Polinomok

Diszkrét modellek alkalmazásai

1. Alapfogalmak

1.1. Definíció. Egy matematikai kifejezést *polinom*nak nevezünk, ha csak a következők szerepelnek benne:

- konstansok (pl. számok),
- egy változó (pl. x),
- összeadás, kivonás, szorzás,
- hatványozás $\mathbb{N}$-beli kitevővel,
- zárójelek.

Például polinom a $3x^5 - 5x^3 + x + 1/2$, az $x^2(x+3)^5$ és a 15, viszont nem polinom például az $1/x$ (mert osztás van benne), az x^{-5} (mert a kitevő nem $\mathbb{N}$-ben van) és a $\sqrt{x}$ (mert nem megengedett művelet van benne).

(Megjegyzés: lehet általánosabban is definiálni a polinomot, ha megengedünk egynél több változót is, például akkor az x^3+xy^2+y egy kétváltozós polinom. Ekkor a fenti definíció az *egyváltozós polinom*ot definiálja. Ebben a tárgyban azonban csak az utóbbiakkal foglalkozunk, ezért nem tesszük ki külön az "egyváltozós" jelzőt.)

1.2. Definíció. Azon polinomok halmazát, melyekben a konstansok a K halmazból vannak, és x a változó, $K[x]$-szel jelöljük.

Például a valós számokat tartalmazó polinomok halmazát $\mathbb{R}[x]$-szel jelöljük, vagy ha a konstansokat leszűkítjük az egész számokra, akkor $\mathbb{Z}[x]$-szel (és persze $\mathbb{Z}[x] \subseteq \mathbb{R}[x]$). (Később majd pontosabban is definiáljuk, mi lehet a K, de addig is legyen egy számhalmaz, pl. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ stb.)

Egy polinomot többféle alakban is felírhatunk, pl. $(2x+1)^2 = 4x^2+4x+1 = x^5+1+x-x^5+4x^2+3x$. Ha egyértelmű felírást szeretnénk, akkor egy kitüntetett alakot használunk:

1.3. Definíció. Egy $p \in K[x]$ polinom *kanonikus alakja* a $p = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2x^2 + a_1x + a_0$ alak, ahol $\forall a_k \in K$ és $a_n \neq 0$.

Például $p = (2x+1)^2$ kanonikus alakja $p = 4x^2 + 4x + 1$. Egy polinomot úgy hozhatunk kanonikus alakra, ha a zárójeleket felbontjuk, a tagokban szereplő x-eket egy hatványba gyűjtjük (pl. $2x \cdot 2x = 4x^2$), az azonos kitevőjű tagokat összevonjuk, és a tagokat kitevő szerint csökkenő sorrendbe írjuk.

1.4. Definíció. A fenti kanonikus alakban szereplő

- a_k-k a polinom *együtthatói* (egészen pontosan a_k a polinom *k-adfokú együtthatója*),
- n a polinom *fokszáma* – jelölés: $\deg p$ –,
- a_n a polinom *főegyütthatója* és
- a_0 a polinom *konstans tagja*.

Például $p = 2x^3 - 5x + 4$ együtthatói 2, 0, -5 és 4, fokszáma 3, főegyütthatója 2 és konstans tagja 4.

Van azonban egy polinom, amely nem írható fel kanonikus alakban (a fenti definíció alapján): a 0 (mert kitötöttük, hogy $a_n \neq 0$). Ezért ezt külön kell kezelni:

1.5. Definíció. A $0 \in K[x]$ polinom neve *nullpolinom*, kanonikus alakja 0, és fokszáma $-\infty$.

(Megjegyzés: azért $-\infty$, hogy kisebb legyen bármely más polinom fokszámánál. Nem definiálhatjuk 0-nak, mert akkor a nullpolinomra nem működnének bizonyos megállapítások, amelyek minden más polinomra igazak, például a lenti 1.7 Tétel. Más források nem definiálják a nullpolinom fokszámát, a Sage pedig -1-nek definiálja.)

Még néhány speciális eset:

1.6. Definíció.

- $p \in K[x]$ *konstans polinom*, ha $\deg p \leq 0$.
- $p \in K[x]$ *lineáris polinom*, ha $\deg p \leq 1$.

Például konstans polinom a 2 és a 0, és lineáris polinomok a $2x-3$, az x, a 2 és a 0.

Ha műveleteket végzünk polinomokkal, akkor a fokszámok a következőképpen alakulnak:

1.7. Tétel. *Ha $p, q \in \mathbb{R}[x]$, akkor:*

1. $\deg(p+q) \leq \max(\deg p,\ \deg q)$ *(és egyenlőség van, ha* $\deg p \neq \deg q$*);*
2. $\deg(p-q) \leq \max(\deg p,\ \deg q)$ *(és egyenlőség van, ha* $\deg p \neq \deg q$*);*
3. $\deg(p \cdot q) = \deg p + \deg q$.

Például ha $p = 2x - 1$ és $q = x^2 + 2$, akkor $\deg p = 1$ és $\deg q = 2$, és valóban: $\deg(p+q) = \deg(x^2 + 2x + 1) = 2 = \max(1, 2)$ és $\deg(p \cdot q) = \deg(2x^3 - x^2 + 4x - 2) = 3 = 1 + 2$.

