Bevezetés az algebrába 1

Polinomok számelmélete

Wettl Ferenc diáinak felhasználásával

Polinomgyűrű

D Legyen R kommutatív gyűrű, $1 \in R$, $a_0, a_1, \ldots, a_n \in R$, x egy szimbólum (változó). Az $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ formális kifejezést R-beli együtthatós (vagy R fölötti) egyváltozós polinomnak nevezzük. Ha $a_n \neq 0$, akkor n-et az f polinom fokának hívjuk és $\deg f$-fel jelöljük. a_n a polinom főegyütthatója, $a_n x^n$ a polinom főtagja. A zéruspolinom foka $-\infty$. Az $f(x) = a_0$ polinomot konstans polinomnak nevezzük.

D Két polinom azonos, ha azonos fokúak, és megfelelő együtthatóik páronként azonosak.

J Az R fölötti polinomok halmaza $R[x]$: pl. $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}[x]$, $\mathbb{Z}_m[x]$.

D $\sum_{k=0}^{n} a_k x^k + \sum_{k=0}^{m} b_k x^k := \sum_{k=0}^{\max(n,m)} (a_k + b_k) x^k$. (A kisebb fokú polinomot kiegészítjük 0 együtthatójú tagokkal.)

D $\sum_{i=0}^{n} a_i x^i \cdot \sum_{j=0}^{m} b_j x^j := \sum_{k=0}^{n+m} c_k x^k$, ahol $c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0$.

Emlékeztető: Egy R gyűrű nullosztómentes, ha $ab = 0 \Rightarrow a = 0$ vagy $b = 0$. Pl. minden test, és azok részgyűrűi (így $\mathbb{Z}$ is) nullosztómentes, de $\mathbb{Z}_m$ nem nullosztómentes, ha m nem prím.

Á (1) $\deg(f + g) \leqslant \max\{\deg f,\ \deg g\}$

(2) Ha R nullosztómentes, akkor $\deg(fg) = \deg f + \deg g$.

B (1): Az összeg definíciójából.

(2): Ha $f(x) = a_n x^n + \ldots + a_0$ és $g(x) = b_m x^m + \ldots + b_0$ $(a_n, b_m \neq 0)$, akkor $f(x)g(x)$ legnagyobb kitevős tagja $a_n b_m x^{n+m}$, és mivel R nullosztómentes, $a_n b_m \neq 0$.

Ha valamelyik polinom a 0 polinom, akkor annak a foka és a fokok összege is $-\infty$, másrészt $\deg fg = \deg 0 = -\infty$.

P Az (1) állításban a felső korlát nem éles, $\deg f + g$ lehet kisebb is a két fok maximumánál: $(x^2 + x) + (-x^2 + 2) = x + 2$ foka csak 1.

A (2) állítás nem igaz, ha nem tesszük fel, hogy R nullosztómentes, pl. $\mathbb{Z}_6[x]$-ben $(3x)(2x + 1) = 3x$.

Á *$R[x]$ egységelemes kommutatív gyűrű, és ha R nullosztómentes, akkor $R[x]$ is az.*

B A gyűrűaxiómák ellenőrizhetők,...

Ha R nullosztómentes, és $f, g \neq 0$, akkor $\deg f,\ \deg g \geqslant 0 \Rightarrow$ $\deg fg = \deg f + \deg g \geqslant 0 \Rightarrow fg \neq 0$.

K $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$, $\mathbb{Z}_m[x]$ egységelemes kommutatív gyűrűk. Nullosztómentesek is, kivéve $\mathbb{Z}_m$-et összetett m esetén.

Mj $R \subseteq R[x]$ mint a konstans polinomok részgyűrűje.

D $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in R[x]$re és $c \in R$-re

az f behelyettesítési értéke c-ben $f(c) = a_n c^n + \ldots + a_1 c + a_0 \in R$.

