אלגברה מופשטת 3 – תרגיל 3

שאלה 1

1. מצאו את הפולינום המינימלי של $\sqrt[3]{3}$ מעל $\mathbb{Q}$.
2. מצאו את הפולינום המינימלי של $\rho_8 = e^{\frac{\pi i}{4}}$ (שורש יחידה פרימיטיבי מסדר 8) מעל $\mathbb{Q}[\sqrt{2}]$.
3. מצאו את הפולינום המינימלי של ρ_8 מעל $\mathbb{Q}[\sqrt{3}]$.

פתרון

תשובה ל-1: $\sqrt[3]{3}$ הוא שורש של $x^3 - 3$. זה פולינום אי פריק כי הוא אייזנשטיין (ביחס לראשוני 3). לכן $x^3 - 3$ הוא הפולינום המינימלי של $\sqrt[3]{3}$ מעל $\mathbb{Q}$.

תשובה ל-2: ρ_8 מקיים $\rho_8^4 = e^{\pi i} = -1$ ולכן הוא שורש של $x^4 + 1$. בתרגיל 1 הראינו שהפירוק של $x^4 + 1$ לגורמים ראשוניים מעל $\mathbb{R}$ הוא $\left(x^2 + \sqrt{2}x + 1\right)\left(x^2 - \sqrt{2}x + 1\right)$. היות ו-$\mathbb{R} \subseteq \mathbb{Q}[\sqrt{2}]$ והפולינומים בפירוק נמצאים ב-$\mathbb{Q}[\sqrt{2}][x]$, זה גם הפירוק לגורמים של $x^4 + 1$ מעל $\mathbb{Q}[\sqrt{2}]$. בדיקה תראה כי ρ_8 הוא שורש של $x^2 - \sqrt{2}x + 1$ ולכן זה הפולינום המינימלי שלו מעל $\mathbb{Q}[\sqrt{2}]$.

תשובה ל-3: גם כאן נעזר בכך ש-$\mathbb{R} \subseteq \mathbb{Q}[\sqrt{3}]$ ולכן הפירוק לגורמים של $x^4 + 1$ מעל $\mathbb{Q}[\sqrt{3}]$ הוא $\left(x^2 + \sqrt{2}x + 1\right)\left(x^2 - \sqrt{2}x + 1\right)$ או $x^4 + 1$. אם האפשרות הראשונה נכונה, אז נובע כי $\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$. אם נראה כי זה בלתי אפשרי אז בהכרח $x^4 + 1$ אי פריק מעל $\mathbb{Q}[\sqrt{3}]$ ולכן הוא הפולינום המינימלי של ρ_8 מעל $\mathbb{Q}[\sqrt{3}]$.

באמת, אם $\sqrt{2} \in \mathbb{Q}[\sqrt{3}]$ אז קיימים $a, b \in \mathbb{Q}$ כך ש-$\sqrt{2} = a + b\sqrt{3}$. ע"י העלאה בריבוע נקבל:

$$2 = a^2 + 2ab\sqrt{3} + 3b^2 = (a^2 + b^2) + (2ab)\sqrt{3}$$

היות ו-$\{1, \sqrt{3}\}$ בסיס של $\mathbb{Q}[\sqrt{3}]$ כמרחב וקטורי מעל $\mathbb{Q}$, נובע ש-$2ab = 0$ ו-$a^2 + b^2 = 2$. קל לבדוק כי למשוואות אלה אין פיתרון ב-$\mathbb{Q}$ ולכן גמרנו.

שאלה 2

יהי $K = \mathbb{Q}[x]/\langle x^3 - x + 1\rangle$. נסמן $\alpha = x + \langle x^3 - x + 1\rangle \in K$. חשבו ב-$K$ את:

1. $(\alpha^2 + 1)^3$
2. $\frac{\alpha+1}{\alpha-1}$

התשובות חייבות להיות פולינומים ממעלה 2 או פחות ב-α. בפיתרון ניתן להשתמש בעובדה ש-K שדה (אם זה עוזר לכם באופן כלשהו).

בונוס: הראו כי K שדה.

