

1. Gyűrűk és testek

1.1. Definíció. Legyenek $\circ$ és $*$ kétváltozós műveletek a nemüres A halmazon. Azt mondjuk, hogy $\circ$ **disztributív** a $*$ műveletre, ha minden $a, b, c \in A$ esetén

$$a \circ (b * c) = (a \circ b) * (a \circ c) \quad \text{és} \quad (b * c) \circ a = (b \circ a) * (c \circ a).$$

1.2. Definíció. Legyen R egy nemüres halmaz, amelyen kettő kétváltozós művelet is értelmezve van, nevezzük az egyiket összeadásnak, a másikat szorzásnak. Azt mondjuk, hogy az $(R; +, \cdot)$ struktúra **gyűrű**, ha

1. $(R; +)$ Abel-csoport,
2. $(R; \cdot)$ félcsoport,
3. a szorzás disztributív az összeadásra.

$$\forall a \in R: a + 0 = a$$

1.3. Tétel. Ha $(R; +, \cdot)$ gyűrű, akkor minden $a \in R$ esetén $a \cdot 0 = 0 \cdot a = 0$.

Bizonyítás. $a \cdot 0 = b$

$$\begin{aligned} b + b &= a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = b \quad / + (-b) \\ b &= 0 \quad \checkmark \end{aligned}$$

□

1.4. Definíció.

- **Kommutatív gyűrű:** olyan R gyűrű, amelyben nemcsak az összeadás, hanem a szorzás is kommutatív:

$$\forall a, b \in R: a \cdot b = b \cdot a.$$

- **Egységelemes gyűrű:** olyan R gyűrű, amelyben nemcsak additív, de **multiplikatív egységelem** is létezik (jelölése: 1):

$$\forall a \in R: a \cdot 1 = 1 \cdot a = a.$$

- **Zérusosztómentes gyűrű:** olyan R gyűrű, amelyben

$$\forall a, b \in R: ab = 0 \implies a = 0 \text{ vagy } b = 0.$$

1.5. Definíció. A kommutatív, egységelemes, zérusosztómentes gyűrűket **integritástományoknak** nevezzük.

1.6. Tétel. Integritástományban lehet nemzéró elemmel egyszerűsíteni:

$$\forall a, b, c \in R: \text{ha } c \neq 0, \text{ akkor } a \cdot \cancel{c} = b \cdot \cancel{c} \implies a = b.$$

Bizonyítás.

$$a \cdot c = b \cdot c \implies a \cdot c - b \cdot c = 0$$

$$\implies (a - b) \cdot c = 0$$

$$\overset{\text{zón}}{\implies} a - b = \overset{0}{0} \implies a = b \quad \square$$

1.7. Definíció. **Testnek** nevezünk egy $(T; +, \cdot)$ gyűrűt, ha $(T \setminus \{0\}; \cdot)$ Abel-csoport (ebből következik, hogy T integritástomány és $|T| \geq 2$).

Checklist. *számtól es etel*

0. $+$ és $\cdot$ műveletek a nemüres R halmazon

$$R \text{ zárt } +, \cdot \text{ ra}$$

~~1. $+$ asszociatív~~

2. van additív egységelem (jelölés: 0) $0 \in R$

3. mindenkinek van additív inverze (jelölés: $-a$)

