

מעריך תרגול 1 מופשטת 3

נבצע חזרה לגבי פריקות של פולינומים מעל שדות. נסביר בהמשך למה זה רלוונטי לקורס שלנו.

תזכורת 1.1 יהי R תחום שלמות. $a \in R$ לא הפיך נקרא איבר אי פריק אם $a = bc$ גורר ש b הפיך או c הפיך.

שאלה 1.2 בהינתן פולינום $f(x) \in \mathbb{F}[x]$ איך ניתן לקבוע אם הוא פריק או לא?

חשוב להדגיש כל הזמן מה השדה שעובדים מעליו. למשל $x^2 - 2$ פריק מעל \mathbb{R} אבל לא מעל \mathbb{Q} .

נציג מספר טכניקות. נתחיל בכמה עובדות קלות.

- כל פולינום מדרגה 1 הוא אי פריק. אז המקרה הזה משעמם. מעכשיו נניח ש $\deg f(x) \geq 2$.
- כל פולינום שיש לו שורש בשדה \mathbb{F} הוא פריק. הסבר: α שורש של $f(x)$ אם ורק אם $x - \alpha \mid f(x)$.
- אם ל $f(x)$ אין שורשים בשדה \mathbb{F} זה לא אומר שהוא אי-פריק. למשל ל $f(x) = (x^2 - 2)^2$ מעל \mathbb{Q} אין שורשים אבל הוא כמובן פריק.

דוגמא 1.3 האם $x^n - 1$ פריק עבור $n > 1$ (נניח מעל \mathbb{Q})? כן. כי מייד לראות ש $x = 1$ הוא שורש.

תרגיל 1.4 יהי $f(x)$ פולינום מדרגה 2 או 3 אזי $f(x)$ אי פריק אם ורק אם אין ל $f(x)$ שורשים.

פתרון: אם ל $f(x)$ יש שורש הסברנו כבר שהוא פריק. מצד שני אם $f(x) = g(x)h(x)$ כאשר $\deg g(x), \deg h(x) \geq 1$ אז אחד מהם חייב להיות מדרגה 1 וזה אומר של $f(x)$ יש שורש.

דוגמא: האם $x^2 - x - 1$ פריק מעל \mathbb{Q} ? פותרים, מגלים שהשורשים הם $\frac{1 \pm \sqrt{5}}{2}$ שאינם ב \mathbb{Q} ולכן הפולינום אי-פריק.

תרגיל 1.5 האם הפולינום $x^3 - x + 1$ פריק מעל \mathbb{Z}_3 ?

פתרון: יש בסך הכל 3 מספרים בשדה. מסתבר שאף אחד מהם לא מאפס את הפולינום ולכן הוא אי פריק.

לשמחנתנו, גם אם עובדים מעל \mathbb{Q} יש דרך להגיע למספר סופי של שורשים אפשריים שצריך לבדוק.

הערה 1.6 אם $f(x) \in \mathbb{Q}[x]$ אז ניתן להכפיל בכופל המשותף של המנות ולקבל פולינום עם מקדמים שלמים שהוא פריק אם ורק אם $f(x)$ פריק. לכן כשעובדים מעל \mathbb{Q} ניתן תמיד להניח שהמקדמים שלמים.

(למשל, לעבוד עם $3x^2 + 2$ במקום עם $\frac{1}{2}x^2 + \frac{1}{3}$)

תרגיל 1.7 יהי $f(x) = a_n x^n + \dots + a_0$ כאשר כל המקדמים שלמים, הוכיחו כי אם השבר המצומצם $\frac{q}{r}$ הוא שורש של $f(x)$ אז

$$q \mid a_0, \quad r \mid a_n$$

פתרון: לפי הנתון

$$a_n \left(\frac{q}{r}\right)^n + \dots + a_0 = 0$$

נכפול ב r^n ונקבל

$$a_n q^n + a_{n-1} q^{n-1} r + \dots + a_1 q r^{n-1} + a_0 r^n = 0$$

מה שאומר ש $a_0 r^n \mid a_n q^n$ ו $q \mid a_n q^n$ אבל בגלל ש r ו q זרים (הרי השבר מצומצם) אז מתקיים

$$q \mid a_0, \quad r \mid a_n$$

תרגיל 1.8 האם הפולינום $x^3 - x - 6$ אי פריק מעל $\mathbb{Q}[x]$?

פתרון: לפי התרגיל הקודם, אם $\frac{q}{r}$ פתרון (שהוא שבר מצומצם) אז

$$q \mid 6, \quad r \mid 1$$

כך שבסך הכל האפשרויות הן:

$$\frac{q}{r} \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$$

אם עוברים עליהן אפשר לראות ש 2 הוא שורש ולכן הפולינום פריק. שווה להזכיר כאן עוד נקודה:

תרגיל 1.9 מצאו את הפירוק של $x^3 - x - 6$ לגורמים אי פריקים (ב $\mathbb{Q}[x]$).

