Diszkrét matematika II
Polinomok témakör jegyzete

Készült Burcsi Péter előadásai
és Harrison-Juhász Zsófia gyakorlatai alapján

Sárközi Gergő, 2021-22-1. félév
Nincsen lektorálva!

Tartalomjegyzék

1. Gyűrű, Test, integritási tartomány

1.1. Gyűrű $(R, +, *)$

- Példa: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_m$ (mod m maradékosztályok gyűrűje)
- $+$: R-en művelet
  - asszociatív, kommutatív
  - létezik nullelem: 0 $(a + 0 = 0 + a = a)$
  - minden elemnek van inverze $(a - a = 0)$
- $*$: R-en művelet
  - asszociatív
  - nem feltétlenül kommutatív (pl. mátrixok miatt: ott nem azok)
- $*, +$: $*$ disztributív $+$-ra: $x * (y + z) = x * y + x * z$

1.2. Integritási tartomány

- Példa: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ ahol p egy prím
- Egy R gyűrű integritási tartomány, ha:
  - legalább 2 eleme van
  - szorzás kommutatív
  - gyűrű (szorzás) nullosztómentes $(a * b = 0 \implies a = 0 \vee b = 0)$
    - ellenpélda: $\mathbb{Z}_{10}$: $6 * 5 = 0$

1.3. Egységelemes Integritási Tartomány (EIT)

- Integritási tartomány, ahol létezik $1 \in R$: $a * 1 = 1 * a = a$
- Van $+, *, -$: ahogy megszoktuk, pl.: $ax = ay \implies a = 0 \vee x = y$

1.4. Test

- Gyakorlatilag: egy E.I.T. ahol van osztás
- $\forall a \in R : a \neq 0 \implies \exists a^{-1} : a * a^{-1} = 1$
- pl.: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_p$ ahol p prím
- Minden f polinom eloszthető maradékosan bármely $g \neq 0$ polinommal

2. Polinom

- Egy R gyűrű feletti polinomokon olyan $(f_0, f_1, f_2, ...)$ végtelen sorozatokat értünk, ahol $f_j \in R$ és $\exists n \in \mathbb{N} : j > n \implies f_j = 0$
- Példa: $6 + 5x + 2x^2 + 3x^4 \to (6, 5, 2, 0, 3, 0, 0, 0, ...)$
- R feletti polinomok halmaza: $R[x]$ (x: polinomok határozatlanja)
  - Ha R E.I.T., akkor $R[x]$ is E.I.T.
- Polinomfüggvény: $f \in R \to R$, $f(r) = f_0 + f_1 * r + ... + f_{deg(f)} * r^{deg(f)}$

2.1. Polinom foka

- polinom foka ($\deg f$): legnagyobb n amelyre $f_n \neq 0$
  - a fok $-\infty$, ha $f = (0, 0, 0, ...)$
- főegyüttható: f_n ahol $n = \deg f$
- konstans tag: f_0
- f lineáris, ha $\deg f \leq 1$
- f konstants, ha $\deg f \leq 0$

2.2. Összeadás, szorzás $R[x]$-en

- $f = (f_0, f_1, f_2, ...)$ és $g = (g_0, g_1, ...)$
- $f + g = (f_0 + g_0, f_1 + g_1, ...)$
  - $deg(f + g) \leq max(deg(f),\ deg(g))$
- $f * g = h$ ahol: $h_k = \sum_{i+j=k} f_i * g_j$
  - Példa: $f = (2, 0, 1, 3, 0, ...)$ és $g = (7, -2, 3, 0, ...)$
    $f * g = (?, 2*3+0*-2+1*7, ...) = (?, f_0 * g_2 + f_1 * g_1 + f_2 * g_0, ...)$
  - $\deg(f * g) \leq \deg(f) + \deg(g)$
    - egyenlő, ha R egy integritási tartomány: $f_{\deg(f)} * g_{\deg(g)} \neq 0$

