

מופשטת 3 תשע"ה - פתרון תרגיל 6

1. יהי $K = \mathbb{Q}[\sqrt[5]{4}]$. הראו ש $Gal(K/\mathbb{Q}) = \{id_K\}$.

פתרון:

$\sqrt[5]{4}$ הוא שורש של הפולינום $x^5 - 4 \in \mathbb{Q}[x]$, ולכן כל \mathbb{Q} -אוטומורפיזם מעביר את $\sqrt[5]{4}$ לשורש של הפולינום. אבל השורש היחיד של הפולינום ב K הוא רק $\sqrt[5]{4}$. ולכן בהכרח כל $\sigma \in Gal(K/\mathbb{Q})$ מקיים $\sigma(\sqrt[5]{4}) = \sqrt[5]{4}$ מה שאומר ש- $\sigma = id_K$.

2. בנו באופן מפורש את \mathbb{F}_{32} . כמה פולינומים אי-פריקים מדרגה 4 יש מעל שדה זה? (אין צורך לפרט אותם).

פתרון:

$32 = 2^5$ ולכן צריך פולינום אי-פריק מדרגה 5 מעל \mathbb{Z}_2 . קל לבדוק (ע"י הצבת 0 ו-1) שהפולינומים האי-פריקים היחידים מדרגות 1,2 הם: $x, x+1, x^2+x+1$. נקח מתחלק ע"י אף פולינום מדרגה 1 או 2 ולכן הוא אי-פריק (כי אם הוא פריק הוא חייב להתפצל לפול' מדרגה 2 ו-1 או 4 - כלומר שהוא מתחלק ע"י איזשהו פולינום מדרגה 1 או 2). אם כן, $\mathbb{Z}_2[x]/\langle f \rangle$ הוא שדה מהגודל הדרוש.

נתבונן בפולינום $x^{32^4} - x$, הוא שווה למכפלת כל הפולינומים האי-פריקים מדרגה המחלקת את 4, דהיינו מדרגות 1,2,4. מכפלת כל הפולינומים האי-פריקים מדרגה 1 ו-2 היא $x^{32^2} - x$ שזה מדרגה 32^2 , ולכן נקבל שמכפלת כל הפולינומים האי-פריקים מדרגה 4 בדיוק היא $(x^{32^4} - x)/(x^{32^2} - x)$ שזה מדרגה $32^4 - 32^2$. ולכן מספר הפולינומים האי-פריקים מדרגה 4 הוא $\frac{32^4 - 32^2}{4}$.

3. כמה גורמים אי-פריקים יש לפולינום $x^{64} - x$ מעל \mathbb{F}_2 ? וכמה מעל \mathbb{F}_4 ?

פתרון:

מעל \mathbb{F}_2 : הפולינום $x^{64} - x = x^{2^6} - x$ הוא מכפלת כל הפולינומים האי-פריקים מדרגה המחלקת את 6, דהיינו מדרגות 1,2,3,6. נסמן ב n_d את כמות הפולינומים האי-פריקים מדרגה d . אזי $64 = n_1 + 2n_2 + 3n_3 + 4n_4$. נחשב את n_1 : הפולינומים הם $x, x+1$. כלומר ש $n_1 = 2$. נחשב את n_2 : מכפלת כל הפולינומים האי-פריקים מסדר 2,1 היא $x^2 - x$ כלומר ש $n_2 = 1$ מה שנותן $4 = n_1 + 2n_2$. נחשב את n_3 : מכפלת כל הפולינומים האי-פריקים מסדר 3,1 היא $x^3 - x$ כלומר ש $n_3 = 2$ מה שנותן $8 = n_1 + 3n_3$. נחשב את n_6 : מכפלת כל הפולינומים האי-פריקים מסדר 2,1,6 היא $x^6 - x$ כלומר ש $n_6 = 9$ מה שנותן $16 = n_1 + 2n_2 + 6n_6$. סך הכל, כמות הגורמים האי-פריקים היא $n_1 + n_2 + n_3 + n_6 = 14$.

מעל \mathbb{F}_4 : הפולינום $x^{64} - x = x^{4^3} - x$ הוא מכפלת כל הפולינומים האי-פריקים מדרגות 1, 3. נסמן n_d כמו קודם ונחשב.
 $n_1 = 4$: כי הפולינומים הם $x, x+1, x+2, x+3$.
נחשב את n_3 : מכפלת כל הפולינומים האי-פריקים מדרגות 1, 3 היא $x^{4^3} - x$ ולכן
 $4^3 = n_1 + 3n_3 = 20$ מה שנותן $n_3 = 20$.
סך הכל, כמות הגורמים האי-פריקים היא $n_1 + n_3 = 24$.