$$R \text{ zárt } - \text{ ra}$$

~~4. $+$ kommutatív~~

~~5. $\cdot$ asszociatív~~

~~6. $\cdot$ disztributív $+$ ra~~

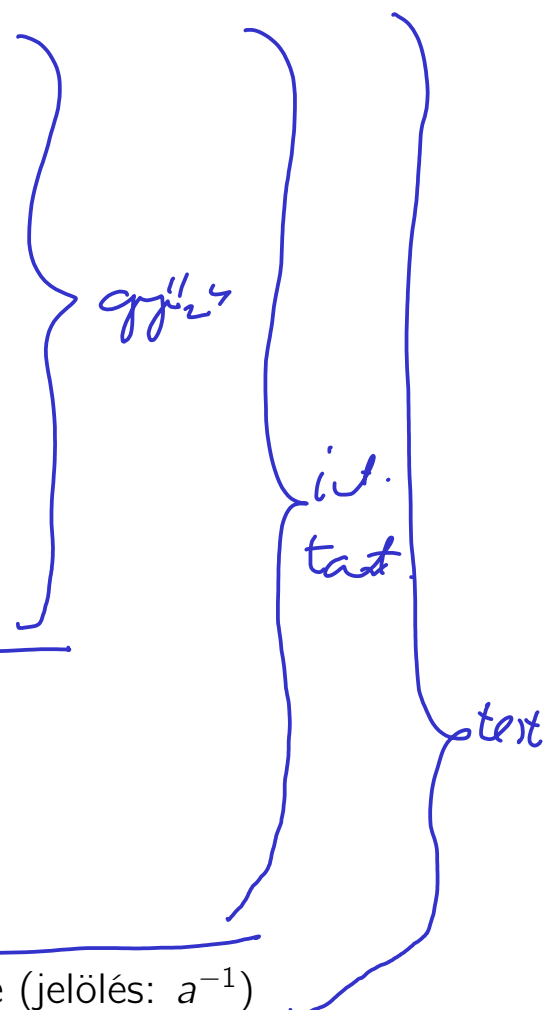
~~7. $\cdot$ kommutatív~~

8. van multiplikatív egységelem (jelölés: 1) $1 \in R$

~~9. nincsenek zérusosztók~~

10. minden nemnulla elemnek van multiplikatív inverze (jelölés: a^{-1})

$$\forall a \in R \setminus \{0\}: a^{-1} \in R$$



gyűrű

integritástartomány

$\mathbb{Z}[x]$ $\mathbb{R}[x]$ $\mathbb{Q}[x]$ $\mathbb{Q}[x]$

test

$\mathbb{Q}$

$\mathbb{R}$

$\mathbb{C}$

$\mathbb{Z}_7$ $\mathfrak{f}$

$(\mathbb{Z}_7^* = \mathbb{Z}_7 \setminus \{0\})$

$\mathbb{Z}$

$\mathbb{Z}[i]$

$\mathbb{P}^5$

$\mathbb{R}^{2 \times 2}$

$\mathbb{N}_0$

$\mathbb{Z}_6$
 $(\bar{2} \cdot \bar{3} = \bar{0})$

$\mathbb{P}H$

1.8. Feladat. Gyűrűt, integritástartományt, testet alkotnak-e az alábbi halmazok a szokásos összeadással és szorzással?

(a) $\mathbb{N}_0$

(g) páros számok

(b) $\mathbb{Z}$

(h) páratlan számok

(c) $\mathbb{Q}$

(i) $\mathbb{Z}_6$

(d) $\mathbb{R}$

(j) $\mathbb{Z}_7$

(e) $\mathbb{C}$

(k) $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ (**Gauss-egészek**)

(f) $\mathbb{R}^{2 \times 2}$

1.9. Tétel.

- (1) Minden $m \geq 2$ egész szám esetén $\mathbb{Z}_m$ egységelemes kommutatív gyűrű.
- (2) Ha m prímszám, akkor $\mathbb{Z}_m$ test.
- (3) Ha m összetett szám, akkor $\mathbb{Z}_m$ még csak nem is integritástartomány.

Bizonyítás.

- (1) Világos.
- (2) Tudjuk, hogy inverze pontosan a redukált maradékosztályoknak van.
Ha m prímszám, akkor $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{\bar{0}\}$.
- (3) Ha m összetett szám, akkor $m = ab$, ahol $1 < a, b < m$.
Ekkor $\bar{a}$ és $\bar{b}$ zérusosztók $\mathbb{Z}_m$ -ben: $\bar{a} \cdot \bar{b} = \overline{ab} = \bar{m} = \bar{0}$, pedig $\bar{a}, \bar{b} \neq \bar{0}$.

□

Időutazás!

1.10. Tétel. Ha R integritástartomány, akkor az R feletti polinomok $R[x]$ halmaza is integritástartomány a polinomok szokásos összeadásával és szorzásával.

$$5x^3 + 3x^2 - 7x + 6 \in \mathbb{R}[x]$$

$$x, 2, 5, 8, 7, 9, -7$$

$$(2 \cdot x \cdot x + 5) \cdot (8 \cdot x \cdot x \cdot x + 9) - 7 \cdot x$$

2. A polinom fogalma

A polinom receptje.

Végy

- egy **határozatlant**: x ;

- **együtthatókat**: egy R integritástartományból néhány elemet,

majd jól keverd őket össze az összeadás (kivonás) és szorzás műveletével.

2.1. Definíció. Az R integritástartomány feletti **polinomnak**

$$f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

alakú **formális kifejezést** nevezünk, ahol

- x **határozatlan**;
- az $a_0, a_1, a_2, \dots, a_n \in R$ elemek az f polinom **együtthatói**.

Az általánosság megszorítása nélkül tfh. $a_n \neq 0$. Ekkor

- az f polinom **fokszáma**: $\deg f = n$;
- az f polinom **főegyütthatója**: a_n .

$$\deg 0 = -\infty$$

Speciális polinomok:

- **főpolinom**: $a_n = 1$, azaz $f = x^n + a_{n-1}x^{n-1} + \dots + a_2x^2 + a_1x + a_0$;
- **konstans polinom**: $\deg f \leq 0$, azaz $f = a_0$.

Jelölés. Az R integritástartomány feletti polinomok halmazát $R[x]$ jelöli.