2.3. Maradékos osztás tétele

- Legyen R egy E.I.T. és $f, g \in R[x]$ és $n = \deg f$ és $m = \deg g$
- Ha $\exists {g_m}^{-1}$ (van reciproka a főegyüttható nak)
- Akkor $\exists! g, r \in R[x] : f = g * q + r \wedge \deg r < \deg g$
- Egyértelműség bizonyítása:
  - Legyen $f = g * q_1 + r_1 = g * q_2 + r_2$
  - Ebből következik: $g * (q_1 - q_2) = r_2 - r_1$
  - Fokokra áttérve: $\deg g + \deg(q_1 - q_2) = \deg(r_2 - r_1)$
  - Ha $q_1 \neq q_2$: a bal oldal $\geq \deg g$, a jobb oldal $< \deg g$
  - Tehát $(q_1 = q_2) \implies (g * 0 = 0) \implies (r_r - r_2 = 0)$
- Létezés bizonyítása:
  - $q = f_n * g_m^{-1} * x^{n-m} + q^*$ (ahol q^* ugyan ez f^*-gal)
  - $f^* = f - g * f_n * g_m^{-1} * x^{n-m} = g * q^* + r^*$
  - Rekurzió alapesete: ha $\deg f < \deg g$ akkor $q = 0$ és $r = f$
  - f fokszáma csökken, $\deg f^* < \deg f$ belátása:
    $f_n^* = f_n * x^n - g * f_n * g_m^{-1} * x^{n-m} = f_n * x^n - f_n * x^n = 0$

2.4. Polinom osztás a gyakorlatban

2.4.1. Bizonyításhoz hasonlóan, rekurzívan

- rekurzívan f-ből mindig kivonjuk $g * f_n * g_m^{-1} * x^{n-m}$-ot
- megállunk, ha $\deg f < \deg g$, ekkor $r = f$
- $q = \sum f_n * g_m^{-1} * x^{n-m}$

2.4.2. Horner táblázat

- $f = (x - c) * q + r$ ahol $\deg r \leq 0$ (azaz $g = x - c$ és $\deg g = 1$)

	f_n	f_{n-1}	f_{n-2}	...	f_0	
c	$\times$	$c_1 = f_n$	$c_2 = c_1 * c + f_{n-1}$	..	$c_n = c_{n-1} * c + f_1$	$c_{n+1} = ... = f(c)$

3. Gyöktényező kiemelése, következményei

3.1. Gyöktényező kiemelése

- Ha R egy E.I.T. és $f \in R[x]$ és $f(c) = 0$
- Akkor $\exists q \in R[x] : f = q * (x - c)$
- Bizonyítás:
  - f osztása $x - c$-vel: $f = q * (x - c) + r$
  - $\deg r < \deg x - c = 1 \implies r$ konstans
  - c gyök $\implies 0 = f(c) = q * (c - c) + r \implies r = 0$

3.2. Gyökök száma max a polinom fokszáma

- Legyen R egy E.I.T. (!!!) és $f \in R[x]$ és $\deg f = n$
- Ekkor f-nek max n gyöke van
- Bizonyítás: (indukcióval)
  - $n = 0 \implies f(x) = r \implies$ nincs gyök ha $r \neq 0$
    - ha $r = 0$ akkor $f = 0$ azaz $\deg f = -\infty$
  - indukciós lépés: $\exists c$ gyök $\implies f = (x - c) * q$
    - $x - c$ az 1 gyök
    - $\deg q = n - 1$, indukciós feltevés alapján max $n - 1$ gyöke van
    - $1+$ max $n - 1 =$ max n, tehát készen vagyunk

