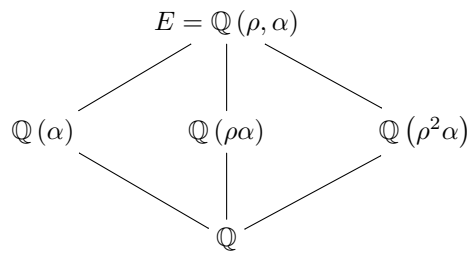


חזרה

נחזור לסוף התרגיל מפעם קודמת: $f(x) = x^3 - 2$

$$\alpha = \sqrt[3]{2} \quad \rho = \rho_3 = \text{cis} \frac{2\pi}{3}$$



$$\text{Gal}(E/\mathbb{Q}) = S_3$$

$$\Phi_2(x) = x^2 + x + 1$$

$$E = \mathbb{Q}(\alpha)(\rho)$$

ρ, ρ^2 הם השורשים של Φ_2 . יש לנו כמה אוטומורפיזמים שמחליף בין ρ ל- ρ^2 :

• $\sigma_1 : \rho \leftrightarrow \rho^2$ קובע את $\mathbb{Q}(\alpha)$.

• $\sigma_2 : \rho \leftrightarrow \rho^2$ קובע את $\mathbb{Q}(\rho\alpha)$.

• $\sigma_3 : \rho \leftrightarrow \rho^2$ קובע את $\mathbb{Q}(\rho^2\alpha)$.

נשים לב שכולם מחליפים בין ρ ל- ρ^2 - אבל הם אוטומורפיזמים שונים! יש שלושה אוטומורפיזמים מסדר 2, והם יוצרים את כל S_3 .

מדלגים על משפט הסולם

משפט

כל שדות הפיצול של פולינום $f(x) \in F[x]$ איזומורפיים מעל F .

נסמן: E/F שדה פיצול של $f(x) \in F[x]$ פולינום אי-פריק.

משפט

$\text{Gal}(E/F)$ פועלת טרנזיטיבית על שורשי $f(x)$.

הגדרה

$f(x) \in F[x]$ ספרבילי אם כל שורשים שונים בשדה פיצול E/F .

משפט

$|\text{Gal}(E:F)| \leq [E:F]$ ויש שוויון אם E שדה פיצול של פולינום ספרבילי.

משפט

אם E/F שדה פיצול של $f(x) \in F[x]$ ספרבילי אי-פריק מדרגה n , אזי $n \mid |\text{Gal}(E/F)|$.

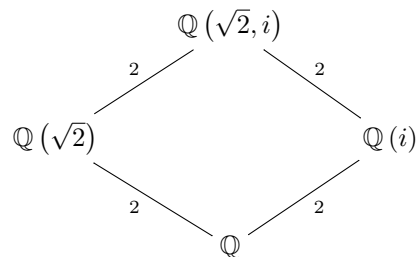
תרגיל

האם שדות הפיצול של $x^4 - 4$, $x^4 + 4$ איזומורפיים?

פתרון

$$f(x) = x^4 - 4 = (x^2 + 2)(x^2 - 2)$$

השורשים הם $\pm\sqrt{2}, \pm i\sqrt{2}$.
שדה הפיצול של f מעל \mathbb{Q} הוא $E_1 = \mathbb{Q}(\sqrt{2}, i)$
מהי $\text{Gal}(E_1/\mathbb{Q})$ מסדר 4?



קיים אוטומורפיזם $\sigma_1 : i \leftrightarrow -i$ שקובע את $\mathbb{Q}(\sqrt{2})$, ואוטומורפיזם $\sigma_2 : \sqrt{2} \leftrightarrow -\sqrt{2}$ שקובע את $\mathbb{Q}(i)$.
אלה 2 אוטומורפיזמים שונים מסדר 2 ולכן החבורה היא בהכרח $\mathbb{Z}_2 \times \mathbb{Z}_2$ (כי ב \mathbb{Z}_4 אין 2 איברים מסדר 2)

$$g(x) = x^4 + 4 = (x^2 + 2i)(x^2 - 2i)$$

$$\pm\sqrt{2i}, \pm i\sqrt{2i}$$

$$\sqrt{2i} = 1 + i$$

כלומר השורשים הם: $\pm(1+i), \pm(i-1)$. שדה הפיצול הוא $E_2 = \mathbb{Q}(i)/\mathbb{Q}$.

תרגיל

הראו שכל שדה עם p^n איברים הוא שדה פיצול של $f(x) = x^{p^n} - x$ מעל \mathbb{Z}_p .

פתרון

נסמן ב- K את השדה.
ב- K^* יש $p^n - 1$ איברים. לכל $a \in K^*$ מתקיים $a^{p^n - 1} = 1$ לכל $a \in K$ מתקיים $a^{p^n} = a$.
לכן כל $a \in K$ הוא שורש של $f \iff f$ מתפרק לגורמים לינאריים (מתפצל) מעל K כי f מדרגה p^n .
ברור ש- K הוא השדה הכי קטן בו זה מתקיים, כי יש בו את כל השורשים ודבר מלבדם.

מסקנה

כל השדות עם p^n איברים הם איזומורפיים.

משפט

$(p(x), p'(x)) = 1 \iff p(x) \in F[x]$ הוא ספרבילי.

טענה

אם $p(x)$ אי-פריק וגם $p'(x) \neq 0$ אזי $p(x)$ ספרבילי.

דוגמה

קיים פולינום אי-פריק ואי-ספרבילי

פתרון

נבנה דוגמה של פולינום מעל $\mathbb{Z}_2[t]$ $\mathbb{Z}_2(t) = \text{Frac}(\mathbb{Z}_2[t])$

$$f(x) \in \mathbb{Z}_2(t)[x]$$

$$f(x) = x^2 - t$$

השורשים $\pm\sqrt{t}$, אבל במאפיין 2 $+\sqrt{t} = -\sqrt{t}$, ולכן $f(x) = (x - \sqrt{t})^2$.
הראינו ש- f אי-ספרבילי. כדי להראות ש- f אי פריק מספיק להראות שאין לו שורש ב- $\mathbb{Z}_2(t)$

$$\left(\frac{a(t)}{b(t)}\right)^2 = t$$

$$a(t)^2 = tb(t)^2$$

אבל ל- $tb(t)^2$ דרגה אי זוגית ול- $a(t)^2$ וזו סתירה.

הגדרה

שדה נקרא משוכלל (perfect) אם כל פולינום אי-פריק מעל השדה הוא ספרבילי.

משפט

1. כל שדה סופי הוא משוכלל.
2. כל שדה ממאפיין 0 הוא משוכלל.

הוכחה של 1

יהי $f(x)$ פולינום אי-פריק מעל שדה סופי.

$$K = F[x]/\langle f(x) \rangle$$

הוא שדה המכיל שורש של f . K הוא שדה עם p^n איברים (כי K הרחבה אלגברית של שדה סופי F). לכן k הוא שדה פיצול של $g(x) = x^{p^n} - x$ לפי תרגיל קודם. ל f ול g יש שורש משותף (כי שורשי g הם כל אברי השדה K) $\iff f \mid g$ מעל F (כי f מחלק כל פולינום שמאפס את α).
 $g(x)$ ספרבילי $\iff f(x)$ ספרבילי.

תרגיל

f פולינום אי-פריק, E/\mathbb{Q} שדה הפיצול.
הראו שאם ${}^1\text{Gal}(E/\mathbb{Q}) = Q_8$ אזי $\deg f \geq 0$.

Q_8^1 היא חבורת הקוורטריונים