Polinomok összegét és szorzatát „természetes módon” definiáljuk (lásd az előadásvázlatban és a videóban).

2.2. Tétel. Tetszőleges $f, g \in R[x]$ polinomokra

$$\deg(f + g) \leq \max(\deg f, \deg g) \quad \text{és} \quad \deg(fg) = \deg f + \deg g.$$

$$-\infty \geq -\infty + \deg g$$
$$\deg(0g) = \deg 0 + \deg g$$

2.3. Tétel. A fent (nem) definiált összeadással és szorzással $R[x]$ integritástartomány.

2.4. Definíció. Az $R[x]$ gyűrűt az R feletti egyhatározatlanú polinomok gyűrűjének, röviden R feletti **polinomgyűrűnek** nevezzük.

3. A polinomok „számelmélete”

$$T = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$$

Megállapodás. Mostantól T mindig tetszőleges testet jelöl, és – hacsak mást nem mondunk – minden polinomot ezen test felett tekintünk.

3.1. Definíció. Legyenek $f, g \in T[x]$ polinomok a T test felett.

• **oszthatóság:** $f \mid g \iff \exists h \in T[x]: g = f \cdot h$.

• **asszociáltság:** $f \sim g \iff f \mid g$ és $g \mid f$.

• **legnagyobb közös osztó:** $d \sim \text{lko}(f, g)$, ha

KO: $d \mid f$ és $d \mid g$;

LN: $\forall k \in T[x]: (k \mid f \text{ és } k \mid g) \implies k \mid d$.

• **legkisebb közös többszörös:** $t \sim \text{lkkt}(f, g)$, ha

KT: $f \mid t$ és $g \mid t$;

LN: $\forall k \in T[x]: (f \mid k \text{ és } g \mid k) \implies t \mid k$.

3.2. Tétel. A $T[x]$ polinomgyűrűn az oszthatósági reláció rendelkezik az alábbi tulajdonságokkal:

(1) reflexív;

(2) tranzitív;

(3) $\forall f, g \in T[x]: f \sim g \iff \exists c \in T \setminus \{0\}: g = cf$;

(4) $\forall f, g \in T[x]: f \mid g \text{ és } g \neq 0 \implies \deg f \leq \deg g$.

$$2x^3 + 5x^2 + 4x + 2 = 2(x^3 + \frac{5}{2}x^2 + 2x + 1) \\ \sim 1x^3 + \frac{5}{2}x^2 + 2x + 1$$

3.3. Tétel.

(1) Az asszociáltság ekvivalenciareláció $T[x]$ -en.

(2) A nulla osztályát kivéve minden asszociáltsági osztály tartalmaz pontosan egy főpolinomot.

(3) Az lko és az lkkt asszociáltság erejéig egyértelmű.

3.4. Tétel (a maradékos osztás tétele). Ha $f, g \in T[x]$ és $g \neq 0$, akkor léteznek olyan egyértelműen meghatározott q és $r \in T[x]$ polinomok, amelyekre

$$f = qg + r \quad \text{és} \quad \deg r < \deg g.$$

Ebben a maradékos osztásban

- f az **osztandó**;
- g az **osztó**;
- q a **hányados**;
- r a **maradék**.

3.5. Feladat. Osszuk el maradékosan az f polinomot a g polinommal az $\mathbb{R}[x]$ polinomgyűrűben.

$$\begin{array}{l} f = x^3 - 2, \quad g = x^2 - 2x + 1 \quad \deg r \leq 1 \\ (x^3 - 2) : (x^2 - 2x + 1) = x + 2 \\ \begin{array}{r} \ominus x^3 - 2x^2 + x \\ \hline 2x^2 - x - 2 \\ \ominus 2x^2 - 4x + 2 \\ \hline 3x - 4 \\ \hline \end{array} \end{array}$$

$$\begin{aligned} 2.1(f) : f &= 4x^4 + 2x^3 + x^2 + x + 2 \in \mathbb{Z}_5[x] \\ g &= 2x^4 + 3x^2 + 1 \in \mathbb{Z}_5[x] \\ g &= qf + r \quad \deg r \leq 3 \end{aligned}$$

$$\begin{array}{l} (2x^4 + 3x^2 + 1) : (4x^4 + 2x^3 + x^2 + x + 2) = 3 \\ \begin{array}{r} 2 \quad 1 \quad 1 \quad 1 \quad 1 \\ 12x^4 + 6x^3 + 3x^2 + 3x + 6 \\ \hline -10x^4 \quad 4x^3 \quad + 2x \end{array} \end{array}$$