Mj $f \mapsto f(c)$ művelettartó leképezés az $R[x]$ gyűrűből az R gyűrűbe, azaz $(f+g)(c) = f(c) + g(c)$ és $(fg)(c) = f(c)g(c)$.

D Az $f(x) \in R[x]$ polinomhoz tartozó polinomfüggvény

$$\begin{array}{ccc} R & \to & R \\ c & \mapsto & f(c) \end{array}$$

P Különböző polinomokhoz is tartozhat ugyanaz a polinomfüggvény, pl. $\mathbb{Z}_2[x]$-ben x és x^2 ugyanazt a polinomfüggvény adja: $0 \mapsto 0$, $1 \mapsto 1$, de polinomként nem egyenlők.

($\mathbb{R}[x]$-ben ilyen nem fordulhat elő.)

D $c \in R$ gyöke az $f(x) \in R[x]$ polinomnak, ha $f(c) = 0$.

P Hány gyöke van az $x^4 - 2$, illetve $x^2 - 1$ polinomnak, ha $\mathbb{Q}[x]$-ben, $\mathbb{R}[x]$-ben, $\mathbb{C}[x]$-ben vagy $\mathbb{Z}_8[x]$-ben nézzük?

m

	$\mathbb{Q}[x]$	$\mathbb{R}[x]$	$\mathbb{C}[x]$	$\mathbb{Z}_8[x]$
$x^4 - 2$	0	2	4	0
$x^2 - 1$	2	2	2	4

Polinomosztás

D Oszthatóság egységelemes kommutatív gyűrűben: Legyen R egységelemes kommutatív gyűrű, $a, b \in R$. Ekkor b osztója a-nak (a osztható b-vel), ha $\exists q \in R$, hogy $a = bq$. Jelölés: $b \mid a$.

P $x - 1 \mid x^n - 1$ a $\mathbb{Z}[x]$ gyűrűben ($n \in \mathbb{N}^+$).

P $3x \mid x^n$ a $\mathbb{Q}[x]$ gyűrűben, mert $x^n = (3x)(\frac{1}{3}x^{n-1})$, de nem osztója $\mathbb{Z}[x]$-ben.

P $x - i \mid x^2 + 1$ a $\mathbb{C}[x]$ gyűrűben, mert $x^2 + 1 = (x - i)(x + i)$.

P Mik az egységek (azaz a mindent osztó elemek) $K[x]$-ben, ha K test?

m Az $1 \in K[x]$ polinom osztói, azaz a nulladfokú polinomok ($a_0 \in K \setminus \{0\}$).

P Mik az egységek *(a)* $\mathbb{Z}[x]$-ben és *(b)* általában $R[x]$-ben, ha R egységelemes, kommutatív, nullosztómentes gyűrű?

m *(a)* $1, -1 \in \mathbb{Z}[x]$, *(b)* R egységei, ugyanis ha $f(x) \mid 1 \Rightarrow$ van olyan $g(x)$, hogy $f(x)g(x) = 1 \Rightarrow \deg f + \deg g = 0 \Rightarrow \deg f = \deg g = 0$.

P Igazoljuk, hogy $\mathbb{Z}_4[x]$-ben $2x + 1$ egység!

m $(2x + 1)(2x + 1) = 1$, tehát $2x + 1$ minden polinomnak osztója.

T **Maradékos osztás polinomgyűrűben**

Legyen K test, és $f, g \in K[x]$ két polinom, ahol $g \neq 0$. Akkor egyértelműen léteznek olyan $h, r \in K[x]$ polinomok, hogy

$$f = gh + r, \text{ és } \deg r < \deg g.$$

B Létezés: Ha $f = 0$, akkor $h = r = 0$.

Ha $\deg f < \deg g$, akkor $h = 0$ és $r = f$, azaz $f = g \cdot 0 + f$.