פיתרון

תשובה ל-1: $(\alpha^2 + 1)^3 = 7\alpha^2 + \alpha$. הסבר:

```
(a^2+1)^2 = a^4 + 2a^2 + 1 = (a^4 + 2a^2 + 1) mod (a^3 - a + 1) = 3a^2 + a + 1

 ------------------------+
 a^4       + 2a^2      + 1 | a^3 - a + 1
 a^4       -  a^2 + a
            ------------
            3a^2 + a + 1

(a^2+1)^3 = (3a^2+a+1)(a^2+1) = 3a^4 + a^3 + a^2 + 3a^2 + a + 1 =
       = 3a^4 + a^3 +4a^2 + a + 1 = (3a^4 + a^3 +4a^2 + a + 1) mod (a^3 - a + 1) = (*)

 ----------------------------+
 3a^4 + a^3 + 4a^2 +   a + 1 | a^3 - a + 1
 3a^4          - 3a^2 + 3a
        a^3 + 7a^2        + 1
        a^3          - 2a + 1
        -------------------
              7a^2 + 2a

(*) = 7a^2 + 2a
```

תשובה ל-2: $\frac{\alpha+1}{\alpha-1} = -2\alpha^2 - 2\alpha + 1$

דרך א: נניח שהתשובה היא $x + y\alpha + z\alpha^2$. נשים לב ש-

$(\alpha - 1)(x + y\alpha + z\alpha^2) = \alpha x - x + y\alpha^2 - y\alpha + z\alpha^3 - z\alpha^2 = -x + (x - y)\alpha + (y - z)\alpha^2 + z(\alpha - 1) = (-x - z) + (x - y + z)\alpha + (y - z)\alpha^2$

כעת מספיק למצוא x, y, z כך ש-$\alpha + 1 = (-x - z) + (x - y + z)\alpha + (y - z)\alpha^2$. ההמשך הוא פתרון משוואות.

דרך ב: נחשב את $(\alpha - 1)^{-1}$ בעזרת אלגוריתם אוקלידס המוכלל – נמצא $f(x), g(x) \in \mathbb{Q}[x]$ כך ש-$f(x)(x - 1) + g(x)(x^3 - x + 1) = 1$ ואז $(\alpha - 1)^{-1} = f(\alpha)$. באמת:

$x^3 - x + 1 = x(x + 1)(x - 1) + 1$

ולכן אפשר לבחור $f(x) = -x - x^2$, $g(x) = 1$. קיבלו ש-$(\alpha - 1)^{-1} = -\alpha - \alpha^2$.

לכן:

$\frac{\alpha+1}{\alpha-1} = (\alpha + 1)(-\alpha - \alpha^2) = -\alpha^3 - 2\alpha^2 - \alpha = -\alpha^3 - 2\alpha^2 - \alpha + (\alpha^3 - \alpha + 1) = -2\alpha^2 - 2\alpha + 1$

בונוס: מספיק להראות כי $x^3 - x + 1$ אי פריק מעל $\mathbb{Q}$. לפי הלמה של גאוס מספיק להראות שהוא אי פריק מעל $x^3 - x + 1$. מספיק לבדוק ש-$x^3 - x + 1$ אי פריק מעל $\mathbb{Z}_2$ (אם הפולינום היה פריק מעל $\mathbb{Z}$ זה היה משרה פירוק מעל $\mathbb{Z}_2$). מעל $\mathbb{Z}_2$ הוא אי פריק כי אין לו שורש (מציבים 0 ו-1 ובודקים).

לחלופין, אם $x^3 - x + 1$ פריק מעל $\mathbb{Z}$ אז יש לו שורש ב-$\mathbb{Z}$ (בדקו) וקל להראות שזה בלתי אפשרי.

שאלה 3

יהי $K = \mathbb{Q}[\sqrt{2}, \sqrt{3}, \sqrt{7}]$.

1. חשבו את $[K:\mathbb{Q}]$.
2. מצאו בסיס ל-K כמרחב וקטורי מעל $\mathbb{Q}$. [הוכיחו כי זה אכן בסיס!]
3. כתבו את $\frac{\sqrt{7}-\sqrt{3}}{\sqrt{3}+\sqrt{2}+1}$ כצירוף לינארי של אברי הבסיס מסעיף 1.
4. מצאו בסיס ל-K כמרחב וקטורי מעל $\mathbb{Q}[\sqrt{7}]$. [הוכיחו כי זה אכן בסיס!]