(Megjegyzés: ezek nullpolinomra is működnek, például $0 \cdot x^2 = 0$, és valóban, $-\infty + 2 = -\infty$.)

2. Polinomok Sage-ben

Sage-ben polinomokkal számolhatunk úgy, mint bármely más szimbolikus kifejezéssel:

```
sage: (2*x - 1)*(x^2 + 2)
(x^2 + 2)*(2*x - 1)
sage: expand(_)
2*x^3 - x^2 + 4*x - 2
sage: type(_)
<class 'sage.symbolic.expression.Expression'>
```

(Emlékeztető: `x` egy beépített szimbolikus változó, mintha `var("x")`-szel hoztuk volna létre, lásd a SageMath bevezetés c. jegyzetet.)

Ez azonban így kissé nehézkes (pl. mindig `expand()` kell), és polinomokra nem a leghatékonyabb megoldás. Vannak a Sage-ben kifejezetten polinomokra optimalizált struktúrák: `ZZ["x"]`, `QQ["x"]` stb., amelyek megfelelnek a matematikai $\mathbb{Z}[x]$-nek, $\mathbb{Q}[x]$-nek stb.:

```
sage: P = ZZ["x"]
sage: p = P(2*x - 1)    # szimbolikus kifejezés konvertálása polinommá
sage: p
2*x - 1
sage: q = P([2, 0, 1])  # polinom létrehozása együtthatókból (első a konstans tag)
sage: q
x^2 + 2
```

```
sage: p * q    # nem kell expand()
2*x^3 - x^2 + 4*x - 2
sage: type(_)
<class 'sage.rings.polynomial.[...]'>
```

Vigyázat, itt `x` két különböző dolgot jelent: a beírt parancsokban `x` továbbra is egy szimbolikus változó (típusa: `Expression`), viszont a válaszokban `x` a polinomok változóját jelenti (típusa: polinom). Ezeket ne keverjük össze:

```
sage: p*(x^2 + 2)     # NE csináljuk! (polinom * szimbolikus kifejezés)
(x^2 + 2)*(2*x - 1)
sage: type(_)         # elvesztettük a polinomok előnyeit:
<class 'sage.symbolic.expression.Expression'>
```

(Megjegyzés: kissé leegyszerűsítve, a Sage a szimbolikus kifejezéseket műveletek sorozatával ábrázolja, például x^2+2-t úgy, hogy "x-et emeljük négyzetre, és adjunk hozzá 2-t". Ez elég általános, de nehéz vele hatékonyan számolni. A polinomokat viszont az együtthatók sorozatával ábrázolja, pl. x^2+2-t úgy, hogy $2, 0, 1$. Ez sokkal hatékonyabb számítást tesz lehetővé.)

Hogy ne keverjük a szimbolikus kifejezéseket a polinomokkal, beállíthatjuk, hogy `x` is polinom legyen:

```
sage: P = ZZ["x"]    # legyen P polinomok halmaza
sage: x = P.gen()    # legyen x a P-beli polinomok változója
```

Sőt, van egy szintaxis, amellyel `P`-t és `x`-et egyszerre is beállíthatjuk:

```
sage: P.<x> = ZZ[]   # ugyanaz, mint: P = ZZ["x"]; x = P.gen()
sage: P
Univariate Polynomial Ring in x over Integer Ring
sage: type(x)              # x-et is felülírta
<class 'sage.rings.polynomial.[...]'>
sage: (2*x - 1)*(x^2 + 2)  # most már ezek is polinomok
2*x^3 - x^2 + 4*x - 2
sage: var("x")             # x visszaállítása
sage: type(x)
<class 'sage.symbolic.expression.Expression'>
```

Egy polinomnak le tudjuk kérdezni a különböző tulajdonságait:

```
sage: P.<x> = ZZ[]
sage: p = 2*x^3 - 5*x + 4
sage: p.degree()                # fokszám
3
sage: p.list()                  # együtthatók listája (konstans tagtól kezdve)
[4, -5, 0, 2]
sage: p[1]                      # elsőfokú együttható
-5
sage: p.leading_coefficient()   # főegyüttható (röviden: p.lc())
2
sage: p.constant_coefficient()  # konstans tag (röviden: p[0])
4
```

3. Helyettesítési érték

3.1. Definíció. Egy $p \in K[x]$ polinom c helyen felvett *helyettesítési értéke* az az érték, amelyet úgy kapunk, hogy p-ben x helyére c-t írunk. Jelölés: $p(c)$.
Például ha $p = x^2 - 3x + 5$ és $c = 2$, akkor $p(2) = 2^2 - 3 \cdot 2 + 5 = 3$.
Megjegyzés: nem kell, hogy $c \in K$ legyen, például ugyanezt a $p = x^2 - 3x + 5 \in \mathbb{Z}[x]$ polinomot kiértékelhetjük a $c = 1/2 \notin \mathbb{Z}$ helyen is: $p(1/2) = (1/2)^2 - 3 \cdot (1/2) + 5 = 15/4$.
A helyettesítési érték kiszámításának nem az a leghatékonyabb módja, ha a kanonikus alakot, azaz a $p(c) = a_n c^n + \ldots + a_1 c + a_0$ felírást használjuk. Ennek ugyanis így nagy a műveletigénye: $a_n c^n$-hez n szorzás kell, $a_{n-1}c^{n-1}$-hez $n-1$ stb., ami összesen $n + (n-1) + \ldots + 2 + 1 = n(n+1)/2$ szorzás, és kell még n összeadás. (Ez például egy tizedfokú polinomra 55 szorzást és 10 összeadást jelent.)
Ezt javíthatjuk úgy, ha jobbról balra számolunk, és mindig megjegyezzük az utolsó c^k értéket, mert akkor a következő c^{k+1}-hez már csak plusz egy szorzás kell: $c^{k+1} = c^k \cdot c$. Így összesen csak $2n-1$ szorzás és n összeadás kell (ami tizedfokú polinomra 19 szorzás és 10 összeadás).
Ennél is hatékonyabb a *Horner-módszer* (vagy *Horner-elrendezés*), amely a polinomot kiemelésekkel olyan alakra hozza, amelyből nagyon hatékonyan lehet kiértékelni. Például:

$$\begin{aligned} p &= 2x^4 + 3x^3 - 2x^2 - 4x + 3 = \\ &= (2x^3 + 3x^2 - 2x - 4)x + 3 = \\ &= ((2x^2 + 3x - 2)x - 4)x + 3 = \\ &= (((2x + 3)x - 2)x - 4)x + 3. \end{aligned}$$

Vagyis minden lépésben kiemelünk x-et azokból a tagokból, amelyekből lehet, és ezt addig folytatjuk, amíg minden kitevő el nem tűnik. Általában ez a következő átírást jelenti:

$$\begin{aligned} p &= a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_2 x^2 + a_1 x + a_0 = \\ &= ((\ldots((a_n x + a_{n-1})x + a_{n-2})x + \ldots + a_2)x + a_1)x + a_0. \end{aligned}$$

Ebből a felírásból a behelyettesítés hatékonyan elvégezhető: minden lépésben megszorozzuk az egyik zárójeles kifejezést (legelőször a_n-et) x-szel (vagyis c-vel), majd ehhez hozzáadjuk a következő együtthatót, és így megkapjuk a következő zárójeles kifejezést, végül pedig a végeredményt. Ehhez tehát összesen csak n szorzás és n összeadás kell.
A Horner-módszert algoritmikusan a következőképpen írhatjuk fel:

1. Bemenet: a polinom $a_0, a_1, \ldots, a_n$ együtthatói és a c érték.
2. $b := a_n$
3. Ciklus $k = n-1$-től 0-ig:
   - $b := b \cdot c + a_k$
4. A helyettesítési érték: b

Itt b menet közben a fenti felírás egy-egy zárójeles részkifejezését jelenti (például az első lépés után $b = a_n c + a_{n-1}$, aztán $b = (a_n c + a_{n-1})c + a_{n-2}$ stb.).
(Megjegyzés: a nullpolinomra így ez az algoritmus nem működik, mert annak nincsenek együtthatói. Ezt megoldhatjuk úgy, ha egyetlen nulla együtthatót adunk meg: $n = 0$ és $a_0 = 0$. Az algoritmushoz ugyanis nem kötelező, hogy $a_n \neq 0$ legyen, azaz lehetnek fölösleges 0-k az együtthatólista végén.)
A helyettesítési értéket természetesen a Sage is ki tudja számítani, pl. a `p(2)` kifejezéssel, ahol `p` egy Sage polinom. (És egyébként a Sage is a Horner-módszert használja.)

