

## Diszkrét matematika 2. – Polinomok beugró

Készítette: Grimm Dániel

1. Algebrai alapok, polinomokkal kapcsolatos alapfogalmak
1. Definiáld a (binér) művelet fogalmát!

Egy  $X$  halmazon értelmezett művelet alatt egy  $* : X^n \rightarrow X$  függvényt értünk.

Egy  $X$  halmazon értelmezett binér (kétváltozós) művelet egy  $* : X \times X \rightarrow X$  függvény. Gyakran  $*(x, y)$  helyett  $x * y$ -t írunk.

2. Definiáld az asszociativitás fogalmát!

A  $* : X \times X \rightarrow X$  művelet  
asszociatív, ha  $\forall a, b, c \in X : (a * b) * c = a * (b * c)$ ;

3. Adj példát nem asszociatív binér műveletre!

Kivonás  $\mathbb{R}$  – ben:  $(3-2)-1$  az 0,  $3-(2-1)$ az 2

4. Definiáld a kommutativitás fogalmát!

A  $* : X \times X \rightarrow X$  művelet  
kommutatív, ha  $\forall a, b \in X : a * b = b * a$ .

5. Adj példát nem kommutatív binér műveletre!

Pi 2x2-es Mátrixok körében a szorzás.

6. Definiáld a grupoid fogalmát!

A  $(H; M)$  pár algebrai struktúra, ha  $H$  egy halmaz,  $M$  pedig  $H$ -n értelmezett műveletek halmaza.  
Az egy binér műveletes struktúrát **grupoidnak** nevezzük.

7. Definiáld a félcsoport fogalmát!

A  $(G; *)$  grupoid **félcsoport**, ha  $*$  asszociatív  $G$ -n.

8. Adj példát olyan grupoidra, amely nem félcsoport!

**Emil Vatai**  $G = \{a,b,c\}$ , és a művelet táblája

*	a	b	c
a			
b			
c			

9/10. Definiáld a semleges elem/monoid fogalmát!

Ha létezik  $s \in G$ :  $\forall g \in G : s * g = g * s = g$ , akkor az  $s$  semleges elem (egységelem),  $(G; *)$  pedig semleges elemes félcsoport (egységelemes félcsoport, monoid).

11. Definiáld az inverz fogalmát!

Legyen  $(G; *)$  egy egységelemes félcsoport  $e$  egységelemmel. A  $g \in G$  elem inverze a  $g^{-1} \in G$  elem, melyre  $g * g^{-1} = g^{-1} * g = e$ .

12. Definiáld a csoport fogalmát!

Ha minden  $g \in G$  elemnek létezik inverze, akkor  $(G; *)$  csoport.

13. Definiáld az Abel-csoport fogalmát!

Ha ezen felül  $*$  kommutatív is, akkor  $(G; *)$  Abel-csoport.

14. Definiáld a disztributivitás fogalmát!

Legyen  $(R; *, \circ)$  algebrai struktúra, ahol  $*$  és  $\circ$  binér műveletek. Azt mondjuk, hogy teljesül a  $\circ$ -nek a  $*$ -ra vonatkozó bal oldali disztributivitása, illetve jobb oldali disztributivitása, ha  
 $\forall k, l, m \in R$ -re:  $k \circ (l * m) = (k \circ l) * (k \circ m)$ , illetve  
 $\forall k, l, m \in R$ -re:  $(l * m) \circ k = (l \circ k) * (m \circ k)$ .

15. Definiáld a gyűrű fogalmát!

Az  $(R; *, \circ)$  két binér műveletes algebrai struktúra gyűrű, ha

- $(R; *)$  Abel-csoport;
- $(R; \circ)$  félcsoport;
- teljesül a  $\circ$ -nek a  $*$ -ra vonatkozó minden oldali disztributivitása.

16. Definiáld a nullelem/egységelem fogalmát gyűrűben!

$(R; *, \circ)$  két binér műveletes algebrai struktúra esetén a  $*$ -ra vonatkozó semleges elemet **nullelemnek**, a  $\circ$ -re vonatkozó semleges elemet **egységelemnek** nevezzük. A nullelem szokásos jelölése **0**, az egységelemé **1**, esetleg **e**.

