אלגברה מופשטת 3 – פתרון תרגיל 1

שאלה 1
חשבו:

1. $\gcd(x^4-4x^2-x+2, 2x^4+3x^3-1)$ ב-$\mathbb{Q}[x]$.
2. $\gcd(x^4+2x^3+2x^2+2x+2, x^4+2x^2+2x+1)$ מעל $\mathbb{Z}_3[x]$.

פיתרון
משתמשים באלגוריתם אוקלידס[1] ובחילוק ארוך של פולינומים. התשובה של 1 היא x^2+x+1. התשובה של 2 היא $x+2$.

פיתרון מלא של 1 לדוגמא:

```
Calculation of gcd(x^4 - 4x^2 - x + 2, 2x^4 + 3x^3 - 1) over the rational numbers

 ----------------------------+
 2x^4 + 3x^3             - 1 | x^4 - 4x^2 - x + 2
 2x^4          - 8x^2 - 2x + 4
 ---------------------------
        3x^3 + 8x^2 + 2x - 5

replace x^4 - 4x^2 - x + 2 with 3x^4 - 12x^2 - 3x + 6

 ------------------------------------+
 3x^4          -   12x^2 -    3x +    6 | 3x^3 + 8x^2 + 2x - 5
 3x^4 + 8x^3 +    2x^2 -    5x
      - 8x^3 -   14x^2 +    2x +    6
      - 8x^3 + 64/3x^2 + 16/3x - 40/3
       ------------------------------
              22/3x^2 + 22/3x - 22/3

replace 22/3x^2 + 22/3x - 22/3 with x^2 + x - 1

 ---------------------+
 3x^3 + 8x^2 + 2x - 5 | x^2 + x - 1
 3x^3 + 3x^2 - 3x
        5x^2 + 5x - 5
        5x^2 + 5x - 5
        -------------
                    0

so gcd(x^4 - 4x^2 - x + 2, 2x^4 + 3x^3 - 1) = x^2 + x - 1
```

שאלה 2
יהי C חוג חילופי, $c\in C$ ו-$f(x)\in C[x]$. הוכיחו כי $f(c)=0$ אם ורק אם $x-c\mid f(x)$.

הוכחה
אם $x-c\mid f(x)$ אז קיים $g(x)$ כך ש-$f(x)=(x-c)g(x)$. כעת $f(c)=(c-c)g(c)=0$.

נניח $f(c)=0$. צ"ל $x-c\mid f(x)$. אם $f(x)=0$ זה ברור. אחרת, נוכיח באינדוקציה על $n=\deg f$.

[1] שאומר, בקצרה, כך: $\gcd(a,b)=a$ אם $a=b$ או $b=0$. אחרת, $\gcd(a,b)=\gcd(b, a \bmod b)$.

כאשר $n=1$ נכתוב $f(x)=a_1x+a_0$. מתקיים $0=f(c)=a_1+ca_0$ ולכן $a_0=-ca_1$. זה אומר ש-$f(x)=a_1x-a_1c=a_1(x-c)$, כדרוש.

עבור n כללי נכתוב $f(x)=a_0+a_1x+\cdots+a_nx^n$. נתבונן ב-$g(x)=f(x)-a_n(x-c)^n$. אזי $g(c)=f(c)-a_n(c-c)^n=0$ ו-$\deg g<n$. לכן, לפי הנחת האינדוקציה יש $h(x)$ כך ש-$g(x)=(x-c)h(x)$. מכאן נובע:

$$f(x)=g(x)+a_n(x-c)^n=(x-c)(h(x)+a_n(x-c)^{n-1})$$

מש"ל.

שאלה 3

פרקו את הפולינום x^4+1:

1. מעל $\mathbb{C}$.
2. מעל $\mathbb{R}$.
3. מעל $\mathbb{Q}$.
4. מעל $\mathbb{Z}_3$.

פיתרון

פיתרון 1: $x^4-1=0$ אם"ם $x^4=-1=e^{\pi i}$. לפי משפט דה-מואבר הפתרונות הם $e^{\frac{k\pi i}{4}}$ עבור $k=1,3,5,7$. לכן:

$$x^4+1=\left(x-e^{\frac{\pi i}{4}}\right)\left(x-e^{\frac{3\pi i}{4}}\right)\left(x-e^{\frac{5\pi i}{4}}\right)\left(x-e^{\frac{7\pi i}{4}}\right)=$$
$$=\left(x-\frac{i+1}{\sqrt{2}}\right)\left(x-\frac{i-1}{\sqrt{2}}\right)\left(x-\frac{-i-1}{\sqrt{2}}\right)\left(x-\frac{-i+1}{\sqrt{2}}\right)$$

פיתרון 2: אפשר לקבל את הפירוק מעל $\mathbb{R}$ ע"י קיבוץ גורמים מהפירוק מעל $\mathbb{C}$. צריך לקבץ כל גורם לינארי עם הצמוד שלו (כי אם $\alpha\in\mathbb{C}$ שורש של פולינום ממשי אז גם הצמוד שלו שורש). לכן:

$$x^4+1=\left[\left(x-\frac{i+1}{\sqrt{2}}\right)\left(x-\frac{-i+1}{\sqrt{2}}\right)\right]\left[\left(x-\frac{i-1}{\sqrt{2}}\right)\left(x-\frac{-i-1}{\sqrt{2}}\right)\right]=$$

$$=\left(x^2-\sqrt{2}x+1\right)\left(x^2+\sqrt{2}x+1\right)$$

שני הגורמים אי פריקים מעל $\mathbb{R}$ כי הם אין להם שורשים ב-$\mathbb{R}$.

פיתרון 3: פירוק מעל $\mathbb{Q}$ הוא בפרט פירוק מעל $\mathbb{R}$. לאור התשובה לסעיף הקודם, הפירוק של x^4+1 הוא x^4+1 או $\left(x^2-\sqrt{2}x+1\right)\left(x^2+\sqrt{2}x+1\right)$. היות והאפשרות השנייה בלתי אפשרית כי $\sqrt{2}\notin\mathbb{Q}$, בהכרח x^4+1.

פיתרון 4: ננסה לבדוק אם ל-x^4+1 יש שורש ב-$\mathbb{Z}_3$. בדיקה תראה שאין.

נחפש את הפולינומים המתוקנים האי פריקים ממעלה 2 מעל $\mathbb{Z}_3$ [ע"י שימוש בכך שפולינום ממעלה 2 אי פריק אם"ם אין לו שורש]. מקבלים שלושה פולינומים: x^2+1, x^2+x+2, x^2+2x+2. ננסה לחלק את x^4+1 בכל אחד מהם. בסוף נקבל $x^4+1=(x^2+x+2)(x^2+2x+2)$.

הערה: בתשובה לתרגיל הבית עליכם להשלים את הפרטים בפיתרון של 4.