פתרון מועד ב' שנת תשעה

תרגיל 1.1 צייר את דיאגרמת תת השדות של שדה הפיצול של x^3-3 מעל $\mathbb{Q}$.

פתרון: ראשית צריך להבין מה שדה הפיצול. נסמן ב $\rho = e^{\frac{2\pi i}{3}} = -\frac{1}{2}+\frac{\sqrt{3}}{2}i$, דהיינו, שורש 3 פרימיטבי של 1. לפולינום יש שלושה שורשים

$$\sqrt[3]{3},\ \sqrt[3]{3}\rho,\ \sqrt[3]{3}\rho^2$$

ולכן שדה הפיצול הוא

$$\mathbb{Q}(\sqrt[3]{3},\ \sqrt[3]{3}\rho,\ \sqrt[3]{3}\rho^2)$$

קל לוודא שהשדה הזה שווה בעצם ל

$$\mathbb{Q}(\sqrt[3]{3},\rho)$$

(על ידי הכלה דו כיוונית)

נסמן את שדה הפיצול ב E.

השלב הבא הוא למצוא את המימד $[E:\mathbb{Q}]$. היות ש x^3-3 לא פריק (אייזנשטיין עם $p=3$), הוא הפולינום המינימלי של $\sqrt[3]{3}$ אז המימד

$$[\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}]=3$$

כעת $\rho\notin\mathbb{Q}(\sqrt[3]{3})$ (הוא מרוכב והשדה הזה מכיל רק ממשיים). ולכן

$$[E:\mathbb{Q}(\sqrt[3]{3})]\neq 1$$

מצד שני, הפולינום המינימלי של ρ מעל $\mathbb{Q}$ הוא x^2+x+1 ממעלה 2. לכן הפולינום המינימלי של ρ מעל $\mathbb{Q}(\sqrt[3]{3})$ הוא לכל היותר ממעלה 2 ולכן

$$[E:\mathbb{Q}(\sqrt[3]{3})]\leq 2$$

ממילא נקבל

$$[E:\mathbb{Q}(\sqrt[3]{3})]=2$$

ולפי כפליות

$$[E:\mathbb{Q}]=6$$

כעת נבין מה חבורת גלואה $G=\mathrm{Gal}(E/\mathbb{Q})$. ראשית נשים לב כי $E/\mathbb{Q}$ היא הרחבת גלואה (ספרבילי כי זה מאפיין 0 ונורמלי כי E הוא שדה פיצול של פולינום).

לכן חבורת גלואה היא מגודל 6. בנוסף G מבצעת פרמוטציה על שלושת שורשי הפולינום x^3-3 ולכן היא משוכנת ב S_3. היות שהגודל של S_3הוא כבר 6 נקבל ש $G\cong S_3$.

עכשיו לשאלה, מבקשים למצוא תתי שדות של E. כל תת שדה של E חייב להכיל את $\mathbb{Q}$ (כל שדה ממאפיין 0 מכיל את $\mathbb{Q}$) ולכן השאלה שקולה למציאת שדות ביניים בין E ל $\mathbb{Q}$. לפי

התאמת גלואה הסריג של שדות הביניים אנטי איזומורפי לסריג תתי החבורות של $G \cong S_3$.
ל S_3 יש 4 תתי חבורות אמיתיות. סריג תתי החבורות של S_3 הוא:

$$S_3$$

$$A_3 \qquad \langle (12) \rangle \qquad \langle (23) \rangle \qquad \langle (13) \rangle$$

$$\{1\}$$

לכן בהתאמה יש 4 שדות ביניים בין E ל $\mathbb{Q}$(חוץ מ E ו $\mathbb{Q}$ עצמם).

שדות הביניים האלה הם: $\mathbb{Q}(\rho)$ שמתאים ל A_3 (כי $[S_3 : A_3] = 2 = [\mathbb{Q}(\rho) : \mathbb{Q}]$).
ו $\mathbb{Q}(\sqrt[3]{3}), \mathbb{Q}(\sqrt[3]{3}\rho), \mathbb{Q}(\sqrt[3]{3}\rho^2)$. איך יודעים שכל אלה שונים? אפשר לבדוק ישירות אבל אפשר גם להשתמש בהתאמת גלואה. לפי התאמת גלואה השדות שאנחנו מחפשים הם

$$E^{\langle (12) \rangle} = E^{(12)}$$

$$E^{\langle (23) \rangle} = E^{(23)}$$

$$E^{\langle (13) \rangle} = E^{(13)}$$

אם אנחנו ממספרים את שורשי הפולינום $x^3 - 3$ לפי $\sqrt[3]{3}, \sqrt[3]{3}\rho, \sqrt[3]{3}\rho^2$ אז הפרמוטציה (12) מחליפה את שני הראשונים ומקבעת את $\sqrt[3]{3}\rho^2$. לכן

$$\mathbb{Q}(\sqrt[3]{3}\rho^2) \subseteq E^{\langle (12) \rangle}$$

אבל

$$[\mathbb{Q}(\sqrt[3]{3}\rho^2) : \mathbb{Q}] = 3$$

ו

$$[E^{\langle (12) \rangle} : \mathbb{Q}] = [S_3 : \langle (12) \rangle] = 3$$

ולכן

$$\mathbb{Q}(\sqrt[3]{3}\rho^2) = E^{\langle (12) \rangle}$$

כנ"ל עבור שאר השדות.