3.3. Polinomok egyenlősége több behelyettesítés alapján

- Legyen R egy E.I.T. és legyen R-nek legalább $n+1$ eleme (pl. végtelen)
- Ha $\deg f_1 \leq n$ és $\deg f_2 \leq n$ és $\forall r \in R : f_1(r) = f_2(r)$
- Akkor $f_1 = f_2$ (azaz az együtthatók és tehát a fokszámok megegyeznek)
- Bizonyítás: tegyük fel, hogy $f_1 \neq f_2$
  - $f_1 - f_2 \neq 0$ és $\deg f_1 - f_2 \leq n \implies$ max n gyöke van (előző tétel)
  - Tehát $(f_1 - f_2)(r)$ nem lehet nulla $n+1$ helyen, azaz ellentmondás

3.4. Lagrange interpoláció

- Legyen R egy test és $\deg f \leq n$
- Ha $n+1$ helyen ismerem $f(r)$ értékét: $y_i = f(x_i) \quad (i = 1..n+1)$
- Akkor f egyértelműen megadható polinomok egyenlősége tétel miatt: $\exists! f \in R[x] : \forall i \in [1, n+1] : f(x_i) = y_i$
- Bizonyítás:
  - Legyen $l_i(x) = (\prod_{j=0 \wedge i \neq j}^{n} (x - x_j)) \; / \; (\prod_{j=0 \wedge i \neq j}^{n} (x_i - x_j))$
  - Ekkor $l_i(x)$ akkor 1 ha $i = j$ egyébként mindig 0
  - Így ez megoldás: $f(x) = \sum_{i=0}^{n} y_i * l_i(x)$

4. Többváltozós polinomok

- pl.: $4x^2 + 3xy + 2y + 1$
- $R[x_1, x_2, ..., x_n] = R[x_1][x_2]...[x_n]$

5. Egység (más fogalom, mint az egységelem)

- Egy együttható egység, ha R minden elemének osztója.
  - Ekvivalens megfogalmazás: egység, ha létezik multiplikatív inverze
- Egy polinom egység, ha minden polinomnak az osztója.
  - Test feletti polinomgyűrű: pontosan a nemnulla konstans polinomok.
- Gyűrűelemet egységgel szorozva annak osztói, többszörösei nem változnak.
- Egy EIT két elemét asszociáltaknak nevezzük, ha egymás egységszeresei.
  - Ez egy ekvivalencia (reflexív, szimmetrikus, tranzitív) reláció.

6. Felbonthatatlan (irreducibilis) polinomok

- $f \in R[x]$ irreducibilis, ha:
  - $f \neq 0$ és f nem egység
  - $f = g * h \implies g$ egység vagy h egység
- Példa irreducibilis-ra $\mathbb{Q}$-ban: $(x^2+1) = \frac{1}{2} * (2x^2+2)$ ($\frac{1}{2}$ egység)
- Példa nem irreducibilis-ra: $(x^2-1) = (x-1)(x+1)$
- Test felett minden elsőfokú polinom felbonthatatlan.

6.1. Algebra alaptétele $\mathbb{C}$-ben

- Ha $f \in \mathbb{C}[x]$ és $\deg f \geq 1$ akkor létezik f-nek gyöke
- Nem bizonyítjuk, nagyon nehéz
- Következmény: $\mathbb{C}$-ben irreducibilis $\Leftrightarrow$ elsőfokú polinom

6.2. Irreducibilis $\mathbb{R}$-ben

- $\mathbb{R}$-ben azok és csak azok az f polinomok irreducibilisak, amik:
  - $\deg f = 1$
  - $\deg f = 2$ és $f = ax^2 + bx + c$ és $b^2 - 4ac < 0$

6.3. Irreducibilis $\mathbb{Z}_p$-ben, $\mathbb{Q}$-ban, $\mathbb{Z}$-ben

- Tétel bizonyítás nélkül
- Minden $n \geq 1$-re létezik n-ed fokú irreducibilis polinom

6.4. Felbonthatóság és gyökök kapcsolata test felett

- van gyöke $\Leftrightarrow$ létezik első fokú faktora (osztója)
- $\deg f \geq 2$ és van gyöke $\implies$ felbontható
- $\deg f = 2 \vee \deg f = 3$: felbontható $\Leftrightarrow$ van gyöke

