# הרחבות שדות סופיים אלגברות

מהם כל הפתרונות השלמים של

$$P(x) \equiv 0 \pmod{n}$$

כאשר $P$ פולינום עם מקדמים שלמים?

תחת הכפל של $\mathbb{Z}_n[x]$ הוא אוסף כל הפולינומים שמקדמיהם מהקבוצה $\mathbb{Z}_n$. למשל $P \in \mathbb{Z}_4[x]$ עבור $P = 3x^4 + 2x^3 + x^2 + 2x + 3$

שניתן לרשום כך שכל המקדמים שלו הם מספרים זוגיים

$$x^3 \notin \mathbb{Z}_3[x]$$

פתרונות שכאלו, $x$ - $\mathbb{Z}_3$ הם פולינומים ב-

$$\left.\begin{aligned} 0^3 &\equiv 0 \\ 1^3 &\equiv 1 \\ 2^3 &\equiv 2 \end{aligned}\right\} \pmod 3$$

חלוקה עם שארית ב-$\mathbb{Z}_n[x]$: אם $P, Q$ פולינומים שמקדמיהם שייכים ל-$\mathbb{Z}_n$ אז קיים $k$ ו-$R$ כך ש-

$$P = kQ + R \qquad (\deg(R) < \deg(Q))$$

כאשר $k$ ו-$R$ נתונים על ידי $Q$ ו-$P$ בצורה יחידה.

תחום $\mathbb{Z}_n[x]$ לא בהכרח יש לו תכונה זו אלא אם $n$ הוא ראשוני. כלומר אם $P, Q \in \mathbb{Z}_n[x]$ כך ש-$\deg(Q) \neq 0$, $k, R \in \mathbb{Z}_n[x]$ קיימים $\deg(R) < \deg(Q)$ כך ש-

$$P = kQ + R$$

**דוגמה:** $P(x) = 5x^4 + 2x^3 - x^2 + 3x + 1$

$Q(x) = 2x^2 + 6x + 5$

$\mathbb{Z}_7$ - פולינומים ב- $\mathbb{Z}_7[x]$.

$$\begin{array}{r|l} 5x^4 + 2x^3 - x^2 + 3x + 1 & 2x^2 + 6x + 5 \\ \hline 5x^4 + 2x^3 + 3x^2 & 4x^2 + 4x + 6 \\ \hline 4x^3 + 6x^2 + 3x + 1 & \\ 4x^3 + 5x^2 + 2x & \\ \hline x^2 + x + 1 & \\ x^2 + 3x + 5 & \\ \hline 5x + 3 & \end{array}$$

$$4 \cdot 2 \equiv 1 \pmod 7$$

נוסחת ה- $P(x) = (6x^2 + 4x + 4)Q(x) + 4x + 6$

Scanned by CamScanner

אלגברה מודרנית 1 – תרגיל בית 9

**שאלה 1** – $f \in \mathbb{Z}_p[x]$ יהי אי פריק. הוכיחו שאם $f$ אינו פריק ב-$\mathbb{Z}_p[x]$ אז $f$ אינו פריק ב-$\mathbb{Z}[x]$.

**פתרון:** נניח ש-$f$ פריק ב-$\mathbb{Z}[x]$, כלומר $f = g \cdot h$ עבור $g, h \in \mathbb{Z}[x]$ לא הפיכים. נסתכל על $\bar{f} = \bar{g}\bar{h}$ ב-$\mathbb{Z}_p[x]$. מכיוון ש-$f$ אינו פריק ב-$\mathbb{Z}_p[x]$, אחד הגורמים, נניח $\bar{g}$, הוא הפיך, כלומר $\deg \bar{g} = 0$. אבל $\deg \bar{g} \leq \deg g$, ולכן $\deg g = 0$, כלומר $g$ קבוע. מכיוון ש-$g$ לא הפיך ב-$\mathbb{Z}[x]$, נקבל $g = p$. אבל אז $p \mid f$ ב-$\mathbb{Z}[x]$, ומכיוון ש-$f$ פרימיטיבי, זה אפשרי רק אם $p \nmid f$ – סתירה.

**שאלה 2** – $f \in \mathbb{Z}_p[x]$ יהי אי פריק. הוכיחו שאם $f$ אינו פריק ב-$\mathbb{Z}_p[x]$ אז $f$ אינו פריק ב-$\mathbb{Z}[x]$.

