אלגברה מופשטת 3 – תרגיל 12 – פתרון

שאלה 1

תהי E/F הרחבת שדות ויהיו L, K שדות ביניים כך ש-$K \cap L = F$. נניח כי K/F ו-L/F הן הרחבות גלואה ממימד סופי. הראו כי KL/F גלואה ו-$Gal(KL/F) \cong Gal(K/F) \times Gal(L/F)$.

הוכחה

קיימים פולינומים $f, g \in F[x]$ כך ש-K שדה פיצול של f מעל F ו-L שדה פיצול של g מעל F. יהיו $a_1, a_2, \dots, a_n \in K$ שורשי f ויהיו $b_1, b_2, \dots, b_m \in L$ שורשי g. אזי $K = F[a_1, \dots, a_n]$ ו-$L = F[b_1, \dots, b_m]$. כעת, KL הוא השדה הקטן ביותר המכיל את K, L, לכן LK הוא השדה הקטן ביותר המכיל את $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_m$, לכן $KL = F[a_1, \dots, a_n, b_1, \dots, b_m]$. זה אומר ש-$KL$ שדה הפיצול של $f \cdot g$ מעל F. לכן, KL/F גלואה. (הערה: יש עוד דרכים להוכיח KL/F גלואה).

נגדיר העתקה $\psi: Gal(KL/F) \to Gal(K/F) \times Gal(L/F)$ ע"י $\psi(\sigma) = (\sigma|_K, \sigma|_L)$. אזי ψ מוגדרת היטב והיא הומומורפיזם חבורות (זה נובע מטענה שהוכחנו בכיתה). $\sigma \in \ker\psi$ אם"ם $\sigma|_K = id_K, \sigma|_L = id_L$ אם"ם $\sigma|_{KL} = id_{KL}$, כלומר $\sigma = id_{KL}$. לכן, $\ker\psi = \{id_{KL}\}$. מצד שני, בכיתה הראינו שהיות ו-$F = K \cap L$ מתקיים $Gal(KL/L) \cong Gal(K/F)$. לכן, $|Gal(KL/F)| = [KL:F] = [KL:L][L:F] = |Gal(KL/L)| \cdot |Gal(L/F)| = |Gal(K/F)| \cdot |Gal(L/F)|$. כלומר, גודל התחום של ψ שווה לגודל הטווח. היות ו-ψ חח"ע זה אומר ש-ψ איזומורפיזם חבורות. **משל.**

<u>דרך אחרת:</u> היות ו-$F = L \cap K$ נובע ש-$Gal(KL/K) \cong Gal(L/F)$ ו-$Gal(KL/L) \cong Gal(K/F)$ (לפי טענה שהוכחנו בשיעור). שתי החבורות באגף ימין הן תתי חבורות של $Gal(KL/F)$. היות ו-K/F ו-L/F גלואה נובע ש-$Gal(K/F), Gal(L/F) \trianglelefteq Gal(KL/F)$. בנוסף, $Gal\left(\frac{KL}{L}\right) \cap Gal\left(\frac{KL}{K}\right) = \left\{\sigma \in Gal\left(\frac{KL}{F}\right) \mid \sigma|_K = id_K, \sigma|_L = id_L\right\} = \left\{\sigma \in Gal\left(\frac{KL}{F}\right) \mid \sigma|_{KL} = id_{KL}\right\} = \{id_{KL}\}$. נסמן $H = Gal\left(\frac{KL}{K}\right) \cdot Gal\left(\frac{KL}{L}\right)$. אזי מתקיים $KL^H \subseteq (KL)^{Gal\left(\frac{KL}{K}\right)} \cap (KL)^{Gal\left(\frac{KL}{L}\right)} = K \cap L = F$. לכן, $Gal(KL/F) = Gal(KL/KL^H) = H = Gal\left(\frac{KL}{K}\right) \cdot Gal\left(\frac{KL}{L}\right)$. לכן, לפי משפט פיצול חבורות[1] $Gal\left(\frac{KL}{F}\right) \cong Gal\left(\frac{KL}{K}\right) \times Gal\left(\frac{KL}{L}\right) \cong Gal\left(\frac{L}{F}\right) \times Gal\left(\frac{K}{F}\right)$. **משל.**