7. Modulo polinom

- Létezik ilyen
- Elvégzem a műveletet, elosztom a modulo-val és a maradékot veszem
- Ha f irreducibilis, akkor $mod\ f$ egy test
- $\mathbb{C}$: mintha $mod\ i^2 + 1$-ben számolnánk
- Euklideszi algoritmussal megoldható pl. $(3 + 2x) * g \equiv 1 \mod x^2 + 1$
  $(3 + 2x)^{-1} \equiv \frac{4}{13} * (-\frac{1}{2}x + \frac{3}{4}) \mod x^2 + 1$

7.1. Véges testek

- Alkalmazás: kódolás, hibajavítás
- Véges test: egyszerre $mod\ p$ (p prím) és $mod\ f$ ($\deg f = n$)
- Ekkor p^n elemű (elemszámú) testről beszélünk
- pl.: $(2x + 1)(x + 2) \equiv 2x\ \ (mod\ 3,\ mod\ x^2 + 1)$
  $3^2 = 9$ elem: $\{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}$

8. Elem rendje, gyűrű karakterisztikája

8.1. Elem additív rendje

- Legyen R egy gyűrű és $0 \neq r \in R$
- r rendje a legkisebb olyan n egész, amelyre $n * r = 0$
- pl.: Z_7-ben 3 rendje 7 mert $7 * 3 = 21\ mod\ 7 = 0$
- Nullosztómentes gyűrűben az összes nemnulla elem rendje megegyezik.

8.2. Gyűrű karakterisztikája

- $char(R)$: nullosztómentes R gyűrű karakterisztikája
  - $char(R) = 0$ ha R elemeinek közös rendje nem véges
  - egyébként $char(R) = R$ elemeinek közös additív rendje
- Példa: $char(\mathbb{Z}_p) = p$ ha p prím
- Példa: $char(\mathbb{Z}) = char(\mathbb{Q}) = char(\mathbb{R}) = char(\mathbb{C}) = 0$

9. Algebrai derivált

- Legyen $f \in R[x]$ ahol R test és $f = a_0 + a_1x + a_2x^2 + ... + a_nx^n$
- Ekkor az algebrai derivált: $f' = a_1 + 2a_2x + 3a_3x^2 + ... + n * a_nx^{n-1}$
  - $f' = \sum_{k=0}^{n} k * f_k * x^{k-1}$

10. Gyökök multiplicitása

- c min. k-szoros gyök: $\exists q : f = (x-c)^k * q$
- c pontosan k-szoros gyök: c k-szoros gyök, de nem $k+1$-szeres

10.1. Algebrai deriválttal összefüggés

- f-nek a c k-szoros gyöke $\implies$ f'-nek c min. $(k-1)$-szeres gyöke
- Bizonyítás:
  - $f = (x-c)^k * q$
  - $f' = ((x-c)^k * q)'$ =nem biz= $((x-c)^k)' * q + (x-c)^k * q' =$
    $= k * (x-c)^{k-1} * q + (x-c)^k * q' = (x-c)^{k-1} * (k * q + (x-c) * q')$
- Ez a tétel "min" helyett "pontosan"-nal akkor működik, ha $char(R) \nmid k$
  - pl. $\mathbb{R}$ esetén, mivel $char(\mathbb{R}) = 0 \nmid k$ (minden $k \neq 0$)

10.2. LNKO-val, algebrai deriválttal összefüggés

- $LNKO(f, f') = d = 1 \implies$ f-nek nincs többszörös gyöke
- $char(R) = 0 \implies$ d gyökei f legalább kétszeres gyökei

10.3. Számolása Horner táblázattal

- Egy Horner táblázatot újrahasználhatunk
  - Mindig kevesebb oszlop kell, ezért mindig eggyel több $\times$-ot rakunk
  - Minden (pl. a maradék) azonos oszlopban van
- Az előző eredmény mindig az új osztandó polinom
- Addig írunk új sort, amíg a maradék 0

