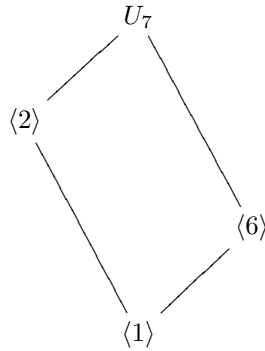


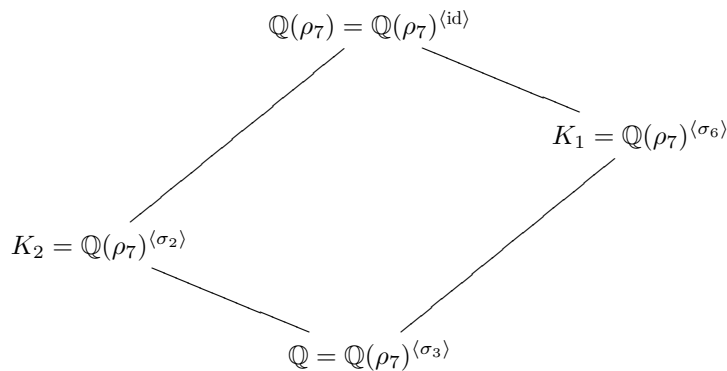
פתרון תרגיל בית 11 בשדות ותורת גלואה 88-311 סמסטר א' תשפ"ב

שאלה 1 (חזרה, ממבחן). רשמו את כל תת־השדות של $\mathbb{Q}(\rho_7)$ (תנו יוצרים לכל תת־שדה).

פתרון. לפי משפט מההרצאה, ההרחבה $\mathbb{Q}(\rho_7)/\mathbb{Q}$ היא גלואה, עם חבורת גלואה $U_7 \cong \mathbb{Z}/6\mathbb{Z}$ (האיזומורפיזם נכון כי 7 ראשוני). נסמן את האוטומורפיזם של $\mathbb{Q}(\rho_7)/\mathbb{Q}$ המתאים ל- $k \in U_7$ על ידי σ_k . סריג תת־החבורות של U_7 הוא



ולכן סריג תת־השדות של ההרחבה $\mathbb{Q}(\rho_7)/\mathbb{Q}$ הוא



כדי לפענח מיהם תת־השדות K_1 ו- K_2 , נבין את תת־החבורות המקבעות אותם. עבור K_1 : מהתאמת גלואה, $[K_1 : \mathbb{Q}] = [\text{Gal}(\mathbb{Q}(\rho_7)/\mathbb{Q}) : \langle \sigma_6 \rangle] = 3$. לפי המבנה של חבורת גלואה בהרחבות ציקלוטומיות, אנחנו יודעים ש- $\rho_7^{-1} = \overline{\rho_7} = \rho_7^6$, כלומר $\sigma_6(\rho_7) = \rho_7^6 = \rho_7^{-1} = \overline{\rho_7}$. לכן $K_1 = \mathbb{Q}(\rho_7) \cap \mathbb{R}$ הוא תת־השדה הממשי המקסימלי של $\mathbb{Q}(\rho_7)$. כיוון שהמימד שלו ראשוני, לכל $a \in K_1 \setminus \mathbb{Q}$ יתקיים $K_1 = \mathbb{Q}(a)$ (ודאו שאתם מבינים מדוע), ולכן אפשר לבחור למשל $a = \rho_7 + \rho_7^6 = 2 \cos \frac{2\pi}{7}$.

