

אלגברה לינארית א2

© ארזים

15 במרץ 2016

1 חלוקה עם שארית

לכל שני שלמים m, n , כאשר $n \neq 0$, קיימים q, r שלמים כך שמתקיים $n = q \cdot m + r$, כאשר הדרישה $|r| < |m|$ לא מבטיחה יחידות, בעוד הדרישה $0 \leq r < |m|$ מבטיחה יחידות. הדרישה $|r| \leq \frac{|m|}{2}$ כמעט מבטיחה יחידות (ספציפית $r = \frac{|m|}{2}$ יכול להגיע בשתי אפשרויות). בפולינומים מתקיים אותו הדבר, רק שנדרוש $\deg r < \deg m$, וכאן מובטחת לנו היחידות.

1.1 מחלק משותף מקסימלי

בהינתן שני שלמים m, n נסמן $d = \gcd(m, n)$ את השלם הגדול ביותר כך שמתקיים $d \mid m, d \mid n$. הגדרה מדויקת יותר תהיה שכל מחלק משותף r של m, n (כלומר $r \mid m, r \mid n$) מקיים $r \mid d$. ברור מהגדרה זו שהמחלק המשותף המקסימלי הוא יחיד עד כדי כפל ביחידה. טענה כללית: עבור חלוקה עם שארית $n = mq + r$:

$$d \mid n, m \Rightarrow d \mid n - qm = r$$

$$d \mid r, m \Rightarrow d \mid qm + r = n$$

לכן נובע

$$\gcd(n, m) = \gcd(m, r)$$

כמו כן, $\gcd(a, 0) = a$ לכל a .
מכאן נקבל אלגוריתם:

$$\begin{aligned} \gcd(55, 34) &= \gcd(34, 21) = \dots = \gcd(0, 1) = 1 \\ 55 &= 1 \cdot 34 + 21 \\ 34 &= 1 \cdot 21 + 13 \\ 21 &= 1 \cdot 13 + 8 \\ 13 &= 1 \cdot 8 + 5 \\ 8 &= 1 \cdot 5 + 3 \\ 5 &= 1 \cdot 3 + 2 \\ 3 &= 1 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

דוגמא נוספת:

$$\begin{aligned}\gcd(140, 63) &= \gcd(7, 0) = 7 \\ 140 &= 2 \cdot 63 + 14 \\ 63 &= 4 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0\end{aligned}$$

תהליך זה נקרא אלגוריתם אוקלידס, וחוג שבו האלגוריתם בוודאות יסתיים בשלב סופי נקרא חוג אוקלידי. דוגמאות עם פולינומים:

$$\begin{aligned}\gcd(x^3 - 2, x^2 + 1) &= 1 \\ x^3 - 2 &= x(x^2 + 1) + (-x - 2) \\ x^2 + 1 &= (x - 2)(x + 2) + 5 \\ x + 2 &= \left(\frac{x + 2}{5}\right) \cdot 5 + 0\end{aligned}$$

$$\begin{aligned}\gcd(x^3 - 2x^2 - 4x - 1, 3x^2 + 7x + 4) &= x + 1 \\ x^3 - 2x^2 - 4x - 1 &= \left(\frac{1}{3}x - \frac{13}{9}\right)(3x^2 + 7x + 4) + \left(\frac{43}{3}x + \frac{43}{3}\right) \\ 3x^2 + 7x + 4 &= (3x + 4)(x + 1) + 0\end{aligned}$$

את כל החלוקות ניתן לבצע על ידי חילוק פולינומים. כמו כן, נשים לב שהעלמנו מקדמים הפיכים בחוג \mathbb{Q} - שכן אם היינו משאירים אותם פשוט היינו צריכים לכפול בהופכי שלהם את יחס החלוקה, אבל אין לכך משמעות בחיפוש אחר מחלק משותף מקסימלי.

$$\begin{aligned}\gcd(x^5 - 1, x^2 - 1) &= x - 1 \\ x^5 - 1 &= (x^3 + x)(x^2 - 1) + (x - 1) \\ x^2 - 1 &= (x + 1)(x - 1) + 0\end{aligned}$$

$$\begin{aligned}\gcd(x^6 - 1, x^4 - 1) &= x^2 - 1 \\ x^6 - 1 &= (x^2 - 1)(x^4 - 1) + (x^2 - 1) \\ x^4 - 1 &= (x^2 + 1)(x^2 - 1) + 0\end{aligned}$$

$$\gcd(x^m - 1, x^n - 1) = x^{\gcd(m, n)} - 1$$

נשים לב ששורשים כפולים של פולינום הם שורשים גם של נגזרתו. בשל הפירוק היחיד של שלמים למפכלת ראשוניים, המחלק המשותף המקסימלי יהיה החפיפה המינימלית בין הפירוקים שלהם לראשוניים. כנ"ל לגבי פולינומים אי-פריקים. כפולה משותפת מינימלית של m, n - $\text{lcm}(m, n)$ - המספר המינימלי שמתחלק בשניהם, או המספר שמחלק את כל המכפלות המשותפות שלהם. כעת המכפלה המשותפת המינימלית של שלמים, כמו המחלק המשותף המקסימלי, היא החפיפה המקסימלית בין הפירוקים (היחידים) של המספרים. לכן הערך המוחלט של מכפלת שני איברים הוא מכפלת המחלק המשותף המקסימלי והכפולה המשותפת המינימלית.

2 חוגים

חוג R הוא מבנה עם פעולות חיבור וכפל (קומוטטיבי, עם יחידה). מטריצות שלמות - לא קומוטטיבי, יש יחידה. זוגיים - קומוטטיבי, אין יחידה. מטריצות זוגיים - לא קומוטטיבי, אין יחידה. אנחנו תמיד יכולים לקחת כחוג את הפולינומים, או המטריצות, מעל כל חוג אחר. חוג השלמים הגאוסיאניים -

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

באופן כללי, לכל פולינום אי פריק ומתוקן מעל \mathbb{Q} ממעלה n , אם α שורש מרוכב שלו, אז נוכל להגדיר את החוג

$$\mathbb{Z}[\alpha] = \{c_0 + c_1\alpha + \dots + c_{n-1}\alpha^{n-1} \mid c_0, \dots, c_{n-1} \in \mathbb{Z}\}$$

בחוג שכזה, כדי שאיבר יהיה הפיך, הנורמה שלו חייבת להיות הפיכה בשלמים - בשל הזהות

$$z^{-1} = \frac{\bar{z}}{\|z\|}$$