אלגברה מופשטת 3 – תרגיל 11 – פתרון

שאלה 1

תהי K/F הרחבת גלואה ממימד סופי.

1. יהיו L, L' שדות ביניים של ההרחבה K/F. נגדיר $H = Gal(K/L),\ H' = Gal(K/L')$. הוכיחו כי התנאים הבאים שקולים
   a. קיים F-איזומורפיזם של שדות $\sigma: L \to L'$.
   b. קיים $g \in Gal(K/F)$ כך ש-$H' = g^{-1}Hg$.
2. יהי p מספר ראשוני. הוכיחו שקיים שדה ביניים $F \subseteq L_p \subseteq K$ כך ש-$\gcd(p, [L_p : F]) = 1$ ו-$[K : L_p]$ הוא חזקה של p. יותר מכך, הוכיחו כי השדה L_p יחיד עד כדי F-איזומורפיזם. *[רמז: משפטי סילוב]*

הוכחה

הוכחת 1: כוון א: נניח שקיים F-איזומורפיזם של שדות $\sigma: L \to L'$. אזי קיים קיים $g \in Gal(K/F)$ כך ש-$g|_L = \sigma'$. *(הסבר: K/F גלואה ממימד סופי ולכן K שדה פיצול של פולינום מסויים f מעל F. לכן, K הוא גם שדה פיצור של f מעל כל אחד מהשדות L, L'. לפי משפט יחידות שדה הפיצול, כל איזומורפיזם בין L ל-L' ניתן להרחבה לאוטומורפיזם של שדה הפיצול K.)* נוכיח כי $H' = g^{-1}Hg$: באמת, $\tau \in H'$ **אם"ם** $\tau(a) = a$ לכל $a \in L'$ **אם"ם** $\tau(\sigma b) = \sigma b$ לכל $b \in L$ **אם"ם** $\tau(gb) = gb$ לכל $b \in L$ **אם"ם** $b \in L$ $g^{-1}(\tau(gb)) = b$ לכל $b \in L$ **אם"ם** $g^{-1}\tau g \in H$. לכן גמרנו.

כוון ב: נניח ש קיים $g \in Gal(K/F)$ כך ש-$H' = g^{-1}Hg$. יהי $a \in L$. אזי לכל $\sigma \in H'$ מתקיים $g^{-1}\sigma g \in H$ ולכן $g^{-1}\sigma g)a = a$). נפעיל את g על שני האגפים ונקבל $\sigma(ga) = ga$. היות וזה נכון לכל $\sigma \in H'$, נובע ש-$ga \in K^{H'} = L'$ (לפי המשפט היסודי של תורת גלואה). לכן, $g(L) \subseteq L'$. באותו אופן, נובע ש-$g^{-1}(L') \subseteq L'$ (כי $H = gH'g^{-1}$). לכן, $\sigma \coloneqq g|_L$ היא F-הומומורפזים הפיך מ-L ל-L' ($\sigma^{-1} = g^{-1}|_{L'}$). **משל.**

הוכחת 2: לפי משפט סילוב הראשון קיימת תת חבורה $P \leq G \coloneqq Gal(K/F)$ כך ש-$|P|$ היא חזקת p ו-$[G : P]$ זר ל-p. נבחר $L_p = K^P$. לפי המשפט היסודי של תורת גלואה, $[L_p : F] = [G : P]$ ולכן $\gcd(p, [L_p : F]) = 1$, וגם $[K : L_p] = |P|$ ולכן $[K : L_p]$ הוא חזקת p.

נניח כי L' הוא שדה ביניים של K/F שגם מקיים $\gcd(p, [L' : F]) = 1$ ו-$[K : L']$ הוא חזקת p. תהי $P' = Gal(K/L')$, אזי לפי המשפט היסודי של תורת גלואה $|P'| = [K : L']$ ולכן P' היא חבורת p. בנוסף, $[G : P'] = [L' : F]$ ולכן $[G : P']$ זר ל-p. זה אומר ש-P' היא תת חבורת p-סילוב של G. לפי משפט סילוב השני, קיים $g \in G$ כך ש-$P' = g^{-1}Pg$. לכן, לפי סעיף 1, קיים F-איזומורפיזם $\sigma: L_p \to L'$. לכן, השדה L_p יחיד עד כדי F-איזומורפיזם. **משל.**

שאלה 2

1. נחשוב על S_{n-1} כתת חבורה של S_n. הראו כי לא קיימת תת-חבורה $S_{n-1} \subsetneq H \subsetneq S_n$.
2. יהי F שדה, f פולינום *ספרבילי* ממעלה n ו-E שדה הפיצול של f מעל F. נניח כי $[E : F] = n!$ ויהי $\alpha \in E$ שורש של f. הראו כי לא קיים שדה K כך ש-$F \subsetneq K \subsetneq F[\alpha]$.

