי פריק ממעלה 3 ויהי  $a$  שורש שלו (בשדה הפיצול). הוכיחו כי  $a^{13} \in \mathbb{F}_3$ .

פתרון. שדה הפיצול של  $f(x)$  הוא השדה  $\mathbb{F}_{3^3} = \mathbb{F}_{27}$ . האיברים ההפכים בשדה זה הם חבורה מסדר 26. בנוסף  $a$  הפיך (אחרת  $a = 0 \in \mathbb{F}_3$  ויש לפולינום שורש ב- $\mathbb{F}_3$ , סתירה) לפי משפט לגראנז'  $a^{26} = 1$  ולכן

$$a^{13} = \pm 1 \in \mathbb{F}_3$$

כי מעל שדה לפולינום  $x^2 = 1$  יש לכל היותר 2 שורשים. פתרון אחר, ויותר "אלגנטי", ישתמש בחישוב הנורמה מהשאלה הקודמת, שתמיד שייכת לשדה הבסיס:

$$N_{\mathbb{F}_{p^n}/\mathbb{F}_p}(a) = a^{(3^3-1)/(3-1)} = a^{13} \in \mathbb{F}_3$$

**שאלה 6** (רשות). יהי  $n > 1$  טבעי, ונתבונן בפולינום הציקלוטומי  $\Phi_n(x)$ .

א. יהי  $a \in \mathbb{Z}$  ויהי  $p$  ראשוני המחלק את  $\Phi_n(a)$ . הוכיחו כי  $p|n$  או  $p \equiv 1 \pmod{n}$ .  
 רמז: הפולינום  $x^n - 1$  הוא ספרבילי מודולו  $p$  אם  $p \nmid n$ . מה הוא הסדר של  $a \in U_p$ ?

ב. הסיקו מהסעיף הקודם שישנם אינסוף מספרים ראשוניים כך ש- $p \equiv 1 \pmod{n}$ .

פתרון.

א. נניח כי  $p \nmid n$ . אז לנגזרת  $(x^n - 1)' = nx^{n-1}$  אין גורם משותף עם  $x^n - 1$  מודולו  $p$ . לכן  $x^n - 1 = \prod_{d|n} \Phi_d(x)$  נזכר בנוסחה ב- $\mathbb{F}_p[x]$ . נזכר בנוסחה  $x^n - 1 = \prod_{d|n} \Phi_d(x)$  ונציב בה  $a$ :

$$a^n - 1 = \prod_{d|n} \Phi_d(a) = \Phi_n(a) \cdot \prod_{d|n, d < n} \Phi_d(a) \equiv 0 \pmod{p}$$

אבל כל השורשים של  $x^n - 1$  שונים, ולכן  $\Phi_n(a) = 0$  בשדה  $\mathbb{F}_p$ . כלומר  $p \nmid \Phi_n(a)$  לכל  $d|n$  כאשר  $d < n$ . כלומר  $a$  הוא שורש יחידה פרימיטיבי מסדר  $n$  ב- $\mathbb{F}_p$ . לכן  $o(a) = n|p - 1$ , כדרוש.

ב. מספיק להראות ש- $\Phi_n(a)$  הוא ראשוני אינסוף פעמים כאשר  $a$  שלם (לאו דווקא כל פעם). נניח בשלילה שזה לא נכון, ויש רק מספר סופי  $k$  של ראשוניים כאלו  $p_1, \dots, p_k$ . אז לכל  $m \in \mathbb{Z}$  מתקיים כי

$$\gcd(\Phi_n(mp_1 \dots p_k), p_1 \dots p_k) = 1$$

כי  $\Phi_n(mp_1 \dots p_k)$  מחלק את  $(mp_1 \dots p_k)^n - 1$ . לכן למספר  $\Phi_n(mp_1 \dots p_k)$  יש גורם ראשוני שאינו בקבוצה  $\{p_1, \dots, p_k\}$ , כל עוד  $|\Phi_n(mp_1 \dots p_k)| > 1$ . אבל  $\Phi_n(mp_1 \dots p_k)$  הוא פולינום ב- $m$ , ולכן אפשר לבחור  $m \in \mathbb{Z}$  כך שמתקיים תנאי זה.

בקורס תורת המספרים האלגבריים אולי תראו הכללה (או יותר) של סעיף זה לפיו יש אינסוף ראשוניים מן הצורה  $b + kn$  כאשר  $b$  זר ל- $n$ .

**שאלה 7** (רשות). יהי  $n$  טבעי. בשאלה זו נראה הכללה לשאלות 6 ו-7 מתרגיל בית 9 שתאפשר לחשב את הפולינום הציקלוטומי  $\Phi_n(x)$  קצת יותר מהר.

א. יהי  $p$  ראשוני. הוכיחו שאם  $p$  זר ל- $n$ , אז  $\Phi_n(x^p) = \Phi_n(x) \Phi_{pn}(x)$ . אחרת, אם  $p|n$ , הוכיחו כי  $\Phi_{pn}(x) = \Phi_n(x^p)$ .

ב. יהי  $r$  הרדיקל של  $n$  (כלומר מכפלת הראשוניים שמחלקים את  $n$ ). הוכיחו שהפולינום הציקלוטומי מקיים  $\Phi_n(x) = \Phi_r(x^{n/r})$ .

בהצלחה!