פתרון: היות ש 2 שורש של הפולינום אנחנו יודעים ש $x - 2 \mid x^3 - x - 6$. נשתמש בחילוק פולינומים ונגלה ש

$$\frac{x^3 - x - 6}{x - 2} = x^2 + 2x + 3$$

ל $x^2 + 2x + 3$ אין שורשים מעל \mathbb{Q} ולכן הוא אי-פריק. לסיכום הפירוק הוא

$$x^3 - x - 6 = (x - 2)(x^2 + 2x + 3)$$

כמובן שטכניקה זו עובדת גם מעל שדות סופיים. גם עבור פולינום ממעלה גבוהה מ 3 או פולינומים מעל \mathbb{R} אפשר להשתמש בטכניקה הזו אבל רק כדי למצוא שורש רציונאלי ולהראות פריקות. אם לא מוצאים שורש אי אפשר להגיד כלום.

הערה 1.10 זכרו כי לפולינום מדרגה אי זוגית מעל \mathbb{R} תמיד יש שורש אחד לפחות ולכן הוא תמיד פריק.

נעבור לטכניקות אחרות לבדיקת פריקות.

תזכורת 1.11 קריטריון אייזנשטיין: יהי $f(x) = a_n x^n + \dots + a_0$ פולינום עם מקדמים שלמים. אם יש ראשוני כך ש $p \mid a_i$ לכל $i < n$ אבל $p \nmid a_n$ ו $p^2 \nmid a_0$. אזי $f(x)$ אי פריק מעל \mathbb{Q} .

דוגמא 1.12 $x^n - 4x + 2$ אי פריק מעל \mathbb{Q} . לפעמים צריך להתחכם.

תרגיל 1.13 האם הפולינום $x^4 + 4x^3 + 6x^2 - 1$ אי פריק מעל \mathbb{Q} ?

כדי לפתור את התרגיל נעזר בעובדה ההבאה:

טענה 1.14 $f(x)$ אי פריק אם ורק אם $f(x+c)$ אי פריק לכל $c \in \mathbb{F}$.

הוכחה: קל לוודא שתמיד $f(x)$ ו $f(x+c)$ מאותה דרגה ולכן $f(x) = g(x)h(x)$ פירוק אם ורק אם $f(x+c) = g(x+c)h(x+c)$ פירוק. ■

פתרון: אם נסתכל חזק נשים לב שהפולינום שלנו הוא

$$(x+1)^4 - 4(x+1) + 2$$

היות ש $x^4 - 4x + 2$ אי פריק לפי קריטריון אייזנשטיין. גם הפולינום שלנו אי פריק. לטכניקה הבאה שנציג צריך תזכורת נוספת:

תזכורת 1.15 (הלמה של גאוס) יהי $f(x)$ פולינום שכל מקדמיו שלמים. נניח שהמחלק המשותף המירבי של מקדמיו הוא 1. אז $f(x)$ אי פריק ב $\mathbb{Z}[x]$ אם ורק אם הוא אי פריק מעל $\mathbb{Q}[x]$.

משפט 1.16 (שיטת הרדוקציה) יהי $f(x) \in \mathbb{Z}[x]$ ויהי p ראשוני כלשהוא. נסמן ב $\bar{f}(x)$ את הפולינום המתקבל מביצוע מודולו p למקדמי f . אם $\deg \bar{f}(x) = \deg f(x)$ ו $\bar{f}(x)$ אי פריק אז גם $f(x)$ אי פריק.

את ההוכחה נשאיר כתרגיל מודרך לשיעורי בית. נראה יישום

תרגיל 1.17 האם הפולינום $8x^3 - 6x - 1$ אי פריק ב $\mathbb{Q}[x]$?

פתרון: היות ש $\gcd(8, 6, 1) = 1$ הפולינום אי פריק ב $\mathbb{Q}[x]$ אם ורק אם הוא אי פריק ב $\mathbb{Z}[x]$. ננסה להשתמש בשיטת הרדוקציה.

ננסה $p = 2$: מתקבל -1 שאינו באותה דרגה כמו f .

ננסה $p = 3$: מתקבל $2x^3 - 1$ שהוא פריק ($x = 2$ שורש)

ננסה $p = 5$: מתקבל $3x^3 - x - 1$ שהוא במקרה אי פריק (בודקים 5 אפשרויות).

לכן גם הפולינום $8x^3 - 6x - 1$ אי פריק.

נחזור לשאלה מתחילת השיעור: למה כל זה יהיה חשוב לנו? זה קורס בתורת השדות. נזכיר כי החוג $\mathbb{F}[x]$ הוא תחום אוקלידי. בחוג כזה מתקיים:

$f(x) \in \langle f(x) \rangle \Leftrightarrow f(x)$ ראשוני $\langle f(x) \rangle \Leftrightarrow \langle f(x) \rangle$ אידיאל ראשוני $\langle f(x) \rangle \Leftrightarrow \mathbb{F}[x]/\langle f(x) \rangle$ שדה.

כלומר אם לוקחים שדה \mathbb{F} ופולינום אי פריק מעליו, אפשר לבנות שדה חדש (גדול יותר). אנחנו נשתמש בבניה הזאת כל הזמן במהלך הקורס, אבל היא עובדת (כלומר, מתקבל שדה) רק אם f פולינום אי פריק.