

אלגברה ב2

© ארזים

22 במרץ 2017

1 פולינומים

נמשיך מהשיעור שעבר.

הגדרה 1.1 פולינום $f \in \mathbb{Z}[x]$ ייקרא פרימיטיבי אם

$$f(x) = \sum_{i=0}^n a_i x^i$$
$$\gcd(a_0, \dots, a_n) = 1$$

באופן שקול, $(a_0, \dots, a_n) = \mathbb{Z}$.

משפט 1.2 (הלמה של גאוס) אם $f, g \in \mathbb{Z}[x]$ פרימיטיבי, אזי גם $f \cdot g \in \mathbb{Z}[x]$ פרימיטיבי.

הוכחה: נניח בשלילה שלא, כלומר קיים p ראשוני שמחלק את כל מקדמי $h = fg$. נסתכל על $\bar{h}, \bar{f}, \bar{g} \in (\mathbb{Z}/p\mathbb{Z})[x]$ שמתקבלים מתוך h, f, g על ידי לקיחת המקדמים מודולו p . אזי

$$\bar{h} = 0$$

מהנחה.

$$\bar{f}, \bar{g} \neq 0$$

כי הם לא פרימיטיביים. החוג $\mathbb{Z}/p\mathbb{Z}[x]$ הוא תחום שלמות, כי $\mathbb{Z}/p\mathbb{Z}$ שדה, בסתירה -
כי עדיין $\bar{f} \cdot \bar{g} = \bar{h}$. ■

מסקנה 1.3 יהי $f \in \mathbb{Z}[x]$ פרימיטיבי. אם f פריק מעל \mathbb{Q} , אזי f פריק מעל \mathbb{Z} .

הוכחה: נניח כי f פריק מעל \mathbb{Q} . נכתוב $f = gh$, כאשר $g, h \in \mathbb{Q}[x]$. נרשום

$$h = c_1 h_0, g = c_2 g_0$$

כאשר $h_0, g_0 \in \mathbb{Q}[x], c_1, c_2 \in \mathbb{Q}$ מתוקנים. נכפיל את h_0, g_0 בשלמים מינימליים m, n כל שיתקיים $mh_0 \in \mathbb{Z}[x], ng_0 \in \mathbb{Z}[x]$ פרימיטיביים, ואז

$$\frac{nm}{c_1 c_2} f = (mh_0)(ng_0)$$

אגף ימין הוא מכפלת שני פרימיטיביים, ולכן פרימיטיבי. כפולה של f היא פרימיטיבית, ולכן בהכרח $\frac{nm}{c_1 c_2} = 1$, ולכן

$$f = (mh_0)(ng_0)$$

■ וזהו פירוק של f מעל \mathbb{Z} .

מסקנה 1.4 אם $f \in \mathbb{Z}[x]$ מתוקן, $g \in \mathbb{Q}[x]$ מחלק מתוקן של f בחוג $\mathbb{Q}[x]$, אזי $g \in \mathbb{Z}[x]$.
הוכחה: נרשום $f = gh$. מתוקנים, ולכן גם h מתוקן. נכפיל את g פי טבעי מינימלי n שעבורו $ng \in \mathbb{Z}[x]$ פרימיטיבי, כלומר n הוא המכנה המשותף המינימלי של מקדמי g . באותו אופן נכפול את h פי טבעי מינימלי m שעבורו $mh \in \mathbb{Z}[x]$ פרימיטיבי. כעת,

$$nmf = (ng)(mh)$$

מהלמה של גאוס נקבל כי nmf פרימיטיבי. לכן נקבל כי $nm = 1$, כלומר $n = 1, m = 1$.
 ■ לכן $g, h \in \mathbb{Z}[x]$ פרימיטיביים.

1.1 קריטריון איזנשטיין

דוגמא $x^5 + 3x^4 + 12x^3 + 6x^2 + 3x + 15$ אי פריק.

טענה 1.5 (קריטריון איזנשטיין) אם $f(x) \in \mathbb{Z}[x]$ מתוקן, נרשום

$$f(x) = x^n + \sum_{i=0}^{n-1} a_i x^i$$

כעת אם יש ראשוני המקיים:

1. $a_i \mid p$ לכל i .

2. $p^2 \nmid a_0$.

אזי f אי פריק בחוג $\mathbb{Q}[x]$.