4. נסמן φ_n את הפולינום הציקלוטומי של שורש היחידה ה- n הפרימיטיבי.

(א) חשבו את $\varphi_{15}, \varphi_{16}, \varphi_{18}$.

פתרון:

זכור $x^n - 1 = \prod_{d|n} \varphi_d$. ועבור p ראשוני $x^p - 1 = (x-1)\varphi_p$.

נחשב את φ_{15} : אנחנו יודעים $x^{15} - 1 = \varphi_1 \varphi_3 \varphi_5 \varphi_{15}$ ולכן $\varphi_{15} = \frac{x^{15} - 1}{(x-1)(x^2+x+1)(x^4-x^2+1)}$

$\frac{x^{15} - 1}{(x^5 - 1)(x^2 + x + 1)} = \frac{x^{10} + x^5 + 1}{x^2 + x + 1} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$
(השוויון האחרון הוא חילוק ארוך, השוויון שלפניו הוא לפי הנוסחה של חזקה שלישית).

נחשב את φ_{16} : אנחנו יודעים ש $x^{16} - 1 = \varphi_1 \varphi_2 \varphi_4 \varphi_8 \varphi_{16}$

וכן ש $x^8 - 1 = \varphi_1 \varphi_2 \varphi_4 \varphi_8$ ולכן $\varphi_{16} = \frac{x^{16} - 1}{x^8 - 1} = x^8 + 1$. דרך אחרת: לפרק

את $x^{16} - 1 = (x^8 + 1)(x^8 - 1)$, מכיוון ששורשי היחידה ה-16 פרימיטיביים לא מאפסים את $x^8 - 1$, נשאר ש $\varphi_{16} | (x^8 + 1)$ ומכיוון ו- $\deg(\varphi_{16}) = \varphi(16) = 8$ נקבל ש $\varphi_{16} = x^8 + 1$.

נחשב את φ_{18} : אנחנו יודעים ש-

$x^{18} - 1 = (x^9 - 1)(x^9 + 1) = (x^9 - 1)(x^3 - 1)(x^6 - x^3 + 1)$ שורשי היחידה הפרימיטיביים מסדר 18 הם לא שורשים של $(x^9 - 1), (x^3 - 1)$ ולכן $\varphi_{18} | (x^6 - x^3 + 1)$. ומכיוון ו- $\deg(\varphi_{18}) = \varphi(18) = 6$ אז $\varphi_{18} = x^6 - x^3 + 1$.

(ב) איך φ_{18} מתפרק מעל $\mathbb{Q}[\rho_3]$?

פתרון:

נחשב $[\mathbb{Q}[\rho_{18}, \rho_3] : \mathbb{Q}[\rho_3]] = [\mathbb{Q}[\rho_{18}] : \mathbb{Q}[\rho_3]] = \frac{[\mathbb{Q}[\rho_{18}] : \mathbb{Q}]}{[\mathbb{Q}[\rho_3] : \mathbb{Q}]} = \frac{\varphi(18)}{\varphi(3)} = \frac{6}{2} = 3$

זה אומר שכל שורש של φ_{18} (כלומר של שורש יחידה 18 - פרימיטיבי) יש לו פולינום מינימלי מדרגה 3 מעל $\mathbb{Q}[\rho_3]$. הפולינומים המינימליים האלה מחלקים את φ_{18} מעל $\mathbb{Q}[\rho_3]$.

ננסה לחשב את הפולינומים המינימליים האלה: נקח $\rho_6 = \rho_3 + 1 \in \mathbb{Q}[\rho_3]$ נשימו לב שהוא שורש פרימיטיבי. יש רק 2 שורשים - 6 פרימיטיביים (לפי $\varphi(6) = 2$) והם ρ_6 ו- ρ_6^5 . אם ρ הוא שורש יחידה 18 - פרימיטיבי אז ρ^3 הוא שורש 6 - פרימיטיבי ולכן $\rho^3 = \rho_6$ או $\rho^3 = \rho_6^5$. במקרה הראשון ρ הוא שורש של הפולינום $x^3 - \rho_6$, ובמקרה השני הוא שורש של הפולינום $x^3 - \rho_6^5$. אלו פולינומים אי פריקים כי הם מדרגה 3 (וחישובנו למעלה שהדרגה של הפולינום המינימלי היא 3). סך הכל נקבל ש $\varphi_{18} = (x^3 - \rho_6^5)(x^3 - \rho_6)$.