

אלגברה לינארית 2א

© ארזים

22 במרץ 2016

הגדרה 0.1 אומרים ששני איברים a, b הם זרים אם $\gcd(a, b) = 1$.

דוגמה: ניקח $p = 101$ ראשוני שדה F_p . ניקח $a = 39$. נרצה לחשב את $a^{-1} \in F_p$. האלגוריתם האוקלידי מאפשר לנו לחשב במהירות את a^{-1} .

$$\begin{aligned} 101 &= 2 \cdot 39 + 23 \\ 39 &= 1 \cdot 23 + 16 \\ 23 &= 1 \cdot 16 + 7 \\ 16 &= 2 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \end{aligned}$$

כעת נתחיל לעבוד בחזרה בכיוון ההפוך.

$$\begin{aligned} 1 &= 7 - 3 \cdot 2 = 7 - 3 \cdot (16 - 2 \cdot 7) = 7 \cdot 7 - 3 \cdot 16 = 7 \cdot (23 - 16) - 3 \cdot 16 = \\ &= 7 \cdot 23 - 10 \cdot 16 = 7 \cdot 23 - 10 \cdot (39 - 23) = 17 \cdot 23 - 10 \cdot 39 = \\ &= 17 \cdot (101 - 2 \cdot 39) - 10 \cdot 39 = 17 \cdot 101 - 44 \cdot 39 \end{aligned}$$

לכן נסיק שמתקיים

$$-44 \cdot 39 \equiv 1 \pmod{101}$$

השלמה נוספת: התחום

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

ראינו גם נורמה עבור חוג זה:

$$||\alpha|| = \alpha \cdot \bar{\alpha} = a^2 + b^2$$

אזי

$$||\alpha \cdot \beta|| = ||\alpha|| \cdot ||\beta||$$

בתרגול נוכיח שבתחום זה קיים חילוק עם שארית ביחס לנורמה, כלומר לכל $\alpha, \beta \in R$ מתקיים $\alpha \mid \beta$ או שמתקיים $\alpha = h \cdot \beta + r$, כאשר $\|r\| \leq \|\beta\|$. זה מאפשר בקלות להראות שזהו גם תחום ראשי, בדיוק כמו בהוכחות של $F[x]$ או $\mathbb{Z}$. מכאן נובע גם שראשוניות ואי־פריקות שקולות בתחום זה. שאלה טבעית: אילו ראשוניים מהשלמים נשארים כאלה כאירים בחוג שלנו?

נשים לב שההפיכים בחוג שלנו הם בדיוק $\pm 1, \pm i$.

$$1 = \|1\| = \|\alpha \cdot \beta\| = \|\alpha\| \cdot \|\beta\|$$

ואם מכפלת שני טבעיים היא 1 אזי שניהם 1, ולכן קיבלנו את שאמרנו. כעת ניתן את אותו טיעון על ראשוני p :

$$p^2 = \|p\| = \|\alpha \cdot \beta\| = \|\alpha\| \cdot \|\beta\|$$

כיוון שהאיברים α, β לא הפיכים, הנורמות שלהם אינן 1, ולכן $\|\alpha\| = \|\beta\| = p$. מצד שני, אם קיימים $a, b \neq 0$ כך שמתקיים

$$p = a^2 + b^2 = (a + bi)(a - bi)$$

אזי רואים שהאיבר p מתפרק בחוג $\mathbb{Z}[i]$.

מסקנה 0.2 $p \in \mathbb{Z}$ נשאר ראשוני בחוג $\mathbb{Z}[i] \iff$ לא קיימים $a, b \in \mathbb{Z}$ כך שמתקיים $a^2 + b^2 = p$.

הוכחה: מצד אחד אם p פריק הראינו כבר שקיים $\alpha \in \mathbb{Z}[i]$ כך שמתקיים $\|\alpha\| = p$, ולכן הוא אכן סכום של שני ריבועים. ■

כמו כן ניתן לבדוק שראשוני נכתב כסכום של ריבועים אם ורק אם $p \equiv 1 \pmod{4}$, או $p = 2$.

1 הפולינום המינימלי

נחזור לדבר על מטריצות וטרנספורמציות.

משפט 1.1 יהי F שדה ותהי $A \in M_n(F)$ מטריצה. קבוצת כל הפולינומים $p(x) \in F[x]$ שמתאפסים על A היא אידאל בחוג $F[x]$. קיים בה איבר יחיד מתוקן בעל דרגה מינימלית ולו קוראים הפולינום המינימלי של A . הוא מסומן $m_A(x)$ ומקיים

$$\forall f \in F[x]. f(A) = 0 \Rightarrow m_A(x) \mid f$$

כמובן שמשפט זה נכון לגבי טרנספורמציות לינאריות.