17. Definiáld az egységelemes gyűrű fogalmát!

Az  $(R; *, \circ)$  gyűrű **egységelemes gyűrű**, ha  $R$ -en a  $\circ$  műveletre nézve van egységelem.

18. Definiáld a kommutatív gyűrű fogalmát!

Az  $(R; *, \circ)$  gyűrű **kommutatív gyűrű**, ha a  $\circ$  művelet (**is**) kommutatív.

19. Definiáld a nulosztómentes gyűrű fogalmát!

Ha egy  $(R, *, \circ)$  gyűrűben  $\forall r, s \in R, r, s \neq 0$  esetén  $r \circ s \neq 0$ , akkor  $R$  **nulosztómentes gyűrű**.

20. Definiáld az integrási tartomány fogalmát!

A **kommutatív, nulosztómentes** gyűrűt **integrási tartománynak** nevezzük.

## Példa

- $(\mathbb{Z}; +, \cdot)$

21. Definiáld a karakterisztika fogalmát!

**Nulosztómentes** gyűrűben a nem-nulla elemek additív rendje megegyezik, és vagy egy **p** prímszám vagy végtelen.

## Definíció

Ha az előző állításban szereplő közös rend **p**, akkor a gyűrű **karakterisztikája p**, ha a közös rend végtelen, akkor pedig **0**. Jelölése: **char(R)**.

22. Definiáld az osztó/többszörös fogalmát!

Az  $(R; *, \circ)$  egységelemes integritási tartományban az  $a, b \in R$  elemekre azt mondjuk, hogy  $a$  osztója  $b$ -nek, ha van olyan  $c \in R$ , amire  $b = a \circ c$ . Jelölése:  $a|b$ .

23. Definiál az egység fogalmát!

**Az egységelem osztóját egységnak nevezzük.**

24. Definiál a felbonthatatlan elem fogalmát!

A  $b = cd$  a  $b$ -nek *triviális* felbontása, ha  $c$  és  $d$  egyike egység. A  $p \in R$  *felbonthatatlan* (irreducibilis), ha nem nulla, nem egység, és nincs nemtriviális felbontása.

**Ekvivalens:**  $p$  minden osztója egység, vagy  $p$  egységszerese.

25. Adj példákat gyűrűkre!

- $(\mathbb{Z}; +, \cdot)$  egységelemes kommutatív gyűrű.
- $(2\mathbb{Z}; +, \cdot)$  gyűrű, de nem egységelemes.
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  a szokásos műveletekkel egységelemes kommutatív gyűrűk.
- $\mathbb{C}^{k \times k}$  a szokásos műveletekkel egységelemes gyűrű, de nem kommutatív, ha  $k > 1$ .

26. Adj példát véges, és végtelen testekre!

**Emil Vatai** 2.: Véges test példának csak  $Zp$  (p prímszám) jó, vagy van más is? Igen,  $Zp$  tökéletes példa. Az összes véges testre van egy bevett jelölés ami az:  $IFq$  (az egy duplaszárú F és egy alsóindex q akar lenni), ahol  $q = p^n$ , p prím n pozegész. És ez lényegében  $Zp[x]$  maradékosztályai mod f valamelyen f eleme  $Zp[x]$  irreducibilis,  $deg(f)=n$  polynomra. Szal végestestek: "mod p együtthatós mod f polinomok".

Tetszik · Válasz · 1 · június 3., 8:59

**Emil Vatai** 3.: Végtelen test példának jó Q,R,C?  
TÖKÉLETES

27. Mi teljesül nullemmel való szorzás esetén gyűrűben?

az hogy r művelet  $0 = 0$  művelet  $r = 0$

a 0 elem az  $(R, +, \cdot)$  gyűrűben az első műveletre vonatkozó semleges ele

és az a lényeg hogy bármely  $R$ -beli elemre ha a második műveletet 0-val alkalmazva 0-t kapunk

28. Mit mondhatunk testben a nulosztókról?

Legyen  $T$  test. Ekkor  $T$  nulosztómentes.

29. Definiáld a polinomokat a műveletekkel!

### Definíció

Legyen  $(R; +, \cdot)$  gyűrű. A gyűrű elemeiből képzett  $f = (f_0, f_1, f_2, \dots)$  ( $f_j \in R$ ) végtelen sorozatot  $R$  fölötti **polinomnak** nevezzük, ha csak véges sok eleme nem-nulla.

