

פתרון תרגיל בית 7 בשדות ותורת גלואה 88-311 סמסטר א' תשפ"ב

שאלה 1. תהינה $K_1/F, K_2/F$ שתי הרחבות. נניח שיש איזומורפיזם $\varphi: K_1 \rightarrow K_2$ המקיים $\varphi|_F = \text{id}_F$. הוכיחו כי

$$\text{Aut}_F(K_1) \cong \text{Aut}_F(K_2)$$

פתרון. נגדיר העתקה

$$\begin{aligned} \psi: \text{Gal}(K_1/F) &\rightarrow \text{Gal}(K_2/F) \\ \sigma &\mapsto \varphi \circ \sigma \circ \varphi^{-1} \end{aligned}$$

כלומר לכל $\sigma \in \text{Gal}(K_1/F)$ ולכל $a \in K_1$ הגדרנו $\psi(\sigma): a \mapsto \varphi(\sigma(\varphi^{-1}(a)))$. נבדוק כי ψ מוגדרת היטב: קל לראות שלכל $\sigma \in \text{Gal}(K_1/F)$ ההעתקה $\varphi \circ \sigma \circ \varphi^{-1}$ היא אוטומורפיזם של K_2 . האוטומורפיזמים $\sigma, \varphi, \varphi^{-1}$ כולם שומרים על אברי F , ולכן הרכבתם שומרת על F .

נבדוק כי ψ הומומורפיזם: לכל $\sigma, \tau \in \text{Gal}(K_1/F)$ מתקיים

$$\psi(\sigma)\psi(\tau) = \varphi \circ \sigma \circ \varphi^{-1} \circ \varphi \circ \tau \circ \varphi^{-1} = \varphi \circ \sigma \circ \tau \circ \varphi^{-1} = \psi(\sigma\tau)$$

נראה כי ψ חח"ע לפי זה שהגרעין טריוויאלי. יהי $\sigma \in \text{Gal}(K_1/F)$ המקיים $\psi(\sigma) = \text{id}_{K_2}$. לכן $\varphi\sigma\varphi^{-1}(a) = a$ לכל $a \in K_2$. מכיוון ש- φ הוא איזומורפיזם זה אומר ש- $\sigma(\varphi^{-1}(a)) = \varphi^{-1}(a)$ וזה אומר ש- $\sigma(b) = b$ לכל $b \in K_1$ (כי φ^{-1} הוא על) ולכן $\sigma = \text{id}_{K_1}$. נראה כי ψ על: אם החבורות סופיות, אז הן באותו גודל, ולכן זה מייד נובע. באופן ישיר ניתן לראות כי $\psi(\varphi^{-1}\sigma\varphi) = \sigma$. ההוכחה הזו דומה, ולא במקרה, להוכחה שאם שתי קבוצות X ו- Y הן מאותה עוצמה, אז $S_X \cong S_Y$.

שאלה 2. תהי K/\mathbb{F}_p הרחבת שדות סופית. הוכיחו כי $\sigma(x) = x^p$ הוא איבר של $\text{Aut}_{\mathbb{F}_p}(K)$.

פתרון. זה אוטומורפיזם שכן במאפיין p מתקיים $(x+y)^p = x^p + y^p$, $(xy)^p = x^p y^p$ (בדקו שאתם יודעים למה). בנוסף σ שומר על \mathbb{F}_p , כי לפי משפט פרמה הקטן מתקיים ש- $a^p = a$ לכל $a \in \mathbb{F}_p$.

שאלה 3. חשבו את חבורות האוטומורפיזמים של ההרחבות הבאות:

א. K/\mathbb{F} כאשר $F = \mathbb{Q}(\sqrt{2})$ ו- $K = \mathbb{Q}(\sqrt[4]{2})$.

ב. E/\mathbb{Q} כאשר E הוא שדה הפיצול של $x^5 - 1$.

ג. E/F כאשר $[E:F] = 2$ עבור F ממאפיין שונה מ-2. רמז: העזרו בשאלה מתרגיל 5 והראו $E = F(\sqrt{\alpha})$ עבור $\alpha \in F$.

