תרגיל 10

שאלה 1. קבעו האם הפולינומים הבאים הם אי פריקים בחוג הנתון, ואם הם פריקים מצאו את פירוק שלהם לגורמים אי פריקים.

1. x^2+x+1 בחוג $\mathbb{F}_2[x]$.
2. $x^6-4x^4+6x^2$ בחוג $\mathbb{Z}[x]$.
3. $2ix^5+71$ בחוג $\mathbb{Z}[i][x]$.
4. x^2+y^2-1 בחוג $\mathbb{Q}[x,y]$. העשרה: x^n+y^m-1 לכל $n,m\in\mathbb{N}$.

1. אי פריק. פולינום מדרגה 2 ללא שורשים.

(א) הפירוק הוא $x\cdot x\cdot(x^4-4x^2+6)$. הגורם האחרון אי פריק בעזרת קריטריון אייזנשטיין עם $p=2$.

(ב) בעזרת המיון של ראשוניים ב-$\mathbb{Z}[i]$, אנחנו יודעים כי ישנו פירוק $71=(4+i)(4-i)$. כעת ניתן להשתמש בקריטריון אייזנשטיין עם $p=4+i$. צריך להוכיח כי $4+i$ ראשוני וגם שהוא לא מחלק את $2i$, למשל לפי חישוב נורמות.

(ג) שתי דרכים: בדרך הראשונה, לפולינום $y^2+(x^2-1)$ אין שורשים מעל $\mathbb{Q}[x]$, כי $x^2-1=(x-1)(x+1)$. אנחנו בתחום פריקות יחידה, ולכן אין פירוק אחר ל-x^2-1 שבו הוא ריבוע.
בדרך השנייה, אפשר להשתמש בקריטריון אייזנשטיין עם $p=x-1$, שהוא ראשוני כי $\mathbb{Q}[x]/\langle x-1\rangle\cong\mathbb{Q}$ תחום שלמות.

שאלה 2. יהי $f(x)=x^4-5x^2+6$. פרקו את $f(x)$ לגורמים ראשוניים מעל החוגים הבאים:

1. $\mathbb{Q}$
2. $\mathbb{R}$
3. $\mathbb{Z}/5\mathbb{Z}$

פתרון. פתרון:
ראשית, נשים לב $x^4-5x^2+6=(x^2-2)(x^2-3)$. לכן מספיק לפרק את הפולינומים האלו. מכיוון שאנחנו מעל שדות, פירוק של פולינום ממעלה 2 שקול לשאלה אם יש לפולינום שורש. כמו כן, שדה הוא תחום פריקות יחידה באופן טריוויאלי, ולכן חוג הפולינומים מעליו הוא תפ"י. כלומר, אי פריק= ראשוני.

1. מעל $\mathbb{Q}$ לשני הפולינומים אין שורשים, ולכן הם אי פריקים. כלומר, זהו הפירוק של f לגורמים ראשוניים.

2. מעל $\mathbb{R}$ שני הפולינומים פריקים. $f(x)=(x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{3})(x+\sqrt{3})$.

3. מעל $\mathbb{Z}/5\mathbb{Z}$ לשני הפולינומים אין שורש, ולכן הם אי פריקים. כלומר, זהו הפירוק של f לגורמים ראשוניים.

שאלה 3. נתבונן בפולינום $f(x)=x^2+4$ מעל $\mathbb{Z}$. הראו ש-$f(ax+b)$ לא מקיים את קריטריון אייזנשטיין לכל $a,b\in\mathbb{Z}$, $a\neq 0$, למרות ש-$f(x)$ אי פריק.

פתרון. פתרון:

ראשית, f אינו פריק מעל $\mathbb{Z}$ כי הוא אי פריק מעל $\mathbb{Q}$, מכיוון ש $\mathbb{Q}$ שדה ואין בו שורשים לf. ומכיוון ש $f(x)$ פרימיטיבי פריקות מעל $\mathbb{Z}$ שקולה לפריקות מעל $\mathbb{Q}$.

כעת, $f(ax+b)=(ax+b)^2+4=a^2x^2+2abx+b^2+4$.

יהי p ראשוני שמחלק את b^2+4. אם $p=2$ אז $p\mid b^2$ ולכן $p^2\mid b^2+4$. כלומר, קריטריון איזנשטיין לא יכול להתקיים עם $p=2$.

אם $p\neq 2$, אז כדי שיתקיים $p\mid 2ab$ צריך להתקיים $p\mid a\vee p\mid b$. אם $p\mid a$ אז הוא מחלק את המקדם המוביל, ולכן קריטריון איזנשטיין לא מתקיים.

אחרת, $p\mid b$. אבל אז נקבל ש$p\mid 4$, וחזרנו למקרה ש$p=2$.

שאלה 4. העשרה: הוכיחו שלכל $n\in\mathbb{N}$ הפולינום

$$p_n(x)=(x-1)\,(x-2)\cdots(x-n)-1$$

הוא אי פריק בחוג $\mathbb{Z}[x]$.

פתרון. נשים לב כי $p_n(x)$ הוא מתוקן, ולכן פרימיטיבי. נניח בשלילה כי $p_n(x)=f(x)g(x)$ עבור פולינומים $f(x),g(x)\in\mathbb{Z}[x]$ מדרגה שקטנה ממש מ-$\deg p_n(x)=n$.

לכל $1\leq i\leq n$ מתקיים $p_n(i)=f(i)g(i)=-1$. מפני שהפולינומים מעל $\mathbb{Z}$, והצבנו ערכים שלמים, אז בהכרח $\{f(i),g(i)\}=\{-1,1\}$. בפרט $f(i),g(i)$ הם עם סימנים הפוכים. נתבונן בפולינום $h(x)=f(x)+g(x)$, שעבורו כל $1\leq i\leq n$ הוא שורש כי $h(i)=\pm1\mp1=0$ (נעזרים בכך שהסימנים הפוכים).

הדרגה של $h(x)$ קטנה ממש מ-n, כי הדרגות של $f(x),g(x)$ קטנות ממש מ-n. לכן קיבלנו ש-$h(x)\equiv 0$. כלומר $f(x)=-g(x)$. נציב בחזרה ונקבל $p_n(x)=-f(x)^2$. בפרט $p_n(x)$ תמיד לא חיובי, אבל לפי הגדרת $p_n(x)$ אפשר לראות שעבור x מספיק גדול הפולינום הוא חיובי. זו סתירה, ולכן הפולינום $p_n(x)$ אי פריק.

הערה: אפשר להחליף את $1,\ldots,n$ בכל קבוצה $\{a_1,\ldots,a_n\}$ של שלמים שונים כלשהם.