הוכחה: נסתכל מודולו p . אם f פריק, אזי לפי הלמה של גאוס $f = gh$ כאשר $g, h \in \mathbb{Z}[x]$ מתוקנים. נסמן $\bar{f}, \bar{g}, \bar{h}$ את הפולינומים מתוך $\mathbb{F}_p[x]$ המתקבלים מתוך f, g, h על ידי לקיחת המקדמים מודולו p . אזי

$$x^n = \bar{f} = \bar{g}\bar{h}$$

נטען כי בהכרח $\bar{g} = x^{\deg g}$, $\bar{h} = x^{\deg h}$. אחרת, ניקח את המונום ממעלה הכי נמוכה של \bar{g} ונסמנו ax^r , כאשר $r \leq \deg g$, $a \neq 0$. באותה צורה, bx^s המונום ממעלה הכי נמוכה של h עם $s \leq \deg h$, $b \neq 0$. אם $s = \deg h$, $r = \deg g$, אחרת, בלי הגבלת הכלליות, $r < s$, ואז המקדם הכי קטן של $\bar{g}\bar{h}$ הוא abx^{s+r} , כאשר $s+r < n$, ולכן לא מתקיים $\bar{g}\bar{h} = x^n$. בסתירה.

לכן כל המקדמים של g, h מתחלקים בראשוני p , פרט לעליון. המקדם החופשי של f הוא מכפלת המקדמים החופשיים של g, h , ולכן $a_0 \equiv p^2 \pmod{p}$. לכן f אי פריק. ■

טענה 1.6 יהי $f \in \mathbb{Z}[x]$ מתוקן, ונניח שיש ראשוני p כך שהפולינום \bar{f} שמתקבל על ידי לקיחת מקדמי f מודולו p הוא אי פריק בתוך $\mathbb{F}_p[x]$. אזי f אי פריק.

הוכחה: אם f פריק, אזי יש $g, h \in \mathbb{Z}[x]$ מתוקנים ולא קבועים המקיימים $f = gh$. כעת

$$\bar{f} = \bar{g}\bar{h}$$

וכן \bar{g}, \bar{h} לא קבועים כמו כן, בסתירה לאי פריקות של \bar{f} .
 נקודה למחשבה: בהנתן $f \in \mathbb{Z}[x]$ אי פריק, האם יש p כך שהפולינום \bar{f} אי פריק? ■

2 הרחבת שדות

2.1 תכונות בסיסיות

תזכורת שדה הוא חוג שבו כל איבר שאינו 0 הפיך.

הגדרה 2.1 שדה E המכיל תת שדה F נקרא הרחבה של F , ומסומן E/F .

במצב זה, יש מבנה טבעי של מרחב ווקטורי מעל F על E ולכן מוגדר מימד.

הגדרה 2.2 המעלה של הרחבה E/F היא $\dim_F E$ היא $[E : F]$.

הגדרה 2.3 הרחבה E/F תיקרא סופית אם $[E : F] < \infty$.

דוגמאות ההרחבה \mathbb{C}/\mathbb{R} סופית - $[\mathbb{C} : \mathbb{R}] = 2$. ההרחבה \mathbb{R}/\mathbb{Q} ממעלה אינסופית. אם נגדיר את המספרים הגאוסיינים מעל \mathbb{Q} בתור

$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}, i^2 = -1\}$$

אזי $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, עם בסיס $\{1, i\}$.
 באופן כללי, אם \mathbb{F} שדה, x משתנה, אזי $\mathbb{F}[x]$ הוא חוג הפולינומים מעל \mathbb{F} , ואת שדה המנות שלו סימנו $\mathbb{F}(x)$ - שדה הפונקציות הרציונאליות מעל \mathbb{F} במשתנה x . אזי $\mathbb{F}(x)/\mathbb{F}$ הרחבה ממעלה אינסופית.

הגדרה 2.4 לסדרה $F_1 \subseteq F_2 \subseteq \dots \subseteq F_n \subseteq \dots$ נקרא מגדל של שדות אם F_{i+1}/F_i הרחבה של שדות לכל i .

טענה 2.5 יהי $F \subseteq E \subseteq K$ מגדל של שדות. אזי K/F סופית אם ורק אם $E/F, K/E$ סופיות. במקרה כזה,

$$[K : F] = [K : E][E : F]$$

הוכחה: נבחר בסיס $\{e_i\}_{i \in I}$ של E/F , ובסיס $\{k_j\}_{j \in J}$ של K/E . נטען כי $B = \{e_i k_j\}_{i \in I, j \in J}$ בסיס של K/F . אם נוכיח את זה, נסיים את ההוכחה. נראה כי B פורש. נקח $k \in K$. יש $a_1, \dots, a_n \in E$ המקיימים

$$k = \sum_{r=1}^n a_r k_{j_r}$$

אבל $a_r \in E$, ולכן לכל r קיימים $b_{r,s} \in F$ המקיימים

$$a_r = \sum_{s=1}^m b_{r,s} e_{i_s}$$

ולכן

$$k = \sum_{r=1}^n \sum_{s=1}^m b_{r,s} e_{i_s} k_{j_r}$$

ולכן B פורש. כעת נראה כי B בלתי תלוי לינארית. נניח כי קיימים $b_{r,s} \in F$ המקיימים

$$\sum_{r=1}^n \sum_{s=1}^m b_{r,s} e_{i_s} k_{j_r} = 0$$

אזי

$$\sum_{r=1}^n \left(\sum_{s=1}^m b_{r,s} e_{i_s} \right) k_{j_r} = 0$$

אבל $\{k_j\}$ בסיס, ולכן

$$\sum_{s=1}^m b_{r,s} e_{i_s} = 0$$

לכל r . אבל $\{e_i\}$ בסיס, ולכן $b_{r,s} = 0$ לכל r, s .
 ■ קיבלנו כי B בסיס, ולכן הוכחנו את הנדרש.