3.6. Tétel. Bármely két $f, g \in T[x]$ polinomnak létezik legnagyobb közös osztója és legkisebb közös többszöröse. A legnagyobb közös osztó kiszámítható az **euklideszi algoritmus**sal, és kifejezhető f és g „lineáris kombinációjaként”:

$$\exists u, v \in T[x]: fu + gv = \text{Inko}(f, g).$$

3.7. Tétel. Tetszőleges nemzéró $f, g, h \in T[x]$ polinomok esetén az $fu + gv = h$ egyenlet akkor és csak akkor oldható meg az ismeretlen $u, v \in T[x]$ polinomokra nézve, ha $\text{Inko}(f, g) \mid h$:

$$\exists u, v \in T[x]: fu + gv = h \iff \text{Inko}(f, g) \mid h.$$

Handwritten note: $ax + by = c$ van megoldása $\iff \text{hh}(a, b) \mid c$

3.8. Definíció. Tetszőleges $f, g, m \in T[x]$ esetén azt mondjuk, hogy f **kongruens** g -vel modulo m , ha $m \mid f - g$

$$f \equiv g \pmod{m} \iff m \mid f - g.$$

3.9. Tétel. A modulo m kongruencia ekvivalenciareláció $T[x]$ -en, és két polinom akkor és csak akkor kongruens modulo m , ha ugyanazt a maradékot adják m -mel osztva.

3.10. Tétel. Tetszőleges $f, g, h \in T[x]$ esetén az $fu \equiv h \pmod{m}$ lineáris kongruencia akkor és csak akkor oldható meg (az u ismeretlen polinomra nézve), ha $\text{Inko}(f, m) \mid h$:

$$\exists u \in T[x]: fu \equiv h \pmod{m} \iff \text{Inko}(f, m) \mid h.$$

Handwritten note: $ax \equiv b \pmod{m}$ van megoldása $\iff \text{hh}(a, m) \mid b$

3.11. Definíció. Legyen $m \in T[x]$ legalább elsőfokú polinom.

- modulo m **maradékosztály**: $\bar{f} = \{ g \in T[x] : f \equiv g \pmod{m} \}$
- a maradékosztályok halmaza: $T[x]/\langle m \rangle = \{ \bar{f} : f \in T[x] \}$ *$\mathbb{Z}_n = \mathbb{Z}/\langle n \rangle$*
- műveletek: $\bar{f} + \bar{g} = \overline{f + g}$, $-\bar{g} = \overline{-g}$, $\bar{f} \cdot \bar{g} = \overline{f \cdot g}$

3.12. Tétel. A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (additív inverze, szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik elemet választjuk reprezentánsnak, és ezekkel a műveletekkel $T[x]/\langle m \rangle$ kommutatív egységelemes gyűrűt alkot (modulo m **maradékosztály-gyűrű**).

3.13. Tétel. Az $\bar{f} \in T[x]/\langle m \rangle$ maradékosztálynak akkor és csak akkor létezik multiplikatív inverze, ha $\text{Inko}(f, m) \sim 1$. Ilyenkor a multiplikatív inverz egyértelműen meghatározott.

3.14. Feladat. Határozzuk meg az f és g valós polinomok legnagyobb közös osztóját, és adjuk meg az $fu + gv = \text{lko}(f, g)$ egyenlet egy megoldását.

$$f = x^4 + 2x^3 - x^2 - 4x - 2, \quad g = x^4 + x^3 - x^2 - 2x - 2$$

mp.

$$\overbrace{(x^4 + 2x^3 - x^2 - 4x - 2)}^f : \overbrace{(x^4 + x^3 - x^2 - 2x - 2)}^g = 1$$

$$\begin{array}{r} x^4 + x^3 - x^2 - 2x - 2 \\ \hline x^3 \quad -2x \end{array}$$

$$\textcircled{1} f = 1 \cdot g + (x^3 - 2x)$$

$$\overbrace{(x^4 + x^3 - x^2 - 2x - 2)}^g : (x^3 - 2x) = x + 1$$

$$\begin{array}{r} x^4 \quad -2x^2 \\ \hline x^3 + x^2 - 2x - 2 \\ x^3 \quad -2x \\ \hline x^2 \quad -2 \end{array}$$

$$\textcircled{2} g = (x+1) \cdot (x^3 - 2x) + x^2 - 2$$

$$x^2 - 2 \sim \text{lko}(f, g)$$

$$(x^3 - 2x) : (x^2 - 2) = x$$

$$\begin{array}{r} x^3 - 2x \\ \hline 0 \end{array}$$

$$\text{lko}(f, g) \sim x^2 - 2 \stackrel{\textcircled{2}}{=} g - (x+1) \cdot \underbrace{(x^3 - 2x)}_{f-g} \stackrel{\textcircled{1}}{=} g - (x+1)(f-g)$$

$$= \underbrace{(-x-1)}_u \cdot f + \underbrace{(x+2)}_v \cdot g$$

$$f = (x^2 - 2) \cdot (x^2 + x + 1) \quad f \text{ zérói: } \pm\sqrt{2}, -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$$

$$g = (x^2 - 2) \cdot (x^2 + 2x + 1) \quad g \text{ zérói: } \pm\sqrt{2}, -1, -1$$



