

### Irreducibilitás $\mathbb{Q}[x]$ -ben (K3.5. szakasz)

A  $\mathbb{Q}[x]$  legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a *racionális gyökteszt* segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

#### Schönemann–Eisenstein-kritérium (K3.5.2, biz. később)

Legyen  $f$  egész együtthatós, nem konstans polinom. *HA* van olyan  $p$  prímszám, amelyre

- (1)  $p$  nem osztja  $f$  főegyütthatóját;
- (2)  $p$  osztja  $f$  összes többi együtthatóját;
- (3)  $p^2$  nem osztja  $f$  konstans tagját,

*AKKOR*  $f$  irreducibilis  $\mathbb{Q}$  fölött.

Példa:  $21x^4 + 60x - 150$  irreducibilis  $\mathbb{Q}$  fölött ( $p = 2$  jó). A  $p = 3$  nem jó:  $3 \mid 21$ . A  $p = 5$  nem jó:  $5^2 \mid 150$ .

### A Schönemann–Eisenstein-kritérium tanulságai

#### Tanulságok

- (1) *Nem igaz a megfordítása.* Példa:  $x + 1$  irreducibilis  $\mathbb{Q}$  fölött, de nem alkalmazható rá a kritérium.
- (2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa:  $x^7 + (2/3)$ .
- (3) Csak  $\mathbb{Q}$  fölötti, és *nem*  $\mathbb{Z}$  fölötti irreducibilitást biztosít. Példa:  $9x + 18$  irreducibilis  $\mathbb{Q}$  fölött, de  $\mathbb{Z}$  fölött nem: itt  $9(x + 2)$  nemtriviális felbontás.
- (4) A kritérium miatt  $x^n - 2$  irreducibilis minden  $n \geq 1$ -re. *Azaz létezik  $\mathbb{Q}$  fölött akárhányszor fokú irreducibilis polinom.*
- (5) Fordított Schönemann–Eisenstein-kritérium: Ha a  $p$  prím osztja a polinom minden együtthatóját a konstans tag kivételével, és  $p^2$  nem osztja a főegyütthatót, a polinom akkor is irreducibilis  $\mathbb{Q}$  fölött (K3.5.7).

### További módszerek $\mathbb{Q}$ fölött

#### Állítás (K3.5.5)

$f \in \mathbb{Q}[x]$  irreducibilis  $\mathbb{Q}$  fölött, ha alkalmas *eltolja*, vagyis az  $f(x + c)$  polinom irreducibilis  $\mathbb{Q}$  fölött ( $c \in \mathbb{Q}$ ).

Valóban,  $f(x) = g(x)h(x) \iff f(x + c) = g(x + c)h(x + c)$ .

Példa:  $x^4 + 1$ -re nem alkalmazható a Schönemann–Eisenstein. De  $(x + 1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$ , erre már igen,  $p = 2$ -vel. Tehát  $x^4 + 1$  is irreducibilis  $\mathbb{Q}$  fölött.

**Tétel**

Létezik algoritmus az irreducibilitás eldöntésére  $\mathbb{Q}$  fölött, például interpoláció segítségével. Van hatékony algoritmus is.

A módszerek összefoglalása: a Kiss-könyv 111. oldalán.

**1. Egész együtthatós polinomok****Oszthatóság egész számmal**

Emlékeztető (K3.1.3): Ha  $f, g \in \mathbb{Z}[x]$ , akkor  $f \mid g$  akkor és csak akkor, ha van olyan  $h \in \mathbb{Z}[x]$ , hogy  $g = fh$ .

**Állítás (K3.1.6)**

Az  $f(x) \in \mathbb{Z}[x]$  akkor és csak akkor osztható  $\mathbb{Z}[x]$ -ben a  $c$  egész számmal, ha  $f$  minden együtthatója osztható  $c$ -vel.

**Bizonyítás**

Ha  $c \mid f(x)$ , akkor van olyan  $h(x) = b_0 + b_1x + \dots + b_nx^n \in \mathbb{Z}[x]$ , melyre  $ch(x) = f(x)$ . Ezért  $f(x)$  együtthatói a  $cb_i$  számok, amik mind  $c$ -vel oszthatók. Megfordítva: Legyen  $f(x) = a_0 + a_1x + \dots + a_nx^n$ . Ha minden  $a_i$  osztható  $c$ -vel, akkor vannak olyan  $b_i$  egészek, hogy  $cb_i = a_i$  minden  $i$ -re.

