

שדות סופיים

משפט האיזומורפיזם הראשון לחוגים: $R_1/\ker \phi \cong R_2$.

הגדרה: מאפיין של שדה $\min \{k > 0 : k \cdot 1 = 0\}$.

טענה: המאפיין ראשוני. הוכחה: אחרת שווה ל ab ואז $(a \cdot 1) \cdot (b \cdot 1) = 0$ ואלו מחלקי

אפס. סתירה.

יהא \mathbb{F} שדה סופי אזי מתקיים כי $|\mathbb{F}| = p^n$ עבור p ראשוני ו n טבעי כלשהו.

פתרון: נגדיר $K = \{0, 1, 1+1, \dots\}$ אז \mathbb{F} מ"ו מעליו.

משפט: לכל p ראשוני ו n טבעי קיים שדה \mathbb{F} עם p^n איברים.

לכל p השדה עם p איברים הוא פשוט \mathbb{Z}_p . מה עם שאר המקרים? לצורך זה נכיר את

האידיאלים.

הגדרה: קבוצה $I \subseteq \mathbb{F}[x]$ תקרא אידיאל אם

- מתקיים כי I היא חבורה ביחס לחיבור פולינומים

- לכל $y(x) \in \mathbb{F}[x]$ ולכל $i(x) \in I$ מתקיים כי $y(x)i(x) \in I$.

דוגמא: יהא $f(x) \in \mathbb{F}[x]$ אזי $\langle f \rangle = \{fg \mid g \in \mathbb{F}[x]\}$ הוא אידיאל. הוכחה: $\langle f \rangle$ חבורה כי:

- קיים סגירות $fg_1 + fg_2 = f(g_1 + g_2) \in \langle f \rangle$

- מתקיים קיבוציות כתת קבוצה של הפולינומים

- הנטרלי קיים כי $0 = f \cdot 0 \in \langle f \rangle$

- קיים נגדי: לכל $fg \in \langle f \rangle$ מתקיים כי $-(fg) = f(-g) \in \langle f \rangle$

ומתקיים כי לכל $y(x) \in \mathbb{F}[x]$ ולכל $f(x)g(x) \in \langle f \rangle$ מתקיים כי $f(x)g(x)y(x) \in \langle f \rangle$.

משפט: כל אידיאל $I \subseteq \mathbb{F}[x]$ הוא מהצורה $I = \langle f \rangle$ עבור f מסוים.

הוכחה: יהא I אידיאל. נגדיר $f(x) \neq 0$ להיות הפולינום עם הדרגה הכי נמוכה ב I

שהוא מתוקן. טענה $I = \langle f \rangle$. בכיוון (\subseteq) יהא $i(x) \in I$ אזי נבצע חילוק פולינומים ונקבל

$$i(x) = q(x)f(x) + r(x)$$

כאשר $\deg(r(x)) < \deg(f(x))$ או $r = 0$. אם $r \neq 0$ אז $r(x) = q(x)f(x) - i(x) \in I$

בסתירה למינמאליות של f . לכן $r(x) = 0$ ואז $i(x) = f(x)q(x) \in \langle f \rangle$. בכיוון השני

(\supseteq) יהא $fg \in \langle f \rangle$ אזי $fg = gf \in I$ כי I בולע.

בניה חוג המנה: יהא $I = \langle f \rangle$ אידיאל של $\mathbb{F}[x]$. נגדיר יחס על $\mathbb{F}[x]$ כך

$$g_1 \equiv_f g_2 \iff g_1 - g_2 \in \langle f \rangle$$

זהו יחס שקילות. את קבוצת המנה מסמנים כ $\mathbb{F}[x]/\langle f \rangle$

טענה: נסמן $\deg(f) = n$. כל $y(x) \in \mathbb{F}[x]$ שקול לפולינום מדרגה קטנה מ n הוכחה: נבצע חילוק פולינום

$$y(x) = q(x)f(x) + r(x)$$

ואז $r(x)$ שקול ל $y(x)$ כי

$$y(x) - r(x) = q(x)f(x) \in \langle f \rangle$$

מסקנה:

$$\mathbb{F}[x]/\langle f \rangle = \{[y(x)]_{\equiv_f} : \deg(y(x)) < n\}$$

דוגמא: עבור $\mathbb{R}[x]$ והאידיאל $I = \langle x^2 + 1 \rangle$ נקבל כי

$$\mathbb{R}[x]/\langle x^2+1 \rangle = \{[a + bx] : a, b \in \mathbb{R}\}$$

הגדרה: בסימונים הנ"ל $\mathbb{F}[x]/\langle f \rangle$ הוא חוג ביחס לפעולות

$$[y_1] + [y_2] = [y_1 + y_2]$$

$$[y_1] \cdot [y_2] = [y_1 y_2]$$

למשל ב $\mathbb{R}[x]/\langle x^2+1 \rangle$ מתקיים כי

$$[x][x] = [x^2] = [-1]$$

ולכן $[x]$ הוא הפיך וההופכי שלו $[x]^{-1} = [-x]$ למשל ב $\mathbb{Z}_2[x]/\langle x^2+1 \rangle$ מתקיים כי

$$[x+1][x] = [x^2+x] = [-1+x] = [1+x]$$

ולכן $[1+x]$ אינו הפיך כי אחרת נכפול בהופכי שלו ונקבל $[x] = [1]$ סתירה כי 1 לא שקול ל x

שדות סופיים המשך

ראינו כי עבור $f(x) \in \mathbb{F}[x]$ מתקיים $\mathbb{F}[x]/\langle f \rangle$ חוג.

טענה: $f(x)$ ראשוני-אי-פריק אמ"מ $\mathbb{F}[x]/\langle f \rangle$ הוא שדה.

הוכחה: (\Rightarrow) נניח כי f פריק אז $f = g_1 g_2$ ואז נקבל כי $[g_1][g_2] = 0$ ויש מחלקי אפס. סתירה.

(\Leftarrow) יהא $[a]$ אזי f לא מחלק אותו ולכן $\gcd(f, a) = 1$ לכן $1 = g_1 f + g_2 a$ מודלו f

נקבל $[g_2][a] = [1]$ ולכן הפיך.

למשל ב $\mathbb{R}[x]/\langle x^2+1 \rangle$ מתקיים כי

$$[x][x] = [x^2] = [-1]$$

ולכן $[x]$ הוא הפיך וההופכי שלו $[x]^{-1} = [-x]$

הערה: יהא $p(x) \in \mathbb{F}[x]$ ראשוני מתוקן אזי לכל $a(x)$ מתקיים כי $\gcd(a, p) = 1$ אם p לא מחלק את a אחרת.

תרגיל: הוכיח כי עבור $f(x) = 1 + x + x^3 \in \mathbb{Z}_5[x]$ מתקיים כי $\mathbb{Z}_5[x]/\langle f \rangle$ שדה ומצאו את ההופכי של $[1 + x + x^2]$ בשדה זה.

פתרון: כיוון ש $f(x)$ מדרגה 3 מספיק להראות כי ל $f(x)$ אין שורש ב \mathbb{Z}_5 . אכן $\mathbb{Z}_5 = \{0, \pm 1, \pm 2\}$ ומתקיים

$$f(\pm 2) = 1 + (\pm 2) + (\pm 2)^3 = 1 + (\pm 2) + (\pm 3) = 1$$

$$f(\pm 1) = 1 + (\pm 1) + (\pm 1)^3 = 1 + (\pm 1) + (\pm 1) \in \{-1, 3\}$$

$$f(0) = 1$$

ולכן ל $f(x)$ אין שורש ב \mathbb{Z}_5 .