3.15. Feladat. Határozzuk meg az f és g valós polinomok legnagyobb közös osztóját, és adjuk meg az $fu + gv = \text{lko}(f, g)$ egyenlet egy megoldását.

$$f = x^3 - 2, \quad g = x^2 - 2x + 1$$

$$\begin{array}{r} \overbrace{(x^3 - 2)}^f : \overbrace{(x^2 - 2x + 1)}^g = x + 2 \\ \underline{x^3 - 2x^2 + x} \\ 2x^2 - x - 2 \\ \underline{2x^2 - 4x + 2} \\ 3x - 4 \end{array}$$

$$\textcircled{1} f = (x+2)g + (3x-4)$$

$$\begin{array}{r} \overbrace{(x^2 - 2x + 1)}^g : \overbrace{(3x - 4)}^f = \frac{1}{3}x - \frac{2}{9} \\ \underline{x^2 - \frac{4}{3}x} \\ -\frac{2}{3}x + 1 \\ \underline{-\frac{2}{3}x + \frac{8}{9}} \\ \frac{1}{9} \end{array}$$

$\frac{1}{9} \sim 1 \sim \text{lko}(f, g)$

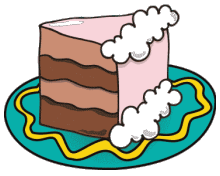
$$\textcircled{2} g = \left(\frac{1}{3}x - \frac{2}{9}\right) \cdot (3x - 4) + \frac{1}{9}$$

$$\text{lko}(f, g) \sim 1 \stackrel{\textcircled{2}}{=} gg - (3x-2) \cdot \underbrace{(3x-4)}_{f-(x+2)g} \stackrel{\textcircled{1}}{=} gg - (3x-2)(f-(x+2)g)$$

$$= gg - (3x-2) \cdot f + (3x-2) \cdot (x+2)g$$

$$= (-3x+2) \cdot f + (g + 3x^2 + 4x - 4)g$$

$$= \underbrace{(-3x+2)}_u \cdot f + \underbrace{(3x^2 + 4x + 5)}_v \cdot g$$



$$\frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} + 1} = \frac{1}{g(\sqrt[3]{2})}$$

$$f(\sqrt[3]{2}) = 0$$

$$(-3x + 2) \cdot f(x) + (3x^2 + 4x + 5) \cdot g(x) = 1$$

$$\underbrace{(-3\sqrt[3]{2} + 2) \cdot \underbrace{f(\sqrt[3]{2})}_0}_{0} + \underbrace{(3 \cdot \sqrt[3]{4} + 4\sqrt[3]{2} + 5) \cdot g(\sqrt[3]{2})}_{\frac{1}{g(\sqrt[3]{2})}} = 1 \quad x = \sqrt[3]{2}$$

$$\frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} + 1} = 3 \cdot \sqrt[3]{4} + 4 \cdot \sqrt[3]{2} + 5$$

3.16. Feladat. Készítsük el meg a $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$ maradékosztály-gyűrűben az összeadás és a szorzás művelettáblázatát.

$$\begin{aligned} \mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle &= \{ \bar{f} \mid f \in \mathbb{Z}_2[x] \} \\ &= \{ \bar{f} \mid f \in \mathbb{Z}_2[x], \deg f \leq 1 \} = \\ &= \{ \overline{ax+b} \mid a, b \in \mathbb{Z}_2 \} = \\ &= \{ \bar{0}, \bar{1}, \bar{x}, \overline{x+1} \} \end{aligned} \quad \left| \quad \begin{aligned} \mathbb{Z}_4 &= \{ \bar{a} \mid a \in \mathbb{Z} \} = \\ &= \{ \bar{0}, \bar{1}, \bar{2}, \bar{3} \} \end{aligned} \right.$$

+	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

||S
V

.	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

GALOIS FIELD



$$\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle = \text{GF}(4)$$

lent e? IGEN

$$\bar{1}^{-1} = \bar{1}$$

$$\bar{x}^{-1} = \overline{x+1}$$

$$\overline{x+1}^{-1} = \bar{x}$$

$x^2 + x + 1$ irreducibilis: $\mathbb{Z}_2$ feletti

$$x^2 \equiv 1 \pmod{x^2 + x + 1}$$

$$x^2 : (x^2 + x + 1) = 1$$

$$\begin{array}{r} x^2 + x + 1 \\ -x - 1 \\ \hline x + 1 \end{array}$$

$$(x^2 + x) : (x^2 + x + 1) = 1$$

$$\begin{array}{r} x^2 + x + 1 \\ -x - 1 \\ \hline -1 = 1 \end{array}$$

3.17. Feladat. Határozzuk meg az $\bar{f}$ maradékosztály multiplikatív inverzét a $\mathbb{Z}_5[x]/\langle m \rangle$ maradékosztály-gyűrűben. Hány eleme van ennek a gyűrűnek?

