אלגברה מופשטת 3 - תרגיל 6 - פתרון

1. הראו שאם $E \supseteq B \supseteq F$ שדות כך ש E/F היא הרחבת גלואה, אזי E/B היא הרחבת גלואה.
פתרון: E/F הוא שדה פיצול של פולינום ספרבילי $f(x) \in F[x]$.
אם כך $f(x) \in B[x]$ והוא עדיין ספרבילי. נשאר להוכיח רק ש E הוא שדה הפיצול של הפולינום מעל B, אבל זה ברור, כי אם $E' \subset E$ הוא שדה מפצל קטן יותר של $f(x) \in B[x]$, אזי הוא גם מפצל את $f(x) \in F[x]$ בסתירה לכך ש E הוא שדה הפיצול.
2. הראו שאם $\rho_n \in E - F$ שורש יחידה n-י פרימיטיבי, אזי לכל $\sigma \in Gal(E/F)$ מתקיים ש $\sigma(\rho_n)$ הוא שורש יחידה פרימיטיבי (תזכורת: שורש יחידה n-י נקרא פרימיטיבי אם הוא יוצר את חבורת שורשי היחידה ה n-ים).
פתרון: נסמן את חבורת שרשי היחידה ה n-ים ב Ω_n. החבורה הזאת היא חבורה ציקלית מסדר המחלק את n. אם $\sigma \in Gal(E/F)$ אזי $\sigma|_{\Omega_n} : \Omega_n \to \Omega_n$ הוא אוטומורפיזם חבורות, ויוצר של חבורה ציקלית חייב לעבור ליוצר, כלומר שורש פרימיטיבי עובר לשורש פרימיטיבי.
3. תהי E/F הרחבת גלואה, ויהיו B,C שדות ביניים (כלומר $E \supseteq B,C \supseteq F$). הראו שמתקיים:
א. $Gal(E/B) \vee Gal(E/C) = Gal(E/B \cap C)$
ב. $Gal(E/B) \cap Gal(E/C) = Gal(E/B \vee C)$

פתרון:

א. מתקיים $Gal(E/B), Gal(E/C) \subseteq Gal(E/B \cap C)$, כיוון שאם σ קובע את B אזי בוודאי שהוא קובע את $B \cap C$, ואותו דבר עבור C, ולכן $Gal(E/B) \vee Gal(E/C) \subseteq Gal(E/B \cap C)$.
בכיוון השני, הת"ח $H = Gal(E/B) \vee Gal(E/C)$ מתאימה לתת-שדה E^H כלומר $Gal(E/E^H) = H$ (לפי משפט עבור הרחבות גלואה). מתקיים $E^H \subseteq B,\ E^H \subseteq C$ כיוון שאברי E^H קבועים תחת האוטומורפיזמים ב $Gal(E/B), Gal(E/C)$ (משתמשים כאן במשפט היסודי של תורת גלואה, כי $H \geq Gal(E/B) \Leftrightarrow E^H \subseteq E^{Gal(E/B)}$). לכן בהכרח $E^H \subseteq B \cap C$. אבל אז בהכרח מתקיים $H = Gal(E/E^H) \supseteq Gal(E/B \cap C)$, כנדרש.

ב. מתקיים $B = F[b_1,...,b_k], C = F[c_1,...,c_m]$ אזי $B \vee C = F[b_1,...,b_k,c_1,...,c_m]$.
אם $\sigma \in Gal(E/B) \cap Gal(E/C)$ אזי $\sigma|B = id, \sigma|C = id$ ולכן בהכרח $\sigma(b_i) = b_i,\ \sigma(c_j) = \sigma(c_j)$ לכל $1 \leq i \leq k, 1 \leq j \leq m$, ולכן $\sigma|B \vee C = id$, כלומר $\sigma \in Gal(E/B \vee C)$. אם $\sigma \in Gal(E/B \vee C)$ אזי ברור ש σ קובע את B,C ולכן $\sigma \in Gal(E/B) \cap Gal(E/C)$.