שאלה 2

1. תהי K/F הרחבת גלואה ממימד סופי. יהי f פולינום אי פריק מעל F ויהי $g \in K[x]$ מחלק ראשוני של f כפולינום <u>מעל K</u>. הוכיחו כי $\deg g \mid \deg f$. (המלצה: התבוננו בפולינומים $(\{\sigma g \mid \sigma \in Gal(K/F)\})$.
2. יהי F שדה ויהיו $F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r$ שדות כך ש-$[L_i : L_{i-1}] = 2$ לכל $0 < i \le r$. נניח ש-L_r/F ספרבילית ויהי E סגור גלואה של L_r מעל F. הוכיחו כי $[E:F]$ הוא חזקת 2.
3. הראו כי אם E/F היא הרחבת גלואה ו-$[E:F]$ היא חזקת 2 אז קיימים שדות $F = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r = E$ כך ש-$[L_i : L_{i-1}] = 2$ לכל $0 < i \le r$. *[רמז: משפט מתורת החבורות קובע שאם p ראשוני, אז לכל חבורה בגודל p^n (חבורת-p) יש מרכז לא טרוויאלי (כלומר שונה מ-$\{e\}$).]*

---

[1] אם G חבורה ו-$H, K \trianglelefteq G$ כך ש-$K \cap H = \{e\}$ וגם $KH = G$ אז $G \cong K \times H$.

הוכחה

הוכחה 1: נסמן $S=\{\sigma g \mid \sigma\in Gal(K/F)\}$. נגדיר $h(x)=\prod_{u(x)\in S}u(x)$. $Gal(K/F)$ פועלת על S (ע"י $\sigma\cdot u=\sigma u$) לכן כל איבר ב-$Gal(K/F)$ משרה תמורה על אברי S . לפיכך, לכל $\sigma\in Gal(K/F)$ מתקיים $\sigma(h)=\prod_{u\in S}\sigma u=\prod_{u\in S}u=h$. לכן, $h\in F[x]$ (כי כל מקדם ב-h נמצא ב-$K^{Gal\left(\frac{K}{F}\right)}=F$). לכל $u\in S$ מתקיים $u=\sigma g$ עבור $\sigma\in Gal(K/F)$. לכן, u ראשוני ובנוסף, $u=\sigma g|\sigma f=f$. לכן, f מתחלק ב-$h=\prod_{u\in S}u=\gcd\{u|u\in S\}$. היות ו-$f$ ראשוני, $\deg f=\deg h$ או $\deg h=0$. האפשרות האחרונה בלתי אפשרית כי $g|h$ ו-$\deg g>0$ כי g ראשוני המחלק את f (ולכן לא הפיך ב-$F[x]$). לכן, $\deg f=\deg h=\sum_{u\in S}\deg u=|S|\cdot\deg g$. **משל.**

הוכחה 2: יהיו $F=L_0\subseteq L_1\subseteq\cdots\subseteq L_r$ כנ"ל. יהי E_i סגור גלואה של L_i/F (L_i/F ספרבילית כי L_r/F ספרבילית ו-$F\subseteq L_i\subseteq L_r$). נוכיח באינדוקציה על i ש-$[E_i:F]$ חזקת 2. <u>זה נכון עבור $i=0$</u> כי סגור גלואה של F/F הוא $E_0=F$.

<u>נניח ש-$[E_{i-1}:F]$ חזקת 2.</u> קיים $a\in L_i\setminus L_{i-1}$ אזי $1<[L_{i-1}[a]:L_{i-1}]\le[L_i:L_{i-1}]=2$ ולכן $[L_{i-1}[a]:L_{i-1}]=2$, כלומר $L_i=L_{i-1}[a]$ ומעלת הפולינום המינימלי של a מעל L_i היא 2. יהי f הפולינום המינימלי של a מעל F ויהי g הפולינום המינימלי של f מעל E_{i-1}. אזי $\deg g\le 2$ (כי $L_{i-1}\subseteq E_{i-1}$). לפי הוכחה 1 נובע ש-$f=\prod_{u\in\left\{\sigma g\middle|\sigma\in Gal\left(\frac{E_{i-1}}{F}\right)\right\}}u$ ולכן, מעל E_{i-1}, f מתפרק לגורמים ממעלה 1 או 2. יהי K שדה פיצול של f מעל E_{i-1} ויהיו $a_1,\dots,a_n$ שורשי f ב-K. נסמן $d_k=\left[E_{i-1}[a_1,\dots,a_k]:E_i[a_1,\dots,a_{k-1}]\right]$. הפולינום המינימלי של a_k מעל E_{i-1} הוא גורם ראשוני של f ולכן ממעלה 2 או 1. לכן, הפולינום המינימלי של a_k מעל $E_{i-1}[a_1,\dots,a_{k-1}]$ הוא 2 או 1, כלומר $d_k\in\{1,2\}$. אבל מתקיים $[K:E_{i-1}]=d_1d_2\dots d_n$ ולכן $[K:E_{i-1}]$ הוא מכפלה של מספרים בקבוצה $\{1,2\}$ ולכן חזקת 2. כעת, לפי הנחת האינדוקציה $[K:F]=[K:E_{i-1}][E_{i-1}:F]$ הוא גם חזקת 2.