נמצא הופכי ע"י שימוש ב gcd: כיוון ש $f(x)$ אי פריק לא מחלק את $1 + x + x^2$ אזי $\gcd(1 + x + x^2, p) = 1$ נחלק

$$1 + x + x^3 = (x - 1)(1 + x + x^2) + x + 2$$

$$1 + x + x^2 = (x - 1)(x + 2) + 3$$

ולכן

$$3 = (1 + x + x^2) - (x - 1)(x + 2)$$

$$= (1 + x + x^2) - (x - 1)[(1 + x + x^3) - (x - 1)(1 + x + x^2)]$$

$$= (1 + (x - 1)^2)(1 + x + x^2) - (x - 1)(1 + x + x^3)$$

נכפיל ב $3^{-1} = 2$ ונקבל

$$1 = 2 \cdot (1 + (x - 1)^2)(1 + x + x^2) - 2(x - 1)(1 + x + x^3)$$

ולכן

$$[1] = \left[2 \cdot (1 + (x-1)^2) \right] \left[(1 + x + x^2) \right]$$

ולכן

$$\left[(1 + x + x^2) \right]^{-1} = \left[2 \cdot (1 + (x-1)^2) \right]$$

תרגיל: הוכיחו כי קיים שדה \mathbb{F} עם 8 איברים בו יש פתרון למשוואה $X^3 + X + 1 = 0$.
פתרון: $f(x) = x^3 + x + 1$ פולינום אי פריק מעל \mathbb{Z}_2 ולכן

$$\mathbb{F} = \mathbb{Z}_2[x]/\langle f \rangle$$

שדה. משיעורי בית יש בו $2^3 = 8$ איברים. בנוסף $[x] \in \mathbb{F}$ הוא פתרון למשוואה $X^3 + X + 1 = 0$.

תרגיל: יהא $p(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}_2[x]$ מדרגה $1 \leq n$. הוכיחו כי קיים שדה עם 2^k איברים בו קיים פתרון למשוואה $p(x) = 0$.
פתרון: כ באינדוקציה על n . אם $n = 1$ אזי $p(x) = x + a_0$ ואז בשדה \mathbb{Z}_2 יש פתרון שהוא a_0 .

נניח נכונות עד n ונוכיח עבור n . יהא $p(x) = \sum_{i=0}^n a_i x^i$. אם $p(x)$ אי פריק אזי $\mathbb{F} = \mathbb{Z}_2[x]/\langle p \rangle$ שדה עם 2^n איברים בו $\alpha = [x]_p$ פתרון כי

$$p(\alpha) = \sum_{i=0}^n a_i [\alpha]_p^i = \sum_{i=0}^n a_i [x]_p^i = \left[\sum_{i=0}^n a_i x^i \right] = [0] = 0$$

. אחרת $p(x) = a(x)b(x)$ מדרגות קטנות ממש $p(x)$ ולפי הנחת האינדוקציה קיים שדה עם 2^k איברים בו יש פתרון ל $a(x) = 0$. נסמן α ואז

$$p(\alpha) = a(\alpha)b(\alpha) = 0$$

וסיימנו.

תרגיל: יהא $p(x) \in \mathbb{F}[x]$ מדרגה n אזי יש לו לכל היותר n שורש ב \mathbb{F} .
הוכחה: באינדוקציה על n : עבור $n = 0$ נקבל כי $p(x) = c \in \mathbb{F}$ פולינום קבוע שונה מאפס אזי יש לו 0 שורשים וסיימנו.

נניח נכונות עד n ונוכיח עבור n . יהא $p(x) \neq 0$ פולינום מדרגה n . אם אין לו שורש סיימנו. אם יש לו שורש נסמנו α אזי $(x - \alpha)$ מחלק את $p(x)$ ונקבל $p(x) = q(x)(x - \alpha)$ כאשר $q(x)$ מדרגה $n - 1$ ולפי הנחת האינדוקציה יש לו לכל היותר $n - 1$ שורשים. כעת כל שורש של $p(x)$ הוא שורש של $q(x)$ או של $x - \alpha$ ולכן יש לו לכל היותר $n - 1 + 1 = n$ שורשים.

תרגיל יהא \mathbb{F} שדה סופי עם p^n איברים. הוכיחו כי לכל $a \in \mathbb{F}$ מתקיים כי $a^{p^n} = a$.