תרגיל 1.2 הוכח: חבורת גלואה של שדה הפיצול של הפולינום המינימלי של מספר בר בניה הוא מסדר חזקת 2.

פתרון: נניח ש a הוא המספר בר הבניה המדובר. נסמן ב $f(x)$ את הפולינום המינימלי וב E את שדה הפיצול. נסמן את השורשים של $f(x)$ ב

$$a = a_1, a_2, \ldots, a_n$$

היות ש a הוא בר בניה הוא מוכל בשדה L כלשהוא שהוא מוגדר ריבועית (=הרחבה ריבועית חוזרת). תת שדה של שדה מוגדר ריבועית הוא גם מוגדר ריבועית (יש לזה הוכחה במערך תרגול 12, לא טענה טריויאלית) ולכן גם $\mathbb{Q}(a)$ מוגדר ריבועית.

היות שלכל i מתקיים ש

$$\mathbb{Q}(a_i) \cong \mathbb{Q}(a)$$

(יש ל a ול a_i אותו פולינום מינימלי) נקבל שלכל i, $\mathbb{Q}(a_i)$ הוא מוגדר ריבועית. עכשיו נזכור ש

$$E = \mathbb{Q}(a_1, \ldots, a_n) = \mathbb{Q}(a_1)\mathbb{Q}(a_2)\cdots\mathbb{Q}(a_n)$$

(כזכור KL הוא השדה הקטן ביותר שמכיל גם את K וגם את L). נזכור שאם K מוגדר ריבועית ו L מוגדר ריבועית את גם KL מוגדר ריבועית (הוכחה נמצאת במערך תרגול 12) ולכן גם E מוגדר ריבועית. כל שדה מוגדר ריבועית הוא ממימד שהוא חזקת 2. כמובן ש $E/\mathbb{Q}$ היא הרחבת גלואה (נורמלית כי E שדה פיצול וספרבילית כי המאפיין 0) ולכן הגודל של חבורת גלואה הוא המימד של E מעל $\mathbb{Q}$ שהוא חזקת 2 ובזה סיימנו.

תרגיל 1.3 מצא את כל הפולינומים האי פריקים מעל $\mathbb{Z}_2$ מדרגה 4.

פתרון: ראשית נמצא כמה כאלה יש. נסמן ב $n_q(k)$ את מספר הפולינומים האי פריקים (המתוקנים) ממעלה k מעל $\mathbb{F}_q$. לפי משפט מההרצאה מכפלת כל הפולינום המתוקנים ממעלה שמחלקת את k היא $x^{q^k} - x$ ולכן לפי השוואת דרגות מתקיים

$$q^k = \sum_{d|k} d n_q(d)$$

במקרה שלנו $q = 2$. מתקיים $n_2(1) = 2$ (כי שני הפולינום המתוקנים ממעלה 1 הם אי פריקים). לפי הנוסחא למעלה עבור $k = 2$ נקבל ש

$$2^2 = 1n_2(1) + 2n_2(2)$$

נפתור ונקבל

$$n_2(2) = 1$$

עכשיו נשתמש שוב בנוסחא עם $k = 4$ ונקבל

$$2^4 = 1n_2(1) + 2n_2(2) + 4n_2(4)$$

כלומר

$$16 = 2 + 2 + 4n_2(4)$$

$$n_2(4) = 3$$

אז יש בסה"כ שלושה פולינומים. צריך למצוא אותם. פולינום ממעלה 4 נראה ככה:

$$x^4 + ax^3 + bx^2 + cx + d$$

כאשר $a,b,c,d \in \mathbb{Z}_2$. אם אנחנו רוצים פולינום אי פריק חייבים ש $d=1$ (אחרת 0 הוא שורש).

