פתרון תרגיל בית 6 בשדות ותורת גלואה
88-311 סמסטר א' תש"ף

שאלה 1. תהינה $K_1/F, K_2/F$ שתי הרחבות. נניח שיש איזומורפיזם $\varphi\colon K_1 \to K_2$ המקיים $\varphi(F) = F$. הוכיחו כי

$$\mathrm{Gal}\,(K_1/F) \cong \mathrm{Gal}\,(K_2/F)$$

פתרון. נגדיר העתקה

$$\begin{aligned}\psi\colon\ \mathrm{Gal}\,(K_1/F) &\to \mathrm{Gal}\,(K_2/F)\\ \sigma &\mapsto \varphi\circ\sigma\circ\varphi^{-1}\end{aligned}$$

כלומר לכל $\sigma \in \mathrm{Gal}\,(K_1/F)$ ולכל $a \in K_1$ הגדרנו $\psi(\sigma)\colon a \mapsto \varphi\left(\sigma\left(\varphi^{-1}(a)\right)\right)$.
נבדוק כי ψ מוגדרת היטב: קל לראות שלכל $\sigma \in \mathrm{Gal}\,(K_1/F)$ ההעתקה $\psi(\sigma) = \varphi\circ\sigma\circ\varphi^{-1}$ 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 $\sigma, \tau \in \mathrm{Gal}\,(K_1/F)$ 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 $\sigma \in \mathrm{Gal}(K_1/F)$ המקיים $\psi(\sigma) = \mathrm{id}_{K_2}$. לכן $\varphi\sigma\varphi^{-1}(a) = a$ לכל $a \in K_2$. מכיוון ש-φ הוא איזומורפיזם זה אומר ש-$\sigma\left(\varphi^{-1}(a)\right) = \varphi^{-1}(a)$ וזה אומר ש-$\sigma(b) = b$ לכל $b \in K_1$ (כי φ^{-1} הוא על) ולכן $\sigma = \mathrm{id}_{K_1}$.
נראה כי ψ על: אם החבורות סופיות, אז הן באותו גודל, ולכן זה מייד נובע. באופן ישיר ניתן לראות כי $\psi\left(\varphi^{-1}\sigma\varphi\right) = \sigma$.
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 $\mathrm{Gal}(K/\mathbb{F}_p)$.

פתרון. זה אוטומורפיזם שכן במאפיין p מתקיים $(xy)^p = x^p y^p$, $(x+y)^p = x^p + y^p$ (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. 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 $\mathrm{Gal}(F/\mathbb{Q})$. הסדר של הצמדה הוא 2 ולכן סדר חבורת גלואה $|\mathrm{Gal}(F/\mathbb{Q})|$ הוא זוגי. אבל $F/\mathbb{Q}$ הרחבת גלואה (נתון כי F שדה פיצול, וההרחבה ספרבילית כי המאפיין הוא 0) ולכן

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

זוגי, בסתירה לנתון.

פתרון אחר: נניח $\alpha_1,\ldots,\alpha_n \in F$ הם שורשי $f(x)$ וש-$m_1(x),\ldots,m_n(x) \in \mathbb{Q}[x]$ 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

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

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

שאלה 4. חשבו את חבורות גלואה של ההרחבות הבאות:

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

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

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

פתרון.

א. 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. 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 טרזיטיבית על השורשים) אזי מתקיים

$$\varphi\varphi(\rho)=\rho^4\neq 1$$

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

ב. כבר ראינו (בתרגיל בית 5 שאלה 5) שבהרחבה ממימד 2, השדה E חייב להיות שדה פיצול של פולינום מעל F. אז זו הרחבה נורמלית. נניח E הוא שדה פיצול של $f(x)=x^2+bx+c$. כמובן שיש ל-$f(x)$ שני שורשים שונים (אם היה לו שורש אחד, אז לפי נוסחת שורשים הוא היה $-\frac{b}{2}$ ואז $f(x)$ היה מתפצל כבר מעל F) ופה בעצם משתמשים בעובדה שהמאפיין שונה מ-2. לכן $f(x)$ ספרבילי, וההרחבה היא הרחבת גלואה.
יהי $r\in E\backslash F$ 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 גלואה היא איזומורפית לתת־חבורה של S_2, ואין יותר מדי אפשרויות. ישנו איבר $\varphi \in \mathrm{Gal}(E/F)$ המקיים $\varphi(\sqrt{\alpha}) = -\sqrt{\alpha}$. כלומר φ אינו איבר היחידה id, ולכן חבורת גלואה היא עד כדי איזומורפיזם $S_2 \cong \mathbb{Z}/2\mathbb{Z}$.

ג. יהי E הוא שדה הפיצול של פולינום אי פריק $f(x) \in \mathbb{Q}[x]$ ממעלה 3. ראינו כבר כי

$$[E : F] \leq (\deg f)! = 3! = 6$$

ובנוסף $3 | [E : F]$. לכן חבורת גלואה היא תת־חבורה של S_3 מסדר 6 או 3. לפי סריג תת־החבורות של S_3 שראינו (למשל בקורס תורת החבורות) אנחנו יודעים שיש לה רק תת־חבורה אחת מסדר 6, שהיא S_3 ורק תת־חבורה אחת מסדר 3, שהיא A_3. לפי הנתון על השורש המרוכב ושאלה 3, אפשר להסיק כי $|\mathrm{Gal}(E/\mathbb{Q})|$ זוגי, ולכן יחד נקבל $6 \mid |\mathrm{Gal}(E/\mathbb{Q})|$ ולכן $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$.

שאלה 5. 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 בשאלה הקודמת ובתרגיל בית 5.

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-$E = \mathbb{Q}(\sqrt[3]{2}, \rho)$ כאשר ρ שורש יחידה פרימיטבי 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.

בהצלחה!