A továbbiakban $\deg f \geqslant \deg g$. $\deg f$-re vonatkozó teljes ind.:

$\deg f = 0$: $f = a_0$ $(a_0 \in K) \rightsquigarrow g = b_0$, $h = \frac{a_0}{b_0}$, $r = 0$, ✓

$\deg f < n \to \deg f = n$: $f(x) = a_n x^n + \ldots$, $g(x) = b_m x^m + \ldots$

$\hat{f}(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x) \rightsquigarrow \deg \hat{f} < n$

Az indukciós feltevés miatt $\hat{f} = gh + r \rightsquigarrow$

$f(x) = (h(x) + \frac{a_n}{b_m} x^{n-m}) g(x) + r(x)$

Egyértelműség: Tfh $f = hg + r = \hat{h}g + \hat{r} \rightsquigarrow (h - \hat{h})g = \hat{r} - r$, de $h - \hat{h} \neq 0$ esetén $\deg((h - \hat{h})g) \geqslant \deg g > \deg(\hat{r} - r)$, így $h = \hat{h} \rightsquigarrow$ $r = \hat{r}$ ✓

Mj A maradékos osztás $R[x]$-ben is elvégezhető, ha $g(x)$ főegyütthatója egység: $b_m b'_m = 1 \rightsquigarrow (b_m x^m + \ldots)(b'_m a_n x^{n-m}) = a_n x^n + \ldots$.

P Osszuk el maradékosan az $f(x) = x^4 - 4x^3 + x^2 + 1$ polinomot a $g(x) = x^2 + x + 2$-vel!

m

$$
\begin{array}{rrrrrcl}
(x^4 & -\,4x^3 & +\,x^2 & & +\,1) & : \; (x^2+x+2) & = \quad x^2 - 5x + 4 \\
-\,(x^4 & +\,x^3 & +\,2x^2 & &) & & \\
\hline
 & -5x^3 & -\,x^2 & & +\,1 & & \\
- & (-\,5x^3 & -\,5x^2 & -\,10x &) & & \\
\hline
 & & 4x^2 & +\,10x & +\,1 & & \\
 & - & (4x^2 & +\,4x & +\,8) & & \\
\hline
 & & & 6x & -\,7 & &
\end{array}
$$

Tehát $x^4 - 4x^3 + x^2 + 1 = (x^2 + x + 2)(x^2 - 5x + 4) + (6x - 7)$.

F Osszuk el (x^3+1)-et maradékosan $(2x-1)$-gyel!

m

$$
\begin{array}{rrrrl}
(x^3 & & & +1) & : \; (2x-1) \;=\; \frac{1}{2}x^2+\frac{1}{4}x+\frac{1}{8} \\
-(x^3 & -\frac{1}{2}x^2 & &) & \\
\hline
 & \frac{1}{2}x^2 & & +1 & \\
 & -(\frac{1}{2}x^2 & -\frac{1}{4}x &) & \\
\hline
 & & \frac{1}{4}x & +1 & \\
 & & -(\frac{1}{4}x & -\frac{1}{8}) & \\
\hline
 & & & \frac{9}{8} &
\end{array}
$$

$x^3+1=(2x-1)(\frac{1}{2}x^2+\frac{1}{4}x+\frac{1}{8})+\frac{9}{8}$.

Mj $\mathbb{Z}[x]$-ben nem lehetne ezt a maradékos osztást elvégezni (a maradékos osztás egyértelmű, és a $\mathbb{Q}[x]$-ben kapott hányados nem $\mathbb{Z}[x]$-beli.).

Mj Ha $f(x)$-et $cg(x)$-szel osztjuk maradékosan (ahol $c \neq 0$ konstans), akkor a maradék ugyanaz lesz, mint ha $g(x)$-szel osztanánk: $f(x)=g(x)h(x)+r(x)=cg(x)\left(\frac{1}{c}h(x)\right)+r(x)$.

