Bevezetés az algebrába 1

Irreducibilis polinomok

Wettl Ferenc diáinak felhasználásával

Irreducibilitás $\mathbb{Q}[x]$-ben és $\mathbb{Z}[x]$-ben

Ha $f(x) \in \mathbb{Q}[x]$ és $c \in \mathbb{Q}$, $c \neq 0$, akkor
$f(x)$ irreducibilis $\mathbb{Q}[x]$-ben $\iff$ $cf(x)$ irreducibilis $\mathbb{Q}[x]$-ben.
Másrészt minden $\mathbb{Q}[x]$-beli polinom felszorozható $\mathbb{Z}[x]$-belivé, tehát elég $\mathbb{Q}[x]$-ben az egész eh.-s polinomok irreducibilitását vizsgálni.

D $f(x) \in \mathbb{Z}[x]$ primitív, ha együtthatóinak legnagyobb közös osztója 1.

P $3x^2 - 6x + 12$ nem primitív: 3 osztja mindegyik együtthatót.
$6x^2 + 10x - 15$ primitív: $(6, 10, 15) = 1$.
$f(x) = c$ konstans polinom primitív $\iff$ $c = \pm 1$

Á Minden $0 \neq f(x) \in \mathbb{Q}[x]$ polinom felírható előjeltől eltekintve egyértelműen $f(x) = rg(x)$ alakban, ahol $g \in \mathbb{Z}[x]$ primitív és $r \in \mathbb{Q}$.

B $f(x)$-et felszorozzuk az együtthatók nevezőjének lkkt-ével $\rightsquigarrow$ $\mathbb{Z}[x]$-beli, és ezután kiemeljük az együtthatók legnagyobb közös osztóját.
Egyértelműség: Ha $r_1 g_1(x) = r_2 g_2(x) \neq 0$, akkor alkalmas egésszel felszorozva $c_1 g_1(x) = c_2 g_2(x)$, ahol $c_1, c_2 \in \mathbb{Z}$, $c_i \neq 0$. $\rightsquigarrow$
$c_i g_i(x)$ együtthatóinak lnko-ja $|c_i|$, mert g_i primitív $\rightsquigarrow$
$|c_1| = |c_2|$, azaz $c_2 = \pm c_1 \rightsquigarrow g_2(x) = \pm g_1(x)$.

P $\frac{6}{5}x^3 + \frac{14}{15}x - \frac{2}{3} = \frac{1}{15}(18x^3 + 14x - 10) = \frac{2}{15}(9x^3 + 7x - 5)$

T **Gauss-lemma**

Primitív polinomok szorzata primitív.

B Tegyük fel, hogy $f(x)$, $g(x)$ primitív, de $f(x)g(x)$ nem, pl. egy $p \in \mathbb{N}^+$ prím osztója az fg összes együtthatójának.

Tekintsük az $f(x)$ és $g(x)$ polinomokat $\mathbb{Z}_p[x]$-belinek (n-et azonosítjuk n mod p-vel).

A feltétel miatt $f(x), g(x) \neq 0$, de $f(x)g(x) = 0$ a $\mathbb{Z}_p[x]$-ben.

De $\mathbb{Z}_p$ nullosztómentes (sőt test), ezért $\mathbb{Z}_p[x]$-nek is nullosztómentesnek kell lennie. $\lightning$

T **A Gauss-lemma következménye**

Ha $f(x) \in \mathbb{Z}[x]$ felbomlik két kisebb fokú polinom szorzatára $\mathbb{Q}[x]$-ben, akkor $\mathbb{Z}[x]$-ben is.

B Tegyük fel, hogy $f(x) = g(x)h(x)$, ahol $g, h \in \mathbb{Q}[x]$ nem konstans $g(x) = rg_1(x)$, $h(x) = sh_1(x)$ valamely $r, s \in \mathbb{Q}$ számokra és $g_1, h_1 \in \mathbb{Z}[x]$ primitív polinomokra.

Legyen továbbá $f(x)$ együtthatóinak legnagyobb közös osztója $c \in \mathbb{Z}$, és $f(x) = cf_1[x]$.