$$f = 2x^2 - 3x + 2, \quad m = x^3 + 1$$

pr. $\mathbb{Z}_5[x]/\langle x^3+1 \rangle = \{ \bar{f} \mid f \in \mathbb{Z}_5[x], \deg f \leq 2 \} =$
 $= \{ \overline{ax^2 + bx + c} \mid a, b, c \in \mathbb{Z}_5 \}$

$$5 \cdot 5 \cdot 5 = 125 \text{ eleme van}$$

$$\bar{f}^{-1} = \bar{u} \Leftrightarrow \bar{f} \cdot \bar{u} = \bar{1} \Leftrightarrow f \cdot u \equiv 1 \pmod{m} \Leftrightarrow m \mid f \cdot u - 1 \Leftrightarrow$$

$$\Leftrightarrow f \cdot u - 1 = m \cdot v \quad (\exists v \in \mathbb{Z}_5[x])$$

$$f \cdot u - m \cdot v = 1 \sim \text{hb}(f, m)$$

$$\overbrace{(x^3+1)}^m : \overbrace{(2x^2-3x+2)}^f = 3x+2$$

$$\begin{array}{r} x^3 + x^2 + x \\ \underline{4x^2 + 4x + 1} \\ 4x^2 + 4x + 4 \\ \underline{} \\ 2 \end{array}$$

$$\textcircled{1} \quad m = (3x+2) \cdot f + 2$$

$$2 \sim 1 \sim \text{hb}(f, m)$$

$$\textcircled{2} \quad 2 = m - (3x+2) \cdot f \quad / \cdot 3$$

$$1 = 3m - (9x+6) \cdot f$$

$$1 = \underbrace{3m}_{-v} + \underbrace{(x+4) \cdot f}_u$$

$$\bar{f}^{-1} = \overline{2x^2 - 3x + 2}^{-1} = \overline{x + 4}$$

4. Polinomfüggvények, gyökök

4.1. Definíció. Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinom.

- Az f polinom $c \in T$ helyen vett **helyettesítési értéke**:

$$f(c) = a_n c^n + \dots + a_1 c + a_0 \in T.$$

- Az f polinomhoz tartozó **polinomfüggvény**:

$$f: T \rightarrow T, c \mapsto f(c).$$

- A $c \in T$ elem **gyöke** az $f \in T[x]$ polinomnak, ha $f(c) = 0$.

4.2. Példa. Az $f = x^2 \in \mathbb{Z}_2[x]$ és $g = x^3 \in \mathbb{Z}_2[x]$ polinomokhoz ugyanaz a polinomfüggvény tartozik:

$$\mathbb{Z}_2 \rightarrow \mathbb{Z}_2, \quad \bar{0} \mapsto \bar{0}, \bar{1} \mapsto \bar{1}.$$

gyözteljesítés

4.3. Tétel (Bézout tétele). Bármely $f \in T[x]$ és $\alpha \in T$ esetén

$$f(\alpha) = 0 \iff x - \alpha \mid f. \iff f = (x - \alpha) \cdot (\dots)$$

Bizonyítás. Osszuk el f -et maradékosan $(x - \alpha)$ -val.

$$f = (x - \alpha) \cdot q + r$$

$\deg r < 1$, azaz r konstans

$$x = \alpha: f(\alpha) = \underbrace{(\alpha - \alpha)}_0 \cdot q(\alpha) + r$$

$$f(\alpha) = r$$

$$f(\alpha) = 0 \iff r = 0 \iff x - \alpha \mid f$$

□

4.4. Következmény. Tetszőleges $f, g \in T[x]$ polinomok esetén f és g közös gyökei ugyanazok, mint $\underbrace{\text{Inko}(f, g)}_d$ gyökei.

Bizonyítás.

$$f(\alpha) = 0 \wedge g(\alpha) = 0 \xrightarrow{B} x - \alpha \mid f \wedge x - \alpha \mid g$$

$$\iff x - \alpha \mid d$$

$$\iff d(\alpha) = 0$$

□

4.5. Következmény. Ha $f \in T[x]$ és $\alpha_1, \dots, \alpha_k \in T$ páronként különböző elemek, akkor

$$f(\alpha_1) = \dots = f(\alpha_k) = 0 \iff (x - \alpha_1) \cdot \dots \cdot (x - \alpha_k) \mid f.$$