4. Gyökök

4.1. Definíció. A c érték a $p \in K[x]$ polinom *gyöke*, ha $p(c) = 0$.
Például $c = 1$ gyöke a $p = 2x^2 - 3x + 1$ polinomnak, mert $p(1) = 2 \cdot 1^2 - 3 \cdot 1 + 1 = 0$.
Itt sem kell, hogy $c \in K$ legyen, például ugyanennek a p-nek (amely $p \in \mathbb{Z}[x]$) gyöke a $c = 1/2 \notin \mathbb{Z}$ is: $p(1/2) = 2 \cdot (1/2)^2 - 3 \cdot (1/2) + 1 = 0$. Másik példa: $q = x^2 + 1 \in \mathbb{R}[x]$, de ennek nincsenek valós gyökei, csak komplexek: $x_1 = i$ és $x_2 = -i$.
4.2. Tétel. *$c \in K$ akkor és csak akkor gyöke $p \in K[x]$-nek, ha $\exists q \in K[x] : p = (x - c)\, q$.*
Például a fenti $p = 2x^2 - 3x + 1$-nek gyöke $c = 1$, és valóban: $p = (x - 1)(2x - 1)$.
4.3. Definíció. A fenti tételben az $x - c \in K[x]$ polinomot a c-hez tartozó *gyöktényezőnek* nevezzük.
Vagyis a fenti tételt úgy is megfogalmazhatjuk, hogy c akkor és csak akkor gyöke p-nek, ha p-ből kiemelhető a c-hez tartozó gyöktényező.
Érdemes foglalkozni azzal az esettel, ha a kiemelés után kapott q polinomnak is gyöke ugyanaz a c. Ekkor q-ból is kiemelhető a gyöktényező: $q = (x - c)\, r$, vagyis $p = (x - c)^2\, r$, tehát p-ből többször is kiemelhető $x - c$. Ekkor azt mondjuk, hogy c *többszörös gyöke* p-nek, egészen pontosan:
4.4. Definíció. $c \in K$ a $p \in K[x]$ polinom *k-szoros gyöke*, ha $\exists q \in K[x]$, hogy $p = (x - c)^k\, q$, de q-nak nem gyöke a c. Azt is mondjuk, hogy ekkor a c gyök *multiplicitása* k.
Vagyis c egy k-szoros gyök, ha pontosan k-szor emelhető ki az $x - c$ gyöktényező. Például a $p = 2x^3 - 3x^2 + 1$ polinomnak kétszeres gyöke a $c = 1$, mert $p = (x - 1)^2\,(2x + 1)$, de $2x + 1$-nek már nem gyöke az 1.
A gyöktényezők kiemelhetőségéből következik a következő tétel:
4.5. Tétel. *Ha K egy számhalmaz, akkor egy n-edfokú $p \in K[x] \setminus \{0\}$ polinomnak legfeljebb n gyöke lehet K-ban. Ez igaz úgy is, ha a gyökeket multiplicitással számoljuk, azaz a gyökök multiplicitásainak az összege is legfeljebb n.*
Tehát például egy harmadfokú polinomnak legfeljebb 3 gyöke lehet. Sőt, ha van egy kétszeres gyöke (mint például a fenti p esetén a $c = 1$), akkor azonkívül már csak egy gyöke lehet, mert a kétszeres gyök "kétszer számít".
(Bizonyítás: emeljünk ki annyi gyöktényezőt p-ből, amennyit csak lehet: $p = (x - c_1) \cdots (x - c_m)\, q$, ahol q-nak már nincs gyöke. Ekkor p-nek nem lehet más gyöke, mint $c_1, \ldots, c_m$, mert ha $p(c) = 0$, akkor valamelyik tényező 0, azaz vagy valamelyik $c_i = c$, vagy q-nak mégis lenne gyöke. Viszont minden kiemeléskor csökken a maradék fokszáma, ezért legfeljebb $n = \deg p$ gyöktényező lehet.)
(Megjegyzés: a tételben szereplő "ha K egy számhalmaz" feltételt egy későbbi jegyzetben fogjuk megmagyarázni és általánosítani.)
Néhány speciális eset:

- Elsőfokú polinomnak, azaz $p = ax + b$ alakú polinomnak csak egy gyöke lehet (és csak egyszeres): $x = -b/a$ (de $\mathbb{Z}$-ben ez az osztás nem mindig végezhető el).
- Nulladfokú polinomnak (azaz nemnulla konstans polinomnak) nincs gyöke.
- A nullpolinomnak viszont bármely $c \in K$ érték gyöke (ezért kellett ezt kizárni a tételből).

Korábban megismertük a polinomok kanonikus alakját. A gyöktényezők segítségével definiálhatunk egy másik fontos alakot:
4.6. Definíció. Egy $p \in K[x]$ polinom *gyöktényezős alakja* $p = a(x - c_1)(x - c_2) \cdots (x - c_m)$, ahol $a, c_1, \ldots, c_m \in K$ és $a \neq 0$.

Például a kanonikus alakban felírt $p = 2x^2 - 8x + 6$ polinom gyöktényezős alakja $p = 2(x-1)(x-3)$. Ennek az alaknak az a jelentősége, hogy leolvasható belőle a polinom összes gyöke, multiplicitással együtt. (És vegyük észre, hogy a konstans szorzó (a, itt 2) éppen a polinom főegyütthatója.)
Viszont gyöktényezős alak nem mindig létezik. Ehhez ugyanis az kell, hogy a polinomnak az alaphalmazban, K-ban pontosan n gyöke legyen (multiplicitással számolva), ahol n a fokszáma. A fenti tétel viszont csak azt garantálja, hogy *legfeljebb* n gyöke lehet. Ráadásul az, hogy hány gyöke van, függ az alaphalmaztól, K-tól. Például a $p = 16x^4 - 1$ polinomnak $\mathbb{Z}$-ben nincs gyöke, $\mathbb{R}$-ben két egyszeres gyöke van: $x_1 = 1/2$ és $x_2 = -1/2$, $\mathbb{C}$-ben pedig négy: $x_1 = 1/2$, $x_2 = -1/2$, $x_3 = i/2$, $x_4 = -i/2$; így tehát csak $\mathbb{C}$-ben van gyöktényezős alakja: $p = 16(x-1/2)(x+1/2)(x-i/2)(x+i/2)$.
A következő tétel azt mondja, hogy a komplex számok halmaza, $\mathbb{C}$ nemcsak a fenti példában, hanem általában is különleges:

4.7. Tétel (Az algebra alaptétele)**.** *Minden n-edfokú $p \in \mathbb{C}[x] \setminus \{0\}$ polinomnak – multiplicitással számolva – pontosan n gyöke van $\mathbb{C}$-ben.*

Ez tehát garantálja, hogy *bármely* $\mathbb{C}$ fölötti (nemnulla) polinomnak van gyöktényezős alakja.
Sage-ben egy polinom gyökeit a `roots()` tagfüggvénnyel kereshetjük meg:

```
sage: P.<x> = ZZ[]
sage: p = 16*x^4 - 1
sage: p.roots()
[]
sage: p.roots(QQ)          # megadhatunk egy bővebb alaphalmazt
[(1/2, 1), (-1/2, 1)]      # az 1-esek a multiplicitások
sage: p.roots(QQ, False)   # de azokat kikapcsolhatjuk
[1/2, -1/2]
sage: p.roots(CC)          # RR-ben és CC-ben csak közelítőleg lehet számolni
[(-0.5000000000, 1), (0.5000000000, 1), (-0.5000000000*I, 1), (0.5000000000*I, 1)]
```