Ekkor $cf_1(x) = rsg_1(x)h_1(x)$, ahol f_1 és a Gauss-lemma miatt g_1h_1 is primitív, így a felbontás egyértelműsége miatt $f_1 = \pm g_1h_1$, és $rs = \pm c$, tehát $f(x) = (\pm cg_1(x))h_1(x)$ $\mathbb{Z}[x]$-beli felbontás.

P $f(x) = 2x^3 + 5x^2 - x - 1$-nek gyöke az $\frac{1}{2} \rightsquigarrow \mathbb{Q}[x]$-ben felbomlik:
$f(x) = (x - \frac{1}{2})(2x^2 + 6x + 2) = (2x - 1)(x^2 + 3x + 1) \rightsquigarrow \mathbb{Z}[x]$-ben is.

K Ha $f(x)$ nem konstans, primitív polinom, akkor
f reducibilis $\mathbb{Z}[x]$-ben $\iff$ f reducibilis $\mathbb{Q}[x]$-ben.

B ($\Rightarrow$): valódi felbontásnak nem lehet konstans tényezője, mert akkor f nem lenne primitív. $\rightsquigarrow$ Ez valódi felbontás $\mathbb{Q}[x]$-ben is

($\Leftarrow$): A Gauss-lemma következményéből.

T **Tétel**

(1) $\mathbb{Z}[x]$ irreducibilisei: $\begin{cases} \mathbb{Z} \text{ prímjei} \\ \mathbb{Q} \text{ fölött irred. primitívek} \end{cases}$

(2) $\mathbb{Q}[x]$ irreducibilisei: $\mathbb{Q}$ fölött irred. primitívek $\neq 0$ konstansszorosai

B (1): Ezek irreducibilisek: konstans polinom csak konstansok szorzata lehet. Másrészt, ami $\mathbb{Q}$ fölött irred. és primitív, az $\mathbb{Z}$ fölött is.

Más nem irred.: Tfh. f irred. Ha konstans, akkor csak prím lehet.

Ha $\deg f \geqslant 1$, és f nem primitív, akkor $f(x) = d \cdot f_1(x)$ valódi felb., ahol f_1 primitív. $\lightning$

Ha $\deg f \geqslant 1$, és f primitív és $\mathbb{Z}[x]$-ben irred., akkor $\mathbb{Q}$ fölött is irred.-nek kell lennie a korábbiak szerint.

(2): Az irreducibilisek $\neq 0$ konstansszorosai nyilván irreducibilisek.

Fordítva, ha f irred. $\mathbb{Q}$ fölött, akkor felszorozható primitívvé: $g(x) = rf(x) \in \mathbb{Z}[x]$, $0 \neq r \in \mathbb{Q}$, és akkor g is irred., de primitív is, vagyis $f(x) = \frac{1}{r}g(x)$ egy primitív irred. konstanszorosa.

P 5 irred. $\mathbb{Z}[x]$-ben, de nem irred $\mathbb{Q}[x]$-ben (egység!)

$2x + 4$ nem irred. $\mathbb{Z}[x]$-ben $(2(x + 2))$, de irred. $\mathbb{Q}[x]$-ben.

T **A számelmélet alaptétele $\mathbb{Z}[x]$-ben**

$\mathbb{Z}[x]$-ben minden $\neq 0, \pm 1$ polinom felbomlik irreducibilisek szorzatára, és ez a felbontás sorrendtől es egységszeresektől (előjelektől) eltekintve egyértelmű.