Bizonyítás. $\boxed{\Leftarrow}$ $f = (x - \alpha_1) \cdot \dots \cdot (x - \alpha_k) \cdot (\dots)$

$$f(\alpha_1) = \underbrace{(\alpha_1 - \alpha_1)}_0 \cdot \dots \cdot (\alpha_1 - \alpha_k) \cdot (\dots) = 0$$

$$\boxed{\Rightarrow} f(\alpha_1) = 0 \stackrel{B}{\Rightarrow} f = (x - \alpha_1) \cdot f_1$$

$$f(\alpha_2) = 0 \Rightarrow 0 = \underbrace{(\alpha_2 - \alpha_1)}_{\neq 0} \cdot \underbrace{f_1(\alpha_2)}_0 \stackrel{B}{\Rightarrow} f_1 = (x - \alpha_2) \cdot f_2$$

$$\Rightarrow f = (x - \alpha_1) \cdot (x - \alpha_2) \cdot f_2$$

$$f(\alpha_3) = 0 \Rightarrow 0 = \underbrace{(\alpha_3 - \alpha_1)}_{\neq 0} \cdot \underbrace{(\alpha_3 - \alpha_2)}_{\neq 0} \cdot \underbrace{f_2(\alpha_3)}_0 \stackrel{B}{\Rightarrow} f_2 = (x - \alpha_3) \cdot f_3 \quad \square$$

4.6. Következmény. Ha a **nemnulla** $f \in T[x]$ polinom fokszáma n , akkor legfeljebb n különböző gyöke van a T testben.

Bizonyítás. Legyen $\alpha_1, \alpha_2, \dots, \alpha_k$ az összes gyök f -vel.

$$(x - \alpha_1) \cdot \dots \cdot (x - \alpha_k) \mid f$$

$$\deg((x - \alpha_1) \cdot \dots \cdot (x - \alpha_k)) \leq \deg f$$

$$\begin{aligned} &\mathbb{Z}_8 \text{ nem test} \\ &f = x^2 - 1 \in \mathbb{Z}_8[x] \\ &\text{gyökei: } 1, 3, 5, 7 \end{aligned} \quad \square$$

4.7. Definíció. Azt mondjuk, hogy az $f \in T[x]$ polinomnak az $\alpha \in T$ elem **k -szoros gyöke**, ha

$$(x - \alpha)^k \mid f \text{ de } (x - \alpha)^{k+1} \nmid f.$$

A k számot az α gyök **multiplicitásának** nevezzük.

4.8. Megjegyzés. Megengedjük a $k = 0$ esetet is: α pontosan akkor nullaszoros gyök, ha nem gyök.

4.9. Feladat. Hányszoros gyöke $c = 2$ az $f = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8 \in \mathbb{R}[x]$ polinomnak?

$$(x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8) : (x - 2) = x^4 - 3x^3 + x^2 + 4$$

$$\begin{array}{r} x^5 - 2x^4 \\ \hline -3x^4 + 7x^3 - 2x^2 + 4x - 8 \end{array}$$

$$\begin{array}{r} -3x^4 + 6x^3 \\ \hline \end{array}$$

$$\begin{array}{r} x^3 - 2x^2 + 4x - 8 \\ \hline \end{array}$$

$$\begin{array}{r} x^3 - 2x^2 \\ \hline \end{array}$$

$$\begin{array}{r} 4x - 8 \\ \hline \end{array}$$

$$\begin{array}{r} 4x - 8 \\ \hline \end{array}$$

$$\begin{array}{r} 0 \end{array}$$

$$f = (x - 2) \cdot \underbrace{(x^4 - 3x^3 + x^2 + 4)}_q + \underbrace{0}_{r = f(2)}$$

$$(x^4 - 3x^3 + x^2 + 4) = (x - 2) \cdot (\dots)$$

$$(1 \cdot x^5 - 5 \cdot x^4 + 7 \cdot x^3 - 2 \cdot x^2 + 4 \cdot x - 8) : (x - 2) = 1 \cdot x^4 - 3 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 4$$

$$\begin{array}{r} 1 \cdot x^5 - 2 \cdot 1 \cdot x^4 \\ \hline -3 \cdot x^4 + 7 \cdot x^3 - 2 \cdot x^2 + 4 \cdot x - 8 \\ -3 \cdot x^4 - 2 \cdot (-3) \cdot x^3 \\ \hline 1 \cdot x^3 - 2 \cdot x^2 + 4 \cdot x - 8 \\ 1 \cdot x^3 - 2 \cdot 1 \cdot x^2 \\ \hline 0 \cdot x^2 + 4 \cdot x - 8 \\ 0 \cdot x^2 - 2 \cdot 0 \cdot x \\ \hline 4 \cdot x - 8 \\ 4 \cdot x - 2 \cdot 4 \\ \hline 0 \end{array}$$

$-5 + 2 \cdot 1$ $7 + 2 \cdot (-3)$ $-2 + 2 \cdot 1$ $4 + 2 \cdot 0$

$$f = (x - 2) \cdot \underbrace{(1 \cdot x^4 - 3 \cdot x^3 + 1 \cdot x^2 + 0 \cdot x + 4)}_q + \underbrace{0}_{r = f(2)}$$

	1	-5	7	-2	4	-8
2	1	-3	1	0	4	0

	...			...
C	...			...

