

אלגברה לינארית 2א

© ארזים

15 במרץ 2016

נמשיך להוכיח את משפט קיילי המילטון. הוכחה: מחלקים לשלבים:

1. כאשר לטרנספורמציה יש ייצוג משולשי - הוכחנו בשיעור שעבר.

2. כאשר הפולינום האופייני של המטריצה מתפרק למכפלת גורמים לינאריים - ראינו בשבוע שעבר שבמצב כזה המטריצה דומה למטריצה משולשית (ראינו זאת על טרנספורמציות - מקבלים זאת גם על מטריצות על ידי הסתכלות על T_A). לכן קיימת הפיכה P כך שהמטריצה $C = PAP^{-1}$ משולשית, ולכן מהשלב הראשון, $f_C(C) = 0$. בנוסף, A, C דומות, ולכן $f_A = f_C$, וראינו כי אם A, C דומות אזי $f(C) = 0 \iff f(A) = 0$, ולכן $f_C(A) = 0 = f_A(A)$.

3. כאן נשתמש בטענה הבאה:

טענה 0.1 יהי F שדה כלשהו ויהי $f \in F[x]$ פולינום מעל F . אזי קיים שדה $K \subseteq F$ כך שמעל K הפולינום f מתפצל למכפלת גורמים לינאריים.

כעת, נוכל להמשיך באותה הוכחה - מעל K הפולינום מתפצל, ולכן מהשלב השני קיילי המילטון מתקיים.

■

1 חוג הפולינומים

כאשר F שדה, נגדיר את חוג הפולינומים מעליו:

$$F[x] = \left\{ p(x) = \sum_{i=0}^n a_i x^i \mid a_i \in F \right\}$$

הדרגה של p ($\deg p$) מוגדרת להיות i המקסימלי בפולינום עבור $a_i \neq 0$. אנחנו יודעים לחבר ולכפול את האיברים באופן טבעי. תכונה בסיסית של פעולות אלה היא חילוק עם שארית, בדיוק כמו בשלמים. שם מתקיים שלכל $n \neq 0, m, n \in \mathbb{Z}$ קיימים $k, r \in \mathbb{Z}$ יחידים כך שמתקיים $m = k \cdot n + r$ עבור $0 \leq r < |n|$. עבור $F[x]$ מתקיימת הטענה הבאה:

טענה 1.1 יהיו $f(x), g(x) \in F[x], g(x) \neq 0$. אזי קיימים $h(x), r(x) \in F[x]$ יחידים כך שמתקיים $f(x) = h(x) \cdot g(x) + r(x)$ וכן $\deg r < \deg g$.

הוכחה: נוכיח באינדוקציה על $\deg f$. אם $\deg f = 0$, הטענה טריוויאלית, כי f קבועה. כעת נניח שהטענה נכונה עבור $\deg f \leq n$ ונוכיח עבור $\deg f = n + 1$.

1. אם $\deg g > \deg f$, אז ניקח $r = f$, $h = 0$.

2. נסמן

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

$$g(x) = \sum_{i=0}^m b_i x^i$$

ונניח $m \leq n + 1$. נגדיר

$$h'(x) = \frac{a_{n+1}}{b_m} \cdot x^{n+1-m}$$

ואז ברור שמתקיים

$$\deg(f - h'g) \leq n$$

כעת, מהנחת האינדוקציה, קיימים h'', r כך שמתקיים

$$\begin{aligned} f - h'g &= h''g + r \\ f &= (h' + h'')g + r \end{aligned}$$

וכעת נסמן $h = h' + h''$. הוכחה זו נותנת למעשה אלגוריתם מדויק לחישוב של חילוק עם שארית.

כעת נוכיח את היחידות. נניח

$$f = h_1 g + r_1 = h_2 g + r_2$$

כלומר מתקיים

$$(h_1 - h_2)g = r_2 - r_1$$

הדרגה של $h_1 g$ היא לפחות דרגתו של g , אלא אם הוא מתאפס. אבל דרגת $h_1 g$ ימין תמיד קטנה מדרגת g , לכן בהכרח

$$\begin{aligned} (h_1 - h_2)g &= 0 \\ h_1 - h_2 &= 0 \\ h_1 &= h_2 \end{aligned}$$

■

כעת, ברור שמתקיים גם $r_1 = r_2$.

שלוש מסקנות מן המשפט:

מסקנה 1.2 אם α שורש של הפולינום $f(x)$ אזי $x - \alpha \mid f(x)$, כלומר קיים $h(x)$ כך שמתקיים $f(x) = (x - \alpha)h(x)$.

הוכחה: נבצע חילוק עם שארית בפולינום $g(x) = (x - \alpha)$. נקבל $f(x) = h(x)(x - \alpha) + r(x)$, כאשר r פולינום האפס או שדרגתו נמוכה משל g - כלומר הוא קבוע. נציב α :

$$\begin{aligned} 0 &= f(\alpha) = h(\alpha) \cdot 0 + r \\ 0 &= r \end{aligned}$$

■

מסקנה 1.3 אם $\deg f = n$, כאשר $f \neq 0$, אזי יש לפולינום f לכל היותר n שורשים שונים.

הוכחה: נוכיח באינדוקציה על הדרגה של f . אם f קבוע הטענה טריוויאלית, וכלל לגבי פולינום לינארי. נניח שהטענה נכונה כאשר $\deg f = n$. כעת נניח שהמספרים $\alpha_1, \dots, \alpha_k$ שורשים שונים של f . מהמסקנה הקודמת אנחנו יודעים שמתקיים $x - \alpha_k \mid f(x)$, כלומר $f(x) = h(x)(x - \alpha_k)$. כעת, $\deg h = \deg f - 1 = n$, ולכל $1 \leq i \leq k - 1$, α_i הוא שורש של h , שכן כל השורשים שונים. מהנחת האינדוקציה על h , נובע שמתקיים $k - 1 \leq n$, ולכן $k \leq n + 1$ כמו שרצינו להראות.