5. מצאו את הפולינום המינימלי של $\sqrt{7}+\sqrt{2}$ מעל $\mathbb{Q}$ והראו כי $\mathbb{Q}[\sqrt{2}+\sqrt{7}]=\mathbb{Q}[\sqrt{2},\sqrt{7}]$.
6. מה הפולינום המינימלי של $\sqrt{7}+\sqrt{2}$ מעל $\mathbb{Q}[\sqrt{3}]$? נמקו את תשובתכם.

פתרון

תשובה ל-1: נגדיר $K_1=\mathbb{Q}[\sqrt{2}]$, $K_2=\mathbb{Q}[\sqrt{2},\sqrt{7}]$, $K_3=\mathbb{Q}[\sqrt{2},\sqrt{3},\sqrt{7}]$. מתקיים:

$[K_3:\mathbb{Q}]=[K_3:K_2][K_2:K_1][K_1:\mathbb{Q}]$

$\sqrt{2}$ מאפס את הפולינום x^2-2. זה פולינום אי פריק מעל $\mathbb{Q}$ (אייזנשטיין ביחס ל-2) ולכן הוא הפולינום המינימלי של $\sqrt{2}$. לכן נובע $[K_1:\mathbb{Q}]=\deg(x^2-2)=2$ ו-$\{1,\sqrt{2}\}$ בסיס של K_1 מעל $\mathbb{Q}$.

יהי f הפולינום המינימלי של $\sqrt{7}$ מעל K_1. מתקיים $f|x^2-7$. לכן $f=x^2-7$ או $\deg f=1$. אם האפשרות האחרונה נכונה, אז $\sqrt{7}\in K_1$. נראה כי זה לא ייתכן: נניח בשלילה שקיים $a,b\in\mathbb{Q}$ כך ש-$\sqrt{7}=a+b\sqrt{2}$ (כאן השתמשנו בכך ש-$\{1,\sqrt{2}\}$ בסיס). מהעלאה בריבוע נובע $7=a^2+2b^2+2ab\sqrt{2}$. ברור כי לא ייתכן $a=0$ או $b=0$ (בדקו!) ולכן נקבל $\sqrt{2}=\frac{7-a^2-2b^2}{2ab}\in\mathbb{Q}$ - סתירה! לכן, $f=x^2-7$ ו-$[K_2:K_1]=2$.

<u>טענה</u>: $\{1,\sqrt{2},\sqrt{7},\sqrt{14}\}$ בסיס של K_2 מעל $\mathbb{Q}$.

<u>הוכחה</u>: $\{1,\sqrt{2},\sqrt{7},\sqrt{14}\}$ פורש את K_2 כמרחב וקטורי מעל $\mathbb{Q}$ כי כל האיברים ב-K_2 הם פולינומים $g(x,y)\in\mathbb{Q}[x,y]$ שהציבו בהם $x=\sqrt{2},y=\sqrt{7}$. קל לראות כי ניתן להסתפק בפולנומים שמעלתם ב-x וב-y היא 1 או פחות (אם x^2,y^2 מופיעים אז אפשר להחליף אותם ב-2,7 בהתאמה). אבל לפי מה שהראינו $[K_2:\mathbb{Q}]=[K_2:K_1][K_1:\mathbb{Q}]=2\cdot 2=4$ ולכן $\{1,\sqrt{2},\sqrt{7},\sqrt{14}\}$ בסיס.

יהי f הפולינום המינימלי של $\sqrt{3}$ מעל K_2. אזי $f|x^2-3$. לכן, $f=x^2-3$ או $\deg f=1$. נראה שהמקרה השני בלתי אפשרי. במקרה זה, $\sqrt{3}\in K_2$. לכן, קיימים $a,b,c,d\in\mathbb{Q}$ כך ש:

$$\sqrt{3}=(a+\sqrt{2}b+\sqrt{7}c+\sqrt{14}d)$$

נעלה בריבוע ונקבל:

$$3=(a^2+2b^2+7c^2+14d^2)+2(ab+7cd)\sqrt{2}+2(ac+2bd)\sqrt{7}+2(ad+bc)\sqrt{14}$$

היות ו-$\{1,\sqrt{2},\sqrt{7},\sqrt{14}\}$ בסיס, נובע כי $ab+7cd=ac+2bd=ad+bc=0$. בפרט, נובע $ab=-7cd$ ו-$ac=-2bd$. נכפול את שתי המשוואות האחרונות, נעביר אגפים ונקבל את $bc(a^2-14d^2)=0$ $(*)$. באופן דומה, נקבל גם $bd(a^2-7c^2)=0$ $(**)$ וגם את $cd(a^2-2b^2)=0$ $(***)$.

