

פתרון תרגיל בית 9 אלגברה מופשטת 2

1. (*) הוכח כי עבור פולינום מתוקן $p(x) \in \mathbb{Z}[x]$, אם $\alpha \in \mathbb{Q}$ הוא שורש של $p(x)$ אז $\alpha \in \mathbb{Z}$.

פתרון:

נרשום $p(x) = x^n + c_{n-1}x^{n-1} + \dots + c_1x + c_0$

נרשום $\alpha = \frac{a}{b}$ כשבר מצומצם, אזי לפי הנתון:

$$\frac{a^n}{b^n} + c_{n-1}\frac{a^{n-1}}{b^{n-1}} + \dots + c_1\frac{a}{b} + c_0 = 0$$

$$a^n = -(c_{n-1}a^{n-1} + c_{n-2}a^{n-2}b + \dots + c_0b^{n-1}) \cdot b$$

מה שגורר ש a^n מתחלק ב b . כלומר $\alpha \in \mathbb{Z}$.

2. (*) מצא יוצר לאידיאל $\langle x^3 - x^2 - x + 1, x^5 + x^2 - x - 1 \rangle \triangleleft \mathbb{Z}[x]$.

פתרון:

זה בעצם למצוא gcd של $x^3 - x^2 - x + 1, x^5 + x^2 - x - 1$.

אחרי אלגוריתם אוקלידס (או פירוק של הפולינומים הנ"ל) נמצא ש $\gcd = x^2 - 1$.

3. (***) עבור שדה F , הוכיחו כי בחוג $F[x]$ יש אינסוף פולינומים ראשוניים.

פתרון:

אם F הוא שדה אינסופי אז $x - a$ הם אינסוף פולינומים ראשוניים.

אם F סופי, נניח בשלילה שיש מספר סופי של ראשוניים: $p_1(x), p_2(x), \dots, p_n(x)$ מדרגות k_1, k_2, \dots, k_n בהתאמה.

נשים לב שבהכרח $1 \leq k_i$ כי פולינומים מדרגה אפס הם איבר בשדה ולכן הפיכים (ולא ראשוניים).

נתבונן בפולינום $q(x) = 1 + \prod p_i(x)$, ונטען שהוא ראשוני. אם הוא לא ראשוני אז יש לו פירוק לראשוניים (כי אנחנו בתחום אוקלידי).

נניח $p_1 \mid q$ אז $q = p_1 q'$ אבל $1 = p_1 (q' - \prod_2^n p_i)$ וזה סתירה! הפיך, סתירה!

4. (*) פרקו את הפולינום $x^4 - 5x^2 + 6$ לגורמים ראשוניים מעל:

בכל סעיף דרוש הסבר למה הגורמים הם ראשוניים!

(א) \mathbb{Q}

$$(x^2 - 2)(x^2 - 3)$$

(ב) $\mathbb{Q}[\sqrt{2}]$

$$(x - \sqrt{2})(x + \sqrt{2})(x^2 - 3)$$

$x^2 - 3$ הוא ראשוני שם כי אין לו שורש (למה? חישוב $\sqrt{3} \neq a + b\sqrt{2}$).

(ג) \mathbb{R}

$$(x - \sqrt{2})(x + \sqrt{2})(x - \sqrt{3})(x + \sqrt{3})$$

(ד) \mathbb{Z}_5

$$x^4 - 5x^2 + 6 = x^4 + 1 = x^2 - 4 = (x^2 + 2)(x^2 - 2)$$

אלו גורמים אי-פריקים כי אין להם שורשים בשדה.

5. (*) תנו דוגמא לפולינום אי-פריק מעל \mathbb{Q} מדרגה ≤ 3 , שלא מקיים את קריטריון אייזנשטיין לאף מס' ראשוני.

$$x^3 + 4 \text{ למשל.}$$

6. (*) הוכיחו כי הפולינומים הבאים הם אי-פריקים מעל החוגים המצויינים:

(א) $\mathbb{Z}, x^5 + 867x^4 + 153x + 321$

אייזנשטיין, לפי $p = 3$.

(ב) $\mathbb{Z}, x^8 - 6x^3 + 12$

אייזנשטיין, לפי $p = 3$.

(ג) $\mathbb{Z}_3, x^3 + x^2 - 1$

אין שורשים.

(ד) $\mathbb{Z}, 7x^3 - 6x^2 + 2x - 1$

נניח יש שורש $\frac{a}{b}$, אז לפי טענה $-1, a \mid 7, b \mid 7$ כלומר $\pm 1, \pm \frac{1}{7}$.

