

שדות ותורת גלואה  
מערכי תרגול קורס 88-311

אוקטובר 2021, גרסה 0.27

## תוכן העניינים

3	מבוא
4	1 תרגול ראשון
4	1.1 תזכורת מתורת החוגים
7	1.2 קריטריון אייזנשטיין והלמה של גאוס

## מבוא

כמה הערות טכניות לתחילת הקורס:

- דף הקורס נמצא באתר [www.math-wiki.com](http://www.math-wiki.com).
- שאלות בנוגע לחומר הלימודי מומלץ לשאול בדף השיחה באתר של הקורס.
- החומר בחוברת הזו נאסף מכמה מקורות, ומבוסס בעיקרו על שינויים ותוספות למערכי תרגול של איתמר שטיין ושירה גילת.
- נשתדל לכתוב **בגופן הזה** כשהגדרות ומושגים חשובים מופיעים בפעם הראשונה. נוסף בצד גם את השם באנגלית, שעשוי לעזור כשמחפשים חומר נוסף שאינו בעברית.
- נשמח לכל הערה על מסמך זה.

מחבר בתשע"ט ותש"ף: תומר באואר  
עדכונים בתשפ"ב: גיא בלשר

# 1 תרגול ראשון

## 1.1 תזכורת מתורת החוגים

Rng, or  
non-unital ring  
Additive group

**הגדרה 1.1.** חוג בלי יחידה  $(R, +, \cdot, 0)$  הוא מבנה אלגברי המקיים:

1.  $(R, +, 0)$  הוא חבורה אבלית. נקראת החבורה החיבורית של החוג.

2.  $(R, \cdot)$  הוא חבורה למחצה.

3. מתקיים פילוג (משמאל ומימין). כלומר לכל  $a, b, c \in R$  מתקיים

$$(a + b)c = ac + bc, \quad a(b + c) = ab + ac$$

כאשר ההקשר ברור, נכתוב רק  $R$  במקום  $(R, +, \cdot, 0)$ .

**הגדרה 1.2.**  $R$  הוא שדה אם  $(R \setminus \{0\}, \cdot)$  חבורה אבלית.

Field

שדות הם חוגים מאוד טובים. הם חילופיים וכל איבר לא אפסי בהם הפיך.

**הגדרה 1.3.** יהי  $R$  חוג. **אידיאל** של  $R$  הוא תת-חבורה חיבורית  $I \subseteq R$  שמקיימת בליעה ביחס לכפל:  $IR, RI \subseteq I$ .

Ideal

**תזכורת 1.4.** יהי  $F$  שדה. נתבונן בחוג  $F[x]$ .

• זהו תחום אוקלידי – ניתן לחלק פולינומים עם שארית;

• לכן, זהו תחום ראשי – כל אידיאל ב- $F[x]$  נוצר על ידי פולינום אחד. אפשר ממש למצוא את היוצר: היוצר של אידיאל  $I \triangleleft F[x]$  הוא הפולינום הלא אפסי מדרגה מינימלית ששייך ל- $I$ .

• האידיאלים המקסימליים ב- $F[x]$  הם בדיוק האידיאלים מהצורה  $\langle f(x) \rangle$  כאשר  $f \neq 0$  הוא פולינום אי-פריק.

• (אפשר להמשיך למספר משתנים: החוג  $F[x_1, \dots, x_n]$  הוא תחום פריקות יחידה ובפרט תחום שלמות, אבל לא תחום ראשי.)

**מסקנה 1.5.** אם  $F$  שדה ו- $f \in F[x]$  פולינום אי-פריק, אז  $F[x]/\langle f \rangle$  הוא שדה, ו- $F$  משוכן בתוכו:

$$F \hookrightarrow F[x]/\langle f \rangle$$

לפי המסקנה האחרונה, כדי להבין שדות, עלינו להבין פולינומים אי פריקים.

**תזכורת 1.6.** יהי  $R$  תחום שלמות. איבר לא הפיך  $a \in R$  נקרא **אי פריק** אם  $a = bc$  גורר ש- $b$  הפיך או  $c$  הפיך.

Irreducible

**שאלה 1.7.** בהינתן פולינום  $f(x) \in F[x]$  איך ניתן לקבוע אם הוא אי פריק או לא?

חשוב להדגיש כל הזמן מה השדה שעובדים מעליו. למשל  $x^2 - 2$  פריק מעל  $\mathbb{R}$  אבל לא מעל  $\mathbb{Q}$ . עבורנו התכונה אי פריק היא "הבסיסית" יותר, ופולינום נקרא פריק אם הוא לא אי פריק. נציג מספר שיטות, ונתחיל בכמה אבחנות קלות:

- כל פולינום ממעלה 1 הוא אי פריק. אז המקרה הזה משעמם. מעכשיו נניח כי  $\deg f(x) \geq 2$  בטענות לא טריוויאליות.

- כל פולינום שיש לו שורש בשדה  $F$  הוא פריק. הסבר:  $\alpha$  שורש של  $f(x)$  אם ורק אם  $x - \alpha \mid f(x)$ .

- אם ל- $f(x)$  אין שורשים בשדה  $F$  זה לא אומר שהוא אי פריק. למשל ל- $f(x) = (x^2 - 5)^2$  מעל  $\mathbb{Q}$  אין שורשים, אבל הוא פריק.

