פתרון תרגיל בית 4 - תורת גלואה
סמסטר א', תשע"ז

שאלה 1.

1. חשבו את הפולינום המינימלי של $\sqrt[3]{5}$ מעל $\mathbb{Q}$.
2. כמה תתי שדות של $\mathbb{C}$ שונים יש שאיזומורפיים ל$\mathbb{Q}$?

פתרון.
1. הפולינום x^3-5 בודאי מתאפס ב$\sqrt[3]{5}$, והוא אי-פריק (למשל לפי איזנשטיין) ולכן זהו הפולינום המינימלי.
2. השורשים של x^3-5 הם $\left\{\sqrt[3]{5},\ \sqrt[3]{5}\rho_3,\ \sqrt[3]{5}\rho_3^2\right\}$. ולכן השדות $\mathbb{Q}[\sqrt[3]{5}],\ \mathbb{Q}[\sqrt[3]{5}\rho_3],\ \mathbb{Q}[\sqrt[3]{5}\rho_3^2]$ איזומורפיים זה לזה (ואין עוד).
$\mathbb{Q}[\sqrt[3]{5}]\neq\mathbb{Q}[\sqrt[3]{5}\rho_3]$ וכן $\mathbb{Q}[\sqrt[3]{5}]\neq\mathbb{Q}[\sqrt[3]{5}\rho_3^2]$ כי הראשון מרוכב והשני לא.
$\mathbb{Q}[\sqrt[3]{5}\rho_3]\neq\mathbb{Q}[\sqrt[3]{5}\rho_3^2]$ כי אם יש דרך לרשום

$$\sqrt[3]{5}\rho^2=a_0+a_1\sqrt[3]{5}\rho+a_2\left(\sqrt[3]{5}\rho\right)^2$$

אז ע"י העברת אגפים וכפולה בρ נקבל

$$\sqrt[3]{5}-a_2\sqrt[3]{5}^2=a_0\rho+a_1\sqrt[3]{5}\rho^2$$

אבל הצד הימני מספר מרוכב אלא אם $a_0=a_1\sqrt[3]{5}$ מה שלא יתכן כי $\sqrt[3]{5}\notin\mathbb{Q}$.
(הסבר לשיוויון האחרון: אם המספר לא מרוכב אז $a_0\rho+a_1\sqrt[3]{5}\rho^2=\overline{a_0\rho+a_1\sqrt[3]{5}\rho^2}=$ $a_0\rho^2+a_1\sqrt[3]{5}\rho$. ומכיוון ש $\left\{1,\rho,\rho^2\right\}$ בלתי תלויים מעל $\mathbb{R}$ נוכל להשוות מקדמים.)

שאלה 2. הוכיחו כי אם $[F[\alpha]\colon F]$ הוא אי-זוגי אז $F[\alpha]=F[\alpha^2]$.

פתרון. אם $\alpha\notin F[\alpha^2]$ אז $F[\alpha^2]\subsetneq F[\alpha]$ ואז $\left[F[\alpha]\colon F[\alpha^2]\right]>1$.
מצד שני הפולינום $x^2-\alpha^2\in F[\alpha^2]$ מתאפס בα ולכן $\left[F[\alpha]\colon F[\alpha^2]\right]=2$.
אך כעת נקבל $[F[\alpha]\colon F]=\left[F[\alpha]\colon F[\alpha^2]\right]\left[F[\alpha^2]\colon F\right]=2\left[F[\alpha^2]\colon F\right]$ הוא זוגי, בסתירה לנתון.

שאלה 3. מצאו את שדה הפיצול של הפולינומים הבאים, וחשבו את המימד שלהם מעל $\mathbb{Q}$.

1. x^7-5 .
2. x^6-x^3-2.
3. $(x^2-3)(x^2-2)$.

פתרון. 1. השורשים של הפולינום הם $\sqrt[7]{5},\ \rho_7\sqrt[7]{5},\ \ldots,\ \rho_7^6\sqrt[7]{5}$ ולכן שדה הפיצול הוא $E=\mathbb{Q}[\sqrt[7]{5},\ \rho_7\sqrt[7]{5},\ \ldots,\ \rho_7^6\sqrt[7]{5}]=\mathbb{Q}[\sqrt[7]{5},\ \rho_7]$ (את השיוויון האחרון צריך להוכיח).
$[\mathbb{Q}[\sqrt[7]{5}]:\mathbb{Q}]=7$ (כי x^7-5 פולינום מתאפס אי-פריק איזנשטיין).
$[\mathbb{Q}[\rho_7]:\mathbb{Q}]=6$ (ראינו עבור שורש יחידה מסדר ראשוני).
ובגלל שהם מספרים זרים $[E:\mathbb{Q}]=42$.