ולכן הפולינום הוא

$$x^4+ax^3+bx^2+cx+1$$

נותרו 8 אופציות: לא ייתכן שרק אחד מבין a,b,c הוא 0 כי אז 1 הוא שורש. בדומה לא ייתכן שכולם 0 (שוב 1 הוא שורש). נותרנו עם 4 אופציות:

$$x^4+x^3+x^2+x+1$$

$$x^4+x^3+1$$

$$x^4+x^2+1$$

$$x^4+x+1$$

נותרה עוד אופציה אחת לפסול. נשים לב ש

$$(x^2+x+1)^2=x^4+x^2+1$$

ולכן בהכרח 3 הפולינומים שנשארו הם האי פריקים

$$x^4+x^3+x^2+x+1, \quad x^4+x^3+1, \quad x^4+x+1$$

תרגיל 1.4 הוכח: אם K הרחבה של $\mathbb{R}$ אז $[K:\mathbb{R}]$ חזקה של 2.

פתרון: שלב ראשון: נוכיח שלכל הרחבה L של $\mathbb{R}$ מתקיים ש $[L:\mathbb{R}]$ זוגי. הסבר: ניקח $a \in L \backslash \mathbb{R}$. הפולינום המינימלי של a מעל $\mathbb{R}$ הוא אי פריק ולכן ממעלה זוגית (לכל פולינום ממעלה אי זוגית מעל $\mathbb{R}$ יש הרי שורש). ולכן

$$[\mathbb{R}(a):\mathbb{R}]$$

הוא מספר זוגי (הוא שווה לדרגת הפולינום המינימלי) ולכן

$$[L:\mathbb{R}]=[L:\mathbb{R}(a)][\mathbb{R}(a):\mathbb{R}]$$

גם כן זוגי.

כעת נוכיח ש $[K:\mathbb{R}]$ הוא חזקת 2. נסתכל על הסגור הנורמלי של K, נניח E. אם נוכיח ש $[E:\mathbb{R}]$ הוא חזקת 2 סיימנו. נניח בשלילה שהוא לא כלומר נניח $[E:\mathbb{R}]=2^m k$ כאשר k אי זוגי גדול מ 1. נשים לב שההרחבה היא גלואה כי היא נורמלית והמאפיין הוא 0 ולכן היא גם ספרבילית. נסתכל על החבורת גלואה

$$G=\mathrm{Gal}(E/\mathbb{R})$$

לפי תורת החבורות קיימת לה תת חבורה 2 סילו מסדר 2^m, נקרא לה H.

$$[G:H]=k$$

ולכן לפי התאמת גלואה

$$[E^H:\mathbb{R}]=k$$

בסתירה לכך שאין הרחבות ממימד אי זוגי. ולכן המימד של E (ולכן של K) הוא חזקת 2.

הערה: אפשר לחשוב מהשאלה של $\mathbb{R}$ יש מליון הרחבות סופית. בפועל ההרחבות הסופיות היחידות שלו הן $\mathbb{R},\mathbb{C}$.

תרגיל 1.5 תן דוגמא של הרחבה $E/\mathbb{Q}$ כאשר $\mathrm{Gal}(E/\mathbb{Q})\cong\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2$.

פתרון: אפשרות מתאימה היא למשל

$$E=\mathbb{Q}(\sqrt{2},\sqrt{3},i)$$

איך יודעים מה החבורת גלואה? ראשית נשים לב ש

$$[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$$

היות ש

$$\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$$

(קל לוודא ע"י השוואה $\sqrt{3}=a+b\sqrt{2}$ והעלאה בריבוע) ולכן x^2-3 אי פריק מעל $\mathbb{Q}(\sqrt{2})$ ולכן

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$$

כמו כן,

$$i\notin\mathbb{Q}(\sqrt{2},\sqrt{3})$$

(זה שדה ממשי) ולכן x^2+1 אי פריק מעל $\mathbb{Q}(\sqrt{2},\sqrt{3})$ ולכן

$$[E:\mathbb{Q}(\sqrt{2},\sqrt{3})]=2$$

ולכן בסך הכל

$$[E:\mathbb{Q}]=8$$

בנוסף E שדה פיצול של הפולינום הספרבילי $(x^2-2)(x^2-3)(x^2+1)$ ולכן זו הרחבת גלואה וגם הסדר של חבורת גלואה הוא 8. אז הגודל מתאים.

כעת נשים לב שאם φ אוטומורפיזם בחבורת גלואה הוא חייב לשלוח שורש של (x^2-2) לשורש אחר ולכן

$$\varphi(\sqrt{2})=\pm\sqrt{2}$$

בדומה

$$\varphi(\sqrt{3}) = \pm\sqrt{3}$$

$$\varphi(i) = \pm i$$

בגלל ששלושת אלה יוצרים את כל E אנחנו נקבל שהסדר של φ הוא 2 או 1. ולכן כל איבר הוא מסדר 2 (לכל היותר) חבורה כזאת חייבת להיות אבלית. חבורה אבלית מסדר 8 עם איברים מסדר 2 לכל היותר חייבת להיות $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

הערה: דרך אחרת להוכיח היא באמצעות משפט שראינו במערך תרגול 13 (תרגיל 13.7).