

פתרון תרגיל בית 2 בשדות ותורת גלואה 88-311 סמסטר א' תש"ף

שאלה 1. יהיו $f(x) = x^2 - 3x + 3, g(x) = x^3 + 2x + 5 \in \mathbb{Q}[x]$ תזכורת: אלגוריתם אוקלידס המורחב עובד בתחומים אוקלידיים כמו $F[x]$.

א. מצאו את $\gcd(f(x), g(x))$.

ב. מצאו את ההופכי של $g(x)$ בשדה $\mathbb{Q}[x]/\langle f(x) \rangle$.

פתרון.

א. נעזר בתזכורת, ונשתמש באלגוריתם אוקלידס עם הערות לחישוב בסוגריים מרובעים:

$$\begin{aligned} \gcd(g(x), f(x)) &= [x^3 + 2x + 5 = (x + 3)(x^2 - 3x + 3) + 8x - 4] \\ \gcd(f(x), 8x - 4) &= \left[x^2 - 3x + 3 = \left(\frac{1}{8}x - \frac{5}{16}\right)(8x - 4) + \frac{7}{4} \right] \\ \gcd(8x - 4, \frac{7}{4}) &= \left[8x - 4 = \left(\frac{32}{7}x - \frac{16}{7}\right) \cdot \frac{7}{4} + 0 \right] \\ \gcd\left(\frac{7}{4}, 0\right) &= 1 \end{aligned}$$

כלומר הפולינומים זרים (שימו לב ש-1 וגם $\frac{7}{4}$ הפיכים ב- $\mathbb{Q}[x]$).

ב. צריך להשתמש באלגוריתם אוקלידס המורחב ולבחור את מקדם בזו המתאים. נחשב את המקדמים

$$\begin{aligned} 8x - 4 &= 1 \cdot (x^3 + 2x + 5) - (x + 3)(x^2 - 3x + 3) \\ \frac{7}{4} &= 1 \cdot (x^2 - 3x + 3) - \left(\frac{1}{8}x - \frac{5}{16}\right)(8x - 4) \\ &= 1 \cdot (x^2 - 3x + 3) - \left(\frac{1}{8}x - \frac{5}{16}\right)(1 \cdot (x^3 + 2x + 5) - (x + 3)(x^2 - 3x + 3)) \\ &= \left(\frac{1}{8}x^2 + \frac{1}{16}x + \frac{1}{16}\right)(x^2 - 3x + 3) + \left(-\frac{1}{8}x + \frac{5}{16}\right)(x^3 + 2x + 5) \end{aligned}$$

נכפיל ב- $\frac{4}{7}$ את המשוואה האחרונה, ונקבל

$$\gcd(f(x), g(x)) = 1 = \left(\frac{1}{14}x^2 + \frac{1}{28}x + \frac{1}{28}\right)f(x) + \left(-\frac{1}{14}x + \frac{5}{28}\right)g(x)$$

ולכן האיבר ההופכי הוא $\left(-\frac{1}{14}x + \frac{5}{28}\right) + \langle f(x) \rangle$.

שאלה 2. תהי K/F הרחבת שדות. נתבונן בחוג הפולינומים $K[x]$ ובשדה הפונקציות הרציונליות $F(x)$, ונחשוב על שניהם כתת-קבוצות של השדה $K(x)$ באופן הברור. הוכיחו $F(x) \cap K[x] = F[x]$.

פתרון. הוכחת ההכלה (\supseteq) קלה כי כל פולינום מעל F הוא פולינום מעל K וגם פונקציה רציונלית מעל F .

להכלה (\subseteq) נשים לב שלפונקציה רציונלית מעל F (ששייכת ל- $K(x)$) שהיא גם פולינום מעל K יש מכנה 1 ומונה שהוא פולינום מעל F , כלומר פולינום מעל F שנמצא ב- $K(x)$.

שאלה 3. תהי K/F הרחבת שדות. יהי $f(x) \in F[x]$ פולינום מדרגה $n \geq 1$. הוכיחו או הפריכו את הטענות הבאות:

א. אם a איבר אלגברי מעל K אז הוא אלגברי מעל F .

ב. אם a איבר אלגברי מעל F אז הוא אלגברי מעל K .

ג. אם a איבר אלגברי מעל F אז גם $\alpha \cdot a$ הוא אלגברי לכל $\alpha \in F$.

פתרון.

א. הפרכה: π הוא אלגברי מעל $K = \mathbb{R}$ כי הוא מאפס את הפולינום $x - \pi$, אבל הוא לא אלגברי מעל \mathbb{Q} . דוגמה אחרת, שאולי היא יותר פשוטה, זה ש- x אלגברי מעל $\mathbb{C}(x)$, אבל לא מעל \mathbb{C} .

