Polinomok lnko-ja

Diszkrét modellek alkalmazásai

A korábbi jegyzetekben (Oszthatóság, prímszámok; Legnagyobb közös osztó) szó volt az egész számok osztásáról, oszthatóságáról, legnagyobb közös osztójáról és számos kapcsolódó tulajdonságairól. Ebben a jegyzetben ezeknek a fogalmaknak a megfelelőit fogjuk bevezetni polinomokra.

Sőt, ennél általánosabban, *gyűrűkre* fogjuk definiálni a fogalmakat – ezzel az absztakcióval egy csapásra intézzük el az egész számokat és a polinomokat, és lehetővé válik a más struktúrákra való kiterjesztés is. Egészen pontosan a gyűrűk egy speciális fajtáját, az *integritási tartományt* fogjuk alapul venni (lásd: Algebrai struktúrák). Emlékeztető: a legfontosabb integritási tartományok az egész számok halmaza ($\mathbb{Z}$), a polinomgyűrűk ($K[x]$, ahol K tetszőleges integritási tartomány) és bármely test (pl. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, vagy bármely p prímszámra $\mathbb{Z}_p$).

1. Oszthatóság

Először az egész számokra jól ismert oszthatóság ($b \mid a$) fogalmát fogjuk általánosítani:

1.1. Definíció. Egy R integritási tartományban $a \in R$ **osztható** $b \in R$-rel (azaz b **osztója** a-nak), ha $\exists c \in R : a = bc$. Jelölés: $b \mid a$.

Példa. $\mathbb{Z}$-ben $2 \mid 6$, mert $6 = 2 \cdot 3$.

Példa. $\mathbb{R}[x]$-ben $2x^2-x-1$ osztható $x-1$-gyel ($x-1 \mid 2x^2-x-1$), mert $2x^2-x-1 = (x-1)(2x+1)$.

Példa. Testben a fogalom triviális, mert minden elem osztható minden nemnull elemmel, hiszen mindig létezik $c := b/a$. Például $\mathbb{Q}$-ban 5 osztható 2-vel, mert $5 = 2 \cdot (5/2)$.

Az oszthatóság polinomok esetén azért érdekes, mert következtetni lehet belőle a gyökökre: ha $b \mid a$, akkor b minden gyöke egyúttal a-nak is gyöke (és legalább annyiszor, mint b-nek). Például $x-1$-nek gyöke az 1, és $x-1 \mid 2x^2-x-1$, ezért ebből tudjuk, hogy $2x^2-x-1$-nek is gyöke az 1.

Akárcsak egészek esetén, polinomokra is könnyen eldönthető az oszthatóság a maradékos osztás segítségével: ha $b \neq 0$, akkor $b \mid a \iff a \bmod b = 0$.

Az oszthatóság általános tárgyalásához szükségünk lesz néhány új fogalomra:

1.2. Definíció. Az R integritási tartományban $u \in R$ **egység** [*unit*], ha osztója az egységelemnek.

Példa. $\mathbb{Z}$-ben két egység van: 1 és -1 (az 1 osztói).

Példa. $\mathbb{R}[x]$-ben minden nulladfokú polinom (azaz nemnulla konstans polinom) egység.

Példa. Testben minden elem egység, kivéve a nullelemet.

Példa. Egy általános $K[x]$ polinomgyűrűben az egységek a K egységei (mint konstans polinomok), pl. $\mathbb{Z}[x]$-ben 1 és -1, $\mathbb{Q}[x]$-ben pedig az összes nemnulla konstans.

Fontos: ne keverjük össze az *egység* [*unit*] és az *egységelem* [*identity element*] fogalmát: egységelemből csak egy van, egységből viszont, mint láttuk, több is lehet.

(Vegyük észre, hogy az "egység" fogalma egybeesik az "invertálható" elem fogalmával, lásd: Algebrai struktúrák.)

Az oszthatósággal kapcsolatban szükségünk lesz egy másik fontos fogalomra:

1.3. Definíció. Az R integritási tartományban $a \in R$ és $b \in R$ **asszociáltak** [*associates*], ha egymás osztói: $a \mid b$ és $b \mid a$.

Példa. $\mathbb{Z}$-ben az asszociáltak az azonos abszolút értékű számok, pl. 5 és -5.

Példa. $\mathbb{R}[x]$-ben az asszociáltak az egymás nemnulla konstansszorosai, például a következők mind asszociáltak: $x-1$, $2x-2$, $3x-3$, $-x+1$, $-x/2+1/2$ stb.