Az  $R$  fölötti polinomok halmazát  $R[x]$ -szel jelöljük.

$R[x]$  elemein definiáljuk az összeadást és a szorzást.

$f = (f_0, f_1, f_2, \dots)$ ,  $g = (g_0, g_1, g_2, \dots)$  és  $h = (h_0, h_1, h_2, \dots)$  esetén  $f + g = (f_0 + g_0, f_1 + g_1, f_2 + g_2, \dots)$  és  $f \cdot g = h$ , ahol

$$h_k = \sum_{i+j=k} f_i g_j = \sum_{i=0}^k f_i g_{k-i} = \sum_{j=0}^k f_{k-j} g_j.$$

### Megjegyzés

Könnyen látható, hogy polinomok összege és szorzata is polinom.

30. Milyen kapcsolat van egy gyűrű és az adott gyűrű fölötti polinomgyűrű között?

Ha  $(R; +, \cdot)$  gyűrű, akkor  $(R[x]; +, \cdot)$  is gyűrű, és  $R$  fölötti **polinomgyűrűnek** nevezzük.

31. Definiáld az együttható, a főtag, és a konstans tag fogalmát!

Az  $f = (f_0, f_1, f_2, \dots, f_n, 0, 0, \dots)$ ,  $f_n \neq 0$  polinomot  
 $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n$ ,  $f_n \neq 0$  alakba írjuk.

## Definíció

Az előző pontban szereplő polinom esetén  $f_i$ -t az  $i$ -ed fokú tag **együtthatójának** nevezzük,  $f_0$  a polinom **konstans tagja**,  $f_n$  a **főegyütthatója**,  $f_nx^n$  a **főtagja**,  $n$  pedig a **foka**.  $f$  fokának jelölésére  $\deg(f)$  használatos.

32. Definiáld a főegyüttható és a polinom fokának a fogalmát!

A főegyüttható tehát a legnagyobb indexű nem-nulla együttható, a fok pedig ennek indexe.

33./34./35./36./37. Definiáld a konstans/null/lineáris/fő –polinom, és a monom fogalmát!

A  $0 = (0, 0, \dots)$  **nullpolinomnak** nincs legnagyobb indexű nem-nulla együtthatója, így a fokát külön definiáljuk, mégpedig  $\deg(0) = -\infty$ .

A **konstans polinomok** a legfeljebb nullafokú polinomok, a **lineáris polinomok** pedig a legfeljebb elsőfokú polinomok. Az  $f_i x^i$  alakba írható polinomok a **monomok**. Ha  $f \in R[x]$  polinom főegyütthatója  $R$  egységeleme, akkor  $f$ -et **főpolinomnak** nevezzük.

38. Mit mondhatunk polinomok összegének, szorzatának fokáról?

Legyen  $f, g \in R[x]$ ,  $\deg(f) = n$ , és  $\deg(g) = k$ . Ekkor:

- $\deg(f + g) \leq \max(n, k)$ ;
- $\deg(f \cdot g) \leq n + k$ .

39. Adj példát amikor a polinom összegére/szorzatára vonatkozó becslésben szigorú egyenlőség teljesül!

Nulosztómentes gyűrű esetén egyenlőség teljesül a 2. egyenlőtlenségen, hiszen

$$h_{n+k} = \sum_{i=0}^{n+k} f_i g_{n+k-i} = \sum_{i=0}^{n-1} f_i g_{n+k-i} + f_n g_k + \sum_{i=n+1}^{n+k} f_i g_{n+k-i} = f_n g_k \neq 0.$$

40. Definiáld a helyettesítési érték fogalmát!

Az  $f(x) = f_0 + f_1x + f_2x^2 + \dots + f_nx^n \in R[x]$  polinom  $r \in R$  helyen felvett helyettesítési értékén az  $f(r) = f_0 + f_1r + f_2r^2 + \dots + f_nr^n \in R$  elemet értjük.

41. Definiáld a gyök fogalmát!

$f(r) = 0$  esetén  $r$ -et a polinom **gyökének** nevezzük.