פתרון: הקבוצה \mathbb{F}^\times היא חבורה ביחס לכפל של השדה עם $p^n - 1$ איברים. לפי לגרנז' לכל $a \in \mathbb{F}^\times$ $0 \neq a$ מתקיים $a^{p^n - 1} = 1$. נכפיל ב a ונקבל $a^{p^n} = a$. שיוון זה מתקיים גם עבור 0 ולכן לכל $a \in \mathbb{F}$.
 מסקנה: יהא \mathbb{F} שדה סופי עם p^n איברים אזי

$$x^{p^n} - x = \prod_{a \in \mathbb{F}} (x - a)$$

כי כל $a \in \mathbb{F}$ הוא שורש של $x^{p^n} - x \in \mathbb{F}[x]$ ובנוסף קיימים לו לכל היותר p^n שורשים בשדה \mathbb{F} אלו כל שורשיו.

הגדרה: יהא \mathbb{F} שדה תת קבוצה $\mathbb{F}' \subseteq \mathbb{F}$ תקרא תת שדה אם \mathbb{F}' שדה ביחס לפעולות של \mathbb{F} .

$$\text{למשל: } \mathbb{Z}_2 \leq \mathbb{Z}_2[x]/\langle x^2+x+1 \rangle, \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$$

תרגיל: יהא \mathbb{F} עם p^n איברים ויהא \mathbb{F}' תת שדה שלו אזי הגודל שלו הוא p^t איברים כאשר $t|n$

הוכחה: נגדיר $K = \{1, 1+1, \dots\}$ ותראו ב.ש.ב. שיש בקבוצה זאת p איברים, בנוסף $K \subseteq \mathbb{F}'$ ולכן ב \mathbb{F}' קיימים p^t איברים עבור t טבעי. \mathbb{F} הוא מרחב וקטורי מעל \mathbb{F}' ולכן קיים לו בסיס $B = \{v_1, \dots, v_d\}$. כל $x \in \mathbb{F}$ הוא צירוף לינארי יחיד $x = \sum_{i=1}^d \alpha_i v_i$ עבור $\alpha_1, \dots, \alpha_d \in \mathbb{F}'$ ולכן מספר האיברים ב \mathbb{F} הוא

$$|\mathbb{F}| = \left| \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_d \end{pmatrix} : a_1, \dots, a_d \in \mathbb{F}' \right\} \right| = (p^t)^d$$

כיוון ש $p^n = (p^t)^d = p^{td}$ נקבל כי $n = td$ וקיבלנו כי $t|n$.

הצפנת AES – 128

הצפנה סימטרית. צופן בלוקים שמצפין 128 ביט בעזרת מפתח 128 ביט.

1. לוקחים את הפולינום האי פריק $p(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbb{Z}_2[x]$ ועובדים עם השדה $\mathbb{F} = \mathbb{Z}_2[x]/I(p)$. כל איבר בשדה זה הוא $\sum_{i=0}^7 a_i x^i$ שאותו מייצגים בבית כ $(a_7, a_6, \dots, a_1, a_0)$. את הקלט P של 128 ביט מייצגים כמטריצה ב $\mathbb{F}^{4 \times 4}$.

2. מהמפתח הראשי K גוזרים עוד 10 מפתחות סיבוב K_1, \dots, K_{10} .

3. הצופן בנוי מ 10 "סיבובים" כאשר כל סיבוב בנוי מהפונקציות הבאות:

(א) שכבת לא ליארית SB הפעלת פונקציה לא ליארית על כל אחד מ 16 הבתים.

(ב) הוזזת שורות

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} = M \in \mathbb{F}^{4 \times 4} \text{ (ג) הכפלה במטריצה}$$

(ד) AK הוספת מפתח בסיבוב i שהוא K_i

בהינתן קלט P מפעילים את עשרה סיבובים על $P + K$ כאשר בסיבוב האחרון (מספר 10) מושמטת הפונקציה MC .