

פתרון תרגיל בית 1 תורת גלואה - תשע"ח

1. הוכיחו שכל תת־שדה של \mathbb{C} מכיל את \mathbb{Q} .

פתרון:

יהי K תת־שדה של \mathbb{C} . בהכרח $1 \in K$.

מכיוון ש- K שדה הוא סגור לחיבור וחסור ולכן $n = 1 + 1 + \dots + 1 \in K$ וגם

$-\mathbb{Z} \subseteq K$ כלומר ש- $-n = -1 - 1 - \dots - 1 \in K$

K סגור לכפל והופכי ולכן $\frac{m}{n} = n \cdot m^{-1} \in K$ מה שאומר ש- $\mathbb{Q} \subseteq K$.

2. יהי $f(x) \in F[x]$ פולינום מדרגה n . הוכיחו כי הקבוצה $\{\bar{1}, \bar{x}, \dots, \bar{x}^{n-1}\}$ היא

בסיס של המנה $F[x]/\langle f(x) \rangle$ (כמרחב וקטורי מעל F).

פתרון:

בת"ל: נניח כי $\alpha_0 \bar{1} + \alpha_1 \bar{x} + \dots + \alpha_{n-1} \bar{x}^{n-1} = \bar{0}$ זה אומר ש- $\alpha_0 + \dots + \alpha_{n-1} x^{n-1}$

$\bar{0}$ כלומר ש- $\alpha_0 + \dots + \alpha_{n-1} x^{n-1} \in \langle f(x) \rangle$.

זה אומר ש- $f(x) \mid \alpha_0 + \dots + \alpha_{n-1} x^{n-1}$ אבל זה לא ייתכן כי $\deg(f(x)) = n >$

$n-1$. ולכן בהכרח זהו פולינום האפס (כלומר ש- $\alpha_i = 0$) ולכן הקבוצה בת"ל.

פורשת: מכיוון שכל הפולינומים נפרשים ע"י $\{x^i\}$, ברור שהמנה נפרשת ע"י $\{\bar{x}^i\}$.

כעת, לכל $i \geq n$ נרשום $x^i = x^{kn} x$

3. הציגו את

$$x^4 - x^3 + x - 2 \in \mathbb{Q}[x]/\langle x^3 - x^2 - 1 \rangle$$

כצירוף לינארי של אברי הבסיס $\{\bar{1}, \bar{x}, \bar{x}^2\}$.

פתרון:

נשתמש ביחס $\bar{x}^3 = \bar{x}^2 + 1 \Leftarrow \bar{x}^3 - \bar{x}^2 - 1 = \bar{0}$

$$\overline{x^4 - x^3 + x - 2} = \overline{x(x^2 + 1) - (x^2 - 1) + x - 2} = \overline{x^3 - x^2 + 2x - 1} = \overline{2x}$$

4. בנו שדה ממאפיין 3 ומגודל 9.

פתרון:

נקח את

$$\mathbb{Z}_3[x]/\langle x^2-2 \rangle$$

ל- $x^2 - 2$ אין שורש ב- \mathbb{Z}_3 והוא מדרגה 2 ולכן הוא אי-פריק והמנה היא שדה. המימד של השדה הוא $\deg(x^2 - 2) = 2$ ולכן גודל השדה ההוא $|\mathbb{Z}_3|^2 = 9$.

5. קבע האם הפולינומים הבאים פריקים או אי-פריקים מעל השדה הנתון, מצאו את הפירוק במידה וקיים.

() $x^6 + 26x + 52$ מעל \mathbb{Q} .

אי-פריק לפי אייזנשטיין בעזרת הראשוני 13.

() $x^4 + 6x^2 + 3x - 12$ מעל \mathbb{Q} .

אי-פריק לפי אייזנשטיין בעזרת הראשוני 3.

() $x^6 - 1$ מעל \mathbb{Q} .

נשתמש בפירוק $x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$.

זהו פירוק לגורמים אי-פריקים: $(x-1)$ ו- $(x+1)$ לינאריים ולכן ודאי אי-פריקים. ושאר הגורמים הם ריבועיים וללא שורשים רציונליים ולכן אי-פריקים.

() $x^6 - 1$ מעל \mathbb{R} (מה קורה מעל \mathbb{C} ?)

אותו פירוק כמו סעיף קודם. הגורמים עדיין אי-פריקים.

מעל \mathbb{C} יש פירוק מלא לגורמים לינאריים $x^6 - 1 = \prod (x - \rho_6^i)$ כאשר ρ_6 הוא שורש יחידה 6-פרימיטיבי.

() $x^6 - 1$ מעל \mathbb{Z}_3 .

מעל \mathbb{Z}_3 : $x^6 - 1 = (x^2 - 1)^3 = (x - 1)^3(x + 1)^3$.

() $x^3 - 6x - 9$ מעל \mathbb{Z}_5 .

מודולו 5 נקבל ש $x^3 - 6x - 9 \equiv x^3 - x + 1$. קל בדוק שאין לו שורשים ב- \mathbb{Z}_5 ומכיוון והפוינום מדרגה 3 נסיק שהוא אי-פריק.

() $x^3 - 6x - 9$ מעל \mathbb{Q} .

מכיוון שברדוקציה מודולו 5 הדרגה נשארת 3 ומקבלים פולינום אי-פריק, נסיק שהפולינום אי-פריק מעל \mathbb{Q} .

6. הראו שאין פולינום מדרגה $1 < p$ מעל \mathbb{Z} שהוא אי-פריק מודולו p לכל מספר ראשוני p .

פתרון:

יהי $p(x)$ פולינום מדרגה $1 < p$. נחפש מספר ראשוני p כך שיש ל- $p(x)$ שורש ב- \mathbb{Z}_p .

מכיוון שמדובר בפולינום לא קבוע, אפשר למצוא מספר שלם כלשהו a , עבורו הערך של הפולינום $p(a)$ מתחלק באיזשהו ראשוני p .
אזי $p(a) \equiv 0 \pmod{p}$ כלומר a הוא שורש של $p(x)$ מודולו p ולכן הפולינום פריק מעל \mathbb{Z}_p .