42. Definiáld a polinomfüggvény fogalmát!

Az  $\hat{f} : r \mapsto f(r)$  leképezés az  $f$  polinomhoz tartozó **polinomfüggvény**.

43. Adj példát, amikor különböző polinomokhoz ugyanaz a polinomfüggvény tartozik!

Ha  $R$  véges, akkor csak véges sok  $R \rightarrow R$  függvény van, míg végtelen sok  $R[x]$ -beli polinom, így vannak olyan polinomok, amikhez ugyanaz a polinomfüggvény tartozik, például  $x, x^2 \in \mathbb{Z}_2[x]$ .

### Példa

$f(x) = x^2 + x - 2 \in \mathbb{Z}[x]$ -nek a  $-2$  helyen felvett helyettesítési értéke  $(-2)^2 + (-2) - 2 = 0$ , ezért  $-2$  gyöke  $f$ -nek.

## 2. Polinomok maradékos osztásának tétele és következményei

44. Hogyan szól a polinomok maradékos osztásának a tétele?

### Tétel (polinomok maradékos osztása)

Legyen  $R$  egységelemes integritási tartomány,  $f, g \in R[x]$ , és tegyük fel, hogy  $g$  főegyütthatója egység  $R$ -ben. Ekkor egyértelműen léteznek olyan  $q, r \in R[x]$  polinomok, melyekre  $f = qg + r$ , ahol  $\deg(r) < \deg(g)$ .

45. Definiáld a gyöktényező fogalmát!

Ha  $c \in R$  az  $f \in R[x]$  polinom gyöke, akkor  $(x - c) \in R[x]$  a **c-hez tartozó gyöktényező**.

46. Hogy szól a gyöktényező leválasztására vonatkozó téTEL?

Ha  $0 \neq f \in R[x]$ , és  $c \in R$  gyöke  $f$ -nek, akkor létezik olyan  $q \in R[x]$ , amire  $f(x) = (x - c)q(x)$ .

47. Hány gyöke lehet egy polinomnak?

Az  $f \neq 0$  polinomnak legfeljebb  $\deg(f)$  gyöke van.

48. Mit mondhatunk két,  $n+1$  helyen megegyező, legfeljebb  $n$ -ed fokú polinomról?

Ha két, legfeljebb  $n$ -ed fokú polinomnak  $n + 1$  különböző helyen ugyanaz a helyettesítési értéke, akkor egyenlők.

49. Mit mondhatunk végtelen  $R$  esetén a polinomfüggvényekről?

Ha  $R$  végtelen, akkor két különböző  $R[x]$ -beli polinomhoz nem tartozik ugyanaz a polinomfüggvény.

50. Definiál az oszthatóságot polinomok körében!

Azt mondjuk, hogy  $f, g \in R[x]$  polinomok esetén  $f$  osztója  $g$ -nek ( $g$  többszöröse  $f$ -nek), ha létezik  $h \in R[x]$ , amire  $g = f \cdot h$ .

51. Definiál polinomok kitüntetett közös osztóját!

Az  $f, g \in R[x]$  polinomok kitüntetett közös osztója (legnagyobb közös osztója) az a  $d \in R[x]$  polinom, amelyre  $d|f$ ,  $d|g$ , és tetszőleges  $c \in R[x]$  esetén  $(c|f \wedge c|g) \Rightarrow c|d$ .

52. Milyen polinomokra tudjuk biztosan alkalmazni az euklideszi algoritmust?

**Emil Vatai** 5.:Milyen polinomokra tudjuk biztosan alkalmazni az euklideszi algoritmust? Válaszodat indokold! Itt elég annyi indoklásnak hogy test fölötti polinomgyűrűben tetszőleges nem-nulla polinommal tudunk maradékos osztást végezni, ezért működik a bővített euklideszi algoritmus, vagy kell más is?

Bőven, a lényeg: TEST FÖLÖLÖTTI.

53. Ismertesd a bővitett euklideszi algoritmust!

Legyen  $R$  test,  $f, g \in R[x]$ . Ha  $g = 0$ , akkor  $(f, g) = f = 1 \cdot f + 0 \cdot g$ , különben végezzük el a következő maradékos osztásokat:

$$\begin{aligned}f &= q_1g + r_1; \\g &= q_2r_1 + r_2; \\r_1 &= q_3r_2 + r_3; \\&\vdots \\r_{n-2} &= q_nr_{n-1} + r_n; \\r_{n-1} &= q_{n+1}r_n.\end{aligned}$$

Ekkor  $d = r_n$  jó lesz kitüntetett közös osztónak.

