פתרון תרגיל בית 5 - תורת גלואה
סמסטר א', תשע"ז

שאלה 1. יהי F שדה ממאפיין p, ו$a \in F$. הוכיחו כי $x^p - x + a$ הוא פולינום ספרבילי.

פתרון. הנגזרת של הפולינום היא $px^{p-1} - 1 \equiv -1 \neq 0$ ולכן הפולינום ספרבילי.

שאלה 2. חשבו את חבורת גלואה של ההרחבות הבאות:

1. שדה הפיצול של $x^3 - 5$ מעל $\mathbb{Q}$.
2. שדה הפיצול של $x^7 - 1$ מעל $\mathbb{Q}$.
3. שדה הפיצול של $x^4 + 1$ מעל $\mathbb{Q}[\sqrt{2}]$ (שימו לב ש $\rho_8 = \dfrac{1+i}{\sqrt{2}}$).

פתרון. 1. השורשים הם $\sqrt[3]{5}, \sqrt[3]{5}\rho_3, \sqrt[3]{5}\rho_3^2$ ולכן שדה הפיצול הוא

$$E = \mathbb{Q}[\sqrt[3]{5}, \sqrt[3]{5}\rho_3, \sqrt[3]{5}\rho_3^2] \stackrel{!}{=} \mathbb{Q}[\rho_3, \sqrt[3]{5}]$$

(את המעבר האחרון צריך לנמק).
לפי תרגיל ישן, בגלל שההרחבות $\mathbb{Q}[\sqrt[3]{5}]$ ו$\mathbb{Q}[\rho_3]$ הם ממימדים זרים (2,3) אז $[E \colon \mathbb{Q}] = 2 \cdot 3 = 6$ ולכן נצפה ל6 איברים בחבורת גלואה.
אך יותר מזה, מכפליות המימד נקבל ש $\left[E \colon \mathbb{Q}[\sqrt[3]{5}]\right] = 2$ מה שאומר ש$\sqrt[3]{5}, \rho_3$ לא תלויים אלגברית זה בזה.
אם כן, ה$\mathbb{Q}$-אוטומורפיזמים האפשריים הם כל הבאים:

תמורה על השורשים	יוצרים	אוטומורפיזם
Id	$\sqrt[3]{5} \mapsto \sqrt[3]{5}$ $\rho_3 \mapsto \rho_3$	Id
(123)	$\sqrt[3]{5} \mapsto \sqrt[3]{5}\rho_3$ $\rho_3 \mapsto \rho_3$	σ
(23)	$\sqrt[3]{5} \mapsto \sqrt[3]{5}$ $\rho_3 \mapsto \rho_3^2$	τ
(132)	$\sqrt[3]{5} \mapsto \sqrt[3]{5}\rho_3^2$ $\rho_3 \mapsto \rho_3$	σ^2
(13)	$\sqrt[3]{5} \mapsto \sqrt[3]{5}\rho_3^2$ $\rho_3 \mapsto \rho_3^2$	$\tau\sigma$
(12)	$\sqrt[3]{5} \mapsto \sqrt[3]{5}\rho_3$ $\rho_3 \mapsto \rho_3^2$	$\sigma\tau$

כבר אחרי השורה השלישית אנחנו רואים שיש לנו את יוצרים של S_3, ומכיוון והחבורה שלנו היא מגודל 6 אז קיבלנו בדיוק ש $G \cong S_3$.

2. השורשים הם $\rho_7^i =$ "i" לכל $1 \le i \le 7$. כמובן שהם מאוד תלויים זה בזה, התמונה של כל השורשים נקבעת לפי התמונה של ρ_7. מכיוון ו ρ_7^i עבור $1 \le i \le 6$ הם כולם שורשים של הפולינום האי-פריק $x^6 + x^5 + \cdots + x + 1$ חבורת גלואה פועלת עליהם טרנזיטיבית, וכך מובטח לנו שכל העתקה $\sigma_i\colon \rho_7 \mapsto \rho_7^i$ היא איבר של חבורת גלואה. נסכם בטבלה:

תמורה על השורשים	יוצרים	אוטומורפיזם
Id	$\rho_7 \mapsto \rho_7$	$\sigma_1 = Id$
$(124)(365)$	$\rho_7 \mapsto \rho_7^2$	$\sigma_2 = \sigma^2$
(132645)	$\rho_7 \mapsto \rho_7^3$	$\sigma_3 = \sigma$
$(142)(356)$	$\rho_7 \mapsto \rho_7^4$	$\sigma_4 = \sigma^4$
(154623)	$\rho_7 \mapsto \rho_7$	$\sigma_5 = \sigma^5$
$(16)(34)(25)$	$\rho_7 \mapsto \rho_7$	$\sigma_6 = \sigma^3$

אפשר לראות שהחבורה היא צקלית $G = \langle \sigma \rangle \cong \mathbb{Z}_6$.

