פתרון תרגיל בית 5 בשדות ותורת גלואה
88-311 סמסטר א' תשפ"ב

שאלה 1 (חימום)**.** הוכיחו ששדות הפיצול של $(x^2-2x-2)(x^2+1)$ ושל $x^5-3x^3+x^2-3$ מעל $\mathbb{Q}$ זהים זה לזה.

פתרון. נשים לב כי

$$x^5-3x^3+x^2-3=(x^3+1)(x^2-3)=(x+1)(x^2-x+1)(x^2-3).$$

השורשים של הפולינום הזה הם $-1,\pm\sqrt{3},\frac{1\pm\sqrt{-3}}{2}$, ולכן שדה הפיצול שלו הוא

$$\mathbb{Q}(\pm\sqrt{3},\frac{1\pm\sqrt{-3}}{2})=\mathbb{Q}(\sqrt{3},\sqrt{-3})=\mathbb{Q}(\sqrt{3},i).$$

מצד שני, השורשים של $(x^2-2x-2)(x^2+1)$ הם $\pm i,\frac{2\pm\sqrt{12}}{2}=1\pm\sqrt{3}$, ולכן שדה הפיצול שלו הוא גם $\mathbb{Q}(\sqrt{3},i)$.

שאלה 2. תהי K/F הרחבת שדות ויהיו $f,g\in F[x]$ פולינומים עם שדות פיצול L_1,L_2 בהתאמה. הוכיחו כי תת־השדה הכי קטן של K שמכיל את L_1 ו-L_2 הוא גם שדה פיצול מעל F (אולי של פולינום אחר).

פתרון. יהי L שדה הפיצול של המכפלה $f\cdot g$ מעל F. מצד אחד כל השורשים של f,g נמצאים ב-L ולכן L מכיל את L_1,L_2. מצד שני, אם L' הוא שדה אחר המכיל את L_1,L_2, אז הוא מכיל גם את כל השורשים של f,g ולכן הוא מפצל את $f\cdot g$. לכן לפי ההגדרה של שדה פיצול $L\subseteq L'$ כנדרש.

שאלה 3. יהי פולינום $f(x)\in F[x]$, ויהיו $\alpha_1,\dots,\alpha_n$ כל שורשי הפולינום.
הוכיחו כי שדה הפיצול של $f(x)$ מעל F הוא $F[\alpha_2,\dots,\alpha_n]$.

פתרון. נסמן את הפולינום $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_0$ כאשר $a_i\in F$. מעל שדה הפיצול $f(x)=(x-\alpha_1)\cdots(x-\alpha_n)$ נכפול ונקבל שהמקדם החופשי הוא

$$\alpha_1\cdots\alpha_n=a_0\in F$$

לכן $\alpha_1=\frac{a_0}{\alpha_2\cdots\alpha_n}\in F[\alpha_2,\dots,\alpha_n]$ ומכאן ששדה הפיצול הוא $F[\alpha_1,\dots,\alpha_n]=F[\alpha_2,\dots,\alpha_n]$.

שאלה 4. תהי K/F הרחבת שדות ממימד 2. הסיקו מהשאלה הקודמת ש-K הוא שדה פיצול של פולינום כלשהו ב-$F[x]$.

פתרון. ניקח $\alpha\in K\backslash F$. ברור ש-$K=F(\alpha)$ ולכן הפולינום המינימלי של α ממעלה 2. כלומר

$$f(x)=x^2+bx+c$$

נניח שהמאפיין של השדות שונה מ-2, אזי השורשים הם כמובן

$$\frac{-b\pm\sqrt{b^2-4c}}{2}$$

מפני ש-$\alpha\in K$ קל לראות ש-$\sqrt{b^2-4c}\in K$, ולכן גם השורש השני ב-K. כלומר K שדה מפצל של הפולינום. היות ואין עוד שדות בין K לבין F, אז K הוא שדה הפיצול.
פתרון שמתאים לכל מאפיין: α הוא שורש של הפולינום $f(x)$ שלמעלה. לכן ב-K מתקיים

$$x-\alpha \mid f(x)$$

אבל $f(x)$ בסך הכל ממעלה 2 וזה אומר שב- K מתקיים $f(x)=(x-\alpha)(x-\beta)$. לכן $\alpha^{-1}\cdot\alpha\beta=\beta\in K$ כי $\alpha^{-1}\in K$ וגם $\alpha\beta\in F\subseteq K$. לכן K מפצל את $f(x)$, והוא ממש שדה הפיצול כי כל שדה קטן יותר יהיה F בעצמו.