B Felbonthatóság: $f(x) = cg(x)$, $c \in \mathbb{Z}$, $g(x)$ primitív.
$c = c_1 \cdots c_k$ $\mathbb{Z}$-beli prímekre bontás, $g(x) = g_1(x) \cdots g_r(x)$ kisebb fokúak szorzatára bomlik, amíg lehet. Ezek irreducibilisek, mert g primitívsége miatt 0-adfokú nem-egység már nem emelhető ki.
Egyértelműség: $f(x) = c_1 \cdots c_k g_1(x) \cdots g_r(x)$, ahol $c_i \in \mathbb{Z}$ prímek, $g_j(x)$-ek nem konstans irreducibilisek, tehát $\mathbb{Q}$ fölött irred. primitívek. A konstans szorzó és a primitív $g_1 \cdots g_r$ rész előjel erejéig egyértelmű, és c felbontása is egyértelmű $\mathbb{Z}$-ben.
Ha $g_1 \cdots g_r = h_1 \cdots h_s$ primitív irreducibilisekre bontás, akkor a $\mathbb{Q}[x]$ fölötti egyértelmű felbontás miatt $r = s$, és az egymásnak megfelelő tényezőkre $g_i = th_j$ valamely $t \in \mathbb{Q}$-ra, ahol g_i, h_j primitív $\rightsquigarrow t = \pm 1$.

K $\mathbb{Z}[x]$-ben is van legnagyobb közös osztó, bár nincs euklideszi algoritmus.

P Bontsuk fel a következő polinomokat irreducibilisek szorzatára $\mathbb{Z}[x]$-ben! a) $12x^3 - 6x^2 + 24$ b) $x^4 + 4$ c) $x^4 + 1$

m a) $f(x) = 12x^3 - 6x^2 + 24 = 6(2x^3 - x^2 + 4) = 2 \cdot 3 \cdot (2x^3 - x^2 + 4)$.
A harmadfokú komponens primitív, és csak akkor lehet reducibilis, ha $\mathbb{Q}$ fölött az, azaz ha van elsőfokú faktora, és így gyöke $\mathbb{Q}$-ban.
A rac. gyökteszt szerint csak $\pm 1, \pm 2, \pm 4, \pm \frac{1}{2}$ jöhet szóba, de egyik sem gyök, Így $2x^3 - x^2 + 4$ irred. $\mathbb{Z}[x]$-ben is.
b) $x^4 + 4 = x^4 + 4x^2 + 4 - 4x^2 = (x^2 + 2)^2 - (2x)^2 = (x^2 + 2x + 2)(x^2 - 2x + 2)$. A két faktor primitív és nincs racionális gyökük, így irreducibilisek $\mathbb{Z}[x]$-ben is.
c) Racionális gyöke nincs. Ha felbomlik két másodfokúra, akkor $\mathbb{Z}$ fölött is felbomlik, de az csak $(x^2 + ax + 1)(x^2 - ax + 1)$ vagy $(x^2 + ax - 1)(x^2 - ax - 1)$ lehetne, ahol x^2 együtthatója $2 - a^2$ vagy $-2 - a^2$ nem lehet 0. Tehát $x^4 + 1$ irred ($\mathbb{Q}[x]$ fölött is!).

Irreducibilitási kritériumok

T **Schönemann–Eisenstein-kritérium**

Tfh. $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, és van olyan $p \in \mathbb{N}^+$ prímszám, hogy

$$p \nmid a_n, \quad p \mid a_{n-1}, \ldots, a_0, \quad p^2 \nmid a_0.$$

Ekkor $f(x)$ irreducibilis $\mathbb{Q}[x]$-ben. (Ha $f(x)$ primitív, akkor $\mathbb{Z}[x]$-ben is irreducibilis.)

B Indirekt. Tfh $f(x) = g(x)h(x)$ valódi felbontás $\mathbb{Q}[x]$-ben. A Gauss-lemma következménye miatt feltehető, hogy $g, h \in \mathbb{Z}[x]$. Tekintsük ezeket modulo p, azaz $\mathbb{Z}_p$ fölötti polinomokként.
$\mathbb{Z}_p[x]$-ben $f(x) = a_n x^n = a_n x \cdot x \cdots x$ az f irred.-ekre bontása. $\Rightarrow$
Az alaptétel miatt g és h is x-hatvány konstansszorosa $\mathbb{Z}_p[x]$-ben, és egyik se vált konstanssá a $p \nmid a_n$ feltétel miatt. $\Rightarrow$
g, h-nak mint $\mathbb{Z}_p[x]$-beli polinomoknak a konstans tagja $0 \Rightarrow$
$g, h \in \mathbb{Z}[x]$ konstans tagja osztható p-vel $\Rightarrow p^2 \mid a_0$ ↯

P $x^n - p$ irreducibilis $\mathbb{Q}[x]$-ben, és mivel primitív, $\mathbb{Z}[x]$-ben is irred., ha p prímszám. $\rightsquigarrow$ $\mathbb{Q}[x]$-ben van akármilyen nagy fokú irred. pol.

