פתרון תרגיל בית 8 בשדות ותורת גלואה
88-311 סמסטר א' תשע"ט

שאלה 1. תהי $E/\mathbb{Q}$ הרחבת גלואה כך ש-$\mathrm{Gal}(E/\mathbb{Q}) \cong S_n$ הוכיחו כי יש ל-E תת־שדה K כך ש-$[K:\mathbb{Q}]=2$.

פתרון. ל-S_n יש תת־חבורה ידועה מאינדקס 2 והיא A_n. לפי התאמת גלואה E^{A_n} הוא תת־שדה כך ש-$[E:E^{A_n}]=\frac{n!}{2}$ ולכן $[E^{A_n}:\mathbb{Q}]=2$, כדרוש.

שאלה 2. תהי $E=\mathbb{Q}[\alpha]/\mathbb{Q}$ הרחבת גלואה. נניח שקיים $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$ כך ש-$\sigma(\alpha)=\alpha^2$.

א. האם ייתכן כי $[E:\mathbb{Q}]=2$? אם כן, מצאו α מתאים.

ב. האם ייתכן כי $[E:\mathbb{Q}]=3$? אם כן, מצאו α מתאים.

פתרון.

א. נניח שיש שדה E כזה. זו הרחבת גלואה ולכן $|\mathrm{Gal}(E/\mathbb{Q})|=2$. אז $\alpha \notin \mathbb{Q}$ ולכן $\alpha \neq \alpha^2$, כלומר $\sigma \neq \mathrm{id}$. בהכרח σ מסדר 2, ולכן

$$\alpha=\sigma^2(\alpha)=\sigma(\alpha^2)=\alpha^4$$

כלומר $\alpha=\alpha^4$. לכן $\alpha^3=1$ וקיבלנו ש-α-הוא שורש יחידה פרימיטיבי מסדר 3. זה יתכן, כמו שראינו בכיתה שאם $E=\mathbb{Q}[\rho_3]$, אז $[E:\mathbb{Q}]=2$.

ב. נניח שיש שדה E כזה. לכן $|\mathrm{Gal}(E/\mathbb{Q})|=3$. לכן σ היא מסדר 3. לכן

$$\alpha=\sigma^3(\alpha)=\alpha^8$$

כלומר $\alpha^7=1$. אבל אז $E=\mathbb{Q}[\rho_7]$ וראינו כי $[\mathbb{Q}[\rho_7]:\mathbb{Q}]=6$, וזו סתירה.

שאלה 3. נסמן שורש יחידה $\rho=\exp(\frac{2\pi i}{3})$ מסדר 3. חשבו את הפולינום המינימלי מעל $\mathbb{Q}$ של $2\rho+\sqrt[3]{49}$.

רמז: העזרו בשאלה 1 מתרגיל בית 7 ובפעולה של חבורת גלואה המתאימה.

פתרון. זה סיפוח של איבר אחד, ותחילה נגלה את מעלת הפולינום המינימלי שלו. כבר ראינו שחבורת גלואה של $\mathbb{Q}(\rho,\sqrt[3]{7})/\mathbb{Q}$ היא S_3. ראינו כבר בתרגול שמעלת הפולינום המינימלי היא גודל המסלול של $2\rho+\sqrt[3]{49}$ תחת הפעולה של חבורת גלואה. השורשים של x^3-7 הם $\sqrt[3]{7},\sqrt[3]{7}\rho,\sqrt[3]{7}\rho^2$, ונסמן אותם $1,2,3$ בהתאמה. חבורת גלואה היא S_3 ולכן כל התמורות על קבוצת השורשים רלוונטיות. נבין מה כל תמורה עושה ל $2\rho+\sqrt[3]{49}$. שימו לב לאבחנה כי $\rho=\sqrt[3]{7}\rho/\sqrt[3]{7}$:

$\varphi_1=\mathrm{id}$ מקבע את $2\rho+\sqrt[3]{49}$.

$\varphi_2=(1\ 2)$ מחליף בין $\sqrt[3]{7}$ ל-$\sqrt[3]{7}\rho$ ולכן שולח את ρ ל-$\frac{1}{\rho}=\rho^2=-1-\rho$. לכן

$$\varphi_2(2\rho+\sqrt[3]{49})=2\rho^2+\sqrt[3]{49}\rho^2=-2-2\rho-\sqrt[3]{49}-\sqrt[3]{49}\rho$$

$\varphi_3 = (1\ 3)$ שולח את ρ ל-ρ^2 ולכן $\varphi_3(2\rho+\sqrt[3]{49}) = 2\rho^2+\sqrt[3]{49}\rho = -2-2\rho+\sqrt[3]{49}\rho$.
$\varphi_4 = (2\ 3)$ שולח את ρ ל-ρ^2 ולכן $\varphi_4(2\rho+\sqrt[3]{49}) = 2\rho^2+\sqrt[3]{49} = -2-2\rho+\sqrt[3]{49}$.
$\varphi_5 = (1\ 2\ 3)$ שולח את ρ ל-ρ ולכן $\varphi_5(2\rho+\sqrt[3]{49}) = 2\rho+\sqrt[3]{49}\rho^2 = 2\rho-\sqrt[3]{49}-\sqrt[3]{49}\rho$.
$\varphi_6 = (1\ 3\ 2)$ שולח את ρ ל-ρ ולכן $\varphi_6(2\rho+\sqrt[3]{49}) = 2\rho+\sqrt[3]{49}\rho$.