**פתרון:** נניח ש-$f$ פריק ב-$\mathbb{Z}[x]$, כלומר $f = g \cdot h$ עבור $g, h \in \mathbb{Z}[x]$ לא הפיכים. נסתכל על $\bar{f} = \bar{g}\bar{h}$ ב-$\mathbb{Z}_p[x]$. מכיוון ש-$f$ אינו פריק ב-$\mathbb{Z}_p[x]$, אחד הגורמים, נניח $\bar{g}$, הוא הפיך, כלומר $\deg \bar{g} = 0$. אבל $\deg \bar{g} \leq \deg g$, ולכן $\deg g = 0$, כלומר $g$ קבוע. מכיוון ש-$g$ לא הפיך ב-$\mathbb{Z}[x]$, נקבל $g = p$. אבל אז $p \mid f$ ב-$\mathbb{Z}[x]$, ומכיוון ש-$f$ פרימיטיבי, זה אפשרי רק אם $p \nmid f$ – סתירה.

**שאלה 3** – יהי $f \in \mathbb{Z}[x]$ פולינום פרימיטיבי ממעלה חיובית. הוכיחו שקיים $p$ ראשוני כך ש-$f$ אינו פריק ב-$\mathbb{Z}_p[x]$.

**פתרון:** נניח בשלילה שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Z}_p[x]$. נסתכל על $f$ ב-$\mathbb{Z}[x]$. מכיוון ש-$f$ פרימיטיבי, $f$ אינו פריק ב-$\mathbb{Z}[x]$ אם ורק אם $f$ אינו פריק ב-$\mathbb{Q}[x]$. מכיוון ש-$f$ פריק ב-$\mathbb{Z}_p[x]$ לכל $p$, נקבל שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Q}[x]$. אבל זה אומר שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Q}[x]$, כלומר $f$ אינו פריק ב-$\mathbb{Q}[x]$. אבל זה אומר ש-$f$ אינו פריק ב-$\mathbb{Z}[x]$, כלומר $f$ אינו פריק ב-$\mathbb{Z}[x]$.

**שאלה 4** – יהי $f \in \mathbb{Z}[x]$ פולינום פרימיטיבי ממעלה חיובית. הוכיחו שקיים $p$ ראשוני כך ש-$f$ אינו פריק ב-$\mathbb{Z}_p[x]$.

**פתרון:** נניח בשלילה שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Z}_p[x]$. נסתכל על $f$ ב-$\mathbb{Z}[x]$. מכיוון ש-$f$ פרימיטיבי, $f$ אינו פריק ב-$\mathbb{Z}[x]$ אם ורק אם $f$ אינו פריק ב-$\mathbb{Q}[x]$. מכיוון ש-$f$ פריק ב-$\mathbb{Z}_p[x]$ לכל $p$, נקבל שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Q}[x]$. אבל זה אומר שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Q}[x]$, כלומר $f$ אינו פריק ב-$\mathbb{Q}[x]$. אבל זה אומר ש-$f$ אינו פריק ב-$\mathbb{Z}[x]$, כלומר $f$ אינו פריק ב-$\mathbb{Z}[x]$.

**שאלה 5** – יהי $f \in \mathbb{Z}[x]$ פולינום פרימיטיבי ממעלה חיובית. הוכיחו שקיים $p$ ראשוני כך ש-$f$ אינו פריק ב-$\mathbb{Z}_p[x]$.

**פתרון:** נניח בשלילה שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Z}_p[x]$. נסתכל על $f$ ב-$\mathbb{Z}[x]$. מכיוון ש-$f$ פרימיטיבי, $f$ אינו פריק ב-$\mathbb{Z}[x]$ אם ורק אם $f$ אינו פריק ב-$\mathbb{Q}[x]$. מכיוון ש-$f$ פריק ב-$\mathbb{Z}_p[x]$ לכל $p$, נקבל שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Q}[x]$. אבל זה אומר שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Q}[x]$, כלומר $f$ אינו פריק ב-$\mathbb{Q}[x]$. אבל זה אומר ש-$f$ אינו פריק ב-$\mathbb{Z}[x]$, כלומר $f$ אינו פריק ב-$\mathbb{Z}[x]$.

**שאלה 6** – יהי $f \in \mathbb{Z}[x]$ פולינום פרימיטיבי ממעלה חיובית. הוכיחו שקיים $p$ ראשוני כך ש-$f$ אינו פריק ב-$\mathbb{Z}_p[x]$.