ב. הוכחה: a אלגברי מעל F ולכן יש פולינום $p(x) \in F[x]$ כך ש- $p(a) = 0$. אבל $F \subseteq K$ ולכן $p(x) \in K[x]$. כלומר שיש פולינום מעל K שמתאפס ב- a ולכן a אלגברי מעל K .

ג. הוכחה: a אלגברי ולכן יש $p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in F[x]$ כך ש- $p(a) = 0$ אז

$$0 = p(a) = \frac{1}{\alpha^n}(\alpha a)^n + a_{n-1} \frac{1}{\alpha^{n-1}}(\alpha a)^{n-1} + \dots + a_1 \frac{1}{\alpha}(\alpha a) + a_0$$

שהרי $\alpha^{-i} \cdot (\alpha a)^i = a^i$. נשים לב ש- $a_i \frac{1}{\alpha^i} \in F$ לכל i, j . לכן

$$q(x) = \frac{1}{\alpha^n}x^n + \frac{a_{n-1}}{\alpha^{n-1}}x^{n-1} + \dots + \frac{a_1}{\alpha}x + a_0$$

הוא פולינום מעל F שמתאפס ב- αa .

שאלה 4. תהי K/F הרחבה סופית (כלומר $[K:F] < \infty$). הוכיחו כי כל איבר של K הוא אלגברי מעל F . רמז: חשבו על הקבוצה $\{1, a, a^2, a^3, \dots\}$. רשות: להרחבה כמו בשאלה קוראים הרחבה אלגברית. האם כל הרחבה אלגברית היא סופית?

פתרון. יהי $a \in K$. מכיוון שדרגת ההרחבה סופית, הקבוצה $\{1, a, a^2, \dots\}$ חייבת להיות תלויה לינארית מעל F . כלומר יש צירוף לינארי לא טריוויאלי של החזקות שמתאפס:

$$b_n a^n + b_{n-1} a^{n-1} + \dots + b_0 = 0$$

ולכן $b_n x^n + \dots + b_0 \in F[x]$ הוא פולינום שמתאפס ב- a . כלומר a אלגברי מעל F , כדרוש.

שאלה 5. הוכיחו כי $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

פתרון. ברור כי $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ ולכן $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \supseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. מצד שני

$$(\sqrt{2} + \sqrt{3})^2 = 2 + 2\sqrt{2}\sqrt{3} + 3 = 2\sqrt{6} + 5$$

ולכן $\sqrt{6} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. בנוסף $2\sqrt{3} + 3\sqrt{2} = \sqrt{6}(\sqrt{2} + \sqrt{3})$ ולכן

$$2\sqrt{3} + 3\sqrt{2} - 2(\sqrt{2} + \sqrt{3}) = \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

ובוודאי

$$\sqrt{3} = \sqrt{2} + \sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$$

ולכן $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$, כנדרש. הזכרו שאם α אלגברי מעל F , אז $F[\alpha] = F(\alpha)$, ולכן הסתפקנו "רק" בהוכחת $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$.

שאלה 6. יהי F שדה, ותהי $G \leq F^*$ תת-חבורה סופית של החבורה הכפלית של השדה. הוכיחו כי G ציקלית. הדרכה: העזרו בתורת המבנה של חבורות אבליות סופיות ובחישוב $\exp(G)$.

פתרון. לפי משפט המבנה של חבורות אבליות סופיות, ניתן להציג את G כמכפלה

$$G \cong \left(\mathbb{Z}/p_1^{k_1}\mathbb{Z}\right) \times \left(\mathbb{Z}/p_2^{k_2}\mathbb{Z}\right) \times \dots \times \left(\mathbb{Z}/p_t^{k_t}\mathbb{Z}\right)$$

כאשר p_1, \dots, p_t ראשוניים כלשהם (אולי שווים) ו- $k_1, \dots, k_t \in \mathbb{N}$. נסמן

$$m = \text{lcm}(p_1^{k_1}, p_2^{k_2}, \dots, p_t^{k_t})$$

וכידוע לנו מתורת החבורות $\exp(G) = m$ ולכן $m \leq |G|$. כלומר $x^m = e_G$ לכל $x \in G$. אבל לפולינום $x^m - 1$ ישנם לכל היותר m פתרונות בשדה F . כלומר $|G| \leq m$, וקיבלנו $|G| = m$. לכן בהכרח $p_i \neq p_j$ לכל $i \neq j$, שכן אחרת

$$m = \text{lcm}(p_1^{k_1}, p_2^{k_2}, \dots, p_t^{k_t}) < p_1^{k_1} p_2^{k_2} \dots p_t^{k_t} = |G|$$

וקיבלנו ש- G היא מכפלה ישרה של חבורות ציקליות מסדרים זרים בזוגות. לפי משפט השאריות הסיני נסיק שהיא ציקלית מסדר $p_1^{k_1} p_2^{k_2} \dots p_t^{k_t}$.

בהצלחה!