קיבלנו שישה איברים שונים (הם שונים כי $1, \sqrt[3]{7}, \sqrt[3]{49}, \rho, \sqrt[3]{7}\rho, \sqrt[3]{49}\rho$ הוא בסיס למרחב) ולכן הדרגה של הפולינום המינימלי היא 6. הפולינום המינימלי עצמו הוא המכפלה של כל גורמים מהצורה $(x-b)$ כאשר b הוא איבר במסלול. בעזרת מחשב נחשב שהוא

$$x^6+6x^5+24x^4-42x^3-198x^2+684x+3249$$

שאלה 4. יהי $f(x) \in \mathbb{Q}[x]$ פולינום אי פריק עם שדה פיצול E. נניח שחבורת גלואה $\mathrm{Gal}(E/\mathbb{Q})$ היא אבלית. יהי a שורש של $f(x)$.

א. הוכיחו כי $\mathbb{Q}(a)/\mathbb{Q}$ הרחבת גלואה.

ב. הוכיחו כי $E = \mathbb{Q}(a)$.

פתרון. ניתן להחליף את $\mathbb{Q}$ בשדה אחר F, עם הדרישה שההרחבה E/F היא גלואה.

א. ההרחבה $\mathbb{Q}(a)/\mathbb{Q}$ היא גלואה אם ורק אם $\mathrm{Gal}(E/\mathbb{Q}(a)) \leq \mathrm{Gal}(E/\mathbb{Q})$ היא תת־חבורה נורמלית. היא אכן נורמלית כי $\mathrm{Gal}(E/\mathbb{Q})$ אבלית, ולכן כל תת־חבורה שלה נורמלית.

ב. נסמן את שורשי הפולינום $f(x)$ ב-$a = a_1, \dots, a_k$. חבורת גלואה פועלת טרנזיטיבית על קבוצת השורשים. כלומר לכל i יש $\varphi \in \mathrm{Gal}(E/\mathbb{Q})$ כך ש-$\varphi(a) = a_i$. אבל מפני ש-$\mathbb{Q}(a)/\mathbb{Q}$ נורמלית אפשר לצמצם את φ ל-$\mathbb{Q}(a)$, ולכן $\varphi|_{\mathbb{Q}(a)}(a) = a_i \in \mathbb{Q}(a)$ לכל i. כלומר $\mathbb{Q}(a)$ שווה לשדה הפיצול E.

שאלה 5. יהי F שדה ממאפיין שונה מ-2, ויהי K שדה הפיצול של פולינום מתוקן ספרבילי $f(x) \in F[x]$. נסמן את שורשי $f(x)$ ב-$\alpha_1, \dots, \alpha_n$. נגדיר את הדיסקרימיננטה של $f(x)$ להיות

$$\Delta(f) \coloneqq \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2$$

א. בדקו שהדיסקרמיננטה של x^2+bx+c זה מה שאתם חושבים שזה.
זה קצת יותר קשה להראות שהדיסקרמיננטה של $x^3+ux+v \in \mathbb{Q}[x]$ היא $4u^3+27v^2$.
הדיסקרימיננטה כשמה כן היא: לפולינומים ב-$\mathbb{R}$ היא "מאבחנת" את מספר השורשים הממשיים.

ב. הוכיחו כי $\Delta(f) \in F$. רמז: חילופים ב-S_n.

ג. נתבונן ב-$G \coloneqq \mathrm{Gal}(K/F)$ כתת־חבורה של S_n, ונסמן $G_0 = G \cap A_n$. הוכיחו כי $F\big[\sqrt{\Delta(f)}\big] = K^{G_0}$. רמז: מה היא ההגדרה של תמורה זוגית?

ד. הסיקו כי G משוכנת ב-A_n אם ורק אם $\sqrt{\Delta(f)} \in F$.

פתרון.