טענה 1.8. לפולינום  $f(x) \in F[x]$  ממעלה  $n$  מעל שדה יש לכל היותר  $n$  שורשים.

**דוגמה 1.9.** האם  $x^n - 1$  פריק עבור  $n > 1$  (נניח מעל  $\mathbb{Q}$ )? כן, כי מייד רואים ש- $x = 1$  הוא שורש.

**תרגיל 1.10.** יהי  $f(x)$  פולינום ממעלה 2 או 3. אז  $f(x)$  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 ממעלה 1 וזה אומר של- $f(x)$  יש שורש.

**דוגמה 1.11.** האם  $x^2 - x - 1$  פריק מעל  $\mathbb{Q}$ ? בעזרת "נוסחת השורשים" מגלים שהשורשים הם  $\frac{1 \pm \sqrt{5}}{2}$  שאינם רציונליים, ולכן הפולינום אי פריק.

**תרגיל 1.12.** 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.

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

1.13. הערה. אם  $f(x) \in \mathbb{Q}[x]$  אז ניתן להכפיל במכפלה משותפת של המכנים 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 1.14.** 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 1.15.** 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.

**תרגיל 1.16.** מצאו את הפירוק של  $x^3 - x - 6$  לגורמים אי פריקים מעל  $\mathbb{Q}$ .

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

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

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 ששיטה זו עובדת גם מעל שדות סופיים.

גם עבור פולינום ממעלה גבוהה מ-3 או פולינומים מעל  $\mathbb{R}$  אפשר להשתמש בשיטה הזו, אבל רק כדי למצוא שורש רציונלי ולהראות פריקות. אם לא מוצאים שורש אי אפשר להגיד כלום (בינתיים).

הערה 1.17. זכרו כי לפולינום ממעלה אי זוגית מעל  $\mathbb{R}$  תמיד יש שורש אחד לפחות ולכן הוא תמיד פריק.

## 1.2 קריטריון אייזנשטיין והלמה של גאוס

נעבור לטכניקות אחרות לבדיקת פריקות. מעכשיו נניח כי  $R$  תחום שלמות ו- $F$  שדה השברים שלו. הדוגמה שבדרך כלל תשמש אותנו היא  $R = \mathbb{Z}$  ו- $F = \mathbb{Q}$ .

Eisenstein's  
criterion

**משפט 1.18** (קריטריון אייזנשטיין). יהי  $P \triangleleft R$  אידאל ראשוני. יהי  $f(x) = a_n x^n + \dots + a_1 x + a_0 \in R[x]$  פולינום המקיים

$$i \neq n \text{ לכל } a_i \in P \bullet$$

$$a_n \notin P \bullet$$

$$a_0 \notin P^2 \bullet$$

אז  $f$  אי פריק ב- $F[x]$  (אין לו פירוק אמיתי מעל  $R$ ). אם  $f$  פרימיטיבי ב- $R$  (המחלק המשותף המרבי של מקדמיו הוא 1), אז  $f$  אי פריק ב- $R[x]$ . במקרה הפרטי שבו  $P = \langle p \rangle$  עבור איבר ראשוני  $p$  התנאים לעיל שקולים לכך ש- $p$  לא מחלק את  $a_n$ , מחלק את  $a_i$  עבור  $i \neq n$  ו- $p^2$  לא מחלק את  $a_0$ .

**דוגמה 1.19**.  $x^n - 4x + 2$  אי פריק מעל  $\mathbb{Q}$  כי הוא אייזנשטיין עבור  $p = 2 \in \mathbb{Z}$ . לפעמים צריך להתחכם יותר.

**תרגיל 1.20**. האם הפולינום  $x^4 + 4x^3 + 6x^2 - 1$  אי פריק מעל  $\mathbb{Q}$ ?

כדי לפתור את התרגיל נעזר בעובדה ההבאה:

טענה 1.21.  $f(x)$  אי פריק אם ורק אם  $f(x+c)$  אי פריק לכל  $c \in F$ .

הוכחה. קל לוודא שתמיד  $f(x)$  ו- $f(x+c)$  מאותה מעלה ולכן  $f(x) = g(x)h(x)$  פירוק אם ורק אם  $f(x+c) = g(x+c)h(x+c)$  פירוק.  $\square$

פתרון. אם נשים לב שהפולינום שלנו הוא למעשה

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

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

**תזכורת 1.22** (גרסה ללמה של גאוס). יהי  $R$  תחום שלמות ויהי  $F$  שדה השברים שלו. יהי  $f(x) \in R[x]$ . אז  $f(x)$  אי פריק ב- $F[x]$  אם ורק אם הוא לא ניתן לפירוק למכפלת פולינומים לא קבועים שמעלתם קטנה מ- $\deg f(x)$ .

**תזכורת 1.23** (גרסה ללמה של גאוס). יהי  $f(x)$  פולינום שכל מקדמיו שלמים. נניח שהוא פרימיטיבי. אז  $f(x)$  אי פריק ב- $\mathbb{Z}[x]$  אם ורק אם הוא אי פריק ב- $\mathbb{Q}[x]$ .

**משפט 1.24** (שיטת הרדוקציה). יהי  $f(x) \in \mathbb{Z}[x]$  ויהי  $p$  ראשוני כלשהו. 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. כעת נראה יישום.

**תרגיל 1.25.** 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 מעלה 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.