4.

א. הראו שכל הרחבה מדרגה 2 של שדה ממאפיין שונה מ 2 היא הרחבת גלואה.
פתרון: נסמן את ההרחבה E/F. מתקיים $E = F(a)$ לכל איבר $a \in E - F$: כי $2 = [E:F] = [E:F(a)][F(a):F]$, וגם $[F(a):F] > 1$.

הפולינום המינימלי $m_a \in F[x]$ של a הוא מדרגה 2, וגם E מכיל שורש שלו <= E מכיל את שני השורשים שלו <= E שדה פיצול של m_a. נשאר להראות שהפולינום m_a הוא ספרבילי. אבל אם $m_a(x)=x^2+cx+d$ אזי $m_a'(x)=2x+c$ וזה פולינום שונה מאפס במאפיין שונה מ 2. ראינו שפולינום אי-פריק שנגזרתו שונה מ 0 הוא ספרבילי.

ב. הראו ש"יחס הרחבת גלואה" אינו טרנזיטיבי; כלומר אם $E/B, B/F$ אזי לא בהכרח מתקיים E/F היא הרחבת גלואה (יש להראות דוגמא נגדית).

פתרון:

ניקח $f(x)=x^4-2\in\mathbb{Q}[x]$. מתקיים $\mathbb{Q}(\sqrt[4]{2})=\mathbb{Q}(\sqrt[2]{2})(\sqrt[4]{2})$. מתקיים $[\mathbb{Q}(\sqrt[2]{2}):\mathbb{Q}]=2,\ [\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}(\sqrt[2]{2})]=2$ לכן שתי ההרחבות $\mathbb{Q}(\sqrt[2]{2})/\mathbb{Q},\ \mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt[2]{2})$ הן הרחבות גלואה.

לפי משפט אנחנו יודעים ש E/F היא הרחבת גלואה אם ורק אם לכל איבר $a\in E$, הפולינום המינימלי של a מעל F מתפצל מעל E.

ההרחבה $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ אינה הרחבת גלואה, כי היא אינה מפצלת את הפולינום $f(x)=x^4-2$.

5. מצאו את חבורת גלואה של x^4+1 מעל $\mathbb{Q}[\sqrt{2}]$ והציגו את פעולת החבורה על השורשים כתמורות.

פתרון:

השורשים של x^4+1 ב-$\mathbb{C}$ הם $\rho_8,\rho_8^3,\rho_8^5,\rho_8^7$ באשר $\rho_8=\exp\left(\frac{\pi i}{4}\right)$. נמספר אותם ב-1,2,3,4 בהתאמה. שדה הפיצול מעל $\mathbb{Q}[\sqrt{2}]$ הוא $E:=\mathbb{Q}[\sqrt{2}][\rho_8,\rho_8^3,\rho_8^5,\rho_8^7]=\mathbb{Q}[\sqrt{2}][\rho_8]$. היות ו-$\rho_8=\frac{1+i}{\sqrt{2}}$, מתקיים $E=\mathbb{Q}[\sqrt{2},i]$. $i\notin\mathbb{Q}[\sqrt{2}]$ כי הוא מרוכב ולכן $\left[E:\mathbb{Q}[\sqrt{2}]\right]>1$. מצד שני, i שורש של x^2+1 ולכן $\left[E:\mathbb{Q}[\sqrt{2}]\right]\leq 2$. לכן בהכרח $\left[E:\mathbb{Q}[\sqrt{2}]\right]=2$ והפולינום המינימלי של i מעל $\mathbb{Q}[\sqrt{2}]$ הוא x^2+1. זה אומר ש-$\mathbb{Q}[\sqrt{2}]$-הומומורפיזם יכול לשלוח את i רק ל-$\pm i$. לפי שאלה 2 סעיף 2 אכן קיימים איברים שעושים זאת ב-$Gal(E/\mathbb{Q}[\sqrt{2}])$ ולכן חבורת גלואה היא:

ייצוג ע"י תמורה	ייצוג ע"י יוצרים	שם
	$i\mapsto i$	id_E
(1,4)(2,3)*	$i\mapsto -i$	σ

* שימו לב ש-$\rho_8^7=\frac{1-i}{\sqrt{2}}=\frac{1+\sigma(i)}{\sqrt{2}}=\sigma\left(\frac{1+i}{\sqrt{2}}\right)=\sigma(\rho_8)$.

6. יהי $f(x)=x^4-10x^2+1\in\mathbb{Q}[x]$.

א. הראו ש $f(x)$ הוא פולינום מינימלי של $\sqrt{2}+\sqrt{3}$ בעזרת חבורת גלואה $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$.

פתרון: $\sqrt{2}+\sqrt{3}$ הוא שורש של $f(x)$ (בדקו). בנוסף $\sqrt{2}+\sqrt{3}\in\mathbb{Q}(\sqrt{2},\sqrt{3})$, וגם $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ היא הרחבת גלואה, ולכן הפולינום המינימלי של $\sqrt{2}+\sqrt{3}$ מתפצל מעל

$\mathbb{Q}(\sqrt{2},\sqrt{3})$. האוטומורפיזמים של $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ נקבעים ע"י פעולתם על $\sqrt{2},\sqrt{3}$ כלומר $\sqrt{2} \mapsto \pm\sqrt{2},\sqrt{3} \mapsto \pm\sqrt{3}$. התמונות של $\sqrt{2}+\sqrt{3}$ תחת האוטומורפיזמים האלה הן $\sqrt{2}+\sqrt{3}.\sqrt{2}-\sqrt{3},-\sqrt{2}+\sqrt{3},-\sqrt{2}-\sqrt{3}$ והן כולן שורשים של $m_{\sqrt{2}+\sqrt{3}}(x)$. יש ארבעה שורשים שונים, ולכן הפולינום המינימלי של $\sqrt{2}+\sqrt{3}$ בעל 4 שורשים, כלומר הוא מדרגה 4. לכן בהכרח $m_{\sqrt{2}+\sqrt{3}}(x) = f(x)$.

ב. הציגו את פעולת חבורת גלואה על השורשים של $f(x)$ כתת-חבורה של של S_4.

פתרון: $r_1 = \sqrt{2}+\sqrt{3}, r_2 = \sqrt{2}-\sqrt{3}, r_3 = -\sqrt{2}+\sqrt{3}, r_4 = -\sqrt{2}-\sqrt{3}$.

$id: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$ פועל כתמורת הזהות על השורשים.

$\sigma: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$ פועל כתמורה $(13)(24)$ על אינדקסי השורשים.

$\tau: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}$ פועל כתמורה $(12)(24)$.

$\theta: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}$ פועל כתמורה $(14)(23)$.

זוהי חבורת קליין $V \subseteq S_4$.

ג. הראו של $f(x), g(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$ יש את אותו שדה פיצול ואותה חבורת גלואה, אך חבורת הגלואה פועלת שונה על שורשיהם.

פתרון: ברור ש $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ הוא שדה הפיצול של שניהם. השורשים של $g(x)$ הם $r_1 = \sqrt{2}, r_2 = -\sqrt{2}, r_3 = \sqrt{3}, r_4 = -\sqrt{3}$.

$id: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$ פועל כתמורת הזהות על השורשים.

$\sigma: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$ פועל כתמורה (12) על אינדקסי השורשים.

$\tau: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}$ פועל כתמורה (34).

$\theta: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3}$ פועל כתמורה $(12)(34)$.

החבורה פועלת טרנזיטיבית על שרשי הפולינום $f(x)$, אבל אינה פועלת טרנזיטיבית על שרשי $g(x)$.