Példa. Testben bármely két elem asszociált, kivéve a nullelemet.

Vegyük észre, hogy az asszociáltak mindig egymás egységszeresei, pl. $\mathbb{Z}$-ben $-5 = -1 \cdot 5$, $\mathbb{R}[x]$-ben $2x-2 = 2 \cdot (x-1)$ stb. Az asszociáltaknak az a jelentősége, hogy oszthatóság szempontjából pontosan ugyanúgy viselkednek, pl. $2 \mid 6 \implies 2 \mid -6,\ -2 \mid 6,\ -2 \mid -6$. Ezt úgy is megfogalmazhatjuk, hogy az asszociáltak "lényegében" ugyanazok.

2. Irreducibilis elemek

Most következzen a *prímszám* fogalmának általánosítása:

2.1. Definíció. Egy R integritási tartományban $a \in R$ **irreducibilis** elem (vagy **felbonthatatlan**), ha nem a nullelem, nem egység, és nincs más osztója, csak az egységek és a-nak az asszociáltjai.

A "nem a nullelem, nem egység" annak felel meg, hogy a prímszámoknál kizártuk a 0-t és az 1-et, a "csak az egységek és a-nak az asszociáltjai" pedig annak, hogy "csak 1 és n az osztója".

Hasonlóan általánosíthatjuk az *összetett szám* fogalmát is:

2.2. Definíció. Egy R integritási tartományban $a \in R$ **reducibilis** elem (vagy **felbontható**), ha nem a nullelem, nem egység, és nem is irreducibilis.

Példa. $\mathbb{Z}$ irreducibilis elemei a prímszámok és azok ellentettjei: $2, 3, 5, 7, \ldots,\ -2, -3, -5, -7, \ldots$. (A prímszámokat az egyszerűség kedvéért úgy definiáltuk, hogy pozitívak legyenek, azaz minden asszociált pár közül kiválasztottunk egy-egy kitüntetett elemet. Általánosan azonban nem tudunk ilyen szabály adni, ezért az irreducibilis elem fogalmába minden asszociáltat is beleértünk.)

Példa. Az x^2-2 polinom $\mathbb{Z}[x]$-ben irreducibilis, de $\mathbb{R}[x]$-ben reducibilis: $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$.

Példa. Testben nincs sem irreducibilis, sem reducibilis elem, mert minden elem nullelem vagy egység.

Megjegyzés: az irreducibilis elemek asszociáltjai is irreducibilisek.

Polinomgyűrűkben ($K[x]$) vizsgáljuk meg alaposabban is az irreducibilis polinomokat:

1. Test fölött minden elsőfokú polinom irreducibilis, hiszen $p = ax + b$ osztói csak konstans és elsőfokú polinomok lehetnek, az előbbiek egységek, az utóbbiak pedig p asszociáltjai.
2. Elsőnél magasabbfokú irreducibilis polinomnak nem lehet gyöke (az adott K alapgyűrűben), mert ha lenne, akkor kiemelhetnénk belőle egy gyöktényezőt, és akkor nem lenne irreducibilis.
3. $\mathbb{C}[x]$-ben *csak* az elsőfokú polinomok irreducibilisek, mert az algebra alaptétele miatt (Polinomok alapjai, 4.8. Tétel) minden nemkonstans polinomnak van gyöke.
4. $\mathbb{R}[x]$-ben csak az első- és másodfokú polinomok lehetnek irreducibilisek, pl. $2x+3$ és x^2+1 irreducibilisek $\mathbb{R}$ fölött. (De a másodfokúak nem mindig, pl. $x^2-1 = (x-1)(x+1)$.)
5. $\mathbb{Z}[x]$-ben és $\mathbb{Q}[x]$-ben viszont az irreducibilis polinomok fokszáma tetszőlegesen nagy lehet, pl. ott minden $x^n - 2$ alakú polinom irreducibilis.

Egész számok esetén a prímszámok jelentőségét a számelmélet alaptétele mutatta meg (Oszthatóság, prímszámok, 3.4. Tétel), amely a prímtényezős felbontás egyértelműségéről szólt. Ezt közvetlenül nem tudjuk általánosítani, mert nem minden integritási tartományra fog teljesülni, viszont külön kiemeljük azokat, amelyekre igen:

2.3. Definíció. Az R integritási tartomány **Gauss-gyűrű** [*unique factorization domain (UFD)*], ha a nullelem és az egységek kivételével minden elem egyértelműen felírható irreducibilis elemek szorzataként, ahol az egyértelműséget sorrendtől és asszociáltságtól eltekintve értjük.