$F[a_1,\dots,a_n]$ הוא שדה הפיצול של f מעל F ולכן $F[a_1,\dots,a_n]/F$ גלואה (f ספריבילי כי L_i/F ספרבילית). $K=E_{i-1}\cdot F[a_1,\dots,a_n]$ ולכן K/F גלואה (כקומפוזיטום של שתי הרחבות גלואה).[2] K מכיל את L_i ולכן מכיל סגור גלואה שלו – E_i (למעשה, לא קשה להוכיח ש-$E_i=K$). לכן מתקיים $[E_i:F]\mid[K:F]$. אגף ימין הוא חזקת 2 ולכן $[E_i:F]$ חזקת 2. **משל.**

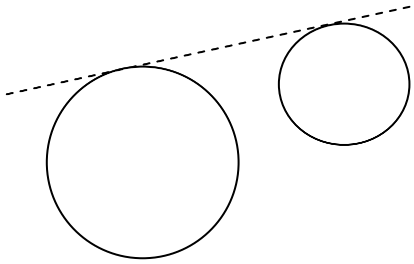
הוכחה 3: אם $E=F$ אז אין מה להוכיח. אחרת, $G=Gal(E/F)$ היא חבורה בגודל חזקת 2 (גדולה מ-1). לפי משפט מתורת החבורות, המרכז של G, $Z(G)$, מכיל יותר מאיבר 1. היות ו-$|G|\mid|Z(G)|$ נובע ש-$|Z(G)|$ חזקת 2 (גדולה מ-1). לכן, לפי משפט קושי, קיימת תת חבורה $H\le Z(G)$ עם $|H|=2$. H מרכזית ב-G ולכן נורמלית. נגדיר $E_0=E^H$. אזי $[E:E_0]=|H|=2$ ו-E_0/F גלואה. לפי אינדוקציה על $[E:F]$, קיימים שדות $F=L_1\subseteq L_2\subseteq\cdots\subseteq L_r=E_0$ כך ש-$[L_i:L_{i-1}]=2$ לכל i. נגדיר $L_{r+1}=E$ ונקבל ש-$F=L_1\subseteq L_2\subseteq\cdots\subseteq L_r\subseteq L_{r+1}$ מקיימת $[L_i:L_{i-1}]=2$ לכל i.
משל.

שאלה 3

נתונים שני מעגלים במישור (ראו ציור). מרכזי המעגלים גם נתונים ורדיוס המעגל הראשון הוא 1. הוכיחו כי ניתן לבנות ע"י סרגל (ללא שנתות) ומחוגה משיק משותף לשני המעגלים (כמו בציור[3]).

[2] זהירות: באופן כללי אם K/E ו-E/F שתי הרחבות גלואה אז K/F לא חייבת להיות גלואה. לכן היינו חייבים להוכיח ישירות ש-K/F גלואה (הנימוק ש-E_{i-1}/F ו-K/E_{i-1} גלואה אינו מספיק).

[3] יש עוד שלושה משיקים משותפים! אין צורך לבנות אותם.



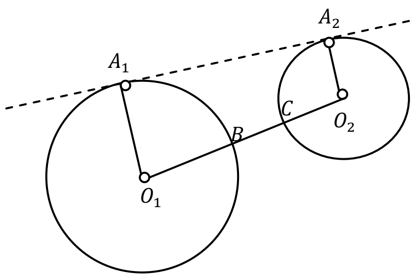
זהירות: רדיוס המעגל השני והמרחק בין מרכזי המעגלים לא חייבים להיות מספרים ברי בנייה.