א. השורשים x^2+bx+c הם $(-b\pm\sqrt{b^2-4ac})/2$ ולכן

$$\Delta(x^2+bx+c) = \left(\frac{-b+\sqrt{b^2-4ac}}{2} - \frac{-b-\sqrt{b^2-4ac}}{2}\right)^2 = \left(\frac{2\sqrt{b^2-4ac}}{2}\right)^2 = b^2-4ac$$

ב. נראה כי $\mathrm{Gal}(K/F) \hookrightarrow S_n$ שומר על הדיסקרמיננטה. נזכר כי S_n נוצרת על ידי חילופים מהצורה $(i, i+1)$ ולכן מספיק להראות שהם שומרים על הדיסקרמיננטה.
אכן, החילוף $(i, i+1)$ שומר על כל הגורמים שאין בהם את α_i או α_{i+1}. את $(\alpha_i - \alpha_{i+1})^2$ הוא שולח ל- $(\alpha_{i+1} - \alpha_i)^2 = (\alpha_i - \alpha_{i+1})^2$, ובנוסף הוא מחליף בין הגורמים $(\alpha_{i+1} - \alpha_j)^2 \leftrightarrow (\alpha_i - \alpha_j)^2$ ובין הגורמים $(\alpha_j - \alpha_{i+1})^2 \leftrightarrow (\alpha_j - \alpha_i)^2$.
בסך הכל S_n שומרת על המכפלה $\Delta(f)$, ולכן על חבורת גלואה, ומכאן ש-$\Delta(f) \in K^G = F$, כדרוש.

ג. לפי החישובים מהסעיף הקודם, החילוף $(i, i+1)$ שולח את $\sqrt{\Delta(f)}$ ל-$-\sqrt{\Delta(f)}$.
כידוע, ניתן לכתוב כל תמורה כמכפלה של חילופים ולכן נקבל $\sigma(\sqrt{\Delta(f)}) = \mathrm{sign}(\sigma)\sqrt{\Delta(f)}$. אם כן, $\sigma(\sqrt{\Delta(f)}) = \sqrt{\Delta(f)}$ אם ורק אם $\mathrm{sign}(\sigma) = 1$ אם ורק אם $\sigma \in A_n$.
מכאן נסיק כי $F\left[\sqrt{\Delta(f)}\right] \subseteq K^{G_0}$, ומצד שני $G_0 \subseteq \mathrm{Gal}\left(K/F\left[\sqrt{\Delta(f)}\right]\right)$. לפי התאמת גלואה זה מוכיח את הדרוש. היה אפשר להוכיח במקום, באופן דומה לסעיף הקודם, כי $\sqrt{\Delta(f)}$ שומר על תמורות זוגיות על ידי זה שנראה כי הוא שומר על מחזורים מהצורה $(i, i+1, i+2)$ שיוצרים את A_n.

ד. לפי הסעיף הקודם והתאמת גלואה: מתקיים $G_o = G$ אם ורק אם $K^{G_0} = K^G = F$ אם ורק אם $F\left[\sqrt{\Delta(f)}\right] = F$ אם ורק אם $\sqrt{\Delta(f)} \in F$.

שאלה 6 (רשות לא קשה)**.** יהיו שני פולינומים

$$f(x) = x^4 - 10x^2 + 1, \qquad g(x) = (x^2-2)(x^2-3)$$

ראינו שיש להם את אותו שדה פיצול $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. כמובן שחבורת גלואה $G = \mathrm{Gal}(E/\mathbb{Q})$ פועלת על השורשים של $f(x), g(x)$. הזכרו כי השורשים של $f(x)$ הם $\pm\sqrt{2} \pm \sqrt{3}, \pm\sqrt{2} \mp \sqrt{3}$ ושל g הם $\pm\sqrt{2}, \pm\sqrt{3}$. הוכיחו כי הפעולות לא איזומורפיות.
רמז: בשפה פשוטה מבקשים להראות שלא משנה איך נמספר את השורשים, הפעולות שונות. אפשר קודם לשים לב שתת־החבורות המתאימות ב-S_4 אינן צמודות למשל.

פתרון. כבר ראינו שחבורת גלואה של הפולינומים מכילה 4 תמורות והן נקבעות לפי הפעולה על $\sqrt{2}, \sqrt{3}$. נזכר שחבורת גלואה של ההרחבה היא $\mathbb{Z}_2 \times \mathbb{Z}_2$. נסמן את האיברים שלה $\{\mathrm{id}, \theta, \tau, \theta\tau\}$ כאשר

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

אם מסתכלים על זה כתמורות על השורשים $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$ של $g(x)$. אז מתקבלות התמורות

$$\mathrm{id}, (12), (34), (12)(34)$$

ואם מסתכלים על זה כתמורות על השורשים $\sqrt{2}+\sqrt{3}, -\sqrt{2}+\sqrt{3}, \sqrt{2}-\sqrt{3}, -\sqrt{2}-\sqrt{3}$ אז מתקבלות התמורות

$$\mathrm{id}, (12)(34), (13)(24), (14)(23)$$

בשני המקרים החבורה איזומורפית ל-$\mathbb{Z}_2 \times \mathbb{Z}_2$. אבל בפעולה השניה לכל איבר בחבורה חוץ מ-id אין נקודות שבת ובפעולה הראשונה יש ולכן הן לא איזומורפיות. במקרה הראשון החבורה מכילה תמורות אי זוגיות, ואילו במקרה השני מדובר בתת־חבורה של A_4. או לפי זה שהראשונה לא טרנזיטיבית, והשנייה כן.

בהצלחה!