פתרון תרגיל בית 8 בשדות ותורת גלואה
88-311 סמסטר א' תשפ"ב

שאלה 1. תהינה K/F ו-E/K הרחבות שדות.

א. הוכיחו או הפריכו: אם E/F הרחבה נורמלית, אז E/K הרחבה נורמלית.

ב. הוכיחו או הפריכו: אם E/F הרחבה נורמלית, אז K/F הרחבה נורמלית.

ג. הוכיחו או הפריכו: אם K/F הרחבה נורמלית ו-E/K הרחבה נורמלית, אז E/F הרחבה נורמלית. רמז: ראינו משהו בתרגילי הבית הקודמים.

פתרון.

א. הוכחה: במקרה כזה E הוא שדה פיצול. לכל $a \in E$ הפולינום המינימלי שלו $m_{a,F}$ מעל F מתפצל ב-E. הפולינום המינימלי $m_{a,K}$ שלו מעל K מחלק את $m_{a,F}$, ולכן גם מתפצל ב-E.

ב. הפרכה: ניקח $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$ ו-$E = \mathbb{Q}(\sqrt[3]{2}, \rho_3)$ כאשר ρ_3 שורש יחידה פרימיטיבי מסדר 3. ההרחבה E/F היא נורמלית כפי שראינו בכיתה, כי היא שדה הפיצול של הפולינום $x^3 - 2$. אבל ההרחבה K/F לא נורמלית. הפולינום המינימלי של $\sqrt[3]{2}$ הוא $x^3 - 2$ (אי פריק לפי אייזנשטיין). לפולינום זה יש שורשים מרוכבים שאינם ב-K ולכן ההרחבה לא נורמלית. אגב, ההרחבה E/K נורמלית כי היא מממד 2.

ג. הפרכה: ניקח $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$ ו-$E = \mathbb{Q}(\sqrt[4]{2})$. שתי ההרחבות K/F ו E/K הן נורמליות כי לפי הסעיף הקודם הן מממד 2. אבל ההרחבה E/F לא נורמלית. הפולינום המינימלי של $\sqrt[4]{2}$ הוא $x^4 - 2$ (אי פריק לפי אייזנשטיין). לפולינום זה יש שורשים מרוכבים שאינם ב-E ולכן ההרחבה לא נורמלית.

שאלה 2. תנו דוגמה להרחבת גלואה $E/\mathbb{Q}$ כך ש-$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

פתרון. נבחר $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. זהו שדה פיצול של $(x^2-2)(x^2-3)(x^2-5)$ ולכן זו הרחבת גלואה. קל לראות שהממד הוא 8 ולכן החבורה בגודל המתאים. בנוסף, כל איבר φ בחבורת גלואה חייב לקיים

$$\varphi(\sqrt{2}) = \pm\sqrt{2}, \qquad \varphi(\sqrt{3}) = \pm\sqrt{3}, \qquad \varphi(\sqrt{5}) = \pm\sqrt{5}$$

כלומר כל האיברים מסדר 1 או 2. חבורה זו חייבת להיות החבורה המבוקשת.

שאלה 3. היעזרו בתרגיל שפתרנו בתרגול לגבי חישוב פולינומים מינימליים לחישוב הפולינומים הבאים:

א. הפולינום המינימלי של $2\sqrt{2} + 3\sqrt{3} + \sqrt{6}$ מעל $\mathbb{Q}$.

ב. הפולינום המינימלי של $\rho_5 + \rho_5^4$ מעל $\mathbb{Q}$, כש-ρ_5 הוא שורש יחידה פרימיטיבי מסדר 5.

פתרון. נזכיר את התרגיל: נניח ש-E/F הרחבת גלואה, ויהי $a \in E$. נגדיר

$$\operatorname{orb}(a) = \{\sigma(a) \mid \sigma \in \operatorname{Gal}(E/F)\}\ .$$

אז הפולינום המינימלי של a הינו

$$f_a(x) = \prod_{b \in \operatorname{orb}(a)} (x-b)\ .$$

א. במקרה הזה נבחר את ההרחבה להיות $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$. נזכור כי חבורת גלואה שלה היא $\operatorname{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, ונסמן את איבריה $\{\mathrm{id}, \sigma, \tau, \sigma\tau\}$ כאשר

$$\begin{aligned} \sigma(\sqrt{2}) &= -\sqrt{2}, \qquad & \sigma(\sqrt{3}) &= \sqrt{3} \\ \tau(\sqrt{2}) &= \sqrt{2}, \qquad & \tau(\sqrt{3}) &= -\sqrt{3} \end{aligned}$$