עבור K_2 : מהתאמת גלואה, $[K_2 : \mathbb{Q}] = [\text{Gal}(\mathbb{Q}(\rho_7)/\mathbb{Q}) : \langle \sigma_2 \rangle] = 2$. שוב מדובר בשדה ממימד ראשוני מעל \mathbb{Q} , ולכן מספיק למצוא איזשהו $b \in K_2 \setminus \mathbb{Q}$. נבחר למשל את

$$b = \rho_7 + \sigma_2(\rho_7) + \sigma_2^2(\rho_7) = \rho_7 + \rho_7^2 + \rho_7^4$$

קל לוודא ש- b נקבע על ידי σ_2 , ולכן $b \in K_2$. כמו כן, $b \notin \mathbb{Q}$, שהרי $\{\rho_7, \rho_7^2, \dots, \rho_7^6\}$ בסיס של $\mathbb{Q}(\rho_7)/\mathbb{Q}$, וסכומם הוא -1 . אילו $b \in \mathbb{Q}$, היינו מקבלים תלות לינארית ביניהם, בסתירה. לכן $K_2 = \mathbb{Q}(\rho_7 + \rho_7^2 + \rho_7^4)$.

שאלה 2. מצאו שדות ביניים של ההרחבה $\mathbb{Q}[\sqrt[3]{2 + \sqrt{5}}, \sqrt[5]{2}]/\mathbb{Q}$ כך שהרחבות הביניים הן רדיקליות.

פתרון. זאת לא אמורה להיות שאלה קשה:

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[5]{2}] \subseteq \mathbb{Q}[\sqrt[5]{2}, \sqrt{5}] \subseteq \mathbb{Q}[\sqrt[5]{2}, \sqrt{5}, \sqrt[3]{2 + \sqrt{5}}] = \mathbb{Q}[\sqrt[3]{2 + \sqrt{5}}, \sqrt[5]{2}]$$

שאלה 3. יהי שדה F המכיל את שורשי היחידה (לפחות) עד סדר n . הוכיחו כי פולינום $f(x) \in F[x]$ ניתן לפתרון על ידי רדיקלים מעל F אם ורק אם $f(x^n)$ ניתן לפתרון על ידי רדיקלים מעל F .

פתרון. שדה הפיצול של $f(x)$ מעל F בוודאי מוכל בשדה הפיצול של $f(x^n)$. לכן אם $f(x^n)$ פתיר על ידי רדיקלים, אז גם $f(x)$.

בכיוון השני, נניח כי $f(x)$ פתיר על ידי רדיקלים, ונסמן את שורשיו ב- $\alpha_1, \dots, \alpha_m$. לפי ההנחה שדה הפיצול שלו מוכל בהרחבה על-רדיקלית E מעל F . קל לראות ש- $f(x^n)$ מתפצל מעל $E[\sqrt[n]{\alpha_1}, \sqrt[n]{\alpha_2}, \dots, \sqrt[n]{\alpha_m}]$ שזו בבירור הרחבה על-רדיקלית מעל E . ביחד נקבל ש- E' היא הרחבה על-רדיקלית מעל F .

שאלה 4. בדקו האם הפולינומים הבאים ניתנים לפתרון על ידי רדיקלים:

א. $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$

ב. $g(x) = x^6 + 2x^3 + 6i \in \mathbb{Q}[i][x]$

ג. $h(x) \in \mathbb{Q}[x]$ עם שדה פיצול K כך ש- $[K : \mathbb{Q}] = 26$.
רשות: מה אם $[K : \mathbb{Q}] = 88311$?

פתרון.

א. הפולינום $f(x)$ אי פריק לפי קריטריון אייזנשטיין עבור $p = 2$. על ידי חקירת פונקציה נקבל כי

$$f(-\infty) < 0 \quad f(0) = 2 > 0 \quad f(1) = -1 < 0 \quad f(\infty) > 0$$

ולכן נסיק שיש ל- $f(x)$ לפחות שלושה שורשים ממשיים. מפני שמעלתו היא 5, אז יש לו בדיוק 3 או 5 שורשים ממשיים. אילו היו לו 5 שורשים ממשיים, אז לנגזרת שלו $f'(x) = 5x^4 - 4$ היו 4 שורשים ממשיים לפי משפט רול, אבל יש לה רק שניים. לכן ל- $f(x)$ יש $3 = 5 - 2$ שורשים ממשיים ובדיוק שני שורשים מרוכבים, ולפי תרגיל שעשינו בכיתה חבורת גלואה שלו (שהיא טרנזיטיבית על קבוצת השורשים) היא S_5 . מפני ש- S_5 אינה פתירה, אזי $f(x)$ לא פתיר על ידי רדיקלים.