הוכחה

הוכחת 1: תהי $S_{n-1} \subsetneq H \subseteq S_n$ תת חבורה. מספיק להוכיח כי $H \subseteq S_n$. אם $n = 2$ זה ברור. נניח $n > 2$. קיים $\sigma \in H \setminus S_{n-1}$, כלומר $\sigma(n) \neq n$. נגדיר $\tau \in S_n$ ע"י: $\tau(i) = \begin{cases} n & i = n \\ \sigma^{-1}(n) & i = \sigma(n) \\ \sigma^{-1}(i) & i \neq n, \sigma(n) \end{cases}$.

לא קשה לבדוק כי τ אכן תמורה וכי $\tau \in S_{n-1}$. לכן, $(\sigma(n), n) = \sigma\tau \in H$ וזה גורר ש-$(n-1, n) = \big(n-1, \sigma(n)\big)\big(\sigma(n), n\big)\big(n-1, \sigma(n)\big) \in H$.

לכן, $(1,2,3,\dots,n) = (1,2,\dots,n-1)(n-1,n) \in H$. היות ו-$n > 2$ מתקיים $(1,2) \in H$. לכן, $S_n = \langle (1,2), (1,2,3,\dots,n) \rangle \subseteq H$ וסיימנו. **משל.**

הוכחת 2: יהיו $\alpha_1, \alpha_2, \dots, \alpha_n$ שורשי הפולינום f ב-E. בה"כ $\alpha_n = \alpha$. f ספרבילי ולכן E/F גלואה. נסמן $G = Gal(E/F)$, אזי $|G| = [E:F] = n!$. קיים שיכון חבורות $\psi: G \to S_n$ הנתון ע"י שליחת $\sigma \in G$ אל התמורה שהוא משרה על $\alpha_1, \alpha_2, \dots, \alpha_n$. היות ו-$|G| = n! = |S_n|$, ψ איזומורפיזם. תהי $H = \psi^{-1}(S_{n-1})$. אזי לכל $\sigma \in G$ מתקיים $\sigma(\alpha) = \sigma(\alpha_n) = \alpha_{(\psi(\sigma))(n)} = \alpha_n = \alpha$ ולכן $\alpha \in E^H$, כלומר $F[\alpha] \subseteq E^H$. היות ו-$[E:F] = n!$ בהכרח $[F[\alpha]:F] = n$ (הסבר בסוף). כעת, $[F[\alpha]:F] = [E^H:F] = [G:H] = [S_n:S_{n-1}] = n$. לכן $E^H = F[\alpha]$.

לפי סעיף 1, אין תתי חבורות בין S_n ל-S_{n-1} . לכן, אין תתי חבורות בין G ל-H. לפי המשפט היסודי של תורת גלואה, זה אומר שאין שדה ביניים בין $F = E^G$ ל-$F[\alpha] = E^H$. (באמת, אם $F \subsetneq K \subsetneq F[\alpha]$ אז $H \subsetneq Gal(E/K) \subsetneq G$.) **משל.**

למה $[F[\alpha]:F] = n$? יהיו $\alpha_1, \alpha_2, \dots, \alpha_n$ שורשי f, רק שהפעם נניח בה"כ ש-$\alpha_1 = \alpha$. נגדיר $F_i = F[\alpha_1, \dots, \alpha_i]$ ($F_0 = F$) ו-$d_i = [F_i:F_{i-1}]$. אזי $n! = [E:F] = [F_n:F_0] = [F_n:F_{n-1}] \dots [F_2:F_1][F_1:F_0] = d_1 d_2 d_3 \dots d_n$. מצד שני, α_i שורש של הפולינום $f_i(x) = \frac{f(x)}{\prod_{j<i}(x-\alpha_j)} \in F_{i-1}[x]$ ולכן $d_i = [F_i:F_{i-1}] \leq n - (i-1)$. זה אומר ש-$n! = \prod_{i=1}^{n} \big(n-(i-1)\big) \geq \prod_{i=1}^{n} d_i = d_1 d_2 d_3 \dots d_n = n!$ ולכן אם קיים i כך ש-$d_i < n-(i-1)$ נקבל סתירה לכך ש-$[F[\alpha]:F] = d_1 = n$ ובפרט $d_i = n-(i-1)$ לכל i. לכן,

