פתרון תרגיל בית 4 בשדות ותורת גלואה
88-311 סמסטר א' תש"ף

שאלה 1. יהי $f(x)\in F[x]$ פולינום אי פריק ממעלה n, ותהי K/F הרחבה מממד m. הראו שאם $(n,m)=1$, אז $f(x)$ הוא אי פריק גם מעל K.

פתרון. נתבונן בהרחבה $K\left[a\right]/F$ עבור a שורש כלשהו של $f(x)$. מצד אחד

$$[K[a]\colon F]=[K[a]\colon K]\,[K\colon F]=[K[a]\colon K]\cdot m$$

ובנוסף, $n=[F[a]\colon F]\mid[K[a]\colon F]$ (הממד הוא n כי הפולינום המינימלי של a הוא $f(x)$, שמתאפס ב-a ואי-פריק). לכן $n\mid[K[a]\colon K]\cdot m$ ומהנתון $(n,m)=1$ נסיק $n|\,[K[a]\colon K]$. מצד שני לפי למה מהכיתה $[K[a]\colon K]\leq[F[a]\colon F]=n$.

לכן $[K[a]\colon K]=n$. כלומר המעלה של הפולינום המינימלי של a מעל K היא גם n, ולכן $f(x)$ הוא הפולינום המינימלי מעל K (הוא מוגדר שם, מתאפס, ובמעלה הנכונה) מה שאומר שהוא אי-פריק מעל K.

שאלה 2 (אימון נוסף)**.** מצאו את הפולינום המינימלי של האיברים הבאים מעל השדה המצויין:

א. $\sqrt[3]{7}$ מעל $\mathbb{Q}$.

ב. $\sqrt[3]{7}$ מעל $\mathbb{Q}(\sqrt{2},\sqrt{3})$. רמז: העזרו בשיקולי ממד.

ג. $\sqrt[3]{7}$ מעל $\mathbb{Q}\left[\sqrt[5]{7}\right]$.

ד. $\sqrt[4]{3}$ מעל $\mathbb{Q}[\sqrt{3}]$.

ה. $\sqrt{x}-1$ מעל $\mathbb{Q}(x)$.

פתרון.

א. $\sqrt[3]{7}$ מאפס את הפולינום x^3-7 שהוא אי פריק מעל $\mathbb{Q}$ לפי אייזנשטיין עבור 7, ולכן זה הפולינום המינימלי המבוקש.

ב. כבר ראינו כי x^3-7 מאפס את $\sqrt[3]{7}$. השאלה היא האם הוא אי פריק גם ב-$\mathbb{Q}(\sqrt{2},\sqrt{3})$. נניח שהוא פריק. כלומר יש לו שורש $a\in\mathbb{Q}(\sqrt{2},\sqrt{3})$. אז כמובן $\mathbb{Q}(a)\subseteq\mathbb{Q}(\sqrt{2},\sqrt{3})$, אבל $[\mathbb{Q}(a):\mathbb{Q}]=3$ וכבר חישבנו

$$[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}]=4$$

בסתירה לכפליות הממד של הרחבת שדות. לכן x^3-7 אי פריק והוא הפולינום המינימלי של $\sqrt[3]{7}$ גם מעל $\mathbb{Q}(\sqrt{2},\sqrt{3})$. זה מקרה פרטי של שאלה 1.

ג. זה מקרה פרטי נוסף של שאלה 1. חישבנו ש-$\left[\mathbb{Q}[\sqrt[3]{7}]\colon\mathbb{Q}\right]=3$, וקל לחשב ש-$\left[\mathbb{Q}[\sqrt[5]{7}]\colon\mathbb{Q}\right]=5$. לכן הפולינום x^3-7 הוא שוב הפולינום המינימלי.

ד. $\sqrt[4]{3}$ מאפס את x^4-3. מעל $\mathbb{Q}[\sqrt{3}]$ הפולינום הזה מתפרק ל-$(x^2-\sqrt{3})(x^2+\sqrt{3})$ כאשר הרכיב $x^2-\sqrt{3}$ מתאפס ב$\sqrt[4]{3}$.
הפולינום המינימלי הוא בודאי לא לינארי כי $\sqrt[4]{3}\notin\mathbb{Q}[\sqrt{3}]$ (לא יכול להיות $\sqrt[4]{3}=a+b\sqrt{3}$ כי אנחנו יודעים ש-$1,\sqrt[4]{3},\left(\sqrt[4]{3}\right)^2,\left(\sqrt[4]{3}\right)^3$ הם בת"ל מעל $\mathbb{Q}$ לפי השדה $\mathbb{Q}[\sqrt[4]{3}]$). לכן הפולינום המינימלי הוא $x^2-\sqrt{3}$.

ה. נסמן $\alpha=\sqrt{x}-1$. נמצא פולינום המאפס את α לפי

$$(\alpha-1)^2=x$$
$$\alpha^2-2\alpha+(1-x)=0$$

לכן α מאפס את הפולינום $\lambda^2-2\lambda+(1-x)\in\mathbb{Q}(x)[\lambda]$. הפולינום המינימלי לא יכול להיות לינארי (כי $\sqrt{x}\notin\mathbb{Q}(x)$ משיקולי מעלה), ולכן זהו הפולינום המינימלי.