Az  $u_{-1} = 1$ ,  $u_0 = 0$ ,  $v_{-1} = 0$ ,  $v_0 = 1$  kezdőértékekkel, továbbá az  $u_k = u_{k-2} - q_k \cdot u_{k-1}$  és  $v_k = v_{k-2} - q_k \cdot v_{k-1}$  rekurziókkal megkapható  $u = u_n$  és  $v = v_n$  polinomok olyanok, amelyekre teljesül  $d = u \cdot f + v \cdot g$ .

54. Ismertesd a Horner-elrendezést!

Legyen  $R$  test,  $f, g \in R[x]$ . Ha  $g = 0$ , akkor  $(f, g) = f = 1 \cdot f + 0 \cdot g$ , különben végezzük el a következő maradékos osztásokat:

$$\begin{aligned}f &= q_1g + r_1; \\g &= q_2r_1 + r_2; \\r_1 &= q_3r_2 + r_3; \\&\vdots \\r_{n-2} &= q_nr_{n-1} + r_n; \\r_{n-1} &= q_{n+1}r_n.\end{aligned}$$

Ekkor  $d = r_n$  jó lesz kitüntetett közös osztónak.

Az  $u_{-1} = 1$ ,  $u_0 = 0$ ,  $v_{-1} = 0$ ,  $v_0 = 1$  kezdőértékekkel, továbbá az  $u_k = u_{k-2} - q_k \cdot u_{k-1}$  és  $v_k = v_{k-2} - q_k \cdot v_{k-1}$  rekurziókkal megkapható  $u = u_n$  és  $v = v_n$  polinomok olyanok, amelyekre teljesül  $d = u \cdot f + v \cdot g$ .

55. Adj példát olyan polinomra, melynek különböző polinomgyűrűben különböző számú gyöke van!

$x^2 + 2 \rightarrow \mathbb{R}$  –ben nincs gyöke,  $\mathbb{C}$  –ben 2 gyöke van,  $\mathbb{Z}_3$ -ban is van 2 gyöke

3. Polinomok algebrai deriváltja, véges testek, racionális gyökökteszt, Lagrange interpoláció

56. Definiáld az algebrai derivált fogalmát!

Legyen  $R$  gyűrű. Az

$f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_2 x^2 + f_1 x + f_0 \in R[x]$  ( $f_n \neq 0$ ) polinom algebrai deriváltja az

$f'(x) = n f_n x^{n-1} + (n-1) f_{n-1} x^{n-2} + \dots + 2 f_2 x + f_1 \in R[x]$  polinom.

57. Milyen tulajdonságokkal rendelkezik az algebrai derivált!

Ha  $R$  egységelemes integratísi tartomány, akkor az  $f \mapsto f'$  algebrai deriválás rendelkezik a következő tulajdonságokkal:

- ① konstans polinom deriváltja a nullpolinom;
- ② az  $x$  polinom deriváltja az egységelem;
- ③  $(f + g)' = f' + g'$ , ha  $f, g \in R[x]$  (additivitás);
- ④  $(fg)' = f'g + fg'$ , ha  $f, g \in R[x]$  (szorzat differenciálási szabálya).

58. Mivel egyenlő elsőfokú polinom n-edik hatványának deriváltja?

Ha  $R$  egységelemes integratísi tartomány,  $c \in R$  és  $n \in \mathbb{N}^+$ , akkor  $((x - c)^n)' = n(x - c)^{n-1}$ .

59. Definiáld a többszörös gyök fogalmát!

Legyen  $R$  egységelemes integratísi tartomány,  $0 \neq f \in R[x]$  és  $n \in \mathbb{N}^+$ .  
Azt mondjuk, hogy  $c \in R$  az  $f$  egy  $n$ -szöres gyöke, ha  $(x - c)^n | f$ , de  $(x - c)^{n+1} \nmid f$ .