5. Maradékos osztás

Ahogy az egész számok körében nem lehet általában osztani (pl. $2/3 \notin \mathbb{Z}$), úgy a polinomoknál sem (például $x/(x+1)$ nem polinom). Viszont ahogy az egész számoknál, úgy itt is bevezethetjük a *maradékos osztás* fogalmát. Egész számoknál ez a következő tételen alapul:

5.1. Tétel (Maradékos osztás tétele)**.** *Ha $a, b \in \mathbb{Z}$ és $b \neq 0$, akkor egyértelműen létezik olyan $q, r \in \mathbb{Z}$, hogy $a = qb + r$ és $0 \leq r < |b|$.*

A tételben szereplő q az osztás hányadosa, és r a maradék. Például ha $a = 36$ és $b = 10$, akkor $q = 3$ és $r = 6$, mert $36 = 3 \cdot 10 + 6$ és $0 \leq 6 < 10$.
Polinomokra is igaz egy nagyon hasonló tétel:

5.2. Tétel (Maradékos osztás tétele polinomokra)**.** *Ha $f, g \in \mathbb{R}[x]$ és $g \neq 0$, akkor egyértelműen létezik olyan $q, r \in \mathbb{R}[x]$, hogy $f = qg + r$ és $\deg r < \deg g$.*

Például ha $f = 2x^3 + x^2 - 2x - 1$ és $g = x^2 - 2x + 1$, akkor $q = 2x + 5$ és $r = 6x - 6$, mert $f = 2x^3 + x^2 - 2x - 1 = (2x+5)(x^2 - 2x + 1) + (6x - 6)$ és $\deg(6x-6) < \deg(x^2 - 2x + 1)$.

5.3. Definíció. A fenti tételben q az f és g *hányadospolinomja*, r pedig a *maradékpolinomjuk*.

Kézzel nagyon hasonlóan lehet polinomokat maradékosan osztani, mint egész számokat, csak nem a számjegyek helyiértéke szerint haladunk, hanem a tagok fokszáma szerint. Az f-ból kiindulva, minden lépésben levonjuk belőle g-nek azt a többszörösét, hogy a főegyüttható eltűnjön, ezáltal a maradék fokszáma kisebb legyen. Ezt addig folytatjuk, amíg a fokszám $\deg g$ alá nem csökken, és akkor megkaptuk a maradékot. A fenti példára ($f = 2x^3 + x^2 - 2x - 1$ és $g = x^2 - 2x + 1$):

$$\begin{aligned} f_0 &:= f &&= 2x^3 + x^2 - 2x - 1, \\ f_1 &:= f_0 - 2x \cdot g &&= 5x^2 - 4x - 1, \\ f_2 &:= f_1 - 5 \cdot g &&= 6x - 6, \end{aligned}$$

ahol $\deg f_2 < \deg g$, ezért készen vagyunk, és a maradék $r := f_2 = 6x - 6$, a hányadost pedig a g szorzóiból állíthatjuk össze: $q = 2x + 5$.

Sage-ben a maradékos osztás ugyanúgy működik, mint egészekre: `f // g`, `f % g` stb. (De a közönséges osztást, `f / g`-t kerüljük, mert annak az eredménye nem polinom típusú, még akkor sem, ha nincs maradék.)

Érdekes speciális eset, ha az osztó $g = x - c$ alakú, vagyis egy gyöktényező. Ekkor, mivel elsőfokú polinommal osztunk, ezért a maradék egy konstans polinom ($\deg r < \deg g = 1$). Ha c gyöke f-nek, akkor $f = (x - c)\,q$, tehát a maradék 0. Ha pedig nem gyöke, akkor a maradék nem más, mint $f(c)$, azaz f helyettesítési értéke c-ben. (Ez könnyen belátható, ha az $f = (x - c)\,q + r$ felírásba behelyettesítjük c-t.) Sőt, ha $f(c)$-t a Horner-módszerrel számítjuk ki (lásd fent), akkor azzal a q hányadospolinomot is automatikusan megkapjuk:

5.4. Tétel. *Ha $f \in \mathbb{R}[x]$ és $c \in \mathbb{R}$, akkor $f = a_n x^n + \ldots + a_1 x + a_0$ és $g := x - c$ maradékpolinomja az $f(c)$ konstans polinom, hányadospolinomjuk pedig $q = b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$, ahol a b_k együtthatókat a következő rekurzív szabállyal kapjuk meg: $b_{n-1} := a_n$ és $b_k := b_{k+1}c + a_{k+1}$.*

Vegyük észre, hogy ezek a b_k-k éppen a Horner-módszer fent leírt algoritmusában szereplő b változó menet közbeni értékei. Például ha $f = 2x^3 - 3x^2 - 4x + 7$ és $c = 2$, akkor a Horner-elrendezés szerint $f(c) = ((2c - 3)c - 4)c + 7$, azaz $b_2 = 2$ (f főegyüttthatója), $b_1 = b_2 c - 3 = 1$, $b_0 = b_1 c - 4 = -2$ és $b_{-1} = b_0 c + 7 = 3$, azaz $q = b_2 x^2 + b_1 x + b_0 = 2x^2 + x - 2$ és $r = f(c) = b_{-1} = 3$.