Így  $f(x) = c(b_0 + b_1x + \dots + b_nx^n)$ , és a zárójelben egész együtthatós polinom áll. Ezért  $c \mid f(x)$ .  $\square$

**Primitív polinomok****Emlékeztető (K3.1. szakasz)**

*Egység:* minden polinomnak osztója.  $\mathbb{Z}$ -ben,  $\mathbb{Z}[x]$ -ben csak a  $\pm 1$ . Az  $f = gh$  *triviális felbontás*, ha  $g$  és  $h$  valamelyike egység. Az  $f$  *felbonthatatlan*, más szóval *irreducibilis*, ha nem nulla, nem egység, és nincs nemtriviális felbontása.

Példa: az  $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$  irreducibilisekre bontása  $\mathbb{Z}[x]$ -ben 4 tényezőssé:  $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$ .

**Definíció (K3.4.1)**

*Primitív polinom:* együtthatóinak legnagyobb közös osztója 1.

Példa:  $60x^6 + 36x^4 + 90 = 6(10x^6 + 6x^4 + 15)$ . Kiemeltük az együtthatók legnagyobb közös osztóját. Nyilván  $(10, 6, 15) = 1$  (de nem páronként relatív prímelek). Ezért  $10x^6 + 6x^4 + 15$  már primitív polinom.

**Felbonthatatlan konstans polinomok****Tétel (K3.4.2)**

Ha egy  $n$  egész szám  $\mathbb{Z}$ -ben felbonthatatlan, akkor polinomként tekintve felbonthatatlan  $\mathbb{Z}[x]$ -ben is.

### Bizonyítás

Mivel  $n$  felbonthatatlan  $\mathbb{Z}$ -ben, ezért nem nulla és nem egység. Tudjuk, hogy a  $\mathbb{Z}$  és a  $\mathbb{Z}[x]$  egységei ugyanazok:  $\pm 1$ . Ezért  $n$  a  $\mathbb{Z}[x]$ -ben sem egység.

Kell:  $n$  minden felbontása triviális  $\mathbb{Z}[x]$ -ben. Tegyük fel, hogy  $n = g(x)h(x)$ , ahol  $g, h \in \mathbb{Z}[x]$ . Mindkét oldal fokát véve  $0 = \text{gr}(n) = \text{gr}(g) + \text{gr}(h)$  adódik. Ezért  $g$  és  $h$  is nem nulla konstans, azaz egész szám. Mivel  $n$  felbonthatatlan  $\mathbb{Z}$ -ben, ez a felbontás triviális, vagyis  $g$  és  $h$  egyike egység  $\mathbb{Z}$ -ben, így  $\mathbb{Z}[x]$ -ben is, és ezért az  $n = g(x)h(x)$  felbontás tényleg triviális  $\mathbb{Z}[x]$ -ben.  $\square$

### Prím konstans polinomok\*

Emlékeztető (K3.1.25):  $f \in \mathbb{Z}[x]$  *prím*, ha nem nulla, nem egység, és minden  $g, h \in \mathbb{Z}[x]$  esetén, ha  $f \mid gh$ , akkor  $f \mid g$  vagy  $f \mid h$ .

### Gauss-lemma I (K3.4.3)

Ha  $p \in \mathbb{Z}$  prím, akkor  $p$  a  $\mathbb{Z}[x]$ -ben is prím (konstans polinomként).

### Bizonyítás

Mivel  $p$  prím, ezért nem nulla, és nem egység  $\mathbb{Z}[x]$ -ben sem. Tegyük fel, hogy  $p \mid g(x)h(x)$ , ahol  $g(x) = a_0 + a_1x + \dots + a_nx^n$  és  $h(x) = b_0 + b_1x + \dots + b_mx^m$ . Indirekt feltevés:  $p \nmid g$  és  $p \nmid h$ . Legyen  $i$ , illetve  $j$  a legnagyobb index, melyre  $p \nmid a_i$ , illetve  $p \nmid b_j$ . Mivel  $p$  prím  $\mathbb{Z}$ -ben,  $p \nmid a_ib_j$ . De minden más tag  $p$ -vel osztható a  $c_{i+j} = a_0b_{j+i} + \dots + a_{i-1}b_{j+1} + a_ib_j + a_{i+1}b_{j-1} + \dots + a_{i+j}b_0$  összegben, ami  $gh$  egy együtthatója. Így  $p \nmid c_{i+j}$ , ellentmondás.  $\square$

### Az első Gauss-lemma első következménye\*

#### Gauss-lemma I, első következmény (K3.4.4)

Primitív polinomok szorzata is primitív.