11. Euklideszi algoritmus polinomokkal

- Legyen R egy test és $f, g \in R[x]$
- Ha $d = LNKO(f, g)$ akkor
  - $d|f$ és $d|g$ (d közös osztó)
  - $\forall h : (h|f) \wedge (h|g) \implies h|d$ (d a legnagyobb)
- A legnagyobb közös osztó egészek körében sem volt egyértelmű (x, $-x$) és polinomok esetén sem az.
- Bővített euklideszi algoritmus is jó: $LNKO(f, g) = d = f * u + g * v$

11.1. Euklideszi algoritmus a gyakorlatban

- Egységgel be szabad szorozni, az nem változtat az eredményen.
- Egymást követő osztások:
  - $f, g, r_1, r_2, ...$ kettesével osztása megadja a következőt
  - 1.: $f/g \implies f = g * q_1 + r_1$
  - 2.: $g/r_1 \implies g = r_1 * q_2 + r_2$
  - 3.: $r_1/r_2 \implies r_1 = r_2 * q_3 + r_3$
- Addig osztunk, amíg a maradék 0 nem lesz.
  Ekkor az utolsó $\neq 0$ maradék a megoldás (LNKO).
  - pl.: $r_2 \neq 0 \wedge r_3 = 0 \implies LNKO(f, g) = d = r_2$
- Bővített euklideszi algoritmus: pontosan úgy, mint skalárokkal

11.2. Kétváltozós diofantikus egyenletek

- Legyen $f * u + g * v = h$
- Bővített euklideszivel ki kell számolni: $f * u' + g * v' = d = gcd(f, g)$
  - Itt is pontosan akkor oldható meg, ha $d|h$
- Megoldások, ahol $w \in R[x]$ egy tetszőleges polinom:
  - $u_w = u_0 + \frac{g}{d}w$ ahol $u_0 = u' * \frac{h}{d}$
  - $v_w = v_0 - \frac{f}{d}w$ ahol $v_0 = v' * \frac{h}{d}$

12. Hibakorlátozó kódolás

12.1. Alapfogalmak

- Σ az ábécé, azaz egy rögzített véges halmaz
  - n hosszú szavak halmaza: Σ^n
- Hamming-távolság 2 n hosszú szó között: pozíciók száma, ahol különböznek
  - Szóhalmaz távolsága: min{ bármely 2 szavának távolsága }
- Kód: Σ^n részhalmaza (azaz bizonyos n hosszú szavak)
  - Kódszó: kód egy eleme
- Szándék: küldeni kívánt szó (ezt alakítjuk kódszóvá)
- Dekódolás: üzenethez legközelebbi kódszó kiválasztása

12.2. t-hibajelző, t-hibajavító kód

- t-hibajelző kód: max t helyen sérült üzenetnél észreveszi, hogy sérült
  - d távolságú kód $\implies$ $d-1$ hibát jelez
  - Bizonyítás: távolság d $\implies$ $d-1$ változás nem adhat új kódszót
- t-hibajavító kód: max t helyen sérül üzenetnek tudja az eredeti kódszavát
  - d távolságú kód $\implies$ $\lfloor \frac{d-1}{2} \rfloor$ hibát javít
  - Bizonyítás:
    - Legyen w az eredeti kódszó, w' a sérült, w_2 egy másik kódszó
    - Kiindulás: $distance(w, w') \leq \lfloor \frac{d-1}{2} \rfloor$
    - Legyen $distance(w', w_2) = x$
    - Be kell látni: $\lfloor \frac{d-1}{2} \rfloor < x$
    - $distance(w, w_2) \geq d \implies x + \lfloor \frac{d-1}{2} \rfloor \geq d$
    - Átrendezve: $x \geq \lfloor \frac{d+1}{2} \rfloor > \lfloor \frac{d-1}{2} \rfloor$
- Példa béna, pazarló kódra: n-szeres ismétlés $\implies$ kód távolsága n