2. השורשים של הפולינום הם $-1,-\rho_3,\ -\rho_3^2,\ \sqrt[3]{2},\ \sqrt[3]{2}\rho_3,\ \sqrt[3]{2}\rho_3^2$.
ולכן שדה הפיצול הוא $E=\mathbb{Q}\left[-1,-\rho_3,\ -\rho_3^2,\ \sqrt[3]{2},\ \sqrt[3]{2}\rho_3,\ \sqrt[3]{2}\rho_3^2\right]=\mathbb{Q}[\rho_3,\sqrt[3]{2}]$
(יש לנמק את השיוויון האחרון).
$\left[\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}\right]=3$ (ראינו).
$[\mathbb{Q}[\rho_3]:\mathbb{Q}]=2$ (ידוע).
ובגלל שהם זרים נקבל $[E:\mathbb{Q}]=6$.

3. השורשים הם $\pm\sqrt{3},\pm\sqrt{2}$ ולכן שדה הפיצול הוא $\mathbb{Q}[\sqrt{2},\sqrt{3}]$ וכבר ראינו שהמימד של ההרחבה הזו הוא 4.

שאלה 4. יהי $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ פולינום מעל שדה F עם שורשים $\alpha_1,\alpha_2,\ldots,\alpha_n$.
הוכיחו כי $\alpha_1\cdot\alpha_2\cdots\alpha_n=\pm a_0\in F$ והסיקו כי שדה הפיצול הוא $F\left[\alpha_1,\alpha_2,\ldots,\alpha_n\right]=F\left[\alpha_2,\ldots,\alpha_n\right]$.

פתרון. נסתכל ב$f(x)$ מעל שדה הפיצול: $f(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$. אם נכפול ונשווה מקדמים נקבל את הדרוש.

אם כן, אפשר לראות ש $\alpha_1=\dfrac{\pm a_0}{\alpha_2\cdots\alpha_n}$ ולכן $\alpha_1\in F\left[\alpha_2,\ldots,\alpha_n\right]$ וכך מתקבל השיוויון.

שאלה 5. חשבו את שדה הפיצול של x^n-a מעל$\mathbb{Q}$ (למעשה עבור כל שדה ממאפיין אפס).
הוכיחו כי כל תת-שדה של $\mathbb{Q}[\sqrt[n]{2}]$ הוא מהצורה $\mathbb{Q}[\sqrt[k]{2}]$ עבור איזשהו מחלק $k\mid n$.

פתרון. השורשים הם תמיד $\sqrt[n]{2}\rho_n^k$ כאשר ρ_n הוא שורש יחידה n-פרימיטיבי ו $k=0,1,\ldots,n-1$.
וקל להשתכנע ששדה הפיצול הוא $\mathbb{Q}[\sqrt[n]{2},\rho_n]$.
בעת נקח איזשהו תת-שדה $\mathbb{Q}\subseteq K\subseteq\mathbb{Q}[\sqrt[n]{2}]$. $\mathbb{Q}[\sqrt[n]{2}]$ הוא ממימד n ולכן $k=[K:F]\mid n$.
נסמן ב$p(x)$ את הפולינום המינימלי של $\sqrt[n]{2}$ מעל $\boldsymbol{K}$ הוא מדרגה $\left[\mathbb{Q}[\sqrt[n]{2}]:K\right]=\dfrac{n}{k}=d$.
d השורשים שלו הם גם שורשים של x^n-2 ולכן הם מהצורה $\sqrt[n]{2}\rho_n^i$.
לפי השאלה הקודמת, המקדם החופשי של $p(x)$ הוא פלוס-מינוס המכפלה של השורשים כלומר הוא $\pm\left(\sqrt[n]{2}\right)^d\rho_n^s$ עבור איזשהו s.
אבל המקדם החופשי הוא גם איבר ב K שהוא ממשי (מוכל ב$\mathbb{Q}[\sqrt[n]{2}]$) ולכן בהכרח $\rho_n^s=\pm1$ ואז קיבלנו ש $\pm\left(\sqrt[n]{2}\right)^d=\pm\sqrt[\frac{n}{d}]{2}=\pm\sqrt[k]{2}\in K$.
אם כן $\mathbb{Q}[\sqrt[k]{2}]\subseteq K$, אבל $\mathbb{Q}[\sqrt[k]{2}]$ גם הוא ממימד k מעל $\mathbb{Q}$, כי x^k-2 הוא פולינום מינימלי , ולכן יש שיוויון.

שאלה 6. יהיו $F\subset L\subset F[a]$ שדות. ויהי $f(x)=a_0+a_1x+\cdots+a_nx^n$ הפולינום המינימלי של a **מעל $\underline{L}$**.
הוכיחו כי L נוצר (מעל F) ע"י כל המקדמים של f, כלומר ש $L=F[a_0,a_1,\ldots,a_n]$.

פתרון. נסמן $K = F[a_{n-1}, \ldots, a_0]$ - השדה הנוצר מהמקדמים. נשים לב ש $F \subseteq K \subseteq L \subseteq F[a]$.

לפי ההגדרה של K, $f(x) \in K[x]$, ובתור פולינום ב$K[x]$ הוא מתאפס בa ואי-פריק (כי הוא אי-פריק בשדה גדול יותר) ולכן הוא הפולינום המינימלי של a גם מעל K.

מכאן נובע כי $[F[a] : L] = degf = [F[a] : K]$ וזה גורר (למשל מכפליות המימד, כשחושבים על המימד מעל F) ש $K = L$.