ד. E/\mathbb{Q} כאשר E הוא שדה פיצול של פולינום אי פריק ממעלה 3 שיש לו שורש מרוכב לא ממשי.

פתרון.

א. הפולינום המינימלי של $\sqrt[4]{2}$ מעל $\mathbb{Q}(\sqrt{2})$ הוא $x^2 - \sqrt{2}$. אם φ בחבורת האוטומורפיזמים, אז לפי מה שראינו קודם $\varphi(\sqrt[4]{2}) = \pm\sqrt[4]{2}$. אם $\varphi(\sqrt[4]{2}) = \sqrt[4]{2}$, אז כבר הסקנו כי $\varphi = \text{id}$ שהוא בוודאי איבר בחבורת האוטומורפיזמים. עבור האפשרות $\varphi(\sqrt[4]{2}) = -\sqrt[4]{2}$ צריך להזהר! בשלב הזה אנחנו לא יודעים בכלל אם קיימת φ שמקיימת את הנ"ל. השוו לתרגיל הקודם בו גילינו עם שיקול הממשיות שאין φ המקיימת $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}\rho$. מפני שזו בסך הכל הרחבה מסדר 2 אנחנו יודעים שאפשר לכתוב איברים של $\mathbb{Q}(\sqrt[4]{2})$ בצורה $a + b\sqrt[4]{2}$ כאשר $a, b \in \mathbb{Q}(\sqrt{2})$. אם אכן קיימת φ כזו, אז בהכרח מתקיים

$$\varphi(a + b\sqrt[4]{2}) = a - b\sqrt[4]{2}$$

ניתן לבדוק את כל הדרישות ולראות שזה אכן אוטומורפיזם המקבע את $\mathbb{Q}(\sqrt{2})$. לכן בחבורת האוטומורפיזמים יש שני איברים בדיוק, ויש רק חבורה אחת (עד כדי איזומורפיזם) בעלת שני איברים והיא $\mathbb{Z}/2\mathbb{Z}$.

ב. נסמן ב- ρ שורש יחידה מסדר 5, וראינו כי $E = \mathbb{Q}(\rho)$. הפולינום המינימלי של ρ הוא $x^4 + x^3 + x^2 + x + 1$ (הוכחנו שהפולינום הזה אי פריק), ואנחנו יודעים כי $[E : \mathbb{Q}] = 4$. לכן הסדר של חבורת גלואה הוא 4 (כי זו הרחבת גלואה). כעת צריך להחליט האם היא $\mathbb{Z}_2 \times \mathbb{Z}_2$ או \mathbb{Z}_4 . בשביל זה נמצא את סדר האיברים בחבורה. השורשים של הפולינום המינימלי הם $\rho, \rho^2, \rho^3, \rho^4$. נסתכל על האיבר φ שמקיים

$$\varphi(\rho) = \rho^2$$

קיים כזה לפי משפט שראינו בעבר (חבורת גלואה פועלת טרזיטבית על השורשים) אזי מתקיים

$$\varphi\varphi(\rho) = \rho^4 \neq \rho$$

כלומר $\varphi^2 \neq \text{id}$. לכן יש בחבורת גלואה איבר מסדר גדול מ-2 ובהכרח $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

פתרון אחר: השורשים הם $\rho, \rho^2, \rho^3, \rho^4$ ונמספר אותם לפי הסדר הזה. אז

id	$\rho \mapsto \rho$	id
(1 2 4 3)	$\rho \mapsto \rho^2$	σ
(1 4)(2 3)	$\rho \mapsto \rho^4$	σ^2
(1 3 4 2)	$\rho \mapsto \rho^3$	σ^3

וקל לראות שהחבורה היא ציקלית, כלומר $\text{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}/4\mathbb{Z}$.