הוכחה: בדיקה פשוטה מראה שקבוצת הפולינומים שמתאפסים על A מכילה את פולינום האפס, סגורה לחיבור, וסגורה לכפל בכל פולינום, ולכן היא אידיאל - נסמנה I_A . יהי $m_A(x)$ איבר מתוקן בעל דרגה מינימלית באידיאל זה. הוכחנו על ידי חילוק עם שארית שמתקיים $I_A = (m_A)$. כעת נוכיח את היחידות. נניח $g(x)$ יוצר אחר של m_A . נובע כי $m_A \mid g, g \mid m_A$ ולכן $g \sim m_A$, לכן הם נבדלים בכפל בקבוע. אבל g מתוקן, לכן הקבוע הוא 1. ■

משפט 1.2 אם מטריצה A מייצגת טרנספורמציה T אזי $m_A = m_T$.

הוכחה: האידיאלים המוגדרים על ידי איפוס T או איפוס A הם זהים ולכן בפרט יש להם את אותו יוצר. מדוע זהים? כי אם $p(x) \in F[x]$ מתקיים

$$p(A) = 0 \iff p(T) = 0$$

$$[p(T)]_B = p([T]_B) \text{ וכן}$$

מסקנה 1.3 אם A, C דומות אזי $m_A = m_C$.

הוכחה: A, C דומות $\iff$ מייצגות את אותה טרנספורמציה לינארית T ביחס לבסיסים שונים. עכשיו נשתמש במשפט הקודם. תרגול קל: תנו הוכחה ישירה. ■

מסקנה 1.4 נניח A לכסינה עם ערכים עצמיים שונים $\lambda_1, \dots, \lambda_k$ אזי

$$m_A(x) = \prod_{i=1}^k (x - \lambda_i)$$

הוכחה: מהמסקנה הקודמת, נוכל להניח שהמטריצה כבר אלכסונית. במקרה זה $A - \lambda_i I$ היא בעלת אפסים בגוש i באלכסון (ואין אפסים מחוץ לו) ולכן המכפלה

$$\prod_{i=1}^k (A - \lambda_i I)$$

היא מכפלה של k מטריצות אלכסוניות שכל איבר אלכסוני מתאפס באחת מהן $\iff$ המכפלה מתאפסת. זה מוכיח שהפולינום הנ"ל מאפס את A . ייתכן שהפולינום המינימלי הוא ממעלה נמוכה יותר? ידוע אז שהפולינום המינימלי חייב לחלק את הפולינום שלנו, ומיחידות הפירוק בחוג $F[x]$, הפולינום המינימלי חייב להיות מורכב מחלק הגורמים של הפולינום שלנו, אבל לא כל k הגורמים, וברור שאז לא יכול להיות שהפולינום יאפס את A . ■

משפט 1.5 תהי d הדרגה של הפולינום המינימלי. אזי

$$d = \dim \text{span} \{I, A, A^2, A^3, \dots\} \subseteq M_n(F)$$

הוכחה: מצד אחד נסמן

$$m_A(x) = \sum_{i=0}^d a_i x^i, \quad a_d = 1$$

$$A^d = \sum_{i=0}^{d-1} -a_i A^i$$

כופלים במטריצה A

$$A^{d+1} = \sum_{i=0}^{d-1} a_i A^{i+1}$$

אז נציב את A^d ונקבל שאת A^{d+1} גם אפשר להציג כצירוף לינארי של $I, A, A^2, \dots, A^{d-1}$. מכפילים שוב במטריצה A ומקבלים כנ"ל עבור A^{d+2} וכולי. מכאן נובע:

$$\text{span}\{I, A, A^2, \dots\} = \text{span}\{I, \dots, A^{d-1}\}$$

ולכן נובע שהמימד במשפט קטן או שווה d . נשאר להוכיח אי שוויון בכיוון השני. ואכן, נראה שהמטריצות $I, A, \dots, A^{d-1}$ הן בת"ל. אכן, נניח שקיים צירוף לינארי

$$\sum_{i=0}^{d-1} b_i A^i = 0$$

כלומר הפולינום שמקדמיו b_i ממעלה $d-1$ לכל היותר מאפס את A , וממינימליות נקבל שהוא פולינום האפס, לכן מקדמיו אפס, כלומר $b_i = 0$ לכל i . לכן הווקטורים בת"ל ואי־השוויון נובע. ■