F Osztható-e $\mathbb{Z}_3[x]$-ben az $x^4 + x^3 + x + 2$ polinom $x^2 + 1$-gyel?

m

$$
\begin{array}{rrrrl}
(x^4 & +\,x^3 & & +\,x & +\,2) \\
-(x^4 & & +\,x^2 & &) \\
\hline
 & x^3 & +\,2x^2 & +\,x & +\,2 \\
 & -(x^3 & & +\,x &) \\
\hline
 & & 2x^2 & & +\,2 \\
 & & -(2x^2 & & +\,2) \\
\hline
 & & & & 0
\end{array}
\quad : \quad x^2 + 1 \quad = \quad x^2 + x + 2
$$

Igen, $x^4 + x^3 + x + 2 = (x^2 + 1)(x^2 + x + 2)$ a $\mathbb{Z}_3[x]$-ben.

T **Polinomosztás Horner-módszerrel**

Legyen R egységelemes kommutatív gyűrű,
$f(x) = a_n x^n + \ldots + a_1 x + a_0 \in R[x]$, $c \in R$, és legyen $f(x)$ maradékos osztása $(x - c)$-vel

$$f(x) = (x - c)(b_{n-1}x^{n-1} + \ldots + b_1 + b_0) + r. \tag{1}$$

Ekkor $b_{i-1} = a_i + cb_i$ minden i-re, azaz a c behelyettesítéséhez használt Horner-táblázat második sorában a hányados együtthatóit és az osztás maradékát kapjuk:

	a_n	a_{n-1}	$\ldots$	a_1	a_0
c	b_{n-1}	b_{n-2}	$\ldots$	b_0	r

ahol $r = f(c)$.

B Az (1) egyenlőség szerint $f(x)$-ben x^i együtthatója $a_i = b_{i-1} - cb_i$.
Az (1)-be c-t behelyettesítve megkapjuk, hogy $f(c) = r$.

P Osszuk el $x^4 - 2x^2 + x + 3$-at $x + 2$-vel!

m

	1	0	-2	1	3
-2	1	-2	2	-3	9

$\rightsquigarrow x^4 - 2x^2 + x + 3 = (x + 2)(x^3 - 2x^2 + 2x - 3) + 9.$

P Osszuk el $x^3 + 1$-et maradékosan $2x - 1$-gyel a Horner-módszer használatával!

m $2x - 1 = 2(x - \frac{1}{2})$

	1	0	0	1
$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{9}{8}$

$\rightsquigarrow x^3 + 1 = (x - \frac{1}{2})(x^2 + \frac{1}{2}x + \frac{1}{4}) + \frac{9}{8} = (2x - 1)(\frac{1}{2}x^2 + \frac{1}{4}x + \frac{1}{8}) + \frac{9}{8}.$

P Osszuk el $x^4 - 2x^2 + x + 3$-at $(x-1)^2$-tel, ismételt Horner-féle maradékos osztással!

m

	1	0	-2	1	3
1	1	1	-1	0	3
1	1	2	1	1	

$\rightsquigarrow x^4 - 2x^2 + x + 3 = (x-1)(x^3 + x^2 - x) + 3 =$

$(x-1)((x-1)(x^2 + 2x + 1) + 1) + 3 =$

$(x-1)^2(x^2 + 2x + 1) + (x-1) + 3 = (x-1)^2(x^2 + 2x + 1) + x + 2.$

Polinom felírása $(x - c)$ polinomjaként:

Az $a_n(x-c)^n + \cdots + a_1(x-c) + a_0 =$

$((\ldots((a_n(x-c) + a_{n-1})(x-c) + \ldots a_1)(x-c) + a_0$ felírásból leolvasható, hogy az $a_0, a_1, \ldots, a_n$ együtthatókat megkaphatjuk mint az $(x-c)$-vel vett ismételt maradékos osztások maradékait.