Példa. $\mathbb{Z}$ a számelmélet alaptétele miatt Gauss-gyűrű. Például $-10 \in \mathbb{Z}$-t többféleképpen is fel lehet bontani: $-10 = (-2) \cdot 5 = 2 \cdot (-5) = 5 \cdot (-2) = (-5) \cdot 2$, de ezek mind csak sorrendben és asszociáltságban (azaz előjelban) térnek el, vagyis "lényegében" ugyanazok. (A számelmélet alaptételénél az asszociáltságról szóló kitételt megúsztuk, mert azt csak pozitív számokra mondtuk ki.)

Példa. Minden test triviálisan Gauss-gyűrű, hiszen nincs más elem, mint a nullelem és az egységek.

Példa. $\mathbb{R}[x]$ Gauss-gyűrű, pl. $x^2-1 = (x+1)(x-1) = (2x+2)(x/2-1/2) = (-3x+3)(-x/3-1/3)$ stb., de ezek mind csak sorrendben és asszociáltságban (azaz konstans szorzóban) térnek el egymástól.

Példa. Ha K Gauss-gyűrű, akkor $K[x]$ is Gauss-gyűrű, azaz $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}_5[x]$ stb. mind Gauss-gyűrű.

Sage-ben az egész számokra megismert `factor()` függvény tetszőleges Gauss-gyűrűre működik, a következő kiegészítéssel: az irreducibilis tényezőket úgy választja meg (az asszociáltak közül), hogy a lehető legegyszerűbbek legyenek (pl. $\mathbb{Z}$-ben pozitívak), viszont ha így nem jönne ki a szorzat (mert pl. negatív számot bontunk fel), akkor a szorzat elejére kiemel egy egységet (pl. -1). A `factor()` eredménye egy `Factorization` típusú objektum, amely sorozatként viselkedik (pl. egy `for`-ciklussal felsorolható), de az esetleges egység ebben nem szerepel, hanem azt külön kell lekérdezni a `unit()` tagfüggvénnyel. Például:

```
sage: F = factor(-60)
sage: F
-1 * 2^2 * 3 * 5
sage: for (p, k) in F:
....:     print(p, k)
2 2
3 1
5 1
sage: F.unit()
-1
sage: P.<x> = QQ[]
sage: F = factor(2*x^2 - 1/2)
sage: F
(2) * (x - 1/2) * (x + 1/2)
sage: [p for (p, k) in F]
[x - 1/2, x + 1/2]
sage: F.unit()
2
```

3. Legnagyobb közös osztó

Most kiterjesztjük a legnagyobb közös osztó és a legkisebb közös többszörös fogalmát (lásd a Legnagyobb közös osztó c. jegyzetet) egészekről tetszőleges integritási tartományra:

3.1. Definíció. Az R integritási tartományban $a \in R$ és $b \in R$ **legnagyobb közös osztója** $c \in R$, ha $c \mid a \ \wedge \ c \mid b \ \wedge \ \forall d \in R : d \mid a \ \wedge \ d \mid b \implies d \mid c$. Jelölés: $\mathrm{lnko}(a, b)$ vagy $\gcd(a, b)$.
Továbbá a és b **relatív prím**, ha legnagyobb közös osztójuk egység.

3.2. Definíció. Az R integr. tartományban $a \in R$ és $b \in R$ **legkisebb közös többszöröse** $c \in R$, ha $a \mid c \ \wedge \ b \mid c \ \wedge \ \forall d \in R : a \mid d \ \wedge \ b \mid d \implies c \mid d$. Jelölés: $\mathrm{lkkt}(a, b)$ vagy $\mathrm{lcm}(a, b)$.

Példa. $\mathbb{Z}$-ben 12 és 20 legnagyobb közös osztója 4, legkisebb közös többszöröse 60.

Példa. $\mathbb{R}[x]$-ben a $p = x^2 - 2x + 1 = (x-1)^2$ és a $q = 2x^2 - x - 1 = (x-1)(2x+1)$ polinomok legnagyobb közös osztója $x - 1$, legkisebb közös többszöröse pedig $(x-1)^2(2x+1) = 2x^3 - 3x^2 + 1$.

De ezekkel a fogalmakkal ilyen általánosan van néhány probléma. Például nem biztos, hogy léteznek. Szerencsére azonban a számunkra fontos speciális esetekben garantálható a létezés:

3.3. Tétel. *Gauss-gyűrűben bármely két elemnek van legnagyobb közös osztója és legkisebb közös többszöröse.*

Tehát $\mathbb{Z}$-ben, $\mathbb{Z}[x]$-ben, $\mathbb{R}[x]$-ben stb. mindig létezik lnko és lkkt. (A tétel nem meglepő, gondoljunk csak arra, hogy $\mathbb{Z}$-ben hogyan lehet ezeket kiszámítani a prímtényezős felbontás segítségével.)

