$R=\mathbb{Z}$	$R=k[x]$
מספרים שלמים הפיכים ± 1	הפולינומים ההפיכים = הפולינומים הקבועים

הגדרה

יהיו $a,b\in R$ פולינומים. אומרים שפולינום $d\in\mathbb{R}$ הוא **מחלק משותף מקסימלי** של a,b אם מתקיימים התנאים הבאים:

- $d|a, d|b$
- אם $c|a, c|b$ אזי $c|d$.

סימון: $d=g.c.d(a,b)$ ($g.c.d$: $greatest\ common\ dividor$).

משפט

$g.c.d(a,b)$ קיים ויחיד.

הוכחה

נשתמש בחילוק עם שארית: אם נתונים שני פולינומים f,g אזי קיימים פולינומים q,r יחידים (עד כדי כפל בקבוע) כך שמתקיים:

- $f=q\cdot g+r$.
- $r\equiv 0$ או $\deg r<\deg g$.

נניח $deg\ a>deg\ b$. נחלק את a ב b עם שארית:

$$\begin{aligned}
a&=q_1\cdot b+r_1\ ,\deg r_1<\deg b\\
b&=q_2\cdot r_1+r_2\ ,\deg r_2<\deg r_1\\
r_1&=q_3\cdot r_2+r_3\ ,\deg r_3<\deg r_2\\
&\vdots\\
r_{k-2}&=q_k\cdot r_{k-1}+r_k\ ,\deg r_k<\deg r_{k-1}\\
r_{k-1}&=q_{k+1}\cdot r_k
\end{aligned}$$

נוכיח ש $d=r_k$ זה $g.c.d(a,b)$.

מהשוויון האחרון: $r_k|r_{k-1}$.

מהשוויון הלפני אחרון: $r_k|r_{k-2}$.

נמשיך ונקבל: $r_k|r_{k-3}$.

$\vdots$

מהשוויון השני: $r_k|b$.

מהשוויון הראשון: $r_k|a$.

ז"א, r_k הוא מחלק משותף של a,b.

כעת, נניח ש - c חלק משותף נוסף של a,b.

מהשוויון הראשון (והעברת אגפים) $c|r_1$.

מהשוויון השני - $c|r_2$

⋮

מהשוויון הלפני אחרון: $c|r_{k-1}$.

מהשוויון האחרון: $c|r_k$.
ולכן: $r_k = d$.
יחידות ה $g.c.d$ נובעת מיחידות הפולינומים q, r באלגוריתם החילוק.

■

מסקנה
יהי $d = g.c.d(a,b)$. אזי קיימים $u, v \in \mathbb{R}$ כך שמתקיים: $d = au + bv$.
לכן, אם $d = 1$ (a, b זרים) אזי קיימים $u, v \in \mathbb{R}$ כך ש-$au + bv = 1$.

הוכחה
"עלייה" מהשוויון התחתון לשוויון העליון, ובדרך מציגים ביטויים של r_{k-1} דרך r_{k-2}, r_{k-3},וכו'.

דוגמה

עבור: $R = \mathbb{Z}$, $a = 2015, b = 555$.

$$2015 = 3 \cdot 555 + 350$$
$$555 = 1 \cdot 350 + 205$$
$$350 = 1 \cdot 205 + 145$$
$$205 = 1 \cdot 145 + 60$$
$$145 = 2 \cdot 60 + 25$$
$$60 = 2 \cdot 25 + 10$$
$$25 = 2 \cdot 10 + 5$$
$$10 = 2 \cdot \mathbf{5}$$

כעת, נרצה למצוא u, v כך ש- $5 = 2015u + 555v$.

$$5 = 25 - 2 \cdot 10 = 25 - 2 \cdot (60 - 2 \cdot 25) = 5 \cdot 25 - 60$$
$$= 5 \cdot (145 - 2 \cdot 60) - 2 \cdot 60 = 5 \cdot 145 - 12 \cdot 60$$
$$= 5 \cdot 145 - 12 \cdot (205 - 1 \cdot 145) = 17 \cdot 145 - 12 \cdot 205$$
$$= 17(350 - 205) - 12 \cdot 205 = 17 \cdot 350 - 29 \cdot 205$$
$$= 17 \cdot 350 - 29(555 - 1 \cdot 350) = 46 \cdot 350 - 29 \cdot 555$$
$$= 46(2015 - 3 \cdot 555) - 29 \cdot 555 = \mathbf{46 \cdot 2015 - 167 \cdot 555}$$

מסקנה
אם $a|bc$ ואם $g.c.d(a,b) = 1$, אזי $a|c$.

הוכחה

$g.c.d(a,b) = 1$, לכן קיימים $u, v \in R$ כך ש $a \cdot u + b \cdot v = 1$. נכפול ב c ונקבל:
$a \cdot c \cdot u + b \cdot c \cdot v = c$.

$$a|bc \to bc = aw$$

לכן, $c = acu + bcv = acu + awv = a(cu + wv)$ זאת אומרת $a|c$.

■

למה

יהי $p \in \mathbb{R}$ אי-פריק. אזי אם $p|bc$, אזי $p|b$ או $p|c$.

הוכחה

נסמן $d = g.c.d(p,b)$.

$$d = p \leftarrow d|p \vee d = 1$$

אם $d = 1$ אזי $g.c.d(p,b) = 1$ לכן (לפי מסקנה קודמת) $p|c$. אם $d = p$ אזי $p|b$.

■