שאלה 3. יהי $f(x)$ פולינום אי פריק ממעלה 7 מעל $\mathbb{Q}$, ויהי $\alpha\in\mathbb{C}$ שורש של f. חשבו את $[\mathbb{Q}(\alpha^3+\alpha):\mathbb{Q}]$.

פתרון. ברור ש-$\mathbb{Q}(\alpha^3+\alpha)\subseteq\mathbb{Q}(\alpha)$. אבל הממד של $\mathbb{Q}(\alpha)$ הוא ראשוני ולכן משיקולי ממד (כמו בתרגיל הבית הקודם) $\mathbb{Q}(\alpha^3+\alpha)=\mathbb{Q}$ או $\mathbb{Q}(\alpha^3+\alpha)=\mathbb{Q}(\alpha)$. נניח כי $\mathbb{Q}(\alpha^3+\alpha)=\mathbb{Q}$. לכן

$$\alpha^3+\alpha=q\in\mathbb{Q}$$

אבל אז x^3+x-q הוא פולינום מאפס עבור α בסתירה לכך שהפולינום המינימלי של α הוא ממעלה 7. לכן בהכרח $\mathbb{Q}(\alpha^3+\alpha)=\mathbb{Q}(\alpha)$ וממד ההרחבה הוא 7.

שאלה 4. חשבו את שדות הפיצול של הפולינומים הבאים מעל $\mathbb{Q}$ ואת הממדים שלהם:

א. x^4+4

ב. x^4-4

ג. x^6-2x^3-3

ד. x^p-2 עבור p ראשוני (בכיתה פתרנו עבור $p=5$)

פתרון.

א. פירוק זריז יגלה כי

$$x^4+4=(x^2-2i)(x^2+2i)=(x^2-2x+2)(x^2+2x+2)$$

ומכאן שהשורשים של הפולינום הם $\pm\sqrt{2i},\pm\sqrt{2i}\cdot i$. ידוע לנו שבמרוכבים $\sqrt{2i}=1+i$, ולכן השורשים הם $\pm(1+i),\pm(1-i)$. נקבל ששדה הפיצול המבוקש הוא $\mathbb{Q}[\pm(1+i),\pm(1-i)]=\mathbb{Q}[i]$. הממד של ההרחבה הוא 2.

ב. פירוק זריז יגלה כי

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

ומכאן שהשורשים של הפולינום הם $\pm\sqrt{2},\pm\sqrt{2}i$. לכן שדה הפיצול שלו הוא $\mathbb{Q}[\sqrt{2},i]$ כפי שראינו בכיתה. הממד של ההרחבה הוא 4.

ג. נציב $t=x^3$ ונפתור את המשוואה t^2-2t-3. נקבל שני פתרונות $t=-1,3$. כלומר

$$x^3=-1,3$$

נסמן ב-ρ שורש יחידה פרימיטיבי מסדר 6. אז כל השורשים הם

$$\rho, \rho^2, \rho^3, \sqrt[3]{3}, \sqrt[3]{3}\rho^2, \sqrt[3]{3}\rho^4$$

ונשים לב כי $\rho^3 = -1$. מכאן קל לבדוק ששדה הפיצול הוא $\mathbb{Q}(\sqrt[3]{3}, \rho)$. את ρ מאפס הפולינום $x^3 + 1$ שהוא פריק ומתפרק כ-$(x+1)(x^2-x+1)$. לכן $x^2 - x + 1$ הוא הפולינום המינימלי של ρ ו-$[\mathbb{Q}(\rho):\mathbb{Q}] = 2$. כמו כן ברור ש-$[\mathbb{Q}(\sqrt[3]{3}):\mathbb{Q}] = 3$. שוב, מפני שהממדים זרים נקבל

$$[\mathbb{Q}(\sqrt[3]{3}, \rho) : \mathbb{Q}] = 6$$

ד. השורשים של הפולינום הם $\sqrt[p]{2}\rho_p^j$ עבור $j = 0, \ldots, p-1$, כאשר ρ_p הוא שורש יחידה p-פרימיטיבי (למשל $\exp(\frac{2\pi i}{p})$). מכאן ניתן להוכיח ששדה הפיצול הוא

$$\mathbb{Q}[\sqrt[p]{2}, \sqrt[p]{2}\rho_p, \ldots, \sqrt[p]{2}\rho_p^{p-1}] = \mathbb{Q}[\sqrt[p]{2}, \rho_p]$$

(ודאו שאתם יודעים להוכיח את השיוויון הזה.) ידוע לנו ש-$[\mathbb{Q}[\rho_p] : \mathbb{Q}] = p - 1$ וקל לחשב ש-$\left[\mathbb{Q}[\sqrt[p]{2}] : \mathbb{Q}\right] = p$. מכיוון שהם זרים, כי p ראשוני, לפי שאלה שכבר פתרנו נקבל $\left[\mathbb{Q}[\sqrt[p]{2}, \rho_p] : \mathbb{Q}\right] = p(p-1)$.

בהצלחה!