60. Milyen kapcsolat van egy polinom gyökei, illetve a deriváltjai gyökei között?

Legyen  $R$  egységelemes integratísi tartomány,  $f \in R[x]$ ,  $n \in \mathbb{N}^+$  és  $c \in R$  az  $f$  egy  $n$ -szöres gyöke. Ekkor  $c$  az  $f'$ -nek legalább  $(n-1)$ -szöres gyöke, és ha  $\text{char}(R) \nmid n$ , akkor pontosan  $(n-1)$ -szöres gyöke.

61. Adj példát olyan polinomra amelynek van olyan n-szeres gyöke, ami a deriváltjának is n-szeres gyöke!

Legyen  $f(x) = x^4 - x \in \mathbb{Z}_3[x]$ . Ekkor 1 3-szoros gyöke  $f$ -nek, mert

$$f(x) = x(x^3 - 1) \stackrel{\mathbb{Z}_3}{=} x(x^3 - 3x^2 + 3x - 1) = x(x - 1)^3.$$

$$f'(x) = 4x^3 - 1 \stackrel{\mathbb{Z}_3}{=} x^3 - 3x^2 + 3x - 1 = (x - 1)^3,$$

tehát 1 3-szoros gyöke  $f'$ -nek is.

62. Milyen alakú egy Lagrange interpolációs polinom?

Legyen  $R$  test,  $c_0, c_1, \dots, c_n \in R$  különbözőek, továbbá  $d_0, d_1, \dots, d_n \in R$  tetszőlegesek. Ekkor létezik egy olyan legfeljebb  $n$ -ed fokú polinom, amelyre  $f(c_j) = d_j$ , ha  $j = 0, 1, \dots, n$ .

### Bizonyítás

Legyen

$$l_j(x) = \frac{\prod_{i \neq j} (x - c_i)}{\prod_{i \neq j} (c_j - c_i)},$$

a  $j$ -edik Lagrange-interpolációs alappolinom, és legyen

$$f(x) = \sum_{j=0}^n d_j l_j(x).$$

$l_j(c_i) = 0$ , ha  $i \neq j$ , és  $l_j(c_j) = 1$ -ből következik az állítás.

63. Ismertesd a Lagrange-interpolációt!

Adjunk meg olyan  $f \in \mathbb{R}[x]$  polinomot, amelyre  $f(0) = 3$ ,  $f(1) = 3$ ,  $f(4) = 7$  és  $f(-1) = 0$ !

A feladat szövege alapján  $c_0 = 0$ ,  $c_1 = 1$ ,  $c_2 = 4$ ,  $c_3 = -1$ ,  $d_0 = 3$ ,  $d_1 = 3$ ,  $d_2 = 7$  és  $d_3 = 0$  értékekkel alkalmazzuk a Lagrange-interpolációt.

$$l_0(x) = \frac{(x-1)(x-4)(x+1)}{(0-1)(0-4)(0+1)} = \frac{1}{4}x^3 - x^2 - \frac{1}{4}x + 1$$

$$l_1(x) = \frac{(x-0)(x-4)(x+1)}{(1-0)(1-4)(1+1)} = -\frac{1}{6}x^3 + \frac{1}{2}x^2 + \frac{2}{3}x$$

$$l_2(x) = \frac{(x-0)(x-1)(x+4)}{(4-0)(4-1)(4+1)} = \frac{1}{60}x^3 - \frac{1}{60}x$$

$$l_3(x) = \frac{(x-0)(x-1)(x-4)}{(-1-0)(-1-1)(-1-4)} = -\frac{1}{10}x^3 + \frac{1}{2}x^2 - \frac{2}{5}x$$

$$f(x) = 3l_0(x) + 3l_1(x) + 7l_2(x) + 0l_3(x) = \frac{22}{60}x^3 - \frac{3}{2}x^2 + \frac{68}{60}x + 3$$

	$\frac{22}{60}$	$-\frac{3}{2}$	$\frac{68}{60}$	3	
1	X	$\frac{22}{60}$	$-\frac{68}{60}$	0	3
4	X	$\frac{22}{60}$	$-\frac{2}{60}$	1	7
-1	X	$\frac{22}{60}$	$-\frac{112}{60}$	3	0

