פתרון תרגיל בית 1 - תורת גלואה

סמסטר א', תשע"ז

שאלה 1. קבעו האם הפולינומים הבאים הם פריקים או אי-פריקים בחוגים המצויינים:

1. $3x^2 - 7x - 5$, $\mathbb{Q}[x]$.
נעשה רדוקציה מודולו 2 ונקבל $x^2 + x + 1$ שהוא אי-פריק כי אין לו שורשים. ולכן הפולינום הוא אי-פריק.

2. $x^3 - 7x + 2$, $\mathbb{Z}_5[x]$.
זה שקול לפולינום $x^3 - 2x + 2$ שהוא אי-פריק כי אין לו שורשים.

3. $x^3 - 6x - 9$, $\mathbb{Q}[x]$.
אם הפולינום פריק זה כי יש לו שורש (כי הדרגה היא 3), ושורש רציונלי $\frac{a}{b}$ מקיים $b|1,\ a|9$ ולכן האופציות הן $\{\pm1, \pm3, \pm9\}$.
קל לבדוק ש3 הוא שורש ולכן נסיק שהפולינום פריק.

4. $x^4 + 4x^3 + 6x^2 + 2x + 1$, $\mathbb{Q}[x]$.
אם נשתמש בהצבה $x - 1$ נקבל את הפולינום $x^4 - 2x + 2$ שהוא אי-פריק לפי אייזנשטין.

5. $x^3 - x^2 + x + 3$, $\mathbb{Q}[x]$.

שאלה 2. מצאו את הפירוק של הפולינום $x^4 + 2x^2 - 8$ לגורמים אי פריקים בחוגים הבאים:

1. $\mathbb{C}[x]$
$(x + 2i)(x - 2i)(x - \sqrt{2})(x + \sqrt{2})$

2. $\mathbb{R}[x]$
$(x^2 + 4)(x - \sqrt{2})(x + \sqrt{2})$ כאשר $x^2 + 4$ אינו פריק כי אין לו שורש בשדה (והוא מדרגה 2).

3. $\mathbb{Q}[x]$
$(x^2+4)(x^2-2)$ כל גורם פה הוא אי-פריק כי אין להם שורשים רציונליים (והם מדרגה 2).

4. $\mathbb{Z}_7[x]$
נעשה רדוקציה לפירוק מהסעיף הקודם: $(x^2+4)(x^2-2) \equiv (x^2-3)(x^2-2)$.
(x^2-3) הוא אי-פריק (אין שורש לו בשדה).
הגורם השני מתפרק $x^2-2=(x+4)(x-4)$ ולכן סך הכל נקבל את הפירוק:
$(x^2-3)(x+4)(x-4)$.

שאלה 3. בנו שדה ממאפיין 3 וגודל 9. רשמו את כל האיברים שלו.
נחפש פולינום אי-פריק מדרגה 2 מעל $\mathbb{Z}_3$: אפשר למשל לקחת את x^2+x-1 שהוא אי-פריק כי אין לו שורשים.
אזי $\mathbb{Z}_3[x]/\left\langle x^2+x-1\right\rangle = \{0,1,2,x,1+x,2+x,2x,1+2x,2+2x\}$ הוא שדה מגודל 9.

שאלה 4. קראו את הנספח על מציאת שורשים של פולינומים מדרגות נמוכות.

1. פתרו את $x^3-3x^2+5x+1=0$
ראשית נפטר מהמקדם של x^2 ע"י הצבה $y=x-1$: נקבל y^3+2y^2+4.
כעת נציב $y=u+v$ ונרצה ש
$$\begin{cases} u^3+v^3=-4 \\ uv=\dfrac{-2}{3} \end{cases}$$
u^3ו v^3 הם שורשים של $t^2-4t+\dfrac{8}{27}=0$ שהם $2\pm\dfrac{10}{\sqrt{27}}$.
כלומר
$$u=\sqrt[3]{2+\frac{10}{\sqrt{27}}}$$
$$v=\sqrt[3]{2-\frac{10}{\sqrt{27}}}$$
ו
$$x=y+1=\sqrt[3]{2+\frac{10}{\sqrt{27}}}+\sqrt[3]{2-\frac{10}{\sqrt{27}}}+1$$
הוא פתרון של המשוואה הנ"ל.

2. פתרו את $x^4-x-1=0$ עד שאתם מגיעים לפולינום מדרגה 3 (אין צורך לפתור עד הסוף).
נחפש $(x^2+ax+b)(x^2+cx+d)=x^4-x-1$ מה שנותן לנו ע"י השוואת מקדמים:

$$\begin{cases} a+c=0 \\ b+d+ac=0 \\ ad+bc=-1 \\ bd=-1 \end{cases}$$

אזי $c=-a$, $b=\dfrac{a^3+1}{2a}$ ו $d=\dfrac{a^3-1}{2a}$ ממשוואות ליניאריות. וכשנציב במשוואה האחרונה נקבל $a^6+4a^2-1=0$.
כך שאם נפתור את $x^3+4x-1=0$ נדע לפתור את המשוואה שלנו.

שאלה 5. יהי $f(x)\in\mathbb{Z}[x]$ פולינום כך ש $f(0),f(1)$ והמקדם העליון (המוביל) הם אי-זוגיים, הוכיחו כי ל $f(x)$ אין שורשים רציונליים.
נרשום $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$.
הנתונים בעצם אומרים ש a_n,a_0 ו $a_n+\cdots+a_1+a_0$ הם אי-זוגיים.
אם בשלילה יש שורש רציונלי $\dfrac{p}{q}$ (בכתיבה מצומצמת) אז $q\mid a_n$ ו $p\mid a_0$ כך ששניהם אי-זוגיים (כלומר $p,q\equiv 1 \pmod 2$).
אבל אם נציב את השורש בפולינום ונכפול בq^n נקבל $a_np^n+a_{n-1}qp^{n-1}+\cdots+a_1q^{n-1}p+a_0q^n=0$
ואם נפעיל על זה מודולו 2 נקבל $a_np^n+a_{n-1}qp^{n-1}+\cdots+a_1q^{n-1}p+a_0q^n\equiv a_n+\cdots+a_1+a_0\equiv 0$,
בתירה לכך שסכום המקדמים הוא אי-זוגי!

שאלה 6. [בונוס חשוב] לכל שדה (ולמעשה לכל חוג) אפשר לבנות הומומורפיזם $\mathbb{Z}\to F$ ע"י כך ששולחים $1\mapsto 1_F$.
הוכיחו כי הגרעין הוא $n\mathbb{Z}$ אם ורק אם המאפיין של F הוא n.
הוכיחו כי n הוא תמיד ראשוני (רמז: אם זה לא ראשוני, אפשר למצוא מחלקי אפס).
הסיקו שכל שדה מכיל עותק של (כלומר תת שדה שאיזומורפי ל-) $\mathbb{Z}_p$ או $\mathbb{Z}$.