

אלגברה מופשטת 3 - תרגול 1

R תחום אוקלידי $\Leftarrow R$ תחום ראשי $\Leftarrow R$ תחום פריקות יחידה

משפט: יהי F שדה. אזי $F[x]$ תחום אוקלידי.

הגדרה: איבר בחוג $a \in R$ נקרא **אי-פריק** אם לכל פירוק $a = bc$ מתקיים b או c הפיכים.

שאלה: יהי F שדה. רוצים לבדוק האם פולינום $p(x) \in F[x]$ הוא אי-פריק?

טענות:

1. יהי $p(x) \in F[x]$ כך ש $\deg p(x) \leq 3$. אי-פריק אם ורק אם ל $p(x)$ אין שורשים ב- F .

2. יהי $p(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$. אם $t \in \mathbb{Q}$ שורש של $p(x)$, נציג $t = \frac{r}{s}$ כך ש $(r, s) = 1$. אזי

מתקיים $r | a_0, s | a_n$.

3. $p(x) \in F[x]$ אי-פריק אם ורק אם $p(ax+b) \in F[x]$ אי-פריק עבור כל $a \in F^*, b \in F$.

משפט גאוס: יהי U תחום פריקות יחידה ו- $F = \text{frac}(U)$ שדה השברים שלו. $p(x) \in U[x]$ לא ניתן לפירוק

למכפלת פולינומים **לא קבועים** שדרגתם קטנה מ $\deg p(x)$ אם ורק אם $p(x)$ אי-פריק ב $F[x]$.

טענה: פולינום $f(x) \in \mathbb{Z}[x]$ הוא אי-פריק אם ורק אם ה \gcd של מקדמיו הוא 1 (כלומר הוא **פרימיטיבי**), ולא

ניתן לפרק אותו למכפלה של פולינומים לא קבועים שדרגתם קטנה מ $\deg f(x)$.

תרגיל: הראו ש $f(x) = 8x^3 - 6x - 1$ אי-פריק ב $\mathbb{Z}[x]$ בעזרת טענות 1 ו 2.

פתרון: נראה שלפולינום הנ"ל אין שורשים ב \mathbb{Q} , ואז לפי טענה 1 יתקיים $f(x)$ אי פריק ב $\mathbb{Q}[x]$ ולפי הלמה

של גאוס הוא יהיה גם אי-פריק ב $\mathbb{Z}[x]$. אם $\frac{r}{s} \in \mathbb{Q}$ שורש של $f(x)$ כך ש $(r, s) = 1$ אזי לפי טענה 2 מתקיים

$r | -1$ וגם $s | 8$. כלומר $r = \pm 1$, $s = 1, 2, 4, 8$ (מספיק לקחת s -ים חיוביים בלבד). כעת צריך לבדוק עבור כל

הערכים הנ"ל שהם אינם שורשים של $f(x)$.

קריטריון איזנשטיין:

$p(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. אזי אם קיים p ראשוני כך ש $p | a_i$ לכל $0 \leq i \leq n-1$, וגם

$p^2 \nmid a_0$ אזי $p(x)$ אי-פריק מעל \mathbb{Q} .

תרגיל:

בדקו האם הפולינום הבא אי-פריק מעל $\mathbb{Z}[x]$:

$$f(x) = x^{p-1} + x^{p-2} + \dots + 1$$

פתרון:

נשים לב ש $g(x) := (1-x)f(x) = x^p - 1$.

נבצע הצבה של $x+1$ במקום x . אזי

$$\begin{aligned} x \cdot f(x+1) &= g(x+1) = (x+1)^p - 1 = x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{p-1}x + 1 - 1 \\ &= x \left(x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-2}x + \binom{p}{p-1} \right) \end{aligned}$$

נחלק את שני האגפים ב x ונקבל $f(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-2}x + p$.

הוכיחו שמתקיים $p \mid \binom{p}{k}$ עבור $1 \leq k \leq p-1$. לכן מתקיים קריטריון איזנשטיין והפולינום $f(x+1)$ אי-פריק.

לפי טענה 3, $f(x+1)$ אי-פריק אם ורק אם $f(x)$ אי-פריק. \square

משפט:

1. $\langle f(x) \rangle \triangleleft F[x]$ אידאל ראשוני/מקסימלי אם ורק אם $f(x)$ אי-פריק.

2. אם $f(x)$ אי-פריק אזי $F[x]/\langle f(x) \rangle$ שדה.

הערה: איך מוצאים את ההפכי של איבר $\bar{q} \in K = F[x]/\langle p(x) \rangle$ כאשר $0 \neq \bar{q} \in K$ אי-פריק?

כיוון ש $0 \neq \bar{q}$ ניתן להרים אותו לאיבר $q(x) \in F[x]$ כך ש $p(x) \nmid q(x)$.

אם כך $(q(x), p(x)) = 1$, כי $p(x)$ אי-פריק. לכן קיימים $r(x), s(x) \in F[x]$ כך ש $p(x)s(x) + q(x)r(x) = 1$. נעשה מודולו $p(x)$ למשוואה ונקבל $\bar{q}\bar{r} \equiv q(x)r(x) \equiv 1 \pmod{p(x)}$, כאשר $\bar{r} = r(x) + \langle p(x) \rangle$. כלומר \bar{r} הוא ההפכי של \bar{q} .

טענה: יהי R תחום F שדה, $\sigma: R \rightarrow F$ הומומורפיזם חוגים. אזי נגדיר $\sigma^*: R[x] \rightarrow F[x]$ ע"י

$$\sigma^*(a_n x^n + \dots + a_1 x + a_0) = \sigma(a_n) x^n + \dots + \sigma(a_1) x + \sigma(a_0)$$

משפט (שיטת הרדוקציה): יהי R תחום F שדה, $\sigma: R \rightarrow F$ הומומורפיזם חוגים. יהי $p(x) \in R[x]$ פולינום. נגדיר $g(x) = \sigma^*(f(x))$. אם $\deg g(x) = \deg f(x)$ וגם $g(x)$ אי-פריק ב $F[x]$ אזי $f(x)$ לא ניתן לפירוק למכפלת פולינומים לא קבועים מדרגה קטנה מ $\deg f(x)$.

תרגיל: הראו ש $f(x) = 8x^3 - 6x - 1$ אי-פריק ב $\mathbb{Z}[x]$ בעזרת שיטת הרדוקציה.

פתרון: ניקח $\sigma: \mathbb{Z} \rightarrow \mathbb{F}_p$ להיות מודולו p . אזי σ^* עושה מודולו p למקדמי הפולינומים. נבדוק האם מתקיימים

תנאי המשפט לכמה ראשוניים p . נסמן $g(x) = \sigma^*(f(x))$.

עבור $p = 2$ מתקיים $\deg(g(x)) = 0 < \deg f(x)$.

עבור $p = 3$ מתקיים $g(x) = -x^3 - 1 = -(x+1)(x^2 - x + 1)$, כלומר $g(x)$ פריק.

עבור $p = 5$ מתקיים $g(x) = 3x^3 - x - 1$. כעת ניתן לבדוק שאין לפולינום זה שורשים ב \mathbb{F}_5 , ולכן הוא אי-פריק לפי טענה 1.