פתרון תרגיל בית 5 תורת גלואה - תשע"ח

1. תארו את חבורת גלואה של ההרחבות הבאות:

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

ב. ${}^{E}/_{\mathbb{Q}}$ כאשר E שדה הפיצול של $x^4 - 2$ מעל $\mathbb{Q}$.

ג. ${}^{E}/_{\mathbb{Q}[\sqrt{2}]}$ כאשר E הוא שדה הפיצול של $x^4 + 1$ מעל $\mathbb{Q}[\sqrt{2}]$.
היעזרו בשורש היחידה $\rho_8 = \frac{1+i}{\sqrt{2}}$.

פתרון. א. השורשים הם $\rho_5, \rho_5^2, \dots, \rho_5^5 = 1$ ונמספר אותם לפי הסדר הזה.

Id	$\rho_5 \mapsto \rho_5$	Id
σ	$\rho_5 \mapsto \rho_5^2$	(1243)
σ^2	$\rho_5 \mapsto \rho_5^4$	$(14)(23)$
σ^3	$\rho_5 \mapsto \rho_5^3$	(1342)

החבורה היא ציקלית ולכן $Gal \cong \mathbb{Z}_4$.

ב. השורשים הם $\sqrt[4]{2}, -\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}i$ ונמספר אותם לפי הסדר הזה.

Id	$\sqrt[4]{2} \mapsto \sqrt[4]{2}$ $i \mapsto i$	Id
τ	$\sqrt[4]{2} \mapsto \sqrt[4]{2}$ $i \mapsto -i$	(34)
σ	$\sqrt[4]{2} \mapsto \sqrt[4]{2}i$ $i \mapsto i$	(1324)
$\tau\sigma\tau = \sigma^3$	$\sqrt[4]{2} \mapsto -\sqrt[4]{2}i$ $i \mapsto i$	(1423)
	$\ldots$	

החבורה מגודל 8 (כי ההרחבה היא גלואה ממימד 8) ויש איברים מסדר 2 ו 4 המקיימים $\tau\sigma\tau = \sigma^{-1}$ ולכן $Gal \cong D_4$.

ג. אולי יעזור לשים לב ש $x^8 - 1 = (x^4 - 1)(x^4 + 1)$, השורשים הם $\rho_8, \rho_8^3, \rho_8^5, \rho_8^7$ ונמספר אותם לפי הסדר הזה.
עוד נשים לב שמעל $\mathbb{Q}[\sqrt{2}]$ היוצר של ההרחבה הוא i. הפולינום המינימלי של i (גם מעל $\mathbb{Q}[\sqrt{2}]$) הוא $x^2 - 1$ ולכן יש רק שני אוטומורפיזמים והחבורה היא$\mathbb{Z}_2 \cong Gal$.

Id	$i \mapsto i$	Id
σ	$i \mapsto -i$	$(14)\,(23)$

2. יהי $f(x) \in \mathbb{Q}[x]$ ונסמן ב E את שדה הפיצול שלו. נניח כי ל$f(x)$ יש שורש מרוכב (שאינו ממשי). הוכיחו כי $|\mathrm{Gal}\,(E/\mathbb{Q})|$ הוא זוגי.

פתרון. . ראשית נשים לב שההרחבה $E/\mathbb{Q}$ היא גלואה ולכן נורמלית. נתבונן באוטומורפיזם ההצמדה $\tau\colon i \mapsto -i$ של $\mathbb{C}$. הצימצום $\tau|_E$ הוא אוטומורפיזם של E ($\tau(E) \subseteq E$) כי זו הרחבה נורמלית. בנוסף, $\tau|_E \neq \mathrm{Id}$ כי יש בE איבר מרוכב שאיננו ממשי ־ו τ פועל עליו בצורה לא טריוויאלית. אם כן, $\tau|_E \in Gal(E/\mathbb{Q})$ הוא איבר מסדר 2 ולכן חבורת גלואה היא מסדר זוגי (לגראנג').

3. יהי $f(x) \in \mathbb{Q}[x]$ פולינום אי־פריק מדרגה 3 ונסמן ב E את שדה הפיצול שלו. נניח כי ל$f(x)$ יש שורש מרוכב שאיננו ממשי, הוכיחו כי $\mathrm{Gal}\,(E/\mathbb{Q}) \cong S_3$.

פתרון. . זו הרחבת גלואה ולכן $Gal(E/\mathbb{Q}) \hookrightarrow S_3$.
יהי $\alpha \in E$ שורש של $f(x)$, אזי

$$3 = deg(f) = [F[\alpha]\colon F] \mid [E\colon F] = |Gal(E/\mathbb{Q}|$$

ומצד שני לפי השאלה הקודמת $2 \mid |Gal(E/\mathbb{Q})|$ ולכן יחד נקבל $6 \mid |Gal(E/\mathbb{Q})|$ ולכן $Gal(E/\mathbb{Q}) \cong S_3$.

4. יהיו K_1, K_2 שתי הרחבות של השדה F, כך שקיים איזומורפיזם $\varphi\colon K_1 \to K_2$ המקיים $\varphi(F) = F$.
הוכיחו כי $\mathrm{Gal}\left(K_1/F\right) \cong \mathrm{Gal}\left(K_2/F\right)$.

פתרון. . נגדיר העתקה $\psi\colon\ \mathrm{Gal}\left(K_1/F\right) \longrightarrow \mathrm{Gal}\left(K_2/F\right)$ ע"י $\psi(\sigma)\colon a \mapsto \varphi\left(\sigma\left(\varphi^{-1}(a)\right)\right)$.
מוגדר היטב: קל לראות שלכל $\sigma \in \mathrm{Gal}\left(K_1/F\right)$ ההעתקה $\psi(\sigma) = \varphi \circ \sigma \circ \varphi^{-1}$ היא אוטומורפיזם של K_2. הוא שומר על אברי F כי $\sigma, \varphi, \varphi^{-1}$ כולם שומרים על אברי F.
הומומורפיזם: $\psi(\sigma)\psi(\tau) = \varphi \circ \sigma \circ \varphi^{-1} \circ \varphi \circ \tau \circ \varphi^{-1} = \varphi \circ \sigma \circ \tau \circ \varphi^{-1} = \psi(\sigma\tau)$.
חח"ע: נראה שהגרעין טריוויאלי. אם עבור $\sigma \in \mathrm{Gal}(K_1/F)$ מתקיים $\psi(\sigma) = Id_{K_2}$ זה אומר ש $\varphi\sigma\varphi^{-1}(a) = a$ 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 $\sigma = Id_{K_1}$.
על: נובע מכך שהחבורות באותו גודל. ניתן גם לתאר באופן ישיר ש $\psi\left(\varphi^{-1}\tau\varphi\right) = \tau$.

5. יהי F שדה ממאפיין $p \neq 0$, כך ש $F/_{\mathbb{Z}_p}$ היא הרחבה סופית. הוכיחו כי $\sigma(x) = x^p$ הוא איבר של $\mathrm{Gal}\left(F/\mathbb{Z}_p\right)$.

פתרון. . זהו אוטומורפיזם שכן במאפיין p: $(x+y)^p = x^p + y^p$, $(xy)^p = x^p y^p$ (בדקו שאתם יודעים למה).
σ שומר על $\mathbb{Z}_p$ כי לפי משפט פרמה הקטן מתקיים שם ש $a^p = a$.