Mj A tétel csak elégséges feltételt ad a $\mathbb{Q}[x]$-beli irreducibilitás eldöntésére, a tétel megfordítása nem igaz: pl. $x + 1$ irreducibilis, de nincs megfelelő prím.

Mj A Sch.–E.-kritérium önmagában a $\mathbb{Z}[x]$-beli irreducibilitást nem biztosítja, csak ha a polinom primitivitását is feltesszük. Pl. a $3x + 6$ polinomra teljesülnek a Sch.–E.-kritérium feltételei $p = 2$-vel, de $\mathbb{Z}[x]$-ben $3x + 6 = 3(x + 2)$ valódi felbontás.

P Irreducibilis-e $\mathbb{Z}$ fölött az $f(x) = 2x^4 + 3x^3 - 9x + 6$ polinom?

m A $p = 3$ prímmel a Sch.–E.-kritérium feltételei fönnállnak $\rightsquigarrow$ $f(x)$ irreducibilis $\mathbb{Q}$ fölött, de primitív is, mert az együtthatók lnko-ja 1, így $\mathbb{Z}$ fölött is irreducibilis.

T **Fordított Schönemann–Eisenstein-kritérium**

Tfh. $f(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$, és van olyan $p \in \mathbb{N}^+$ prímszám, hogy

$$p \nmid a_0, \quad p \mid a_1, \ldots, a_n, \quad p^2 \nmid a_n.$$

Ekkor $f(x)$ irreducibilis $\mathbb{Q}[x]$-ben.

B Indirekt. Tfh. $f(x) = g(x)h(x)$ valódi felbontás. Feltehető, hogy $g, h \in \mathbb{Z}[x]$.
$\mathbb{Z}_p[x]$-ben nézve $f(x) = a_0 \neq 0$ konstans, és $\deg f = \deg g + \deg h \rightsquigarrow$ g, h is nemnulla konstans $\mathbb{Z}_p$ fölött. $\Rightarrow$
g és h mint $\mathbb{Z}[x]$-beli polinomok főegyütthatója osztható p-vel $\Rightarrow$ $p^2 \mid a_n$. $\lightning$

P Irreducibilis-e az $f(x) = 6x^4 - 12x^2 + 6x - 4$?

m A fordított Sch.–E. $p = 3$-mal igazolja, hogy $\mathbb{Q}$ fölött irreducibilis. $\mathbb{Z}$ fölött nem, mert $f(x) = 2(3x^4 - 6x^2 + 3x - 2)$.

Á Legyen $f(x) \in K[x]$, ahol K test, és $a, b \in K$, $a \neq 0$.

$f(x)$ irreducibilis $K[x]$-ben $\iff$ $f(ax+b)$ irreducibilis $K[x]$-ben

B Ha $f(x) = g(x)h(x)$ valódi felbontás, akkor $f(ax+b) = g(ax+b)h(ax+b)$ is valódi, mert a polinomok foka változatlan marad az $ax+b$ behelyettesítésekor.

Ha $f(ax+b) = k(x)\ell(x)$ valódi felbontás, akkor az $y = ax+b$, azaz $x = \frac{1}{a}y - \frac{b}{a}$ behelyettesítéssel azt kapjuk, hogy $f(y) = k\left(\frac{1}{a}y - \frac{b}{a}\right)\ell\left(\frac{1}{a}y - \frac{b}{a}\right)$ is valódi felbontás.

P Igazoljuk, hogy $f(x) = x^5 + 4$ irreducibilis!

m f-re semmilyen prímmel nem teljesül a Sch.–E.-kritérium.