64. Hogyan konstruálunk  $p^n$  elemű testet?

$p^n$  elemű testet (ahol  $p$  prím) úgy konstruálunk hogy veszünk egy  $f$  elem  $\mathbb{Z}_p[x]$ ,  $n$ -ed fokú irreducibilis polinomot, és a test elemei a mod  $f$  polinomok lesznek, a műveletek meg a polinom műveletek (szintén mod  $f$ ), vagy a rövidebb válasz az a  $\mathbb{Z}_p[x] / (f)$ , azaz egy  $f$  eleme  $\mathbb{Z}_p[x]$  által generált főideálnak a  $\mathbb{Z}_p[x]$  re vonatkozó faktorgyűrűje



65. Mit mondhatunk véges testekről az elemszámmal kapcsolatosan?

Minden véges test elemszáma  $p^n$  alakú prímhatvány, és minden  $p^n$  alakú prímhatványhoz tudunk konstruálni ennyi elemű testet! ( $p$  prím,  $n$  pozitív egész)

66.

Legyen  $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2 + 1)$ . Mik lesznek a  $z^2 + 1 \in \mathbb{F}_9[z]$  polinom gyökei?

$x, -x$

67. Mik lehetnek egy primitív egész együtthatós polinom racionális gyökei?

Tekintsük az  $x^2 - 2 \in \mathbb{Z}[x]$  polinomot.

Ennek a  $\frac{p}{q}$  alakú gyökeire ( $p, q \in \mathbb{Z}$ ,  $(p, q) = 1$ ) teljesül, hogy  $p|2$  és  $q|1$ , így a lehetséges racionális gyökei  $\pm 1$  és  $\pm 2$ .

#### 4. Polinomok felbonthatósága

68. Hogyan jellemzhetők test fölötti polinomgyűrűben az egységek?

Legyen  $(F; +, \cdot)$  test. Ekkor  $f \in F[x]$  pontosan akkor egység, ha  $\deg(f) = 0$ .

69. Mit mondhatunk test fölötti elsőfokú polinomokról a gyökökkel kapcsolatban?

Ha  $(R; +, \cdot)$  nem test, akkor egy  $R$  fölötti elsőfokú polinomnak nem feltétlenül van gyöke, pl.  $2x - 1 \in \mathbb{Z}[x]$ .

70. Adj példát olyan elsőfokú polinomra, amelynek nincs gyöke!

$2x-1 \in \mathbb{Z}[x]$

71. Mit mondhatunk a lineáris polinomokról test fölötti polinomgyűrűben felbonthatóság szempontjából?

Legyen  $(F; +, \cdot)$  test, és  $f \in F[x]$ . Ha  $\deg(f) = 1$ , akkor  $f$  felbonthatatlan.

72. Hogyan jellemzhetők a test fölötti másod- illetve harmadfokú polinomok felbonthatóság szempontjából?

Legyen  $(F; +, \cdot)$  test, és  $f \in F[x]$ . Ha  $2 \leq \deg(f) \leq 3$ , akkor  $f$  pontosan akkor felbontható, ha van gyöke.

73. Hogyan jellemzhetők a  $\mathbb{C}$  fölötti felbonthatatlan polinomok?

$f \in \mathbb{C}[x]$  pontosan akkor felbonthatatlan, ha  $\deg(f) = 1$ .

74. Hogyan jellemzhetők a  $\mathbb{R}$  fölötti felbonthatatlan polinomok?

$f \in \mathbb{R}[x]$  pontosan akkor felbonthatatlan, ha

- $\deg(f) = 1$ , vagy
- $\deg(f) = 2$ , és  $f$ -nek nincs (valós) gyöke.

75. Definiáld a primitív polinom fogalmát!

$f \in \mathbb{Z}[x]$ -et **primitív polinomnak** nevezük, ha az együtthatónak a legnagyobb közös osztója 1.

76. Hogy szól a Schönemann-Eisenstein téTEL egész együtthatós polinomokra?

Legyen  $f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0 \in \mathbb{Z}[x]$ ,  $f_n \neq 0$  legalább elsőfokú primitív polinom. Ha található olyan  $p \in \mathbb{Z}$  prím, melyre

- $p \nmid f_n$ ,
- $p \mid f_j$ , ha  $0 \leq j < n$ ,
- $p^2 \nmid f_0$ ,

akkor  $f$  felbonthatatlan  $\mathbb{Z}$  fölött.