מבדיקה ישירה, ± 1 הם לא שורשים של הפולינום, ולכן אין לפולינום שורשים ב \mathbb{Z} .

(ה) $\mathbb{Z}, x^4 + 2x^2 + 4$

דרך א: אפשר לבדוק שאין שורשים, כמו בסעיף הקודם.

ואז להראות שאין פירוק לגורמים ריבועיים,

$$\dots x^4 + 2x + 4 = (x^2 + ax + b)(x^2 + cx + d)$$

דרך ב: לפרק מעל \mathbb{C} לגורמים לינאריים ולראות שאין אף מכפלה שנותנת גורמים ב \mathbb{Z} .

(ו) $\mathbb{Z}[\sqrt{2}], x^7 - 13x^3 + 26$

היינו רוצים להשתמש באייזנשטיין עם 13, אבל צריך להראות שהוא אי-פריק קודם.

אם הוא היה פריק אז $\dots = a^2 - 2b^2 = 13$ מודולו 8 נקבל $a^2 - 2b^2 \equiv 5 \pmod{8}$. ומכיוון $(\mathbb{Z}_8)^2 = \{0, 1, 4\}$ אין לזה פתרון.

7. (**)

(א) הוכיחו כי אם פולינום פרימיטיבי $f(x) \in \mathbb{Z}[x]$ הוא פריק, אז הוא פריק גם מעל \mathbb{Z}_p לכל ראשוני p .

פתרון:

מכיוון ש $\mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ המוגדר ע"י מודולו p על המקדמים הוא הומומורפיזם (הוכיחו זאת),

אז בפרט הוא כפלי. מה שאומר שאם $f = g \cdot h$ אז $\bar{f} = \bar{g} \cdot \bar{h}$.

אם $\bar{g} = 0$ זה אומר ש p מחלק את כל המקדמים של g , בסתירה לכך ש f פרימיטיבי.

נשים לב ש \bar{g} הוא הפיך, זה אומר ש $g \in \mathbb{Z}$ מה שסותר את ההנחה ש f פרימיטיבי.

ולכן קיבלנו פירוק אמיתי של \bar{f} .

(ב) הסיקו כי הפולינום $x^4 + x + 1$ הוא אי פריק מעל \mathbb{Z}

פתרון:

מודולו 2 נקבל $x^4 + x + 1 \equiv x^2 + x + 1$ שהוא אי-פריק כי אין לו אף שורש.

(ג) הוכיחו כי אין פולינום $p(x) \in \mathbb{Z}[x]$ מדרגה $1 < p$ שהוא אי-פריק מעל \mathbb{Z}_p לכל המס' הראשוניים p .

פתרון:

נקח a כך ש $p(a) = n \neq \pm 1$. אם n הוא אפס סיימנו.

אם לא, נקח גורם ראשוני שלו p ואז מודולו p $p(a) \equiv 0$ ולכן פריק.

8. (***) הוכיחו כי הפולינום $p(x) = \prod_{k=1}^n (x - k) - 1$ הוא אי-פריק מעל \mathbb{Z} .

נניח בשלילה שהוא מתפרק $p(x) = f(x)g(x)$ כך ש $f(x), g(x) \in \mathbb{Z}[x]$. שימו לב שבהכרח $deg(f), deg(g) < deg(p) = n$ (כי p פרימיטיבי).

נשים לב שלכל $1 \leq i \leq n$ מתקיים $p(i) = f(i)g(i) = -1$, וכיוון שהפולינומים האלו הם מעל \mathbb{Z} והצבנו ערכים שלמים, אז בהכרח $f(i), g(i) = \pm 1$ ובסימנים הפוכים.

כעת נתבונן בפולינום $h(x) = f(x) + g(x)$, ונשים לב שלכל i בתחום הנ"ל $h(i) = 0$ (כי הסימנים של f ו g הפוכים) - כך של- $h(x)$ יש n שורשים שונים.

אך מצד שני הדרגה של $h(x)$ קטנה ממש מ- n . (כי הוא סכום של פולינומים מדרגות כאלו). ולכן בהכרח $h(x) \equiv 0$ כלומר ש $f(x) = -g(x)$.

נציב אותם בחזרה ונקבל ש $p(x) = -f(x)^2$ כלומר שהפולינום הזה תמיד שלילי, אבל קל לראות שעבור ערכי x גדולים מספיק, $p(x)$ יקבל ערכים חיוביים.

קיבלנו סתירה, ולכן הפולינום הוא אי-פריק.