אם שניים או יותר מבין b,c,d הם 0 נקבל $\sqrt{3}\in\mathbb{Q}[\sqrt{2}]$ או $\sqrt{3}\in\mathbb{Q}[\sqrt{7}]$ או $\sqrt{3}\in\mathbb{Q}[\sqrt{14}]$. ניתן להראות כי זה בלתי אפשרי כמו בשאלה 1.

אם בדיוק אחד מ-b,c,d הוא 0, נאמר b, נקבל מ-$(***)$ ש-$a^2-2b^2=0$ ואז ינבע $\sqrt{2}=\frac{a}{b}\in\mathbb{Q}$ - סתירה! (טיעון דומה עובד גם עובר c,d).

אם אף אחד מ-b,c,d אינו 0, עדיין נקבל סתירה באותו אופן.

לכן, $\sqrt{3}\notin K_2$ ו-$f=x^2-3$. נובע אם כן ש-$[K_3:K_2]=2$.

סה"כ קיבלנו: $[K_3:\mathbb{Q}] = [K_3:K_2][K_2:K_1][K_1:\mathbb{Q}] = 2\cdot 2\cdot 2 = 8$.

תשובה ל-2: $B = \{1, \sqrt{2}, \sqrt{3}, \sqrt{7}, \sqrt{6}, \sqrt{14}, \sqrt{21}, \sqrt{42}\}$ בסיס ל-K_3 מעל $\mathbb{Q}$.

<u>הסבר א</u>: ניתן להשתמש בטענה דומה לזו מסעיף 1 כדי לומר ש-B קבוצה פורשת. היות ומתקיים $|B| = 8 = [K_3:\mathbb{Q}]$, היא גם בסיס.

<u>הסבר ב</u>: נשתמש בטענה הבאה:

אם $F \subseteq K \subseteq L$ שדות, ו-$\{a_i\}_{i\in I}$ בסיס ל-K מעל F ו-$\{b_j\}_{j\in J}$ בסיס ל-L מעל K אז $\{a_i b_j\}_{i\in I, j\in J}$ בסיס ל-L מעל F. [את ההוכחה נשאיר כתרגיל – פשוט משתמשים בהגדרות.]

מסעיף 1 נובע כי $\{1, \sqrt{2}\}$ בסיס לK_1 מעל $\mathbb{Q}$, $\{1, \sqrt{7}\}$ בסיס ל-K_2 מעל K_1 ו-$\{1, \sqrt{3}\}$ בסיס ל-K_3 מעל K_2. שימוש בטענה פעמיים יראה כי B בסיס.

תשובה ל-3:

$$\frac{\sqrt{7}-\sqrt{3}}{\sqrt{3}+\sqrt{2}+1} = \frac{(\sqrt{7}-\sqrt{3})(-\sqrt{3}+\sqrt{2}+1)}{(\sqrt{3}+\sqrt{2}+1)(-\sqrt{3}+\sqrt{2}+1)} = \frac{(\sqrt{7}-\sqrt{3})(-\sqrt{3}+\sqrt{2}+1)}{-3+(\sqrt{2}+1)^2} = \frac{(\sqrt{7}-\sqrt{3})(-\sqrt{3}+\sqrt{2}+1)}{-3+2+2\sqrt{2}+1} =$$
$$\frac{(\sqrt{7}-\sqrt{3})(-\sqrt{3}+\sqrt{2}+1)}{2\sqrt{2}} = \frac{\sqrt{2}}{4}(\sqrt{7}-\sqrt{3})(-\sqrt{3}+\sqrt{2}+1) = \frac{1}{4}(\sqrt{7}-\sqrt{3})(-\sqrt{6}+2+\sqrt{2}) =$$
$$\frac{1}{4}(-\sqrt{42}+2\sqrt{7}+\sqrt{14}+3\sqrt{2}-2\sqrt{3}-\sqrt{6}) = \frac{3}{4}\sqrt{2} - \frac{1}{2}\sqrt{3} + \frac{1}{2}\sqrt{7} - \frac{1}{4}\sqrt{6} + \frac{1}{4}\sqrt{14} - \frac{1}{4}\sqrt{42}$$