De van egy másik probléma is: az lnko és az lkkt nem egyértelmű!

Példa. $\mathbb{Z}$-ben $\mathrm{lnko}(6, 4)$ fenti definícióját kielégíti 2 és -2 is. Az eredeti, $\mathbb{Z}$-beli definícióban is csak azért volt egyértelműség, mert ott kikötöttük, hogy az eredménynek $\mathbb{N}$-ben kell lennie.

Példa. A fenti $p = x^2 - 2x + 1$ és $q = 2x^2 - x - 1$ polinomoknak, 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 nézzük, akkor csak r_1 és r_2 az, mert ott $r_3 \nmid p$ és $r_4 \notin \mathbb{Z}[x]$.)

Ha teljes egyértelműség nem is, de "bizonyos értelemben" való egyértelműség fennáll:

3.4. Tétel. *A legnagyobb közös osztó és a legkisebb közös többszörös, ha létezik, asszociáltságtól eltekintve egyértelmű.*

Példa. $\mathbb{Z}$-ben az lnko *előjeltől eltekintve* egyértelmű: $\mathrm{lnko}(6, 4)$ lehet 2 és -2 is, de más nem. Ha pedig leszűkítjük $\mathbb{N}$-re, akkor teljesen egyértelmű lesz.

Példa. $\mathbb{R}[x]$-beli polinomoknál az lnko *konstans szorzótól eltekintve* egyértelmű: a fenti példában $r_1 = -r_2 = 1/2 \cdot r_3 = -2r_4$. A teljes egyértelműséghez pedig például kiköthetjük, hogy a főegyüttható 1 legyen (pl. akkor $r_1 = x - 1$ az "igazi" lnko). (De $\mathbb{Z}[x]$-ben ez nem mindig működik.)

A következő tétel rámutat arra, hogy miért érdemes a polinomok lnko-jával foglalkozni:

3.5. 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 multiplicitásaik közül a kisebb.*

Példa. A fenti $p = x^2 - 2x + 1$ egyetlen gyöke az 1 (de kétszeres); $q = 2x^2 - x - 1$ gyökei 1 és $-1/2$ (egyszeresek); ezért $r = \mathrm{lnko}(p, q)$-nak (vagy bármelyik r_i-nek) egyetlen gyöke az 1 (és az egyszeres).

Vagyis ha két polinom közös gyökeit szeretnénk meghatározni, akkor elég csak az lnko-juk gyökeit kiszámítani, amely általában alacsonyabbfokú, mint az eredetiek, ezért könnyebb vele számolni; ha pedig konstans, azaz a két polinom relatív prím, akkor rögtön tudjuk, hogy nem lehet közös gyökük.

4. Euklideszi algoritmus

A Legnagyobb közös osztó c. jegyzetben megismertük az euklideszi algoritmust, amellyel egész számok lnko-ját lehet kiszámítani. Az algoritmust egy az egyben alkalmazhatjuk polinomokra is, hiszen azokat is lehet maradékosan osztani (lásd a Polinomműveletek c. jegyzetet).

Példa. Az euklideszi algoritmus a $p = 2x^3 + x^2 - 2x - 1$ és a $q = x^2 - 2x + 1$ polinomokra így néz ki:

$$\begin{aligned} r_0 &:= p && = 2x^3 + x^2 - 2x - 1, \\ r_1 &:= q && = x^2 - 2x + 1, \\ r_2 &:= r_0 \bmod r_1 && = 6x - 6, \\ r_3 &:= r_1 \bmod r_2 && = 0, \end{aligned}$$

vagyis $\text{lnko}(p, q) = r_2 = 6x - 6$. De ez nem az egyetlen helyes megoldás, hiszen fent láttuk, hogy a legnagyobb közös osztó nem egyértelmű. Vehetjük tehát a fenti eredmény bármely konstansszorosát is, pl. $\text{lnko}(p, q) = -2r_2 = -12x + 12$ és $\text{lnko}(p, q) = \frac{1}{6}r_2 = x - 1$ is ugyanúgy helyes megoldás.

