

מבנים דיסקרטיים – תרגיל בית 7

להגשה 11.6.2013

בתרגול לא הספקנו להראות, אבל ניתן להשתמש באלגוריתם מציאת המחלק המשותף המקסימלי של שני איברים כדי להציג אותו כצירוף אלגברי של שני האיברים, כלומר $\gcd(a, b) = au + bv$. לדוגמה הראינו בתרגול:

דוגמא: נפעיל את אלגוריתם הבניה עבור הדוגמא: $\gcd(234, 61) = 1$.

$$234 = 61 \times 3 + 51$$

$$61 = 51 \times 1 + 10$$

$$51 = 10 \times 5 + 1$$

$$10 = 1 \times 10$$

ואז נקבל:

$$\gcd(234, 61) = \gcd(61, 51) = \gcd(51, 10) = \gcd(5, 1) = 1$$

את הצירוף האלגברי המתאים נקבל ע"י הצגת כל שארית כצירוף אלגברי מתאים של השאריות הקודמות:

$$1 = 51 - 10 \times 5$$

$$10 = 61 - 51 \times 1$$

$$51 = 234 - 61 \times 3$$

\Rightarrow

$$\begin{aligned} 1 &= 51 - 10 \times 5 = (234 - 61 \times 3) - (61 - 51 \times 1) \times 5 = (234 - 61 \times 3) - (61 - (234 - 61 \times 3) \times 1) \times 5 = \\ &= 6 \times 234 + (-23) \times 61 \end{aligned}$$

1. מצאו את המחלק המשותף המקסימלי של זוגות הפולינומים הבאים מעל \mathbb{Q} , והציגו אותו כצירוף אלגברי שלהם.

$$a. \quad x^5 - 6x + 1, \quad x^3 - 6x^2 + x + 4$$

סדרת החלוקות באלגוריתם אוקלידס היא הבאה:

$$\begin{aligned}
x^5 - 6x + 1 &= (x^3 - 6x^2 + x + 4) \cdot (x^2 + 6x + 35) + (200x^2 - 65x - 139) \\
x^3 - 6x^2 + x + 4 &= (200x^2 - 65x - 139) \cdot \left(\frac{1}{200}x - \frac{227}{8000}\right) + \left(-\frac{239}{1600}x + \frac{447}{8000}\right) \\
200x^2 - 65x - 139 &= \left(-\frac{239}{1600}x + \frac{447}{8000}\right) \cdot \left(-\frac{320000}{239}x - \frac{3752000}{57121}\right) + -\frac{7730176}{57121} \\
-\frac{239}{1600}x + \frac{447}{8000} &= -\frac{7730176}{57121} \cdot \left(-\frac{13651919}{1600}x + \frac{25533087}{8000}\right) + 0
\end{aligned}$$

אנחנו רואים שהשארית האחרונה שאינה 0 היא איבר הפיך, כלומר ה gcd הוא 1.

לאחר גלגול אחורה של השאריות, נקבל

$$\begin{aligned}
&((5975/120784)x^2 - (33615/120784)x - 639/30196)(x^5 - 6x + 1) + \\
&(x^3 - 6x^2 + x + 4) \frac{1}{120784} (-5975x^4 - 2235x^3 - 4879x^2 - 3139x + 30835) = 1
\end{aligned}$$

$$x^2 + 1, x^6 + x^3 + x + 1 \quad .b$$

$$x^6 + x^3 + x + 1 = (x^2 + 1)(x^4 - x^2 + x + 1) + 0$$

$$.x^2 + 1 = 1 \cdot (x^2 + 1) + 0 \cdot (x^6 + x^3 + x + 1) \text{ ואז } \gcd = x^2 + 1$$

2. מצאו את המחלק המשותף המקסימלי של $x^5 + x^4 + x^2 + x, x^5 + x^2$ מעל \mathbb{Z}_2 והציגו אותו כצירוף אלגברי של שני האיברים.

$$\begin{aligned}
x^5 + x^4 + x^2 + x &= (x^5 + x^2) \cdot 1 + (x^4 + x) \\
x^5 + x^2 &= (x^4 + x) \cdot x + 0
\end{aligned}$$

$$x^4 + x = 1 \cdot (x^5 + x^4 + x^2 + x) - 1 \cdot (x^5 + x^2) = 1 \cdot (x^5 + x^4 + x^2 + x) + 1 \cdot (x^5 + x^2)$$

3. הראו שאם R תחום שלמות, אזי כל איבר הפיך ב $R[x]$ הוא איבר הפיך ב R . פתרון: נשתמש בפונקציה הדרגה של הפולינומים. מתקיים שעבור $f, g \in R[x]$ השונים מאפס,

$$\text{deg}(fg) = \text{deg}(f) + \text{deg}(g)$$

$$, (ab \neq 0 \text{ ובהכרח } fg = abx^{m+n} + \dots \text{ אזי } a, b \neq 0 \text{ עבור } f = ax^n + \dots, g = bx^m + \dots$$

$$\text{ומתקיים לכן שאם } fg = 1 \text{ אזי } \text{deg}(f) = 0, \text{deg}(g) = 0$$

כלומר f, g הם איברים ב R . לכן $fg = 1$ גורר ששני האיברים הפיכים ב R .

4. יהי R חוג. נאמר שאיבר $a \in R$ הוא נילפוטנטי אם קיים n טבעי כך ש $a^n = 0$.

a. הראו שבתחום שלמות אין איברים נילפוטנטיים פרט ל 0.

b. הראו שאם $a \in R$ נילפוטנטי אזי $1 - a$ הפיך. רמז: $x^n - 1 = (x - 1)(x^{n-1} + \dots)$.

פתרון:

א. אם a נילפוטנטי אזי $a^n = 0$ ואז $a \cdot a^{n-1} = 0$ ואז לפי הגדרת תחום שלמות נקבל $a = 0$.
 או $a^{n-1} = 0$. אם $a = 0$ אז סיימנו, אחרת נמשיך $a \cdot a^{n-2} = 0$ ונקבל $a = 0$ או $a^{n-2} = 0$.
 נמשיך כך ונקבל בסוף שבהכרח $a = 0$.

ב. מתקיים $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + x^{n-3} + \dots + x + 1)$ (בדקו זאת). לכן אם $a^n = 0$ אז

$$-1 = a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + a^{n-3} + \dots + a + 1)$$

$$1 = (1-a)(a^{n-1} + a^{n-2} + a^{n-3} + \dots + a + 1) \text{ ולכן}$$

$$(1-a)^{-1} = (a^{n-1} + a^{n-2} + a^{n-3} + \dots + a + 1)$$

5. הראו ש $a\mathbb{Z} + b\mathbb{Z} = \gcd(a,b)\mathbb{Z}$ (כאשר $a \neq 0$ או $b \neq 0$).

פתרון: נסמן $d = \gcd(a,b)$. וגם $d | a$ ולכן $d | ac + bd$ ולכל $c, d \in \mathbb{Z}$. אם כך

$d = au + bv$ ניתן להשתמש בטענה $a\mathbb{Z} + b\mathbb{Z} \subseteq \gcd(a,b)\mathbb{Z}$ ולכן $ac + bd \in d\mathbb{Z}$

עבור $u, v \in \mathbb{Z}$ ולכן $dc = (au + bv)c = auc + bvc \in a\mathbb{Z} + b\mathbb{Z}$ ולכן

$$a\mathbb{Z} + b\mathbb{Z} \supseteq \gcd(a,b)\mathbb{Z}$$