תשובה ל-4: ראשית נבחין כי $\left[K:\mathbb{Q}[\sqrt{7}]\right] = \frac{[K:\mathbb{Q}]}{[\mathbb{Q}[\sqrt{7}]:\mathbb{Q}]} = \frac{8}{2} = 4$ (נשאיר את העובדה ש-$\left[\mathbb{Q}[\sqrt{7}]:\mathbb{Q}\right] = 2$ כתרגיל קל). הקבוצה $A = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ מקיימת $B = A \cdot \{1, \sqrt{7}\}$, באשר B היא הבסיס מסעיף 2. לכן, A פורשת את K כמרחב וקטורי מעל $\mathbb{Q}[\sqrt{7}]$. היות ו-$\left[K:\mathbb{Q}[\sqrt{7}]\right] = 4 =$ $|A|$, A היא למעשה בסיס.

תשובה ל-5: ברור כי $\mathbb{Q}[\sqrt{2}+\sqrt{7}] \subseteq \mathbb{Q}[\sqrt{2}, \sqrt{7}]$. מסעיף 1 אנחנו יודעים כי $\left[\mathbb{Q}[\sqrt{2}, \sqrt{7}]:\mathbb{Q}\right] = 4$. כעת יש שני המשכים דומים:

<u>דרך א:</u> נסמן $\alpha = \sqrt{2}+\sqrt{7}$. נראה כי $1, \alpha, \alpha^2, \alpha^3$ הם בלתי תלויים לינארית מעל $\mathbb{Q}$. נעשה זאת בעזרת הצגת כל אחד מהם כצירוף לינארי של אברי הבסיס מסעיף 2. כל שנותר הוא לדרג את מטריצת המקדמים ולבדוק שאין תלות לינארית בין השורות.

לאחר שעשינו זאת, לפי הטענה מהשיעור ינבע ש-$4 \leq \left[\mathbb{Q}[\sqrt{2}+\sqrt{7}]:\mathbb{Q}\right]$ ולכן בהכרח מתקיים $\mathbb{Q}[\sqrt{2}+\sqrt{7}] = \mathbb{Q}[\sqrt{2}, \sqrt{7}]$.

כדי למצוא את הפולינום המינימלי של α (שחייב להיות מדרגה 4 לפי הטענה), נביע את α^4 כצירוף לינארי של $1, \alpha, \alpha^2, \alpha^3$. ניתן לעשות זאת ע"י פתרון מערכת משוואות לינאריות (זו אותה מטריצה שדורגה מקודם אז אפשר לבצע את זה במקביל).

נבנה רק את מערכת המשוואות אך לא נפרט את הפיתרון שלה.

$\alpha = \sqrt{2}+\sqrt{7}$

$\alpha^2 = 2 + 2\sqrt{14} + 7 = 9 + 2\sqrt{14}$

$\alpha^3 = 9\sqrt{2} + 9\sqrt{7} + 4\sqrt{7} + 14\sqrt{2} = 23\sqrt{2} + 13\sqrt{7}$

$\alpha^4 = (\sqrt{2} + \sqrt{7})(23\sqrt{2} + 13\sqrt{7}) = 46 + 13\sqrt{14} + 23\sqrt{14} + 91 = 137 + 36\sqrt{14}$

לכן מספיק לדרג את המערכת הבאה ולבדוק שהמטריצה באגף ימין הפיכה:

$$\left(\begin{array}{cccc|c} 1 & 0 & 9 & 0 & 137 \\ 0 & 1 & 0 & 23 & 0 \\ 0 & 1 & 0 & 13 & 0 \\ 0 & 0 & 2 & 0 & 36 \end{array}\right)$$

(השורות מקבילות למקדמים של $\{1, \sqrt{2}, \sqrt{7}, \sqrt{14}\}$ בהתאמה. העמודות מקבילות ל-$1, \alpha, \dots, \alpha^4$).