P Írjuk fel az $x^4 - 2x^2 + x + 3$ polinomot mint $x - 2$ polinomját!

m

	1	0	−2	1	3
2	1	2	2	5	**13**
2	1	4	10	**25**	
2	1	6	**22**		
2	**1**	**8**			

$\rightsquigarrow x^4 - 2x^2 + x + 3 =$

$\mathbf{1}(x-2)^4 + \mathbf{8}(x-2)^3 + \mathbf{22}(x-2)^2 + \mathbf{25}(x-2) + \mathbf{13}$

Legnagyobb közös osztó

D **Definíció**

$R[x]$-ben (R 1-elemes, kommutatív gyűrű)

$f(x) \mid g(x)$, ha $\exists h(x) \in R[x]$: $g(x) = f(x)h(x)$.

$f(x)$ egység, ha $\forall g(x) \in R[x]$-re $f(x) \mid g(x)$ ($\Leftrightarrow f(x) \mid 1$)

Á Ha R (és így $R[x]$ is) nullosztómentes, akkor

(1) $f(x) \mid g(x)$, $g \neq 0 \Rightarrow \deg f \leqslant \deg g$

(2) $R[x]$ egységei az R egységei

(3) $f(x) \mid g(x)$ és $g(x) \mid f(x) \Leftrightarrow \exists c \in R$ invertálható, hogy $f(x) = cg(x)$.

B (1): $0 \neq g = fh \Rightarrow \deg g = \deg f + \deg h \geqslant \deg f$, ui. $h \neq 0$.

(2): Ha $f(x) \mid 1 \Rightarrow \exists g(x)$: $f(x)g(x) = 1 \Rightarrow$

$\deg f + \deg g = \deg 1 = 0 \Rightarrow \deg f = \deg g = 0$.

(3): $f(x) \mid g(x) \mid f(x)$. Vagy mindkettő 0, ✓

vagy $\deg f \leqslant \deg g \leqslant \deg f \Rightarrow \deg f = \deg g \geqslant 0$. De

$f(x) = h(x)g(x) \Rightarrow \deg h = 0 \Rightarrow h(x) = c \in R$. Tehát $f(x) = cg(x)$,

és ugyanígy $g(x) = c'f(x)$, amiből $f(x) = cc'f(x) \Rightarrow cc' = 1$.

D **Definíció**

$R[x]$-ben $h(x)$ az $f(x)$ és $g(x)$ legnagyobb közös osztója (= kitüntetett közös osztója), ha

$$\begin{matrix} h(x) \mid f(x) \\ h(x) \mid g(x) \end{matrix} \quad \text{és} \quad \left(\left. \begin{matrix} k(x) \mid f(x) \\ k(x) \mid g(x) \end{matrix} \right\} \Rightarrow \; k(x) \mid h(x) \right)$$

Jele: $(f(x), g(x))$ vagy (f, g).

K Ha R nullosztómentes gyűrű fölött $f(x)$-nek és $g(x)$-nek van legnagyobb közös osztója, az az Állítás/(3) és (2) miatt egység szorzótól eltekintve egyértelmű, és — hacsak nem nulla mindkét polinom — az (1) miatt (f, g) a legnagyobb fokú a közös osztók közül.

T **Test fölötti polinomok legnagyobb közös osztója**

Legyen K test, és $f(x), g(x) \in K[x]$. Ekkor f-nek és g-nek van legnagyobb közös osztója, és $f, g \neq 0$ esetén ez megkapható az euklideszi algoritmus utolsó $\neq 0$ maradékaként. A lnko konstans szorzó erejéig egyértelmű.

B Feltehető, hogy $\deg f \geqslant \deg g$. Ha $\deg g = -\infty$, azaz $g = 0$, akkor nyilván $(f, g) = f$, ha $\deg g = 0$, akkor pedig $(f, g) = g$. Ezután $\min(\deg f, \deg g)$-re vonatkozó teljes indukcióval bizonyítjuk a lnko létezését.

Vegyük az $f = gh + r$ maradékos osztást. Az indukciós feltevés miatt $\exists\ d := (g, r)$ (ahol d a g-re és r-re elvégzett euklideszi algoritmus utolsó nemnulla maradéka).