Tekintsük az $f(x+1)$-et. A binomiális tétel szerint $f(x+1) = (x+1)^5 + 4 = x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 5$ már Sch.–E.-es $p = 5$-tel, tehát irreducibilis, és így $f(x)$ is az.

P Irreducibilis-e az $f(x) = 16x^4 - 8x^2 + 6$ polinom $\mathbb{Q}[x]$ fölött?

m Sem a sima, sem a fordított Sch.–E.-kritérium nem teljesül rá. Viszont $f(x) = (2x)^4 - 2(2x)^2 + 6$, tehát $y = 2x$ helyettesítéssel azt kapjuk, hogy $g(y) = y^4 - 2y + 6$ Sch.–E.-es $p = 2$-vel, ezért $g(y)$ irreducibilis, és így $f(x) = g(2x)$ is az.

F Alkalmas behelyettesítéssel és Sch.–E.-kritériummal adjunk új bizonyítást arra, hogy $x^4 + 1$ irreducibilis!

m $(x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$ Sch.–E.-es $p = 2$-vel.

D Az n. körosztási polinom

$\Phi_n(x) = \prod_{j=1}^{\varphi(n)} (x - \varepsilon_j)$, ahol $\varepsilon_1, \ldots, \varepsilon_{\varphi(n)}$ a primitív n. egységgyökök.

Á (1) $x^n - 1 = \prod_{d|n} \Phi_d(x)$

(2) $\Phi_n(x) \in \mathbb{Z}[x]$

B (1): Minden n-edik egységgyök d-edik primitív egységgyök valamely $d \mid n$-re és minden d-edik primitív egységgyök n-edik egységgyök.

(2): Teljes indukcióval n-re:

$\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, ezekre igaz.

Az (1)-ből

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d|n,\ 0<d<n} \Phi_d(x)}$$

Az ind. felt. miatt $\Phi_d(x) \in \mathbb{Z}[x]$, ha $d < n$, és 1 főegyütthatós is, ezért a nevezőben szereplő szorzat is ilyen. Tehát a maradékos osztás $\mathbb{Z}[x]$-ben is elvégezhető, és a hányados így $\mathbb{Z}[x]$-beli.

P $\Phi_8(x) = \frac{x^8-1}{x^4-1} = x^4 + 1$, mert a nyolcadik egységgyökök közül azokat kell kihagyni, amelyeknek kisebb a rendje ($1, 2$ vagy 4), azaz az $x^4 - 1$ gyökeit. Korábban láttuk (többféle módszerrel is), hogy ez a polinom irreducibilis $\mathbb{Q}$ fölött.

Á $\Phi_p(x)$ irreducibilis, ha p prím.

B $\Phi_p(x) = \dfrac{x^p - 1}{x - 1} = x^{p-1} + \ldots + x + 1.$

Az $x \mapsto x + 1$ behelyettesítéssel Sch.–E.-essé lehet tenni:

$$\frac{(x+1)^p - 1}{(x+1) - 1} = \frac{\left(\sum_{k=0}^{p} \binom{p}{k} x^k\right) - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1},$$ és $p \mid \binom{p}{k}$, ha $0 < k < p$, viszont $\binom{p}{1} = p$, és $\binom{p}{p} = 1$.

T $\Phi_n(x)$ irreducibilis $\mathbb{Q}[x]$-ben minden n-re.

Egyéb módszerek:

- Polinomok $\mathbb{Q}[x]$-beli faktorizálása: LLL-algoritmus (Lenstra, Lenstra, Lovász, 1982)
- A Sch.–E.-tétel általánosítása: Newton-poligonok
- Ha $p \nmid a_n$ és $f(x)$ irred. $\mathbb{Z}_p[x]$-ben, akkor irred. $\mathbb{Q}[x]$-ben is: Ha van valódi felbontása $\mathbb{Q}[x]$-ben, akkor ez $\mathbb{Z}[x]$-beli felbontássá alakítható, és az $\mathbb{Z}_p$ fölött is valódi felbontást ad, mert a főtagok nem tűnnek el.