12.3. Singleton-korlát

12.3.1. Tétel

- Legyen
  - $Q = |\Sigma|$ az abécé mérete
  - c a kódszavak száma
  - n a kódszavak hossza
  - d a kód távolsága
- Állítás: $c \leq Q^{n-d+1} = Q^{n-(d-1)}$
- Bizonyítás
  - A kód távolsága $d \implies d-1$ változtatás nem adhat új kódszót
  - Változtassuk az összes kódban az utolsó $d-1$ betűt ugyan arra
  - Így is páronként különböznek, szóval el is hagyható a $d-1$ betű
  - Szóval max annyi kódszó van, hogy a kódszavakat $d-1$ betűvel rövidítve is páronként különbözik mindegyik

12.3.2. Következmény

- Hibajavító betűk száma $\geq d-1$
  - Azaz legalább ennyivel kell a szándéknál több betűt használni
- MDS-kód: egyenlőség áll fenn a Singleton-korlát tételében

12.3.3. Reed-Solomon kód

- Egy MDS-kód
- Működés
  - $\Sigma = \{f \in R\}$ ahol R egy véges test
  - Szándék: f polinom együtthatói
  - Kód: $f * g$
  - g kódpolinom $d-1$ fokú
- Tétel: g gyökei páronként különböznek $\implies$ d távolságú a kód

12.4. Hamming-korlát

12.4.1. Tétel

- Legyen
  - $Q = |\Sigma|$ az abécé mérete
  - c a kódszavak száma
  - n a kódszavak hossza
  - t hibát javít a kód ($\Longrightarrow$ $2t+1$ vagy $2t+2$ távolságú)
- Állítás: $c * \sum_{k=0}^{t}(\binom{n}{k} * (Q-1)^k) \leq Q^n$
  - Szummán belül: kódszótól pontosan k távolságra hány kódszó van
  - Válasz: $\binom{n}{k}$ ="hol változtatok" $*$ "mire változtatok"$= (Q-1)^k$
  - Szóval a szumma: kódszótól $\leq t$ távolságra lévő szavak száma
  - Q^n pedig az ábécéből kirakható n hosszú szavak száma.
- Bizonyítás
  - A szumma eredményében "megszámolt" szavak diszjunktak különböző "kiindulási" kódszó esetén, hiszen t hibát javít a kód.
  - Így a (diszjunkt halmazok száma) $*$ (diszjunkt halmaz mérete) nem lehet nagyobb, mint a lehetséges szavak száma.

12.4.2. Következmény

- Perfekt kód: egyenlőség áll fenn a Hamming-korlát tételében

13. ZH 2 összefoglaló

13.1. Gyűrű, integritási tartomány, test

- Gyűrű: $*$ disztributív $+$-ra, $+$ asszoc. és kommutatív, $*$ asszoc. és $\exists 0$
- Integritási tartomány: gyűrű, $*$ kommutatív, nullosztómentes (pl. $\mathbb{Z}_{prim}$)
- E.I.T.: integritási tartomány, $\exists 1$
- Test: E.I.T. ahol van osztás ($\forall a \neq 0 : \exists a^{-1}$) (pl. $\mathbb{Q}, \mathbb{Z}_{prim}$)
- Gyűrű elem (additív) rendje: legkisebb n egész, hogy $n*$ az elem $= 0$
- $char(R)$: I.T. elemeinek (megegyező) rendje (pl. $char(\mathbb{Z}_{prim}) = prim$)
  - $char(R) = 0$ ha az elemek rendje nem véges, pl. $char(\mathbb{Z})$, $char(\mathbb{Q})$