A Horner-módszert szokás táblázatos formában is felírni, ahol az első sorba írjuk f együtthatóit, a második sorba pedig kiszámítjuk a b_k-kat:

	2	−3	−4	7	$\longleftarrow\ f = 2x^3 - 3x^2 - 4x + 7$
$c = 2$	2	1	−2	3	$\longleftarrow\ q = 2x^2 + x - 2,\ \ f(c) = 3$

6. Legnagyobb közös osztó

Nemcsak a maradékos osztást, hanem számos további műveletet is át lehet vinni egész számokról polinomokra. Például:

6.1. Definíció. *$p \in K[x]$ osztója $q \in K[x]$-nek, ha $\exists r \in K[x] : q = pr$.* Jelölés: $p \mid q$.

Például a $p = x - 1$ polinom osztója a $q = 2x^2 - x - 1$ polinomnak, mert $q = (x-1)(2x+1) = p\,(2x+1)$.

Miért érdekes az oszthatóság polinomok esetén? Ezt a következő állítás világítja meg:

6.2. Tétel. *Ha $p \mid q$ és c gyöke p-nek, akkor c gyöke q-nak is, és legalább annyiszor, mint p-nek.*

Például a fenti $p = x - 1$-nek gyöke az 1, és valóban, q-nak is gyöke: $q(1) = 2 - 1 - 1 = 0$.

(A bizonyítás a gyöktényezők miatt nyilvánvaló, hiszen ha $x - c$ kiemelhető p-ből, akkor $q = pr$ miatt q-ból is. Megjegyzés: az "$x - c$ kiemelhető p-ből" helyett most már azt is írhatjuk, hogy $x - c \mid p$.)

Az oszthatóság könnyen eldönthető a maradékos osztás segítségével (akárcsak egészek esetén):

6.3. Tétel. $p \in \mathbb{R}[x] \setminus \{0\}$ *akkor és csak akkor osztója* $q \in \mathbb{R}[x]$*-nek, ha* q*-nak a* p*-vel vett osztási maradéka* 0*.*

(De vigyázat: a definíció szerint a nullpolinom osztója önmagának, pedig osztani nem lehet vele – ez hasonlít az egész számoknál a 0-hoz. Ezért van a tételben $\mathbb{R}[x] \setminus \{0\}$.)

Az osztók után a következő fogalom is adja magát:

6.4. Definíció. A $p \in K[x]$ és $q \in K[x]$ polinomok *legnagyobb közös osztója* egy olyan $r \in K[x]$, amelyre $r \mid p \ \wedge \ r \mid q \ \wedge \ \forall s \in K[x] : s \mid p \ \wedge \ s \mid q \implies s \mid r$. Jelölés: $\text{lnko}(p, q)$ (angolul: $\gcd(p, q)$). Továbbá p és q *relatív prím*, ha legnagyobb közös osztójuk 1.

Ez pontosan ugyanaz a definíció, mint egész számokra.

Például $p = x^2 - 2x + 1$ és $q = 2x^2 - x - 1$ legnagyobb közös osztója $r = x - 1$, amely onnan is látszik, hogy $p = (x - 1)^2$ és $q = (x - 1)(2x + 1)$.

De van egy probléma: a polinomoknál a legnagyobb közös osztó nem egyértelmű! Például a fenti p-nek és q-nak, ha $\mathbb{R}[x]$-ben nézzük, legnagyobb közös osztója az $r_1 = x - 1$, az $r_2 = -x + 1$, az $r_3 = 2x - 2$, az $r_4 = -x/2 + 1/2$ stb. (De ha $\mathbb{Z}[x]$-ben, akkor csak r_1 és r_2 az, mert ott $r_3 \nmid p$.)

Viszont könnyen belátható, hogy:

6.5. Tétel. *Ha* $p \in K[x]$ *és* $q \in K[x]$ *legnagyobb közös osztója* $r_1 \in K[x]$ *és* $r_2 \in K[x]$ *is, akkor* $\exists c \in K \setminus \{0\} : r_1 = c \cdot r_2$*.*

Vagyis a legnagyobb közös osztók mindig egymás konstansszorosai. (A fenti példában $r_1 = -r_2 = 1/2 \cdot r_3 = -2r_4$.) Tehát valójában nem akkora probléma, hogy több lnko is van, mert azok "lényegében" ugyanazok (pl. ugyanazok a gyökei). Ha egyértelműséget szeretnénk, akkor például kiköthetjük, hogy az lnko főegyütthatója 1 legyen. (Már ha ez lehetséges, pl. $\mathbb{Z}[x]$-ben nem biztos.)

Miért érdekes a polinomok legnagyobb közös osztója? Például ezért:

6.6. Tétel. *Ha* $p \in K[x]$ *és* $q \in K[x]$ *legnagyobb közös osztója* $r \in K[x]$*, akkor* r *gyökei pontosan a* p *és* q *közös gyökei, és* r*-beli multiplicitásuk a* p*-beli és a* q*-beli multiplicitások közül a kisebb.*

Például a fenti p egyetlen gyöke az 1 (de kétszeres); q gyökei 1 és $-1/2$ (egyszeresek); ezért $r = \text{lnko}(p, q)$-nak (vagy bármelyik r_i-nek) egyetlen gyöke van, az 1 (és az egyszeres).