הגדרה 2.6 תהי E/F הרחבה של שדות, $\alpha \in E$. נאמר כי α אלגברי מעל F אם ההרחבה $F(\alpha)/F$ היא סופית.

כאן $F(\alpha)$ הוא תת השדה המינימלי של E שמכיל את F ואת α (שהוא גם חיתוך כל תת השדות שמקיימים את זה). באופן כללי יותר, אם E/F הרחבה, $\Omega \subseteq E$, נסמן בתור $F[\Omega]$ את תת החוג המינימלי של E שמכיל את F ואת Ω (שוב שקול לחיתוך כל תתי החוגים שמקיימים את ההכלה), ובתור $F(\Omega)$ את תת השדה המינימלי עם אותה תכונה (חיתוך כל תת השדות עם התכונה).

טענה 2.7 1. אם $x \in F[\Omega]$ אז x הוא צירוף לינארי מעל F של מכפלות וחזקות של איברי Ω .

2. השדה $F(\Omega)$ הוא שדה המנות של $F[\Omega]$.

הוכחה: ברור שאוסף הצירופים הלינאריים מעל F של מכפלות וחזקות של איברי Ω מכיל את F ואת Ω , ולכן מכיל את $F[\Omega]$. מצד שני, כל איבר של $F[\Omega]$ הוא צירוף לינארי שכזה, ולכן נקבל שוויון. הטענה השנייה ברורה. ■

$$\text{בפרט, } F(\alpha) = F(\{\alpha\})$$

למה 2.8 תהי E/F הרחבה סופית, ויהי $\alpha \in E$

1. α אלגברי מעל F .

$$2. I = \{f \in F[x] \mid f(\alpha) = 0\} \triangleleft F[x], I \neq 0$$

3. $f \in I, f \neq 0$ ממעלה מינימלית אם ורק אם f אי פריק עם $f(\alpha) = 0$.

4. נקח $f \in I, f \neq 0$ ממעלה מינימלית, שנסמנה n . אזי $\{1, \alpha, \dots, \alpha^{n-1}\}$ היא בסיס של $F(\alpha)/F$. בפרט, $F[\alpha] = F(\alpha)$, וכן $[F(\alpha) : F] = n$.

הוכחה:

1. $F \subseteq F(\alpha) \subseteq E$, ולכן $F(\alpha)/F$ סופית - כלומר α אלגברי.

2. אם $f, g \in I$ אזי

$$(f + g)(\alpha) = f(\alpha) + g(\alpha) = 0 + 0 = 0$$

ולכן I סגור לחיבור. אם $f \in I, g \in F[x]$ אזי

$$(fg)(\alpha) = f(\alpha)g(\alpha) = 0g(\alpha) = 0$$

ולכן I סגור לכפל באיברי $F[x]$, כלומר אידאל. נוכיח שאינו 0. נתבונן בקבוצה $\{1, \alpha, \alpha^2, \dots\} \subseteq \mathbb{E}$, שהיא אינסופית (עם חזרות). $[E : F] < \infty$, ולכן הקבוצה תלוייה לינארית, כלומר קיימים $a_i \in F$ שלא כולם 0 כך שמתקיים

$$\sum_{i=0}^N a_i \alpha^i = 0$$

כעת, אם נגדיר

$$f(x) = \sum_{i=0}^N a_i x^i$$

נקבל בבירור כי $f \in I$ לכן $I \neq 0$.

3. יהי $f \in I$ ממעלה מינימלית. אם f פריק, אזי $f = gh$, כאשר g, h לא קבועים. כעת

$$0 = f(\alpha) = g(\alpha)h(\alpha)$$

ומכאן נובע כי $g(\alpha) = 0$ או $h(\alpha) = 0$, בסתירה למינימליות הדרגה של f .
כעת, אם $f \in I$ אי פריק, וכן $g \in I$ ו- $g \neq 0$ ממעלה מינימלית, אזי

$$I = (g)$$

לכן $f = gh$, ומאי פריקות נובע כי $\deg g = 0$ או $\deg h = 0$. $\deg g \neq 0$, כי $g(\alpha) = 0, g \neq 0$. לכן $\deg h = 0$, ואז $\deg f = \deg g$.

4. נוכיח בשיעור הבא.

■