### Bizonyítás

Ha  $gh$  nem primitív, akkor van olyan  $p \in \mathbb{Z}$  prím, amire  $p \mid gh$ . Ha  $g, h$  primitív, akkor  $p \nmid g$  és  $p \nmid h$ , ez ellentmond Gauss I-nek.  $\square$

### Állítás

Minden  $f \in \mathbb{Q}[x]$  polinom felírható  $(s/t)f_0$  alakban, ahol  $s$  és  $t$  relatív prím egészek,  $f_0 \in \mathbb{Z}[x]$  pedig primitív.

### Bizonyítás

Hozzuk  $f$  együtthatóit közös nevezőre, majd emeljük ki a számlálók legnagyobb közös osztóját, végül egyszerűsítsünk.  $\square$

### Az első Gauss-lemma második következménye\*

#### Gauss-lemma I, második következmény (K3.4.5)

Legyen  $f \in \mathbb{Z}[x]$  primitív. Ha  $g \in \mathbb{Q}[x]$  és  $h = fg \in \mathbb{Z}[x]$ , akkor  $g \in \mathbb{Z}[x]$ . Így ha egy primitív  $f$  osztója egy  $h \in \mathbb{Z}[x]$  polinomnak  $\mathbb{Q}[x]$ -ben, akkor  $f$  osztója  $h$ -nak  $\mathbb{Z}[x]$ -ben is.

### Bizonyítás

Az előző állítás szerint  $g = (s/t)g_0$ , ahol  $(s, t) = 1$  és  $g_0$  primitív.

Ekkor  $th = sf_0$ . Ha  $p$  prímosztója  $t$ -nek, akkor  $p \mid sf_0$ . Az első Gauss-lemma miatt  $p \mid s$ , vagy  $p \mid f$ , vagy  $p \mid g_0$ . Mindhárom lehetetlen, az első azért, mert  $t$  és  $s$  relatív prímekek, a másik kettő azért, mert  $f$  és  $g_0$  primitívek. A  $t$  számnak nincs tehát prímosztója, vagyis  $t$  egység, és így  $g = (s/t)g_0$  tényleg egész együtthatós polinom.  $\square$

### A második Gauss-lemma\*

Példa:  $x^2 - 1 = [(2/3)x - (2/3)][(3/2)x + (3/2)]$ .

Ez az  $x^2 - 1$  egy elbonyolított felbontása. Ki lehet javítani, ha az első tényezőt  $3/2$ -del, a másodikat  $2/3$ -dal szorozzuk. A második Gauss-lemma szerint ez mindig lehetséges.

### Gauss-lemma II (K3.4.7)

Ha  $0 \neq f \in \mathbb{Z}[x]$  és  $f = gh$ , ahol  $g, h \in \mathbb{Q}[x]$ , akkor  $g$  és  $h$  megszorozható racionális számokkal úgy, hogy a kapott  $g_1$  és  $h_1$  polinomok egész együtthatósak legyenek, és  $f = g_1h_1$  teljesüljön.

### Bizonyítás

Legyen  $g = rg_0$  és  $h = sh_0$ , ahol  $r, s \in \mathbb{Q}$  és  $g_0, h_0 \in \mathbb{Z}[x]$  primitív. Ekkor  $f = (rs)(g_0h_0)$ . A Gauss-lemma I első következménye miatt  $g_0h_0$  primitív, így a második következménye miatt  $rs \in \mathbb{Z}[x]$ , azaz  $rs$  egész szám. Így a  $g_1 = rsg_0$  és  $h_1 = h_0$  jó választás.  $\square$

### Az irreducibilitás kapcsolata $\mathbb{Z}$ és $\mathbb{Q}$ fölött\*

- (1) Ha  $f \in \mathbb{Z}[x]$  nem konstans és irreducibilis  $\mathbb{Z}$  fölött, akkor  $f$  irreducibilis  $\mathbb{Q}$  fölött is.
- (2) Ha  $f$  primitív és irreducibilis  $\mathbb{Q}$  fölött, akkor  $\mathbb{Z}$  fölött is.

(1): Mivel  $f$  nem konstans, ezért nem 0 és nem egység  $\mathbb{Q}$  fölött.

Tegyük föl, hogy  $f = gh$  nemtriviális felbontás  $\mathbb{Q}$  fölött, tehát  $g$  és  $h$  nem konstans. A második Gauss-lemma miatt  $f = g_1h_1$ , ahol  $g_1, h_1 \in \mathbb{Z}[x]$ , és  $\text{gr}(g_1) = \text{gr}(g)$ ,  $\text{gr}(h_1) = \text{gr}(h)$ . Az  $f = g_1h_1$  felbontás triviális  $\mathbb{Z}$  fölött, mert  $f$  irreducibilis  $\mathbb{Z}[x]$ -ben. Így  $g_1$  és  $h_1$  egyike  $\pm 1$ , de akkor  $f$  és  $g$  egyike konstans, ami ellentmond annak, hogy  $f = gh$  nemtriviális felbontás.