Vagyis ha két polinom közös gyökeit szeretnénk meghatározni, akkor elég a legnagyobb közös osztójuk gyökeit kiszámítani. Ez azért jobb, mert az lnko fokszáma általában sokkal kisebb, mint az eredetieké, tehát könnyebb vele számolni; ha pedig 1, azaz a két polinom relatív prím, akkor rögtön tudjuk, hogy nincs közös gyökük.

De hogyan tudjuk a legnagyobb közös osztót kiszámítani? Ugyanúgy, mint egész számokra: az euklideszi algoritmussal (lásd a Legnagyobb közös osztó c. jegyzetet), amely polinomokra is pontosan ugyanúgy működik, hiszen azokat is lehet maradékosan osztani. Például $p = x^4 - 4x^3 + 1$ és $q = x^3 - 3x^2 + 1$ legnagyobb közös osztóját így tudjuk kiszámítani:

$$
\begin{aligned}
r_0 &:= p = x^4 - 4x^3 + 1, \\
r_1 &:= q = x^3 - 3x^2 + 1, \\
r_2 &:= r_0 \bmod r_1 = -3x^2 - x + 2, \\
r_3 &:= r_1 \bmod r_2 = 16/9 \cdot x - 11/9, \\
r_4 &:= r_2 \bmod r_3 = -27/256, \\
r_5 &:= r_3 \bmod r_4 = 0,
\end{aligned}
$$

vagyis $\text{lnko}(p,q) = -27/256$. De, mint láttuk, az lnko nem egyértelmű, és vehetjük bármely konstansszorosát is, például $\text{lnko}(p,q) = 1$ is igaz. (Általában, ha konstans az eredmény, akkor bármilyen más nemnulla konstans is jó.) Ez azt jelenti, hogy p és q relatív prímek, tehát nem lehet közös gyökük. Megjegyzés: mivel az eredményben úgysem számít a konstans szorzó, ezért akár menet közben is egyszerűsíthetjük a polinomokat egy-egy konstans szorzóval, pl. r_3 helyett számolhatunk az egyszerűbb $r_3' := 9r_3 = 16x - 11$ polinommal.

Nemcsak a normál euklideszi algoritmus, hanem a bővített verziója is alkalmazható polinomokra – pontosan ugyanúgy, mint egészekre (lásd megintcsak a Legnagyobb közös osztó c. jegyzetet). A bővített euklideszi algoritmus a következő polinomokat számítja ki:

6.7. Tétel (Bézout-lemma polinomokra)**.** *Ha $p \in \mathbb{R}[x]$ és $q \in \mathbb{R}[x]$ legnagyobb közös osztója $r \in \mathbb{R}[x]$, akkor létezik olyan $u, v \in \mathbb{R}[x]$, hogy $pu + qv = r$.*

Sage-ben polinomokra ugyanúgy működik a `gcd(p, q)` és az `xgcd(p, q)`, mint egészekre.

7. Algebrai derivált

Analízisből ismerjük a *derivált* fogalmát, amelynek polinomokra is hasznos tulajdonságai vannak. Itt azonban nem szeretnénk az analízis eszköztárát (pl. határérték, folytonosság) használni, bizonyos esetekben pedig nem is tudjuk (pl. $\mathbb{Z}$-ben nincs folytonosság). Ezért ahelyett, hogy levezetnénk a deriváltat analízisből, inkább egyszerűen csak definiáljuk:

7.1. Definíció. Egy $p = a_n x^n + \ldots + a_k x^k + \ldots + a_2 x^2 + a_1 x + a_0 \in K[x]$ polinom *algebrai deriváltja* a $p' = n a_n x^{n-1} + \ldots + k a_k x^{k-1} + \ldots + 2a_2 x + a_1$ polinom.

(Az "algrebrai" jelző arra utal, hogy analízis nélkül is működik.)

Például a $p = x^3 + 2x^2 - 3x + 5$ polinom deriváltja $p' = 3x^2 + 4x - 3$.

Sage-ben a polinom deriváltját a `p.diff()` tagfüggvénnyel számíthatjuk ki.

Az algebrai derivált (analízisből is ismert) tulajdonságai ($p, q \in K[x]$):

1. ha p konstans ($p \in K$), akkor $p' = 0$;
2. $x' = 1$;
3. $(p+q)' = p' + q'$;
4. $(p-q)' = p' - q'$;
5. $(c \cdot p)' = c \cdot p'$, ha c konstans ($c \in K$);
6. $(p \cdot q)' = p' \cdot q + p \cdot q'$;
7. $(p^n)' = n \cdot p' \cdot p^{n-1}$.

Mire jó a polinom deriváltja? Erre következő tétel választ ad:

7.2. Tétel. *Ha $c \in \mathbb{R}$ a $p \in \mathbb{R}[x]$-nek k-szoros gyöke ($k \geq 1$), akkor p'-nek $k-1$-szeres gyöke.*

Például $p = x^3 - 4x^2 - 3x + 18 = (x+2)(x-3)^2$-nek $c = 3$ kétszeres gyöke, $p' = 3x^2 - 8x - 3 = (x-3)(3x+1)$-nek pedig egyszeres. (Továbbá p-nek $c = -2$ egyszeres gyöke, p'-nek pedig nem gyöke, azaz "nullaszoros" gyöke.)