נמצא את המסלול של האיבר הנתון $a = 2\sqrt{2} + 3\sqrt{3} + \sqrt{6}$:

$$\begin{aligned} \mathrm{id}(a) &= 2\sqrt{2} + 3\sqrt{3} + \sqrt{6} \\ \sigma(a) &= -2\sqrt{2} + 3\sqrt{3} - \sqrt{6} \\ \tau(a) &= 2\sqrt{2} - 3\sqrt{3} - \sqrt{6} \\ \sigma\tau(a) &= -2\sqrt{2} - 3\sqrt{3} + \sqrt{6} \end{aligned}$$

שהם כולם שונים (כי $\left\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\right\}$ בסיס של $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ כמרחב וקטורי. לכן הפולינום המינימלי של a מעל $\mathbb{Q}$ הוא

$$\begin{aligned} f_a(x) &= (x-a)\,(x-\sigma(a))\,(x-\tau(a))\,(x-\sigma\tau(a)) = \\ &= \left(x^2 - 6\sqrt{3}x + 13 - 8\sqrt{3}\right)\left(x^2 + 6\sqrt{3}x + 13 + 8\sqrt{3}\right) = \\ &= x^4 - 82x^2 - 288x - 23 \end{aligned}$$

ב. במקרה הזה נבחר את ההרחבה להיות $\mathbb{Q}(\rho_5)/\mathbb{Q}$. חבורת גלואה היא ציקלית ואיזומורפית ל-$\mathbb{Z}/4\mathbb{Z}$, כשיוצר שלה σ נתון על ידי

$$\sigma(\rho_5) = \rho_5^2\ .$$

נחשב את המסלול של $a = \rho_5 + \rho_5^4$:

$$\begin{aligned} \mathrm{id}(a) &= \rho_5 + \rho_5^4 \\ \sigma(a) &= \rho_5^2 + \rho_5^3 \\ \sigma^2(a) &= \rho_5^4 + \rho_5 = a \\ \sigma^3(a) &= \rho_5^3 + \rho_5^2 = \sigma(a) \end{aligned}$$

לכן הפולינום המינימלי של a מעל $\mathbb{Q}$ הוא

$$\begin{aligned} f_a(x) &= (x - (\rho_5 + \rho_5^4))(x - (\rho_5^2 + \rho_5^3)) = \\ &= x^2 - (\rho_5 + \rho_5^2 + \rho_5^3 + \rho_5^4)x + \rho_5^3 + \rho_5^4 + \rho_5 + \rho_5^2 \end{aligned}$$

נזכור כי $\sum_{i=0}^{4} \rho_5^i = 0$, ונקבל

$$f_a(x) = x^2 + x - 1\ .$$

הערה. אם $\rho_5 = e^{\frac{2\pi i}{5}}$, אז $\rho_5 + \rho_5^4 = 2\cos\frac{2\pi}{5}$; אפשר לפתור את המשוואה הריבועית של הפולינום המינימלי על ידי נוסחת שורשים, ולקבל

$$x_{1,2} = \frac{-1 \pm \sqrt{5}}{2}.$$

כיוון ש-$2\cos\frac{2\pi}{5} > 0$ צריך לבחור את הפתרון החיובי, ולכן

$$\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}.$$

שאלה 4. יהי $0 < a \in \mathbb{Q}$ כך ש-$\sqrt{a} \notin \mathbb{Q}$. נסמן $K = \mathbb{Q}(\sqrt[4]{a}, i)$.

א. הוכיחו כי $K/\mathbb{Q}$ היא הרחבת גלואה.

ב. הוכיחו כי $\mathrm{Gal}(K/\mathbb{Q}) \cong D_4$.

פתרון.

א. K הוא שדה הפיצול של הפולינום $f(x) = x^4 - a$, שהוא ספרבילי מעל $\mathbb{Q}$ כי המאפיין הוא 0.