Példa. Hajtsuk végre az euklideszi algoritmust a $p = x^4 - 4x^3 + 1$ és a $q = x^3 - 3x^2 + 1$ polinomokra:

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

vagyis $\text{lnko}(p, q) = r_4 = -27/256$, vagy ennek bármely konstansszorosa, pl. $\text{lnko}(p, q) = 256r_4 = -27$ vagy $\text{lnko}(p, q) = -256/27 \cdot r_4 = 1$ is jó. Általában, ha konstans az eredmény, akkor bármilyen más nemnulla konstans polinom is jó lehet, és ekkor p és q relatív prím (tehát nem lehet közös gyökük). Megjegyzés: mivel az eredményben úgysem számít a konstans szorzó, ezért akár menet közben is egyszerűsíthetjük a polinomokat egy-egy megfelelően választott konstanssal való szorzással, pl. r_3 helyett számolhatunk az egyszerűbb $\tilde{r}_3 := 9r_3 = 16x - 11$ polinommal, és így tovább.

Fontos: az euklideszi algoritmus általában csak *test* fölötti polinomokra működik, pl. $\mathbb{R}[x]$-ben vagy $\mathbb{Q}[x]$-ben, de nem $\mathbb{Z}[x]$-ben, mert törtekkel kell számolni (ahogy az utolsó példában is). Ez annak ellenére igaz, hogy maga a legnagyobb közös osztó $\mathbb{Z}[x]$-ben is létezik, mint a fenti példában $\text{lnko}(p, q) = 1 \in \mathbb{Z}[x]$ – de ehhez először $\mathbb{Q}[x]$-ben kellett kiszámítani egy másik lnko-t: $-27/256$.

Nemcsak a normál euklideszi algoritmus, hanem annak bővített verziója is működik polinomokra, és az is pontosan ugyanúgy, mint egészekre (lásd a Legnagyobb közös osztó c. jegyzetet):

Példa. A fenti $p = 2x^3 + x^2 - 2x - 1$ és $q = x^2 - 2x + 1$ esetén a bővített euklideszi algoritmus a következőképpen működik:

$2x^3 + x^2 - 2x - 1$	1	0	
$x^2 - 2x + 1$	0	1	$(-(2x + 5))$
$6x - 6$	1	$-2x - 5$	$(-(\frac{1}{6}x - \frac{1}{6}))$
0	$-\frac{1}{6}x + \frac{1}{6}$	$\frac{1}{3}x^2 + \frac{1}{2}x + \frac{1}{6}$	

Tehát $\text{lnko}(p, q) = 6x - 6 = p \cdot 1 + q \cdot (-2x - 5)$. Vagy ezt is megszorozhatjuk bármilyen konstanssal, pl. $\text{lnko}(p, q) = x - 1 = p \cdot \frac{1}{6} + q \cdot (-\frac{1}{3}x - \frac{5}{6})$ is igaz.

A bővített euklideszi algoritmus polinomokra a következő tételen alapul:

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

Megjegyzés: itt is fontos, hogy a polinomok test fölött legyenek. Például ha a fenti példát $\mathbb{Z}[x]$-ben nézzük, akkor hiába $\text{lnko}(p, q) = x - 1 \in \mathbb{Z}[x]$, de a $pu + qv = x - 1$ egyenletnek nincs $\mathbb{Z}[x]$-ben megoldása u-ra és v-re, csak $\mathbb{Q}[x]$-ben.

Sage-ben polinomokra ugyanúgy működik a `gcd(p, q)` és az `xgcd(p, q)`, mint egészekre (azt leszámítva, hogy itt `gcd(p, q)` nem az egyetlen helyes megoldás, hiszen az lnko nem egyértelmű):

```
sage: P.<x> = QQ[]
sage: p = 2*x^3 + x^2 - 2*x - 1
sage: q = x^2 - 2*x + 1
sage: gcd(p, q)
x - 1
sage: xgcd(p, q)
(x - 1, 1/6, -1/3*x - 5/6)
sage: p * _[1] + q * _[2]   # ellenőrzés
x - 1
```

Az euklideszi algoritmust nemcsak egészekre és polinomokra lehet definiálni, hanem általánosabban is. Ehhez általánosítani kell a maradékos osztás műveletét, amelyen az algoritmus alapul.

A probléma az, hogy ez a művelet nem minden integritási tartományban működik. Például $\mathbb{Z}[x]$ integritási tartomány (sőt, Gauss-gyűrű, tehát létezik lnko), de láttuk, hogy a maradékos osztás csak test fölötti polinomokra működik, pl. $\mathbb{Q}[x]$-ben. Így tehát szűkítenünk kell azon gyűrűk körét, amelyekben a maradékos osztásnak van értelme, és ahol így az euklideszi algoritmus is elvégezhető. Ezeket fogjuk alább *euklideszi gyűrű*nek nevezni.