■

שימוש נפוץ במסקנה זו הוא כאשר שני פולינומים שדרגתם לכל היותר n מזדהים על יותר מאשר n ערכים, ואז נובע שהפולינומים שווים - מסתכלים על הפרשם ומקבלים שיש לו "יותר מדי" שורשים, ולכן הוא פולינום האפס.

מסקנה 1.4 נניח $F \subseteq K$ שדות. יהיו $f, g \in F[x]$. אם $g \mid f$ בחוג $K[x]$, אזי $g \mid f$ גם בחוג $F[x]$ (הכיוון השני טריוויאלי).

הוכחה: מעל K ידוע שמתקיים

$$f(x) = h(x) \cdot g(x)$$

מעל F , נבצע חלוקה עם שארית:

$$f(x) = h_1(x) \cdot g(x) + r(x)$$

כעת נחשוב על שניהם כחילוק עם שארית מעל K , ונקבל סתירה ליחידות אם $r \neq 0$.

■

2 חוגים כלליים

הגדרה 2.1 חוג קומוטטבי עם יחידה היא קבוצה R שעליה מוגדרות שתי פעולות המסומנות $+$, $\cdot$ ועם איברים נייטרליים לחיבור (0) ולכפל (1), כך שמתקיימות כל אקסיומות השדה פרט לקיום איבר הופכי.

דוגמאות: $\mathbb{Z}$, $F[x]$ עבור כל שדה שהוא. כמו כן, $\mathbb{Z} \times \mathbb{Z}$ עם פעולות חיבור וכפל בקואורדינטות $(1 = (1, 1), 0 = (0, 0))$.

הגדרה 2.2 איבר $u \in R$ נקרא הפיך או יחידה אם קיים $a \in R$ כך שמתקיים $a \cdot u = 1$.

דוגמאות: $\mathbb{Z}$ - היחידות הן $1, -1$. בפולינומים - הקבועים. $\mathbb{Z} \times \mathbb{Z}$ - $(\pm 1, \pm 1)$.

הגדרה 2.3 חוג כזה נקרא תחום שלמות אם $a \cdot b = 0$ גורר שבהכרח $a = 0$ או $b = 0$.

טענה 2.4 (כלל הצימצום בתחום שלמות) אם $c \neq 0$ ומתקיים $ac = bc$ אזי $a = b$.

הוכחה: $ac - bc = 0$, ולכן $(a - b)c = 0$. ידוע $c \neq 0$, לכן $a - b = 0$, ולכן $a = b$. ■

הגדרה 2.5 יהי R תחום שלמות. $r \in R$ ייקרא אי-פריק אם השוויון $r = a \cdot b$ גורר שבהכרח a הפיך או b הפיך (נשים לב שאם a הפיך נוכל תמיד לכתוב $(r = a \cdot (r \cdot a^{-1}))$).

דוגמאות: עבור $F[x]$ האיברים האי-פריקים הם הפולינומים האי-פריקים במובן הרגיל. בחוג $\mathbb{Z}$ האי-פריקים הם הראשוניים (והנגדיים שלהם).

הגדרה 2.6 איבר $p \in R$ ייקרא ראשוני אם תמיד כאשר $a \cdot b$ אזי $p \mid a$ או $p \mid b$.

הערה 2.7 בתחום שלמות מתקיים שאם $a \mid b$ וגם $b \mid a$ אזי $a \sim b$, כלומר $a = b \cdot u$ כאשר u הפיך.

הוכחה: נתון $a = b \cdot c$, וכן $b = a \cdot d$.

$$1 \cdot a = a \cdot d \cdot c$$

וכעת, מכלל הצימצום,

$$1 = d \cdot c$$

ולכן c, d הפיכים (הופכיים אחד של השני). ■

טענה 2.8 יהי R תחום שלמות, ויהי $p \in R$. אם p ראשוני אזי p אי-פריק (הכיוון ההפוך לא תמיד נכון - דוגמה תהיה בתרגיל הבית).

הוכחה: נניח $p = a \cdot b$ ראשוני. לכן $p \mid a \cdot b$ ומראשוניות נובע, בלי הגבלת הכלליות, $p \mid a$, כלומר $a = p \cdot c$. נציב זאת ונקבל

$$p = p \cdot c \cdot b$$

ושוב מכלל הצימצום,

$$1 = c \cdot b$$

ולכן b הפיך, משמע p אי-פריק. ■

הגדרה 2.9 יהי R תחום שלמות. תת קבוצה $I \subseteq R$ תיקרא אידאל אם היא מקיימת:

1. $0 \in I$

2. סגורה תחת חיבור וחסור: $a, b \in I \Rightarrow a + b \in I$

3. סגורה תחת כפל בכל איבר $r \in R$, כלומר $a \in I, r \in R \Rightarrow ar \in I$

דוגמאות: בתוך $\mathbb{Z}$, ישנו אידאל הזוגיים: $I = \{2n \mid n \in \mathbb{Z}\}$. בחוג $R[x]$ קבוצת כל הפולינומים בעלי מקדם חופשי אפס הם אידאל.

הגדרה 2.10 אידאל מהצורה $Ra = \{ra \mid r \in R\}$ עבור $a \in R$ נקרא אידאל ראשי.