(2): Ha  $f$  primitív, irreducibilis  $\mathbb{Q}$  fölött és  $f = gh$ , ahol  $g, h \in \mathbb{Z}[x]$ , akkor a  $\mathbb{Q}$  fölötti irreducibilitás miatt  $g$  és  $h$  egyike konstans, és így egész szám. Mivel  $f$  primitív, ez az egész szám csak  $\pm 1$  lehet.  $\square$

### $\mathbb{Z}[x]$ irreducibilis polinomjainak jellemzése

#### **Tétel (K3.4.8)**

Egy  $f \in \mathbb{Z}[x]$  polinom pontosan akkor irreducibilis  $\mathbb{Z}$  fölött, ha

- (1) vagy egy  $\mathbb{Z}$ -beli prímszám (mint konstans polinom),
- (2) vagy egy primitív polinom, amely  $\mathbb{Q}$  fölött irreducibilis.

#### **Bizonyítás**

A felsorolt polinomokról már beláttuk, hogy  $\mathbb{Z}[x]$ -ben irreducibilisek. Tegyük fel, hogy  $f \in \mathbb{Z}[x]$  irreducibilis. Emeljük ki együtthatóinak legnagyobb közös osztóját:  $f = nf_0$ , ahol  $f_0$  primitív és  $n$  egész. Ez triviális felbontás kell, hogy legyen, ezért vagy  $f_0 = \pm 1$ , vagy  $n = \pm 1$ . Az első esetben  $f = \pm n$  egy  $\mathbb{Z}$ -beli prímszám. A második esetben  $f$  primitív, és nem konstans, különben  $f$  egység lenne  $\mathbb{Z}[x]$ -ben. Láttuk, hogy ekkor  $f$  irreducibilis  $\mathbb{Q}$  fölött.  $\square$

#### $\mathbb{Z}[x]$ alaptételes: egyértelműség

#### **Tétel (K3.4.10)**

$\mathbb{Z}[x]$ -ben érvényes a számelmélet alaptétele.

#### **Bizonyítás**

Az *egyértelműség* igazolásához elég megmutatni, hogy minden irreducibilis prím (ebből a bizonyítás ugyanaz, mint egészekre).

Legyen  $f \in \mathbb{Z}[x]$  irreducibilis. Ha  $f$  konstans prímszám, akkor az első Gauss-lemma miatt  $f$  prím  $\mathbb{Z}[x]$ -ben. A másik esetben  $f$  primitív és irreducibilis  $\mathbb{Q}$  fölött. Tegyük föl, hogy  $f$  osztója  $\mathbb{Z}[x]$ -ben  $gh$ -nak, ahol  $g, h \in \mathbb{Z}[x]$ . Mivel  $\mathbb{Q}[x]$  alaptételes,  $f$  prímtulajdonságú  $\mathbb{Q}[x]$ -ben, tehát  $f$  osztója  $g$ -nek vagy  $h$ -nak  $\mathbb{Q}[x]$ -ben. Az első Gauss-lemma második következménye miatt ez az oszthatóság  $\mathbb{Z}[x]$ -ben is fennáll. Így  $f$  prím  $\mathbb{Z}[x]$ -ben.

#### $\mathbb{Z}[x]$ alaptételes: a felbontás létezése

Először megmutatjuk, hogy minden nem konstans primitív polinom felbontható felbonthatatlanok szorzatára.

Legyen  $g$  minimális fokú ellenpélda. Ha  $g$  irreducibilis, akkor az egytényezős felbontás jó. Ha nem, akkor  $g = hk$  ahol  $h$  és  $k$  nem egység. Mivel  $g$  primitív,  $h$  és  $k$  is az. Így egyikük sem konstans (mert akkor egység lenne), és ezért mindkettő  $g$ -nél alacsonyabb fokúak. Mivel  $g$  foka minimális,  $h$  és  $k$  már felbomlik irreducibilisek szorzatára. A két felbontást összeszorozva  $g$  felbontását kapjuk.