Ha összehasonlítjuk a maradékos osztás tételét egész számokra (Osztók és prímszámok, 1.1. Tétel) és polinomokra (Polinomműveletek, 3.1. Tétel), akkor a fő különbség az, hogy hogyan definiáltuk, hogy a maradék "kisebb" legyen, mint az osztó: a polinomoknál erre a fokszámot használtuk, az egészeknél pedig az abszolút értéket. Ez a "kisebb" fogalom kulcsfontosságú, mivel ez garantálja, hogy az euklideszi algoritmus előbb-utóbb megálljon, hiszen így minden maradékszámítás után "kisebb" elemet kapunk, tehát előbb-utóbb el kell jutnunk a 0-ba. Ezt a "kisebb" fogalmat általánosan egy f függvénnyel fogjuk leírni, amely a gyűrű elemeihez hozzárendel egy-egy természetes számot.

4.2. Definíció. Az R integritási tartomány **euklideszi gyűrű** [*Euclidean domain*], ha van olyan $f : R \setminus \{0\} \to \mathbb{N}$ függvény, amelyre a következők teljesülnek:

1. $\forall a, b \in R \setminus \{0\} : f(a) \leq f(ab)$,
2. $\forall a, b \in R, b \neq 0 : \exists q, r \in R : a = qb + r \ \wedge \ (r = 0 \ \vee \ f(r) < f(b))$.

Példa. $\mathbb{Z}$ euklideszi gyűrű, például legyen $f(a) := |a|$.

Példa. $K[x]$ euklideszi gyűrű bármely K testre, például $f(a) := \deg a$. (Megjegyzés: a definícióban külön kezeltük a 0-t, így nincs probléma a nullpolinom fokszámával.)

Példa. Minden test triviálisan euklideszi gyűrű, hiszen ott minden elem osztható minden nemnulla elemmel, tehát a maradékos osztáskor mindig $r = 0$, és így az f függvénynek nincs is szerepe (például lehet mindig $f(a) := 1$).

4.3. Tétel. *Minden euklideszi gyűrű egyúttal Gauss-gyűrű is.*

(De ez fordítva nem igaz, például a fent említett $\mathbb{Z}[x]$ Gauss-gyűrű, de nem euklideszi gyűrű.)

(Megjegyzés: az euklideszi gyűrű definíciója nem várja el, hogy r és q egyértelmű legyen. Például egész számokra $b = 10$ esetén csak annyit mond, hogy $|r| < 10$, azaz $-9 \leq r \leq 9$, ami megenged többféle lehetőséget is, például $a = 36 = 3 \cdot 10 + 6 = 4 \cdot 10 + (-4)$. Ahhoz, hogy a maradékos osztás egyértelmű legyen, a gyűrűtől függően további feltételekre lehet szükség, mint például egészeknél $r \geq 0$ – amit a maradékos osztás tétele ki is kötött. Polinomoknál viszont nincs szükség további feltételre, mert ott $\deg r < \deg b$ elegendő az egyértelműséghez.)

5. Négyzetmentesítés

5.1. Definíció. Egy R integritási tartományban $a \in R$ **négyzetmentes** [*square-free*], ha nincs olyan $b \in R$, amely nem egység, és $b^2 \mid a$.

Példa. $\mathbb{Z}$-ben 10 négyzetmentes, mert nincs négyzetszám osztója az 1-en kívül. Nem négyzetmentes viszont a 24, mert $2^2 \mid 24$. Általában $\mathbb{Z}$-ben azok a számok négyzetmentesek, amelyeknek nincs többszörös prímfaktoruk (pl. $10 = 2 \cdot 5$, de $24 = 2^3 \cdot 3$).

Példa. $\mathbb{R}[x]$-ben $x^2 + x - 2 = (x-1)(x+2)$ négyzetmentes, mert a konstanson kívül más polinom négyzete nem osztja, de $x^3 - 4x^2 - 3x + 18 = (x+2)(x-3)^2$ nem négyzetmentes, mert $(x-3)^2 \mid p$.

A négyzetmentes polinomoknak az a jelentősége, hogy mivel nincsenek többszörös *faktorai*, ezért nem lehetnek többszörös *gyökei* sem (lásd a gyöktényezőket a Polinomok alapjai c. jegyzetben).

(Ez azonban fordítva nem igaz: attól, hogy nem négyzetmentes, még nem biztos, hogy van többszörös gyöke, pl. $(x^2+1)^2(x-1) \in \mathbb{R}[x]$-nek van többszörös *faktora*, de nincs többszörös *gyöke*, mert az (x^2+1)-nek nincs valós gyöke.)