שאלה 5. יהיו $a_1,\dots,a_n\neq\pm1$ מספרים טבעיים חופשיים מריבועים וזרים בזוגות. הוכיחו כי $\left[\mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_n}):\mathbb{Q}\right]=2^n$.

פתרון. נוכיח את הטענה באינדוקציה על n.

עבור $n=1$, נשים לב כי $\sqrt{a_1}\notin\mathbb{Q}$ כי a_1 אינו מספר ריבועי, ומצד שני הוא שורש של הפולינום $x^2-a_1\in\mathbb{Q}[x]$. נסיק שהפולינום x^2-a_1 הוא הפולינום המינימלי של $\sqrt{a_1}$, ולכן $\left[\mathbb{Q}(\sqrt{a_1}):\mathbb{Q}\right]=2$.

נניח שהטענה נכונה לכל בחירה של לכל היותר n מספרים $a_1,\dots,a_n$, ונוכיח עבור בחירה של $n+1$ מספרים. יהיו $a_1,\dots,a_{n+1}$ מספרים טבעיים חופשיים מריבועים וזרים בזוגות. לכל $1\le m\le n+1$, נסמן $K_m=\mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_m})$. מכפליות המימד ומהנחת האינדוקציה, נקבל $[K_{n+1}:\mathbb{Q}]=[K_{n+1}:K_n]\cdot[K_n:\mathbb{Q}]=[K_{n+1}:K_n]\cdot 2^n$; מנימוק דומה למקרה $n=1$, מספיק יהיה להוכיח ש-$\sqrt{a_{n+1}}\notin K_n$ ומכך נסיק $[K_{n+1}:K_n]=2$ ונקבל את הדרוש.

אכן, נניח בשלילה $\sqrt{a_{n+1}}\in K_n$. נשים לב כי $K_n=K_{n-1}+K_{n-1}\sqrt{a_n}$, במובן שכל איבר של K_n אפשר לכתוב בצורה $\alpha+\beta\sqrt{a_n}$ עבור אילושהם $\alpha,\beta\in K_{n-1}$. לכן $\sqrt{a_{n+1}}=\alpha+\beta\sqrt{a_n}$ כאשר $\alpha,\beta\in K_{n-1}$. נעלה בריבוע ונקבל

$$a_{n+1}=\alpha^2+2\alpha\beta\sqrt{a_n}+\beta^2a_n$$

ומכאן $2\alpha\beta\sqrt{a_n}=a_{n+1}-\alpha^2-\beta^2a_n\in K_{n-1}$. כיוון ש-$\sqrt{a_n}\notin K_{n-1}$ (אחרת $[K_n:\mathbb{Q}]=[K_{n-1}:\mathbb{Q}]=2^{n-1}$), נקבל שבהכרח $\alpha=0$ או $\beta=0$. לא ייתכן ש-$\beta=0$, אחרת $\sqrt{a_{n+1}}=\alpha\in K_{n-1}$, וזו תהיה סתירה להנחת האינדוקציה (כי אז $\left[\mathbb{Q}(\sqrt{a_1},\dots,\sqrt{a_{n-1}},\sqrt{a_{n+1}}):\mathbb{Q}\right]=2^{n-1}$). לכן בהכרח $\alpha=0$, כלומר קיבלנו $\sqrt{a_{n+1}}=\beta\sqrt{a_n}$ לאיזשהו $\beta\in K_{n-1}$.

כעת נחסיר $\sqrt{a_n}$ משני האגפים; נקבל

$$\sqrt{a_{n+1}}-\sqrt{a_n}=(\beta-1)\sqrt{a_n}$$

ואם נכפול בצמוד של אגף שמאל נקבל

$$a_{n+1}-a_n=(\beta-1)\sqrt{a_n}(\sqrt{a_{n+1}}+\sqrt{a_n})=(\beta-1)(\sqrt{a_na_{n+1}}+a_n).$$

בהכרח $\beta\neq1$, כי $a_n\neq a_{n+1}$; לכן נוכל לכתוב

$$\sqrt{a_na_{n+1}}=\frac{a_{n+1}-a_n}{\beta-1}-a_n\in K_{n-1}$$

וזו שוב סתירה להנחת האינדוקציה, כי $a_1,\dots,a_{n-1},a_na_{n+1}$ גם הם חופשיים מריבועים וזרים בזוגות.

הראינו $\sqrt{a_{n+1}}\notin K_n$, לכן מהנימוק הנ"ל $[K_{n+1}:K_n]=2$, ונקבל $[K_{n+1}:\mathbb{Q}]=2^{n+1}$, כנדרש.

בהצלחה!