Ekkor $d \mid f = gh + r$ is teljesül, így $d \mid f, g$, továbbá ha $c \mid f, g$, akkor $c \mid r = f - gh$ és $c \mid g$, így $c \mid (g, r) = d$. Tehát $d = (f, g)$.

Az egyértelműséget már beláttuk.

P $f(x) = x^4 - 4x^3 - x^2 + 16x - 12$, $g(x) = x^2 - 2x - 3$, $(f(x), g(x)) = ?$

m Az euklideszi algoritmussal:

$$x^4 - 4x^3 - x^2 + 16x - 12 = \left(x^2 - 2x - 3\right) \cdot \left(x^2 - 2x - 2\right) + \left(6x - 18\right)$$

$$x^2 - 2x - 3 = \left(6x - 18\right) \cdot \left(\tfrac{1}{6}x + \tfrac{1}{6}\right) + 0$$

Tehát $(a(x), b(x)) = 6x - 18$ vagy egyszerűbb alakban $x - 3$.

Mj Az euklideszi algoritmus során kapott maradékokat menetközben is felszorozhatjuk tetszőleges nemnulla konstanssal.

Mj Ha a maradék konstans polinom, akkor a következő maradékos osztást már nem érdemes elvégezni, a lnko 1.

D $f(x), g(x) \in K[x]$ relatív prímek, ha $(f, g) = 1$.

F $f(x) = x^3 - 2x^2 + x - 1$, $g(x) = x^2 + 2$, $(f, g) = ?$

m $x^3 - 2x^2 + x - 1 = (x^2 + 2)(x - 2) + (-x + 3)$

$x^2 + 2 = (-x + 3)(-x - 3) + 11$

$\rightsquigarrow (f, g) = 11$, vagy ekvivalensen, $(f, g) = 1$, azaz f és g relatív prímek.

T Legyen K test, $f, g \in K[x]$.
Ekkor $\exists\ u, v \in K[x]$: $\quad fu + gv = (f, g)$

B Ugyanúgy, mint az egészekre, a kibővített euklideszi algoritmussal.

K Pontosan akkor létezik $f, g, c \in K[x]$-hez olyan $u, v \in K[x]$, amelyre $fu + gv = c$, ha c osztható (f, g)-vel.

P Állítsuk elő $f(x) = 2x^3 + x^2 + 1$ és $g(x) = x^3 + 1$ legnagyobb közös osztóját $f(x)u(x) + g(x)v(x)$ alakban!

m $2x^3 + x^2 + 1 = (x^3 + 1)2 + (x^2 - 1) \rightsquigarrow x^2 - 1 = f(x) - 2g(x)$

$x^3 + 1 = (x^2 - 1) \cdot x + (x + 1) \rightsquigarrow$

$x + 1 = g(x) + (f(x) - 2g(x))(-x) = f(x)(-x) + g(x)(2x + 1)$

$x^2 - 1 = (x + 1)(x - 1) + 0$, tehát $x + 1$ a lnko.

Az előállítás táblázatosan:

		$2x^3+x^2+1$	x^3+1
	$2x^3+x^2+1$	1	0
$-2\cdot$	x^3+1	0	1
$-x\cdot$	x^2-1	1	-2
	$x+1$	$-x$	$2x+1$

$x+1=(2x^3+x^2+1)(-x)+(x^3+1)(2x+1)$.

F Állítsuk elő az $f(x)=x^3-2x^2+x-1$ és $g(x)=x^2+2$ korábban kiszámolt legnagyobb közös osztóját $fu+gv$ alakban!

m

		x^3-2x^2+x-1	x^2+2
	x^3-2x^2+x-1	1	0
$(x-2)\cdot$	x^2+2	0	1
$(-x-3)\cdot$	$-x+3$	1	$-x+2$
	11	$x+3$	$-x^2-x+7$

Tehát $11=(x^3-2x^2+x-1)(x+3)+(x^2+2)(-x^2-x+7)$.