Az alábbiakban azzal foglalkozunk, hogy hogyan lehet egy polinom többszörös faktorait – és így a többszörös gyökeit is – kiszűrni, pontosabban egyszeressé alakítani. Ezáltal csökkenthetjük a polinom fokszámát anélkül, hogy a "lényegét", azaz például a gyökeit megváltoztatnánk. Ez az eljárás, a *négyzetmentesítés* számos összetett polinomalgoritmus (pl. gyökkeresés, faktorizáció) első lépése szokott lenni. (Ráadásul egyes gyökkereső algoritmusok kifejezetten rosszul viselkednek többszörös gyökök esetén, ezért ott különösen fontos azokat "kisimítani", azaz egyszeressé alakítani.)

A négyzetmentesítéshez kulcsfontosságú eszköz lesz a polinom *algebrai deriváltja* (lásd az előző jegyzetet). Hogy miért, azt a következő tétel világítja meg:

5.2. Tétel. *Ha $p \in K[x]$-nek $r \in K[x]$ egy k-szoros faktora ($k \geq 1$), azaz $p = r^k q$, de $r \nmid q$, akkor p'-nek ugyanez az r egy $k-1$-szeres faktora. Speciálisan, ha $r = x - c$, akkor ha c a p-nek egy k-szoros gyöke, akkor p'-nek ugyanez a c egy $k-1$-szeres gyöke.*

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

(Bizonyítás: számítsuk ki $p = r^k q$ deriváltját, felhasználva a derivált előző jegyzetben szereplő tulajdonságait:

$$p' = (r^k q)' = (r^k)' q + r^k q' = k r^{k-1} q + r^k q' = r^{k-1}(kq + rq'),$$

tehát p'-nek r *legalább* $k-1$-szeres faktora. Hogy *pontosan* $k-1$-szeres, az abból jön ki, hogy $r \nmid kq + rq'$, mert $r \nmid q$.)

Tehát p' megőrzi p *többszörös* gyökeit (faktorait), eggyel alacsonyabb multiplicitással. A probléma az, hogy p'-nek lehetnek új gyökei (faktorai) is (pl. fent $c = -1/3$). Ezeket azonban könnyen kiszűrhetjük, ha vesszük $\operatorname{lnko}(p, p')$-t, amely már *kizárólag* p többszörös gyökeit (faktorait) tartalmazza.

Példa. A fenti példát folytatva $\operatorname{lnko}(p, p') = x - 3$, amelynek $c = 3$ egyszeres gyöke, és más gyöke nincs. Ez tisztán jelzi, hogy p-nek egyetlen többszörös gyöke van: $c = 3$.

Megjegyzés: ha $\operatorname{lnko}(p, p')$ konstans, akkor ebből rögtön tudjuk, hogy p négyzetmentes.

Ha pedig leosztjuk a polinomot $\operatorname{lnko}(p, p')$-vel: $p \,/\, \operatorname{lnko}(p, p')$ (amely szintén polinom, hiszen $\operatorname{lnko}(p, p') \mid p$), akkor ennek pontosan ugyanazok a gyökei (faktorai), mint p-nek, csak mindegyik egyszeres (hiszen minden r^k-ból leosztottunk r^{k-1}-t). Így tehát négyzetmentesítettük a p polinomot.

Példa. A fenti példából $p = (x+2)(x-3)^2$ négyzetmentes változata $p \,/\, \operatorname{lnko}(p, p') = (x+2)(x-3)$.

Megjegyzés: a négyzetmentesítés számpolinomokra (pl. $\mathbb{R}[x]$-ben) tökéletesen működik, de más struktúrákban, pl. $\mathbb{Z}_m[x]$-ben problémákba ütközhet (még akkor is, ha $\mathbb{Z}_m$ test). Például (az előző jegyzetből) $p = x^6 + x^3 + \overline{1} \in \mathbb{Z}_3[x]$ deriváltja eltűnik: $p' = \overline{0}$. Ez azért baj, mert ilyenkor $v = p \,/\, \operatorname{lnko}(p, p') = p/p = 1$, vagyis nem tudjuk kiszűrni a többszörös gyököket. Pedig lenne mit kiszűrni: $p = x^6 + x^3 + \overline{1} = (x - \overline{1})^6$, azaz van egy hatszoros gyöke, $c = \overline{1}$.