(Bizonyítás: a k-szoros gyök definíciója szerint $p = (x-c)^k q$, ahol q-nak nem gyöke a c. Ebből a deriválás fenti tulajdonságait használva levezethető, hogy $p' = (x-c)^{k-1}(kq + (x-c)q')$, tehát c *legalább* $k-1$-szeres gyöke p'-nek. Azt, hogy *pontosan* $k-1$-szeres gyöke, onnan tudjuk, hogy $kq + (x-c)q'$-nek nem lehet gyöke a c, hiszen q-nak sem gyöke.)

Persze p'-nek lehetnek új gyökei is, mint a fenti példában $c = -1/3$. Ha csak azokat a gyököket szeretnénk megtartani, amelyek p-ben is benne voltak, akkor vegyük a legnagyobb közös osztójukat:

7.3. Tétel. *Adott $p \in \mathbb{R}[x]$-nek $c \in \mathbb{R}$ akkor és csak akkor k-szoros gyöke ($k \geq 1$), ha $\operatorname{lnko}(p, p')$-nek $k-1$-szeres gyöke.*

(A különbség az előző tételhez képest az "akkor és csak akkor", tehát hogy más gyöke nem lehet.)

A fenti példát folytatva $\operatorname{lnko}(p, p') = x - 3$, amelynek $c = 3$ egyszeres gyöke, és más gyöke nincs.

Az $\operatorname{lnko}(p, p')$ ezen tulajdonsága több okból is hasznos:

1. Ha egy p polinomnak csak a többszörös gyökeire vagyunk kíváncsiak, akkor elég az $\operatorname{lnko}(p, p')$ gyökeit kiszámítani. Ez könnyebb, mert alacsonyabbfokú, mint p, és az lnko-t hatékonyan ki tudjuk számítani az euklideszi algoritmussal.
2. Speciális esetként, ha $\operatorname{lnko}(p, p')$ konstans, akkor rögtön tudjuk, hogy p-nek nem lehetnek többszörös gyökei, anélkül, hogy bármilyen gyököt ki kellett volna számítani.
3. A $p \,/\, \operatorname{lnko}(p, p')$ polinomnak (azért polinom, mert $\operatorname{lnko}(p, p') \mid p$) pontosan ugyanazok a gyökei, mint p-nek, csak mindegyik egyszeres (hiszen minden $(x-c)^k$-ból leosztottunk $(x-c)^{k-1}$-t). Ez azért hasznos, mert ha szeretnénk p gyökeit kiszámítani, akkor érdemes először leosztani $\operatorname{lnko}(p, p')$-vel, mert így a gyökök nem változnak, de csökkenthetjük a polinom fokszámát. Ezt az eljárást *négyzetmentesítés*nek nevezzük.

Korábban láttuk, hogy egy p polinom $p(c)$ helyettesítési értékét hogyan lehet hatékonyan kiszámítani a Horner-módszerrel. Ha szükségünk van a derivált helyettesítési értékére, $p'(c)$-re is, akkor azt nyilván kiszámíthatjuk ugyanígy p'-ből. Ehhez azonban szükségünk van a p' polinomra, amelynek kiszámítása további szorzásokat (és memóriát) igényel. De ezt megúszhatjuk: a Horner-módszer kiterjeszthető úgy, hogy a $p(c)$-vel együtt kiszámítsa $p'(c)$-t is, anélkül, hogy közben kiszámítaná a p' polinomot. Erre a következő tétel ad lehetőséget:

7.4. Tétel. *Ha $p \in K[x]$, $c \in K$ és p-nek az $x-c$-vel vett maradékos osztásának hányadosa $q \in K[x]$, azaz $p = (x-c)\,q + p(c)$, akkor $p'(c) = q(c)$.*

(Bizonyítás: $p' = ((x-c)\,q + p(c))' = q + (x-c)\,q'$, ebbe c-t helyettesítve kijön, hogy $p'(c) = q(c)$.)

Ez azért jó, mert a Horner-módszer automatikusan kiszámítja q-t (lásd a maradékos osztásnál), tehát abból egy újabb Horner-módszerrel kiszámíthatjuk $q(c)$-t, azaz $p'(c)$-t is. Ráadásul ezt a két lépést egyszerre is végezhetjük, azaz nem kell eltárolni a teljes q-t. (Ennek a műveletigénye összesen kb. $2n$ szorzás és $2n$ összeadás, míg a p' kiszámítása további n szorzást igényelne.)

Például $p = x^4 - 3x^3 + 6x + 3$ és $c = 2$ esetén a Horner-módszer két lépése így írható fel:

	1	-3	0	6	3	$\longleftarrow\ p = x^4 - 3x^3 + 6x + 3$
$c = 2$	1	-1	-2	2	7	$\longleftarrow\ q = x^3 - x^2 - 2x + 2,\ \ p(c) = 7$
$c = 2$	1	1	0	2		$\longleftarrow\ q(c) = p'(c) = 2$

8. Szerző

Ezt a jegyzetet Uray M. János írta, részben felhasználva Nagy Ádám jegyzetét:
https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa
Hibákat, észrevételeket itt lehet jelezni: uray.janos@inf.elte.hu.