Ha  $f \in \mathbb{Z}[x]$  tetszőleges, akkor legyen  $f = nf_0$ , ahol  $f_0$  primitív polinom és  $n$  egész. Ekkor  $n$  felbontható prím egész számok szorzatára,  $f_0$  pedig a fentiek szerint irreducibilisek szorzatára.  $\square$

## A Schönemann–Eisenstein-kritérium

### Schönemann–Eisenstein-kritérium (K3.5.2)

Legyen  $f$  egész együtthatós, nem konstans polinom.  $HA$  van olyan  $p$  prímszám, amelyre

- (1)  $p$  nem osztja  $f$  főegyütthatóját;
- (2)  $p$  osztja  $f$  összes többi együtthatóját;
- (3)  $p^2$  nem osztja  $f$  konstans tagját,

*AKKOR*  $f$  irreducibilis  $\mathbb{Q}$  fölött.

### Bizonyítás

Tegyük föl, hogy  $f$  mégsem irreducibilis  $\mathbb{Q}$  fölött, vagyis az  $f$ -nél alacsonyabb fokú, racionális együtthatós  $g$  és  $h$  polinomok szorzatára bontható. A második Gauss-lemma miatt feltehetjük, hogy  $g$  és  $h$  egész együtthatós.

### A Schönemann–Eisenstein-kritérium bizonyítása

Legyen  $f(x) = a_0 + \dots + a_n x^n$ ,  $g(x) = b_0 + \dots + b_k x^k$  és  $h(x) = c_0 + \dots + c_\ell x^\ell$ , ahol  $\text{gr}(g) = k < n$  és  $\text{gr}(h) = \ell < n$ . Mivel  $a_n = b_k c_\ell$ , a  $b_k$  és  $c_\ell$  egészek egyike sem osztható  $p$ -vel. Továbbá  $a_0 = b_0 c_0$ , és mivel  $a_0$  osztható  $p$ -vel, de  $p^2$ -tel nem, ezért a  $b_0$  és  $c_0$  számok közül pontosan az egyik osztható  $p$ -vel. A  $g$  és a  $h$  esetleges cseréjével feltehetjük, hogy ez a  $b_0$ . Legyen  $i$  a legkisebb olyan index, amelyre  $b_i$  nem osztható  $p$ -vel. Ilyen  $i$  van, hiszen  $b_0$  osztható  $p$ -vel, de  $b_k$  nem, és  $0 < i \leq k$ . Mivel  $f = gh$ , ezért  $a_i = b_0 c_i + b_1 c_{i-1} + \dots + b_{i-1} c_1 + b_i c_0$ . Ez az együttható nem osztható  $p$ -vel, mert az összeg mindegyik tagja osztható vele, kivéve az utolsó tagot. A feltétel szerint  $f$  együtthatói oszthatók  $p$ -vel, kivéve  $a_n$ -et. Ezért  $i = n$ , azaz  $i \leq k$  miatt  $k \geq n$ . Ez ellentmond a  $k < n$  feltételnek.  $\square$

## A többhatározatlanú polinomok számelmélete

### Tétel (K3.4.10, K3.4.11)

Tudjuk: A  $\mathbb{Z}[x]$  polinomgyűrű alaptételes.

Általánosítás: Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x]$  is az.

### Bizonyítás

Ugyanúgy, mint  $\mathbb{Z}[x]$  esetében. Ehhez meg kell mutatni, hogy ha  $R$  szokásos gyűrű, akkor az elemeiből törteket lehet képezni a szokásos tulajdonságokkal, azaz testet kapunk. Lásd: *hányadostest*, K5.7.

### Következmény (vö. K3.4.12)

Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x_1, x_2, \dots, x_n]$  is az.

Speciálisan  $\mathbb{Z}[x_1, x_2, \dots, x_n]$ , és ha  $T$  test, akkor  $T[x_1, x_2, \dots, x_n]$  is *alaptételes gyűrűk*.

## 2. Összefoglaló

### A 24. előadáshoz tartozó vizsgaanyag

#### Fogalmak

Primitív polinom (K3.4.1).

#### Tételek

A Schönemann–Eisenstein-kritérium (K3.5.2, K3.5.7).

Az eltolt irreducibilitása (K3.5.5).

Gauss-lemma I (K3.4.3\*), ennek két következménye (K3.4.4\*, K3.4.5\*).

Gauss-lemma II (K3.4.7\*).

A  $\mathbb{Z}[x]$  irreducibiliseinek visszavezetése  $\mathbb{Q}[x]$ -re (K3.4.8).

$\mathbb{Z}[x]$  alaptételes (K3.4.10).

$\mathbb{Z}[x_1, x_2, \dots, x_n]$ ,  $T[x_1, x_2, \dots, x_n]$  alaptételes, ahol  $T$  test (K3.4.10–12).