Folytatva a fenti lépéseket, legyen $u := \text{lnko}(p, p')$ és $v := p/u = p \,/\, \text{lnko}(p, p')$, és tekintsük a $w := \text{lnko}(u, v)$ polinomot: ez (az u-hoz hasonlóan) éppen a p polinom többszörös gyökeit (faktorait) tartalmazza, de (v-hez hasonlóan) mindegyiket csak egyszer. Ezeket "kioszthatjuk" a polinomból: a v/w polinom immár *kizárólag* p egyszeres gyökeit (faktorait) tartalmazza.
Példa. Ha $p = (x-4)(x-5)(x-6)^2(x-7)^4$, akkor ebből $u = \text{lnko}(p, p') = (x-6)(x-7)^3$, $v = p/u = (x-4)(x-5)(x-6)(x-7)$, $w = \text{lnko}(u, v) = (x-6)(x-7)$ és $v/w = (x-4)(x-5)$.

Ezt a számítást továbbfejlesztve nemcsak az egyszeres, hanem a kétszeres, háromszoros stb. gyököket (faktorokat) is különválogathatjuk. Például a kétszeres faktorokat úgy kaphatjuk meg, hogy a fenti u-nak – amelyben minden multiplicitás eggyel alacsonyabb, mint p-ben – kiszámítjuk az egyszeres faktorait. Ezt megfelelően folytatva eljuthatunk a következő felbontásig:

5.3. Definíció. Egy $p \in K[x]$ polinom **négyzetmentes felbontása**

$$p = a_1 a_2^2 a_3^3 \cdots a_m^m,$$

ahol minden $a_i \in K[x]$ négyzetmentes, és páronként relatív prímek (azaz $\text{lnko}(a_i, a_j)$ konstans).

Négyzetmentes faktorizáció:

Bemenet: $p \in \mathbb{R}[x]$
Kimenet: $a_1, a_2, \ldots, a_i \in \mathbb{R}[x]$
$u := \text{lnko}(p, p')$
$v := p/u$
$i := 1$
ciklus amíg u *nem konstans*
  $w := \text{lnko}(u, v)$
  $a_i := v/w$
  $i := i + 1$
  $u := u/w$
  $v := w$
$a_i := v$
$a_1 := a_1 \cdot u$

Példa. Ha $p = (x-4)(x-5)(x-6)^2(x-7)^4$, akkor az algoritmus a következő polinomokat számítja ki:

Ciklus előtt: $u = (x-6)(x-7)^3$, $v = (x-4)(x-5)(x-6)(x-7)$.
1. ciklus: $w = (x-6)(x-7)$, $a_1 = (x-4)(x-5)$, $u = (x-7)^2$, $v = (x-6)(x-7)$.
2. ciklus: $w = (x-7)$, $a_2 = (x-6)$, $u = (x-7)$, $v = (x-7)$.
3. ciklus: $w = (x-7)$, $a_3 = 1$, $u = 1$, $v = (x-7)$.
Ciklus után: $a_4 = (x-7)$.

$$a_1 = (x-4)(x-5),\ a_2 = (x-6),\ a_3 = 1,\ a_4 = (x-7),$$
$$p = a_1 a_2^2 a_3^3 a_4^4 = \big((x-4)(x-5)\big)(x-6)^2 1^3 (x-7)^4.$$

Megjegyzés: mivel a polinomok lnko-ja nem egyértelmű, ezért a fenti algoritmus sem ad egyértelmű négyzetmentes felbontást, csak asszociáltságtól eltekintve (minden a_i-ra külön-külön). Viszont az eredményből minden esetben pontosan vissza tudjuk állítani a polinomot (ezt biztosítja az utolsó lépésben a fennmaradó u konstanssal való szorzás).

A négyzetmentes felbontást sokkal hatékonyabb előállítani, mint a polinom teljes faktorizációját. Ez jól jön például a racionális törtfüggvények (azaz polinomok hányadosának) integrálásakor (lásd: Analízis), ahol általános esetben a nevezőnek éppen a négyzetmentes felbontására van szükség.

6. Szerző

Ezt a jegyzetet Uray M. János írta, részben felhasználva az alábbi forrásokat:

[1] https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa
[2] https://en.wikipedia.org/wiki/Polynomial_greatest_common_divisor
[3] H. Cohen (1996): A Course in Computational Algebraic Number Theory (chapter 3).
[4] K.O. Geddes, S.R. Czapor, G. Labahn (1992): Algorithms for Computer Algebra (chapters 2, 7 and 8).

Hibákat, észrevételeket itt lehet jelezni: uray.janos@inf.elte.hu.