**פתרון:** נניח בשלילה שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Z}_p[x]$. נסתכל על $f$ ב-$\mathbb{Z}[x]$. מכיוון ש-$f$ פרימיטיבי, $f$ אינו פריק ב-$\mathbb{Z}[x]$ אם ורק אם $f$ אינו פריק ב-$\mathbb{Q}[x]$. מכיוון ש-$f$ פריק ב-$\mathbb{Z}_p[x]$ לכל $p$, נקבל שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Q}[x]$. אבל זה אומר שלכל $p$ ראשוני, $f$ פריק ב-$\mathbb{Q}[x]$, כלומר $f$ אינו פריק ב-$\mathbb{Q}[x]$. אבל זה אומר ש-$f$ אינו פריק ב-$\mathbb{Z}[x]$, כלומר $f$ אינו פריק ב-$\mathbb{Z}[x]$.

Scanned by CamScanner

$$p(x)=(ax+b)k_2(x)$$
ראשוני > אחד

$p(a)\equiv 0$ כך ש- $a\in\mathbb{Z}$ קיים $p(x)\equiv(x-a)k_2(x)$ כך ש- $k_2(x)\in\mathbb{Z}_p[x]$

לכן כנ"ל.

**כתרגיל הוכיחו את הלמה הבאה:**

יהי $p$ ראשוני. נניח שלפולינום $f(x)\in\mathbb{Z}[x]$ אין שורשים מודולו $p$. אזי קיים מספר טבעי $k$ כך שלמשוואה $f(x)\equiv 0 \pmod{p^k}$ אין פתרונות.

**הוכחה:** נניח בשלילה שלכל $k$ קיים $x_k$ כך ש- $f(x_k)\equiv 0 \pmod{p^k}$. נשים לב שמתקיים $f(x_k)\equiv 0 \pmod{p^{k-1}}$ ולכן $x_k$ הוא פתרון גם למודולו $p^{k-1}$. מכאן נובע שקיים $x_{k-1}$ כך ש- $x_k\equiv x_{k-1} \pmod{p^{k-1}}$ ו- $f(x_{k-1})\equiv 0 \pmod{p^{k-1}}$. באופן דומה קיים $x_{k-2}$ כך ש- $x_{k-1}\equiv x_{k-2} \pmod{p^{k-2}}$ ו- $f(x_{k-2})\equiv 0 \pmod{p^{k-2}}$. נמשיך כך עד שנגיע ל- $x_1$ כך ש- $f(x_1)\equiv 0 \pmod{p}$. מכיוון שלמשוואה $f(x)\equiv 0 \pmod{p}$ אין פתרונות, נקבל סתירה.

**משפט השאריות הסיני:** יהיו $m_1,\dots,m_n$ מספרים טבעיים זרים בזוגות ויהיו $a_1,\dots,a_n$ מספרים שלמים כלשהם. אזי קיים $x$ כך ש- $x\equiv a_i \pmod{m_i}$ לכל $i$. כל שני פתרונות למערכת הם שקולים מודולו $m_1\cdot\dots\cdot m_n$.

**הוכחה:** נשים לב שמספיק להוכיח את המשפט עבור $n=2$ ולהשתמש באינדוקציה. נניח ש- $m_1,m_2$ זרים ונתבונן בקבוצה $\{a_1+km_1 \mid k\in\mathbb{Z}\}$. נשים לב שכל שני איברים בקבוצה זו שקולים מודולו $m_1$. נוכיח שקיים איבר בקבוצה שקול ל- $a_2$ מודולו $m_2$. נניח בשלילה שלא קיים כזה. אזי לכל $k$ מתקיים $a_1+km_1\not\equiv a_2 \pmod{m_2}$. מכיוון שיש $m_2$ שאריות אפשריות מודולו $m_2$, ומכיוון שיש $m_2$ איברים בקבוצה, לפי עקרון שובך היונים קיימים $k_1,k_2$ כך ש- $a_1+k_1m_1\equiv a_1+k_2m_1 \pmod{m_2}$. נקבל $k_1m_1\equiv k_2m_1 \pmod{m_2}$. מכיוון ש- $m_1,m_2$ זרים, נקבל $k_1\equiv k_2 \pmod{m_2}$, סתירה. לכן קיים איבר בקבוצה שקול ל- $a_2$ מודולו $m_2$, ומכאן שקיים $x$ כך ש- $x\equiv a_1 \pmod{m_1}$ ו- $x\equiv a_2 \pmod{m_2}$.

נניח שקיימים $x,y$ שונים מודולו $m_1\cdot\dots\cdot m_n$ כך ש- $x\equiv a_i \pmod{m_i}$ ו- $y\equiv a_i \pmod{m_i}$ לכל $i$. אזי $x-y\equiv 0 \pmod{m_i}$ לכל $i$, ומכיוון ש- $m_1,\dots,m_n$ זרים בזוגות, נקבל $x-y\equiv 0 \pmod{m_1\cdot\dots\cdot m_n}$, כלומר $x\equiv y \pmod{m_1\cdot\dots\cdot m_n}$, סתירה.