A számelmélet alaptétele polinomokra

D Ha R egységelemes, kommutatív, nullosztómentes gyűrű, akkor R-et integritási tartománynak nevezzük.

D **Definíció**

R integritási tartomány, $f(x) \in R[x]$.
f irreducibilis, ha nem nulla és nem egység, és ha csak triviális szorzatra bontása van, azaz $f = gh$, $g, h \in R[x]$ esetén g vagy h egység.
f reducibilis, ha nem nulla, nem egység és nem irreducibilis.
f prím, ha nem nulla és nem egység, és $f \mid gh$, $g, h \in R[x]$ esetén $f \mid g$ vagy $f \mid h$.

P 2 irreducibilis $\mathbb{Z}[x]$-ben, mert nem egység, és csak $2 \cdot 1 = (-2) \cdot (-1)$ triviális felbontásai vannak, de nem irreducibilis $\mathbb{Q}[x]$-ben, mert ott a 2 egység.

P $4x + 2$ irreducibilis $\mathbb{Q}[x]$-ben (minthogy csak konstans·elsőfokú szorzat lehetne), de $\mathbb{Z}[x]$-ben $2(2x + 1)$ valódi felbontás, így ott reducibilis.

T **Tétel**

Ha K test és $p \in K[x]$, akkor
p irreducibilis $\Leftrightarrow$ p prím.

B ($\Leftarrow$): $p = fg \;\Rightarrow\; p \mid fg$, de p prím, így $p \mid f$ vagy $p \mid g$.
Ha pl. $p \mid f$, akkor $f \mid fg \mid f \;\Rightarrow \exists c \in K$: $fg = fc$, így ($f \neq 0$ miatt)
$g = c$ konstans, azaz g egység $K[x]$-ben.
($\Rightarrow$): Tfh p irreducibilis, $p \mid fg$, de $p \nmid f \;\Rightarrow\; (p, f) = 1$
$\Rightarrow\; \exists u, v \in K[x] : up + vf = 1 \Rightarrow\; upg + vfg = g \;\Rightarrow\; p \mid g$.

Á $K[x]$-ben
(1) $\forall$ elsőfokú polinom irreducibilis.
(2) $\deg f = 2$ vagy 3 esetén f irred. $\Leftrightarrow$ nincs gyöke K-ban.
(3) $\deg f \geqslant 4$ eseten lehet f úgy is reducibilis, hogy van gyöke.

B (1),(2): $f \neq 0$, $f = gh \Rightarrow \deg f = \deg g + \deg h$, így ez pontosan akkor nem triviális (valódi) felbontás, ha f-nél kisebb fokúak a tényezők. Elsőfokú polinomnak pedig mindig van gyöke.
(3): Pl. $(x^2 + 1)^2$ reducibilis $\mathbb{R}[x]$-ben, de nincs valós gyöke.

T **Számelmélet alaptétele test fölötti polinomokra**

Legyen K test, és $f \in K[x]$ nullától és egységtől különböző (azaz nem konstans) polinom. Ekkor f egységszorzótól és sorrendtől eltekintve egyértelműen felbontható véges sok $K[x]$-beli irreducibilis polinom szorzatára.

B Felbonthatóság: $\deg f$-re vonatkozó teljes indukcióval.

Ha f irreducibilis ✓

Ha $f = gh$ $(g, h \in K[x])$ valódi felbontás, és $\deg f = n$, akkor $0 < \deg g,\ \deg h < n$, így az indukciós feltevés szerint g és h is felbomlik véges sok irred. pol. szorzatára $\rightsquigarrow$ f is.

Egyértelműség: Indirekt. Legyen $p_1 \dots p_r = q_1 \dots q_s$ a legkisebb fokú polinom, mely két különböző módon is felbomlik.