ב. באופן דומה למה שעשינו בכיתה, נציב $t = x^3$, נקבל פולינום ריבועי ב- t שכמוכן יהיה פתיר על ידי רדיקלים. את $t = x^3$ ניתן לפתור על ידי רדיקלים ולכן יחד נקבל שהפולינום הנתון ניתן לפתרון על ידי רדיקלים.

ג. נתון שחבורת גלואה היא מסדר 26, ולמעשה צריך לבדוק האם היא פתירה. נטען שכל חבורה מסדר $26 = 2 \cdot 13$ מכילה איבר מסדר 13. זה נכון לפי משפט קושי, או בפירוט: הסדר האפשרי של איברים בחבורה הוא 1, 2, 13, 26. אחרת, אם כל האיברים שאינם טריוויאלים הם מסדר 2, אז לכל זוג איברים a, b לא טריוויאלים מתקיים

$$\langle a, b \rangle = \{e, a, b, ab\}$$

שהיא תת-חבורה מסדר 4, שאינו מחלק את 26, סתירה. אז קיים איבר מסדר 26 (ואז ההרחבה ציקלית) או 13. תת-החבורה שיוצר איבר מסדר 13 היא מאינדקס 2 ולכן נורמלית, ומכאן ש- G פתירה. כהערת אגב, חבורה מסדר 26 איזומורפית ל- $\mathbb{Z}/26\mathbb{Z}$ או ל- D_{13} . לכן $h(x)$ פתיר על ידי רדיקלים. גם במקרה שבו $|G| = 88311 = 3 \cdot 29437$ נקבל שההרחבה פתירה. ישנן שתי חבורות מסדר זה עד כדי איזומורפיזם והן $\mathbb{Z}/88311\mathbb{Z}$ ו- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/29437\mathbb{Z}$. לפי משפט ברנסייד כל חבורה סופית שיש לסדר שלה לכל היותר שני מחלקים ראשוניים היא פתירה. לפי משפט פייט-תומפסון, שהוא עוד יותר מסובך להוכחה ממשפט ברנסייד, כל חבורה מסדר אי זוגי היא פתירה.

שאלה 5. הגיעו לפחות עד שלב 8 במשחק [Euclid: The Game](#).

שאלה 6. הוכיחו כי ניתן לבנות מצולע משוכלל עם n צלעות אם ורק אם המספר $\cos \frac{2\pi}{n}$ בר-בנייה. רמז שהוא כמעט פתרון: מצולע משוכלל החסום במעגל היחידה.

פתרון. נניח שניתן לבנות כזה מצולע משוכלל שמרכזו ב- $(0, 0)$, ובלי הגבלת הכלליות אחד מקודקודיו הוא $(1, 0)$, כי אנחנו יודעים להזיז קטעים ולהגדיל (או להקטין) אותם ביחס בר-בנייה. נביט על הקודקוד ה"ראשון" מעל ציר x (אם זזים נגד כיוון השעון). נוריד ממנו אנך לציר x . הוא פוגש אותו בדיוק בנקודה $(\cos \frac{2\pi}{n}, 0)$. בכיוון השני, נצייר אנך לציר x העובר דרך $(\cos \frac{2\pi}{n}, 0)$. נצייר מעגל ברדיוס 1 שמרכזו בראשית הצירים, הם נפגשים בקודקוד של המצולע, שאר הקודקודים נבנים בדרך דומה.

שאלה 7. תהי E/F הרחבת גלואה שהיא ריבועית חוזרת, ויהי שדה ביניים K . הוכיחו כי גם K/F ריבועית חוזרת.