**משפט:** יהי $p$ ראשוני ויהי $f(x)\in\mathbb{Z}[x]$ פולינום שאינו מתאפס מודולו $p$. אזי למשוואה $f(x)\equiv 0 \pmod{p^k}$ יש לכל היותר $k\deg f$ פתרונות מודולו $p^k$.

**הוכחה:** נוכיח באינדוקציה על $k$. עבור $k=1$ המשפט נכון. נניח שהמשפט נכון עבור $k-1$. נניח בשלילה שלמשוואה $f(x)\equiv 0 \pmod{p^k}$ יש יותר מ- $k\deg f$ פתרונות. נסמן $x_1,\dots,x_{k\deg f+1}$ פתרונות שונים מודולו $p^k$. נשים לב שכל $x_i$ הוא פתרון למודולו $p^{k-1}$, ולכן לפי הנחת האינדוקציה קיימים $i,j$ כך ש- $x_i\equiv x_j \pmod{p^{k-1}}$ אך $x_i\not\equiv x_j \pmod{p^k}$. נסמן $x_i=x_j+tp^{k-1}$ עבור $t\not\equiv 0 \pmod{p}$. נציב ונקבל $f(x_j+tp^{k-1})\equiv 0 \pmod{p^k}$. נפתח בטור טיילור ונקבל $f(x_j)+f'(x_j)tp^{k-1}+\dots\equiv 0 \pmod{p^k}$. מכיוון ש- $f(x_j)\equiv 0 \pmod{p^{k-1}}$, נקבל $f'(x_j)t\equiv 0 \pmod{p}$. מכיוון ש- $t\not\equiv 0 \pmod{p}$, נקבל $f'(x_j)\equiv 0 \pmod{p}$. לכן $x_j$ הוא שורש כפול מודולו $p$, ומכאן שיש לכל היותר $\deg f-1$ שורשים כאלה. לכן יש לכל היותר $\deg f$ פתרונות מודולו $p^k$, סתירה.

**מסקנה:** יהי $p$ ראשוני ויהי $f(x)\in\mathbb{Z}[x]$ פולינום שאינו מתאפס מודולו $p$. אזי למשוואה $f(x)\equiv 0 \pmod{p^k}$ יש לכל היותר $k\deg f$ פתרונות מודולו $p^k$.

**משפט:** יהי $p$ ראשוני ויהי $f(x)\in\mathbb{Z}[x]$ פולינום שאינו מתאפס מודולו $p$. אזי למשוואה $f(x)\equiv 0 \pmod{p^k}$ יש לכל היותר $k\deg f$ פתרונות מודולו $p^k$.

**הוכחה:** נוכיח באינדוקציה על $k$. עבור $k=1$ המשפט נכון. נניח שהמשפט נכון עבור $k-1$. נניח בשלילה שלמשוואה $f(x)\equiv 0 \pmod{p^k}$ יש יותר מ- $k\deg f$ פתרונות. נסמן $x_1,\dots,x_{k\deg f+1}$ פתרונות שונים מודולו $p^k$. נשים לב שכל $x_i$ הוא פתרון למודולו $p^{k-1}$, ולכן לפי הנחת האינדוקציה קיימים $i,j$ כך ש- $x_i\equiv x_j \pmod{p^{k-1}}$ אך $x_i\not\equiv x_j \pmod{p^k}$. נסמן $x_i=x_j+tp^{k-1}$ עבור $t\not\equiv 0 \pmod{p}$. נציב ונקבל $f(x_j+tp^{k-1})\equiv 0 \pmod{p^k}$. נפתח בטור טיילור ונקבל $f(x_j)+f'(x_j)tp^{k-1}+\dots\equiv 0 \pmod{p^k}$. מכיוון ש- $f(x_j)\equiv 0 \pmod{p^{k-1}}$, נקבל $f'(x_j)t\equiv 0 \pmod{p}$. מכיוון ש- $t\not\equiv 0 \pmod{p}$, נקבל $f'(x_j)\equiv 0 \pmod{p}$. לכן $x_j$ הוא שורש כפול מודולו $p$, ומכאן שיש לכל היותר $\deg f-1$ שורשים כאלה. לכן יש לכל היותר $\deg f$ פתרונות מודולו $p^k$, סתירה.

**מסקנה:** יהי $p$ ראשוני ויהי $f(x)\in\mathbb{Z}[x]$ פולינום שאינו מתאפס מודולו $p$. אזי למשוואה $f(x)\equiv 0 \pmod{p^k}$ יש לכל היותר $k\deg f$ פתרונות מודולו $p^k$.

Scanned by CamScanner