$p_1 \mid$ bal oldal $\rightsquigarrow$ $p_1 \mid$ jobb oldal. p_1 irreducibilis $\rightsquigarrow$ p_1 prím

$\rightsquigarrow \exists j : p_1 \mid q_j$, de q_j irred., így $q_j = p_1 \cdot$ egység

$\rightsquigarrow$ egyszerűsítünk p_1-gyel $\rightsquigarrow$ kisebb fokú szorzatot kaptunk $\rightsquigarrow$ ez a két felbontás ekvivalens $\rightsquigarrow$ az eredeti is. $\lightning$

K A $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_p[x]$ polinomgyűrűkben minden polinom véges sok irreducibilis polinom szorzata (sorrendtől és nem nulla konstans szorzótól eltekintve egyértelműen).

P $\mathbb{Q}[x]$-ben: $x^4 - 2x^2 - 3 = (x^2+1)(x^2-3) = (\frac{1}{3}x^2 - 1)(3x^2+3)$,
$\mathbb{R}[x]$-ben: $x^4 - 2x^2 - 3 = (x^2+1)(x+\sqrt{3})(x-\sqrt{3})$,
$\mathbb{C}[x]$-ben: $x^4 - 2x^2 - 3 = (x+i)(x-i)(x+\sqrt{3})(x-\sqrt{3})$,

P Mi x^2+1 felbontása $\mathbb{Z}_5[x]$-ben és $\mathbb{Z}_7[x]$-ben?

m $\mathbb{Z}_5[x]$-ben: $(x+2)(x+3) = x^2+1$
$\mathbb{Z}_7$-ben a négyzetszámok csak $0, 1, 2, 4$, tehát x^2+1-nek nincs gyöke, és csak másodfokú, ezért irreducibilis.

P $\mathbb{Z}_8[x]$-ben nem teljesül az egyértelmű irreducibilisekre bontás. Pl. $x^2 - 1 = (x+1)(x-1) = (x+3)(x-3)$. (Valóban irreduciblisek az $x \pm 1$ és $x \pm 3$?)
$\mathbb{Z}_6[x]$-ben $x = (2x+3)(3x+2)$ valódi felbontás, tehát nem nullosztómentes gyűrű fölött még azt sem mondhatnánk, hogy az 1 főegyütthatós, elsőfokú polinomok irreducibilisek.

Mj A lnko, lkkt kifejezhető az irreduciblis tényezőkből is, ugyanúgy, mint $\mathbb{Z}$-ben.

P Mik a másodfokú irreducibilis polinomok $\mathbb{Z}_2[x]$-ben?

m A 0 nem gyöke $\Leftrightarrow$ a konstans tag $\neq 0$.

Az 1 nem gyöke $\Leftrightarrow$ páratlan sok nemnulla tagja van.

Csak $x^2 + x + 1$ irreducibilis a másodfokúak közül.

F Bontsuk fel az $f(x) = x^5 + 3x - 1$ polinomot irreducibilisek szorzatára $\mathbb{Z}_2[x]$-ben! Felbontható-e $\mathbb{Z}[x]$-ben is?

m Gyöke nincs $\mathbb{Z}_2$-ben, tehát ha felbomlik, van másodfokú irred. tényezője, és az csak $g(x) = x^2 + x + 1$ lehet. Osszuk el maradékosan f-et g-vel.

$f(x) = x^5 + 3x - 1 = x^5 + x + 1 = (x^2 + x + 1)(x^3 + x^2 + 1)$, tehát $f(x)$ reducibilis. ($x^3 + x^2 + 1$ nem bontható tovább.)

Ha felbomlana $\mathbb{Z}[x]$-ben, az $\mathbb{Z}_2$ fölötti felbontást is adna, így $f(x) = (x^2 + ax \pm 1)(x^3 + bx^2 + cx \mp 1)$ alakú felbontása lenne, és ehhez nincs megfelelő $a, b, c \in \mathbb{Z}$.