ג. כבר ראינו (בתרגיל בית 5 שאלה 4) שבהרחבה ממימד 2, השדה E חייב להיות שדה פיצול של פולינום מעל F . יהי $r \in E \setminus F$ עם פולינום מינימלי $f(x)$. מפני שהמאפיין שונה מ-2, אנחנו יודעים שמתקיים

$$r = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

נסמן $\alpha = b^2 - 4c$, ואז ברור ש- $E = F(\sqrt{\alpha})$. כלומר E הוא שדה הפיצול של $x^2 - \alpha \in F[x]$. לכן חבורת האוטומורפיזמים איזומורפית לתת-חבורה של S_2 , ואין יותר מדי אפשרויות. ישנו איבר $\varphi \in \text{Aut}_F(E)$ המקיים $\varphi(\sqrt{\alpha}) = -\sqrt{\alpha}$. כלומר φ אינו איבר היחידה id, ולכן חבורת האוטומורפיזמים היא עד כדי איזומורפיזם $S_2 \cong \mathbb{Z}/2\mathbb{Z}$.

ד. יהי E שדה הפיצול של פולינום אי פריק $f(x) \in \mathbb{Q}[x]$ ממעלה 3; לכן $\text{Aut}_{\mathbb{Q}}(E)$ היא תת־חבורה של S_3 . הצמדה מרוכבת היא אוטומורפיזם של E/\mathbb{Q} , ולכן $\text{Aut}_{\mathbb{Q}}(E)$ היא תת־חבורה מסדר 2 או כל S_3 . אבל הפעולה של $\text{Aut}_{\mathbb{Q}}(E)$ היא טרנזיטיבית על השורשים של $f(x)$, ולכן לא יכולים להיות בה רק שני איברים. מכאן נקבל שבהכרח $\text{Aut}_{\mathbb{Q}}(E) \cong S_3$.

שאלה 4. יהי $f \in \mathbb{Q}[x]$ פולינום אי פריק, ויהי F/\mathbb{Q} שדה הפיצול שלו ב- \mathbb{C} . הוכיחו שאם $[F : \mathbb{Q}]$ אי זוגי, אז כל שורשי $f(x)$ הם ממשיים. רמז: הצמדה מרוכבת היא אוטומורפיזם.

פתרון. נניח בשלילה כי יש שורש מרוכב. הצמדה מרוכבת היא אוטומורפיזם של F שאינו אוטומורפיזם הזהות (כי ב- F יש מספרים לא ממשיים), והיא כמובן גם מקבעת את \mathbb{Q} . לכן היא איבר בחבורת גלואה $\text{Gal}(F/\mathbb{Q})$. הסדר של הצמדה הוא 2 ולכן סדר חבורת גלואה $|\text{Gal}(F/\mathbb{Q})|$ הוא זוגי. אבל F/\mathbb{Q} הרחבת גלואה (נתון כי F שדה פיצול, וההרחבה ספרבילית כי המאפיין הוא 0) ולכן

$$|\text{Gal}(F/\mathbb{Q})| = [F : \mathbb{Q}]$$

זוגי, בסתירה לנתון.

פתרון אחר: נניח $\alpha_1, \dots, \alpha_n \in F$ הם שורשי $f(x)$ ו- $m_1(x), \dots, m_n(x) \in \mathbb{Q}[x]$ הם הפולינומים המינימליים שלהם, בהתאמה. לפי כפליות הממד $\deg m_i$ מחלק את $[F : \mathbb{Q}]$ לכל i . לכן $\deg m_i$ אי זוגי לכל i וקיים שורש $\beta_i \in \mathbb{R}$. אבל $\mathbb{Q}[\alpha_i] \cong \mathbb{Q}[\beta_i]$. לכן שדה הפיצול איזומורפי לשדה

$$\mathbb{Q}[\beta_1, \dots, \beta_n] \subseteq \mathbb{R}$$

ומיחידות שדה הפיצול הוא שווה ל- $\mathbb{Q}[\alpha_1, \dots, \alpha_n]$, ולכן כל שורשי $f(x)$ הם ממשיים.

בהצלחה!