3. השורשים של הפולינום הם $\pm\rho_8, \pm\overline{\rho_8}$, ולכן שדה הפיצול מעל $\mathbb{Q}[\sqrt{2}]$ הוא $E = \mathbb{Q}[\sqrt{2}][\rho_8] \overset{!}{=} \mathbb{Q}[\sqrt{2}][i]$ כאשר השיוויון האחרון נובע מכך ש $\rho_8 = \dfrac{1+i}{\sqrt{2}}$.
(לא היינו צריכים להוסיף את הצמוד כי $\rho_8^7 = \overline{\rho_8}$).
השורשים ודאי תלויים זה בזה, מספיק לקבוע לאן ρ_8 הולך. מכיוון ו $x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$ פריק מעל $\mathbb{Q}[\sqrt{2}]$, ρ_8 יכול ללכת רק ל $\{\rho_8, \overline{\rho_8}\}$.
נחשב שאם $\rho_8 \mapsto \overline{\rho_8}$אז $i = \sqrt{2}\rho_8 - 1 \mapsto \sqrt{2}\overline{\rho_8} - 1 = -i$. נסכם בטבלה:

תמורה על השורשים	יוצרים	יוצרים	אוטומורפיזם
Id	$i \mapsto i$	$\rho_8 \mapsto \rho_8$	Id
$(13)(24)$	$i \mapsto -i$	$\rho_8 \mapsto \overline{\rho_8}$	τ

(כמובן שלא חייבים את שתי העמודות של יוצרים, זה רק כדי שתראו).
רואים שהחבורה היא מסדר 2 (זה מתאים כי $[E\colon \mathbb{Q}[\sqrt{2}] = 2$) ולכן $G \cong \mathbb{Z}_2$.

שאלה 3. היעזרו בשאלה הקודמת וחשבו את $\left[\mathbb{Q}[\sqrt[3]{5}\rho_3 - 3\sqrt[3]{5^2}\rho_3] \colon \mathbb{Q}\right]$.

הנחיה: שימו לב שההרחבה מוכלת בשדה הפיצול שבסעיף הראשון של השאלה הקודמת.

כדי לדעת כמה שורשים יש לפולינום המינימלי של α, חשבו $\sigma(\alpha)$ לכל איברי החבורה שחישבתם שם.

פתרון. נחשב את כל הצמודים של α:

$$\begin{aligned}
Id(\alpha) &= \alpha \\
\sigma(\alpha) &= \sqrt[3]{5}\rho_3^2 - 3\sqrt[3]{5^2} \\
\tau(\alpha) &= \sqrt[3]{5}\rho_3^2 - 3\sqrt[3]{5^2}\rho_3^2 \\
\sigma^2(\alpha) &= \sqrt[3]{5} - 3\sqrt[3]{5^2}\rho_3^2 \\
\tau\sigma(\alpha) &= \sqrt[3]{5}\rho_3 - 3\sqrt[3]{5^2} \\
\sigma\tau(\alpha) &= \sqrt[3]{5} - 3\sqrt[3]{5^2}\rho_3
\end{aligned}$$

קיבלנו 6 צמודים שונים (הם אכן כולם שונים זה מזה כי $\left\{\sqrt[3]{5}^i\rho_3^j\right\}$ הוא בסיס של ההרחבה $\mathbb{Q}[\sqrt[3]{5}, \rho_3]$ מעל $\mathbb{Q}$) ולכן המימד הוא 6.

שאלה 4. יהי $f(x) \in \mathbb{Q}[x]$ ו E שדה הפיצול של $f(x)$. הוכיחו כי אם ל $f(x)$ יש שורש מרוכב אז $|Gal\,(E/\mathbb{Q})|$ הוא זוגי.

פתרון. נתבונן באוטומורפיזם הצמוד של $\mathbb{C}$: $\overline{a+bi} = a - bi$.

בצמצום לE זהו אוטומורפיזם של E כיוון ש$E = \mathbb{Q}[\alpha_1, \ldots, , \alpha_n]$ כאשר α_i הם שורשי f והצמוד שומר על $\mathbb{Q}$ ושולח כל שורש לשורש (כידוע עבור פולינומים ממשיים).

מכיוון ונתון של f יש שורש מרוכב, הצימצום של העתקת הצמוד היא לא ההעתקה הטריוויאלית (הזהות).

אם כן זהו אוטומורפיזם של E מסדר 2 ולכן (לגראנז') $2 \mid |Gal(E/\mathbb{Q})|$.

שאלה 5. הוכחתם בהרצאה שאם $\alpha, \beta \in E$ הם שורשים של פולינום **אי-פריק** $f(x) \in F[x]$ אז יש אוטומורפיזם $\sigma \in Gal\,(E/F)$ כך ש $\sigma(\alpha) = \beta$.

הוכיחו את הכיוון ההפוך: אם E/F שדה הפיצול של פולינום פרימיטיבי $f(x) \in F[x]$ ו$Gal\,(E/F)$ פועלת טרנזיטיבית על שורשי $f(x)$ אז $f(x)$ הוא אי-פריק מעל F.

פתרון. אם בשלילה הפולינום פריק $f(x) = g(x)h(x)$.יהי $\alpha, \beta \in E$ כך ש $g(\alpha) = 0$ $h(\beta) = 0$. אזי לכל אוטומורפיזם σ בחבורת גלואה $\sigma(\alpha)$ הוא שורש של g, ומכיוון שהפולינום ספרבילי בהכרח $\sigma(\alpha) \neq \beta$ (כי β לא יכול להיות שורש גם של g). בסתירה להנחה על טרנזיטיביות.