<u>דרך ב:</u> נראה ישירות כי $\sqrt{2}, \sqrt{7} \in \mathbb{Q}[\sqrt{2} + \sqrt{7}]$. זה יוכיח את ההכלה בכוון הנגדי. בפרט, נקבל $[\mathbb{Q}[\sqrt{2} + \sqrt{7}] : \mathbb{Q}] = 4$ ולכן הפולינום המינימלי של $\alpha = \sqrt{2} + \sqrt{7}$ הוא מדרגה 4. אז נמצא ישירות פולינום ממעלה 4 מעל $\mathbb{Q}$ שמאפס את α והוא בהכרח יהיה הפולינום המינימלי של α.

כעת נפרט:

$\alpha^2 = 2 + 2\sqrt{14} + 7 = 9 + 2\sqrt{14}$

$\alpha^2 - 9 = 2\sqrt{14}$

$(\alpha^2 - 9)^2 = 2^2 \cdot 14 = 56$

לכן נובע ש-$0 = (x^2 - 9)^2 - 56 = x^4 - 18x^2 - 25$ מאפס את α. נמשיך:

$\alpha(\alpha^2 - 9) = 2\sqrt{28} + 2\sqrt{98} = 4\sqrt{7} + 14\sqrt{2}$

$(\alpha(\alpha^2 - 9) - 4\alpha) = 4\sqrt{7} + 14\sqrt{2} - 4\sqrt{2} - 4\sqrt{7} = 10\sqrt{2}$

$(\alpha(\alpha^2 - 9) - 14\alpha) = 4\sqrt{7} + 14\sqrt{2} - 14\sqrt{2} - 14\sqrt{7} = -10\sqrt{7}$

משני השוויונות האחרונים נובע ש-$\sqrt{2}, \sqrt{7} \in \mathbb{Q}[\alpha]$ ולכן הפולינום המינימלי של α הוא $x^4 - 18x^2 - 25$.

תשובה ל-6: הפולינום המינימלי של $\sqrt{2} + \sqrt{7}$ מעל $\mathbb{Q}[\sqrt{3}]$ הוא $x^4 - 18x^2 - 25$. בסעיף 5 ראינו שהוא מאפס את $\sqrt{2} + \sqrt{7}$. לכן, לפי הטענה מהתרגול העובדה שהוא הפולינום המינימלי שקולה לכך ש-$4 = \deg(x^4 - 18x^2 - 25) = \left[\mathbb{Q}[\sqrt{3}][\sqrt{2} + \sqrt{7}] : \mathbb{Q}[\sqrt{3}]\right]$. באמת, לפי סעיף 5 מתקיים $K = \mathbb{Q}[\sqrt{3}][\sqrt{2}, \sqrt{7}] = \mathbb{Q}[\sqrt{3}][\sqrt{2} + \sqrt{7}]$ ולכן:

$\left[\mathbb{Q}[\sqrt{3}][\sqrt{2} + \sqrt{7}] : \mathbb{Q}[\sqrt{3}]\right] = \left[K : \mathbb{Q}[\sqrt{3}]\right] = \frac{[K:\mathbb{Q}]}{[\mathbb{Q}[\sqrt{3}]:\mathbb{Q}]} = \frac{8}{2} = 4$.

תזכורת

בשיעור ציינו את הטענה הבאה. אתם רשאים להיעזר בה במידת הצורך.

טענה: יהי R תחום שלמות, $F \subseteq R$ שדה, $a \in F$ ו-$f \in F[x]$ כך ש-$f(a) = 0$. נסמן $n = \deg f$.
אזי התנאים הבאים שקולים:

א. f הוא הפולינום המינימלי של a מעל F.

ב. f אי פריק מעל F.[1]
ג. הקבוצה $\{1, a, a^2, \dots, a^{n-1}\}$ בלתי תלויה לינארית מעל F.
ד. $[F[a]:F] = \deg f$.

בכל מקרה, $F[a]$ הוא שדה ומתקיים $[F[a]:F] \leq \deg f$.

[1] זהירות: אם R אינו תחום, ייתכן ש-f פריק. אם f פריק אז $F[a]$ אינו שדה.