13.2. Polinom alapok

- $f = f_0 + ... + f_{\deg f} * x^{\deg f}$ ahol $\deg f =$ legnagyobb n ahol $f_n \neq 0$
  - $f = 0 \implies \deg f = -\infty$
- $\deg f + g \leq max(\deg f, \deg g)$
- $\deg f * g \leq \deg f + \deg g$ (egyenlő, ha R egy I.T, azaz nullosztómentes)
- Maradékos osztás: $f = g*q+r \wedge \deg r < \deg q$: ($R$ egy E.I.T, $\exists {g_{\deg g}}^{-1}$)
  - Bizonyítások: egyértelműség: fokszámmal; létezés: rekurzióval
  - Gyakorlatban: rekurzióval, $f^* = f - g * f_{\deg f} * g_{\deg g}^{-1} * x^{\deg f - \deg g}$
    - Alapeset, megállás: $\deg f < \deg g$ (ekkor $r = f$)
    - $q = \sum f_{\deg f} * g_{\deg g}^{-1} * x^{\deg f - \deg g}$ (ahol f persze változik)
- Gyökök: c gyök ha $f(c) = 0$, ekkor $f = q * (x - c)$
  - Ha R egy E.I.T. akkor f-nek legfeljebb $\deg f$ darab gyöke van
- Egység: mindennek az osztója (polinom egység, ha $\forall$ polinomnak osztója)
  - R egy test: pontosan nemnulla konstans polinomok az egységek
  - Gyűrűelem egységgel szorzása: osztói, többszörösei nem változnak.
  - Egy gyűrű elemei asszociáltak, ha egymás egységszeresei
- Algebrai derivált: $f' = \sum_{k=0}^{\deg f} k * f_k * x^{k-1}$

13.3. Horner-elrendezés (Horner táblázat)

	f_n	f_{n-1}	f_{n-2}	...	f_0	
c	$\times$	$c_1 = f_n$	$c_2 = c_1 * c + f_{n-1}$	..	$c_n = c_{n-1} * c + f_1$	$c_{n+1} = ... = f(c)$

13.4. Felbonthatatlan (irreducibilis) polinomok

- $f \neq 0$ irreducibilis ha nem egység és $f = g * h \implies g$ vagy h egység
- Test felett: $\deg f = 1 \implies f$ irreducibilis
- $\mathbb{C}$-ben: irreducibilis $\Leftrightarrow$ elsőfokú polinom (algebra alaptétele $\mathbb{C}$-ben)
- $\mathbb{Z}_{prim}$, $\mathbb{Q}$, $\mathbb{Z}$: minden $n \geq 1$-re létezik n-ed fokú irreducibilis polinom

13.5. Gyökök multiplicitása

- c legalább k-szoros gyök $\implies \exists q : f = (x-c)^k * q$
- f-nek a c k-szoros gyöke $\implies f'$-nek c min. $(k-1)$-szeres gyöke
  - Bizonyítás: $f = (x-c)^k * q$ deriválása (szorzat deriváltja azonosság)
  - "min" helyett "pontosan" ha $char(R) \nmid k$ (mert pl. $char(\mathbb{R}) = 0$)
- $char(R) = 0 \implies LNKO(f, f')$ gyökei az f legalább kétszeres gyökei

13.6. (Bővített) euklideszi algoritmus

- Test felett működik; nem egyértelmű: egységgel részeredményeket megszorozhatjuk
- Gyakorlatban: $f, g, r_1, r_2, ...$ kettesével osztása megadja a következőt
- Ugyan úgy megy, mint skalárokkal; utolsó nemnulla az eredmény

13.7. Kétváltozós diofantikus egyenletek

- $u, v = ?$ és $f * u + g * v = h$ és $f * u' + g * v' = d = gcd(f, g)$
- Megoldható $\Leftrightarrow d | h$
- Megoldások, ahol $w \in R[x]$ tetszőleges:
  - $u_w = u_0 + \frac{g}{d} w$ ahol $u_0 = u' * \frac{h}{d}$
  - $v_w = v_0 - \frac{f}{d} w$ ahol $v_0 = v' * \frac{h}{d}$