שאלה 3

1. הוכיחו או הפריכו: אם $F \subseteq K \subseteq L$ שדות כך ש-K/F גלואה ממימד סופי ו-L/K גלואה ממימד סופי אז L/F גלואה.
2. הוכיחו או הפריכו: אם K שדה פיצול של פולינום *ספרבילי* אי פריק ממעלה n מעל F אז ב-$Gal(K/F)$ יש איבר מסדר n. *[רמז: משפט האבר הקדום]*

פיתרון

סעיף 1: הטענה שגויה. נבחר $F = \mathbb{Q}, K = \mathbb{Q}[\sqrt{2}], L = \mathbb{Q}[\sqrt[4]{2}]$. אזי K/F גלואה ו-L/K גלואה כי אלו הרחבות ספרבילית ממעלה 2 וכל הרחבה ספרבילית ממעלה 2 היא גלואה (הוכחתם בהרצה, כמדומני). מצד שני, L/F אינה גלואה כי היא לא נורמלית: לדוגמא, $\sqrt[4]{2} \in L$ והפולינום המינימלי שלו מעל $\mathbb{Q}$ הוא $x^4 - 2$. $i\sqrt[4]{2}$ גם שורש של פולינום זה אך הוא אינו ב-L כי הוא מרוכב. לכן, $x^4 - 2$ לא מתפצל מעל L. נובע ש-L/F לא נורמלית ובפרט לא גלואה.

סעיף 2: הטענה שגויה. ניקח הרחבת גלואה E/F עם חבורת גלואה איזומורפית ל-S_3 (קיום הרחבה כזו יוכח מייד). לפי משפט האבר הקדום קיים $a \in E$ כך ש-$E = F[a]$. יהי f הפולינום המינימלי של

a מעל F. אזי $\deg f = [F[a]:F] = [E:F] = |S_3| = 6$. בנוסף, היות ו-$E/F$ נורמלית, f מתפצל מעל E. לכן, E שדה פיצול של f מעל F. אבל ב-$Gal(E/F) \cong S_3$ אין איברים מסדר $\deg f = 6$.

הרחבה עם חבורת גלואה כנ"ל היא $\mathbb{Q}[\sqrt[3]{2}, \rho_3]/\mathbb{Q}$. נדמה לי שהוכחנו זאת בשיעור. במקרה זה אפשר לקחת $a = \sqrt[3]{2} + \rho_3$.

דוגמא אחרת: יהי f הפולינום המינימלי של $\sqrt{2} + \sqrt{3}$ מעל $\mathbb{Q}$. אזי הוא ממעלה 4 ושדה הפיצול שלו מעל $\mathbb{Q}$ הוא $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. אבל ב-$Gal(\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q})$ אין איברים מסדר 4. (בדקו!)

בונוס

הוכיחו או הפריכו: לכל הרחבת שדות אלגברית L/F (לאו דווקא ממימד סופי) ו-$\sigma \in Gal(L/F)$ קיים n כך ש-$\sigma^n = id_L$.

פיתרון

הטענה השגויה. להלן הדוגמא הכי פשוטה שאני מכיר:

יהי p ראשוני כלשהו. נבחר $F = \mathbb{Z}_p$, נבחר את L להיות הסגור האלגברי של $\mathbb{Z}_p$ ונבחר את σ להיות אוטומורפיזם פרובניוס $\sigma(x) = x^p$. אזי $\sigma \in Gal(L/F)$. <u>נניח בשלילה</u> שקיים n כך ש-$\sigma^n = id_L$, אזי לכל $x \in L$ מתקיים $x = \sigma^n(x) = x^{p^n}$, כלומר $x^{p^n} - x = 0$. לפולינום $x^{p^n} - x$ יש לכל היותר p^n שורשים ולכן L שדה סופי, כלומר $L \cong \mathbb{F}_q$ עבור q כלשהו. זה אומר ש-$\mathbb{F}_q$ סגור אלגברית וזה לא ייתכן כי יש לו הרחבה אלגברית ממימד גדול מ-1: $\mathbb{F}_{q^2}/\mathbb{F}_q$. <u>לכן</u>, לא קיים n כך ש-$\sigma^n = id_L$.