אתם רשאים להשתמש בעובדות הבאות (שכנראה הוכחתם בהרצאה):

- אם אפשר לבנות את המרחק a אז אפשר לבנות מעגל ברדיוס a סביב כל נקודה שבניתם.
- אם אפשר לבנות את $a, b \in \mathbb{R}_{>0}$ אז אפשר לבנות את $a+b, a-b, ab, a^{-1}, \sqrt{a}$.
- אם אפשר לבנות את $a \in \mathbb{R}_{>0}$ אז אפשר לבנות את aq לכל $q \in \mathbb{Q}_{>0}$.

הערה: אין צורך להסביר איך לבנות את המשיק אלא <u>רק להוכיח שאפשר לבנות אותו</u>.

המלצה: נסו להביע גדלים שאתם צריכים כפונקציה של רדיוסי המעגלים והמרחק בין מרכזי המעגלים.



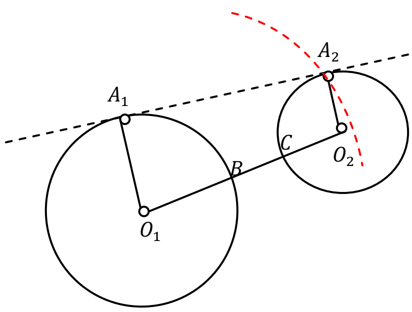
פיתרון

נסמן את מרכזי המעגלים ב-O_1, O_2 ואת נקודות ההשקה ב-A_1, A_2 בהתאמה. נסמן את רדיוסי המעגלים ב-R_1, R_2 ואת המרחק ביניהם ב-L (ראו ציור לא מדוייק בצד; ניתן להניח בה"כ ש- $R_1 = 1$ אך אנו לא נזדקק לכך). אפשר להעביר את הישר המחבר בין O_1, O_2 ולחתוך אותו עם שני המעגלים. כך נקבל נקבל קטעים באורכים R_1, R_2, L (קטעים O_1B, O_2C, O_1O_2 בהתאמה). לכן, הגדלים R_1, R_2, L ניתנים לבנייה.

<u>טענה:</u> $O_1A_2 = \sqrt{L^2 + 2R_1R_2 - R_2^2}$ ו-$O_2A_1 = \sqrt{L^2 + 2R_1R_2 - R_1^2}$

הערה: אנחנו לא בונים את הבניות המוזכרות בהוכחת הטענה.

<u>הוכחת הטענה:</u> נתבונן במרובע $A_1A_2O_2O_1$. הוא טרפז ישר זווית ($\angle A_1 = \angle A_2 = 90°$). נוריד אנך O_2D מ-O_2 אל O_1A_1 . אזי $A_1A_2O_2D$ מלבן ולכן $O_2D = A_1A_2$. לפי משפט פיתגורס על המשולש O_1O_2D נובע ש-$(O_1O_2)^2 = (DO_1)^2 + (DO_2)^2$. לכן, $(A_1A_2)^2 = L^2 - (DO_1)^2 = L^2 - (R_1 - R_2)^2$. לפי משפט פיתגורס על המשולש $A_1A_2O_1$ נקבל $O_1A_2 = \sqrt{(A_1A_2)^2 + (A_1O_1)^2} = \sqrt{L^2 - (R_1 - R_2)^2 + R_1^2} = \sqrt{L^2 + 2R_1R_2 - R_2^2}$. באופן סימטרי, מקבלים $O_2A_1 = \sqrt{L^2 + 2R_1R_2 - R_1^2}$. <u>משל טענה.</u>



בנויים לנו קטעים באורכים R_1, R_2, L ולכן ניתן לבנות את $\sqrt{L^2 + 2R_1R_2 - R_2^2}, \sqrt{L^2 + 2R_1R_2 - R_1^2}$. לכן, ניתן לבנות מעגל שמרכזו ב-O_1 עם רדיוס $\sqrt{L^2 + 2R_1R_2 - R_2^2}$ (ראו באדום מימין). אחת מנקודות החיתוך של המעגל הזה עם המעגל שמרכזו ב-O_2 תהייה A_2. לכן, ניתן לבנות את A_2. באופן דומה ניתן לבנות את A_1. הראינו שניתן לבנות את A_1, A_2 ולכן ניתן לבנות את הישר המחבר ביניהן – שהוא המשיק המשותף לשני המעגלים. **משל.**