P $f(x) = x^4 - 5x^3 + 2x^2 + 4x - 1$ irred. $\mathbb{Q}[x]$-ben?

m $\mathbb{Z}_2[x]$-ben $f(x) = x^4 + x^3 + 1$ irred., mert nincs gyöke, és két másodfokú irred.-re sem bontható, mert $(x^2 + x + 1)^2 = x^4 + x^2 + 1$ az egyetlen, ami két irred. szorzata. Így $\mathbb{Q}[x]$-ben is irred.

P Biz be, hogy $f(x) = x^4 + 5x^3 - x^2 + 1$ irred. $\mathbb{Q}[x]$-ben!

m Rac. gyöke nincs, és $\mathbb{Z}_2$ fölött $(x + 1)(x^3 + x + 1)$ az irred.-ekre bontása, tehát $\mathbb{Z}$ fölött sem lehetett két másodfokú irred.-re bontani.

P Bizonyítsuk be, hogy $\Phi_{12}(x)$ irreducibilis.

m $\Phi_{12}(x) = \dfrac{x^{12}-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x)\Phi_4(x)} = \dfrac{x^{12}-1}{(x^6-1)(x^2+1)} = \dfrac{x^6+1}{x^2+1} = x^4 - x^2 + 1.$

- Nincs racionális gyöke, mert az csak ± 1 lehetne.
- Nem Sch.–E.-es (sem sima, sem fordított), sőt nem is tehető azzá:
  $\Phi_{12}(ax+b) =$
  $a^4x^4 + 4a^3bx^3 + a^2(6b^2-1)x^2 + 2ab(2b^2-1)x + (b^4-b^2+1).$
  Simához $p \nmid a \rightsquigarrow p \mid 2b$ és $p \mid (6b^2-1)$ ↯
  Fordítotthoz $p \mid a^4 \rightsquigarrow p^4 \mid a^4$ ↯ ÍGY NEM MEGY.
- Semelyik p prímre nem irreducibilis a $\mathbb{Z}_p$ fölött:
  $x^4 - x^2 + 1 = \frac{1}{4}((2x^2-1)^2+3) = (x^2+1)^2 - 3x^2 = (x^2-1)^2 + x^2.$
  Tehát reducibilis, ha -3, 3 vagy -1 négyzetszám (kvadratikus maradék) modulo p. Könnyen belátható, hogy két kvadratikus nemmaradék szorzata, illetve hányadosa kvadratikus maradék.
  Tehát ebből sem lehet bizonyítani az irreducibilitást. ÍGY SEM.

- Bontsuk fel $\mathbb{R}[x]$-ben (akár először $\mathbb{C}[x]$-ben) irreducibilisekre!
  $x^4 - x^2 + 1 = (x^2+1)^2 - 3x^2 = (x^2 + \sqrt{3}x + 1)(x^2 - \sqrt{3}x + 1)$, és itt a másodfokúaknak már nincs valós gyöke.
  Ha $\mathbb{Q}[x]$-ben felbontható két másodfokúra (feltehető, hogy 1 főegyütthatósra), az $\mathbb{R}[x]$-ben is felbontás lenne, és az $\mathbb{R}$-ben tovább nem bontható, mert nincs a polinomnak valós gyöke. Tehát az irred.-ekre bontás egyértelműsége miatt az előbbi felbontással egyezne meg, de azok nem $\mathbb{Q}[x]$-beli polinomok. $\lightning$
  Ezzel beláttuk, hogy $\Phi_{12}(x)$ irreducibilis. ÍGY IGEN!
- Egy másik lehetőség annak elemzése, hogy hogyan bontható fel $\mathbb{Z}[x]$-ben két másodfokú szorzatára: $(x^2 + ax + 1)(x^2 - ax + 1)$ vagy $(x^2 + ax - 1)(x^2 - ax - 1)$ jöhet csak szóba, de x^2 együtthatója egyiknél sem lehet -1. ÍGY IS.

Mj $n < 12$-re működik az, hogy behelyettesítéssel Sch.–E.-es alakra hozzuk $\Phi_n(x)$-et, és még jó néhány más esetre is.