ב. ראשית נטען כי $[K : \mathbb{Q}] = 8$. אכן, מכפליות המימד

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt[4]{a})] \cdot [\mathbb{Q}(\sqrt[4]{a}) : \mathbb{Q}].$$

כיוון ש-$K = \mathbb{Q}(\sqrt[4]{a})(i)$ ו-$i \notin \mathbb{Q}(\sqrt[4]{a})$, בהכרח $[K : \mathbb{Q}(\sqrt[4]{a})] = 2$.
לחישוב $[\mathbb{Q}(\sqrt[4]{a}) : \mathbb{Q}]$, נטען כי f אי-פריק מעל $\mathbb{Q}$. אכן, מההנחה אין ל-f שורשים ב-$\mathbb{Q}$, ולכן הפירוק היחיד האפשרי הוא למכפלה של שני גורמים ריבועיים. הפירוק של f מעל $\mathbb{C}$ הוא

$$f(x) = (x - \sqrt[4]{a})(x - i\sqrt[4]{a})(x + \sqrt[4]{a})(x + i\sqrt[4]{a})$$

ואפשר לוודא שמכפלת כל שני גורמים בפירוק היא לא פולינום מעל $\mathbb{Q}$ (כי $\sqrt{a} \notin \mathbb{Q}$).
זה מראה ש-f אי-פריק מעל $\mathbb{Q}$, כלומר הוא הפולינום המינימלי של a, ולכן נקבל כי $[\mathbb{Q}(\sqrt[4]{a}) : \mathbb{Q}] = \deg f = 4$.
בסך הכל הוכחנו עד כה כי $[K : F] = 8$.
כעת נחשב את חבורת גלואה. אפשר לחשב במפורש את כל האיברים שלה, כפי שראינו בתרגול. אפשר גם לחשב אותה בצורה יותר פשוטה. ראשית, כיוון ש-$K/\mathbb{Q}$ הרחבת גלואה, $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 8$.
כל אוטומורפיזם $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ מוגדר לפי התמונות $\sigma(\sqrt[4]{a})$ ו-$\sigma(i)$. לפי תכונות שראינו בתרגול, $\sigma(i)$ חייב להיות מתוך $\pm i$ ו-$\sigma(\sqrt[4]{a})$ חייב להיות מהצורה $\sqrt[4]{a} \cdot i^a$ לאיזשהו $0 \le a \le 3$.
נגדיר שני אוטומורפיזמים: הראשון $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ הוא האוטומורפיזם היחיד המקיים $\sigma(\sqrt[4]{a}) = i\sqrt[4]{a}$ ו-$\sigma(i) = i$, והשני $\tau \in \mathrm{Gal}(K/\mathbb{Q})$ הוא האוטומורפיזם היחיד המקיים $\tau(\sqrt[4]{a}) = \sqrt[4]{a}$ ו-$\tau(i) = -i$ (שהוא למעשה ההצמדה המרוכבת).
נשים לב כי $\sigma^4 = \tau^2 = \mathrm{id}$ (כי שניהם מקבעים את היוצרים). כמו כן, $\tau\sigma\tau = \sigma^{-1}$, כי

$$\tau\sigma\tau(\sqrt[4]{a}) = \tau\sigma(\sqrt[4]{a}) = \tau(i\sqrt[4]{a}) = -i\sqrt[4]{a} = \sigma^{-1}(\sqrt[4]{a})$$
$$\tau\sigma\tau(i) = \tau\sigma(-i) = \tau(-i) = i = \sigma^{-1}(i)$$

מצד שני, $\tau\sigma \neq \sigma\tau$ כי

$$\tau\sigma(\sqrt[4]{a}) = \tau(i\sqrt[4]{a}) = -i\sqrt[4]{a}$$
$$\sigma\tau(\sqrt[4]{a}) = \sigma(\sqrt[4]{a}) = i\sqrt[4]{a}$$

לכן σ, τ יוצרים תת־חבורה מסדר 8 של $\mathrm{Gal}(K/\mathbb{Q})$, שאיזומורפית ל-$D_4$ בגלל היחסים שהראינו. כיוון ש-$\mathrm{Gal}(K/\mathbb{Q})$ מסדר 8, נקבל $\mathrm{Gal}(K/\mathbb{Q}) = \langle \sigma, \tau \rangle \cong D_4$, כנדרש.

בהצלחה!