פתרון. נסמן $G = \text{Gal}(E/F)$ ו- $H = \text{Gal}(E/K)$. נתון כי G היא חבורת-2. לכן G פתירה ויש לה סדרת הרכב

$$\{\text{id}\} = G_n \subseteq G_{n-1} \subseteq \dots \subseteq G_0 = G$$

כך ש- $[G_{i-1} : G_i] = 2$ לכל i . כלומר $G_{i-1}/G_i \cong \mathbb{Z}/2\mathbb{Z}$. כעת נסתכל על $[HG_{i-1} : HG_i]$ ונשים לב שמתקיים

$$G_i \subseteq HG_i \cap G_{i-1} \subseteq G_{i-1}$$

מפני ש- G_{i-1}/G_i היא חבורה פשוטה, אחת ההכלות האלה היא שיוויון (אפשר גם לפי משפט האיזומורפיזם השני

$$HG_{i-1}/HG_i \cong G_{i-1}/(HG_i \cap G_{i-1})$$

ולחשב את החיתוך). לכן $[HG_{i-1} : HG_i] = 2$. כלומר יש סדרה של תת-חבורות

$$H = HG_r \subseteq HG_{r-1} \subseteq \dots \subseteq HG_0 = G$$

שסדר המנות בו הוא בדיוק 2, אחרי שהורדנו את אלו עם אינדקס 1. זה למעשה מקרה פרטי לתרגיל מתורת החבורות לפיו כל תת-חבורה וכל מנה של חבורת- p היא חבורת- p . כעת נגדיר $L_j = E^{HG_j}$ לכל $1 \leq j \leq r$ ולפי משפט ההתאמה הם מהווים סדרה של שדות ביניים

$$F = E^{HG_0} \subseteq \dots \subseteq E^H = K$$

כשהרחבות ריבועיות, כדרוש.

שאלה 8. בדקו האם ניתן לבנות את המספרים הבאים בעזרת סרגל ומחוגה.

א. $e^{2\pi i/15}$.

ב. $\sqrt[5]{3}$.

ג. $\sqrt[n]{2}$ כתלות ב- $n \in \mathbb{N}$.

פתרון.

א. כן. זה שורש יחידה פרמיטיבי מסדר 15 ולכן חבורת גלואה של הפולינום המינימלי שלו $\Phi_{15}(x)$ היא U_{15} . הסדר של U_{15} הוא $\varphi(15) = 8$, וזו חזקה של 2, ולכן חבורת גלואה היא חבורת-2.

ב. לא. הפולינום המינימלי הוא $x^5 - 3$ שמעלתו אינה חזקת 2, ולכן המספר לא ניתן לבניה (כי הסדר של חבורת גלואה המתאימה יתחלק ב-5).

ג. לפעמים. הפולינום המינימלי הוא $x^n - 2$. לכן אם n אינו חזקת 2, אז אי אפשר לבנות. אם $n = 2^k$, אז אפשר כי אנחנו יודעים ששדה המספרים בני-הבניה סגור להוצאת שורש. ולכן $2, \sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \dots$ הם בני-בניה. זה שקול למציאת שדות ביניים של $\mathbb{Q}(\sqrt[n]{2})/\mathbb{Q}$.

שאלה 9. האם ניתן לחלק זזית לחמש בעזרת סרגל ומחוגה?

פתרון. לא. למרות שכן ניתן לבנות את הזזית $e^{2\pi i/5}$ כפי שראינו בתרגול (או ששמים לב כי $(e^{2\pi i/15})^3 = e^{2\pi i/5}$ וממשיכים לפי השאלה הקודמת). אם היה ניתן לחלק זזית לחמש, אז היה אפשר גם לבנות את $e^{2\pi i/25}$ ובמקרה הזה $\varphi(25) = 20$, שזו אינה חזקת 2.

שאלה 10 (העשרה). קראו על **בניות מפתיעות עם סרגל ומחוגה** מאת מוטי בן-ארי (או באנגלית). שימו לב שתורת גלואה לא מוזכרת שם.

בהצלחה!