HORNER - Schema

$$C \cdot \text{flower} + \text{tulip}$$

	1	-5	7	-2	4	-8
2	1	-3	1	0	4	0
2	1	-1	-1	-2		0
2	1	1	1			0
2	1	3	7			

$$f = (x-2) \cdot (1x^4 - 3x^3 + 1x^2 + 0x + 4)$$

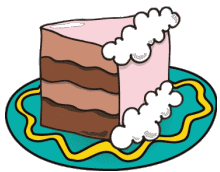
$$(x-2) \cdot (1x^3 - 1x^2 - 1x - 2)$$

$$f = (x-2)^2 \cdot (x^3 - x^2 - x - 2)$$

$$(x-2) \cdot (1x^2 + 1x + 1)$$

$$f = (x-2)^3 \cdot (x^2 + x + 1)$$

$c=2$ f-vel legnagyobb mérete



f mérete: $2, 2, 2, -\frac{1}{2} \pm \frac{\sqrt{3}}{2} i$

4.10. Feladat. Hányszoros gyöke $c = \bar{2}$ az $f = x^4 + 2x + \bar{3} \in \mathbb{Z}_5[x]$ polinomnak?

	1	0	0	2	3
2	1	2	4	0	3

 $f(\bar{2}) = \bar{3}$

$c = \bar{2}$ nem is gyöke f -nek!
(nullas+oszo gyök)

4.11. Feladat. Hányszoros gyöke $c = \bar{3}$ az $f = x^4 + 2x + \bar{3} \in \mathbb{Z}_5[x]$ polinomnak?

pp.

	1	0	0	2	3
3	1	3	4	4	0
3	1	1	2	0	
3	1	4	4		
3	1				
3	1				

$$f = (x-3) \cdot (x^3 + 3x^2 + 4x + 4)$$

$$= (x-3)^2 \cdot \underbrace{(x^2 + x + 2)}_g$$

$$g(3) = 4$$

$c = \bar{3}$ f -nek kétszeres gyöke

5. Irreducibilis polinomok

Emlékeztető. A polinomokat egy tetszőleges T test felett tekintjük (pl. $T = \mathbb{C}$, $T = \mathbb{R}$, $T = \mathbb{Q}$, $T = \mathbb{Z}_p$).

5.1. Definíció. Az $f \in T[x]$ polinom **irreducibilis**, ha legalább elsőfokú, és csak úgy bontható két polinom szorzatára, hogy az egyik tényező asszociált f -hez. Ekkor a másik tényező szükségképpen asszociált 1-hez; ilyenkor **triviális faktORIZÁCIÓRÓL** beszélünk. Formálisan:

$$\forall g, h \in T[x]: f = gh \implies (g \sim f \text{ vagy } h \sim f).$$

$h \sim 1 \quad g \sim 1$

5.2. Definíció. Az $f \in T[x]$ polinom **prím**, ha legalább elsőfokú, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$\forall g, h \in T[x]: f \mid gh \implies (f \mid g \text{ vagy } f \mid h).$$

5.3. Tétel. Test feletti polinomokra az irreducibilitás és a prímtulajdonság ekvivalens.

5.4. Tétel. Minden legalább elsőfokú T feletti polinom felbontható irreducibilis polinomok szorzatára. Ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelműen meghatározott, azaz ha $p_1 \dots p_n$ és $q_1 \dots q_m$ ugyanazon polinom két irreducibilis faktorizációja, akkor $n = m$, és létezik olyan $\pi \in S_n$ permutáció, hogy $p_i \sim q_{\pi(i)}$ minden $i = 1, \dots, n$ esetén.

5.5. Tétel. Egy legalább elsőfokú $f \in T[x]$ polinom akkor és csak akkor irreducibilis, ha f nem bontható $\deg f$ -nél kisebb fokszámú polinomok szorzatára.

Bizonyítás. Ha test feletti polinomokról van szó, akkor a felbontás (nem)triviális volta csak a fokszámoktól függ:

- $f = gh$ triviális felbontás, ha $\deg g = \deg f$ és $\deg h = 0$, vagy fordítva;
- $f = gh$ nemtriviális felbontás, ha $1 \leq \deg g, \deg h < \deg f$. □

$T[x]$ -ben $\underbrace{2x}_f = \underbrace{2}_g \cdot \underbrace{x}_h$ $2 \nmid 1 \quad 1 \nmid 2$ de $2 \nmid 1$
 $x \nmid f \quad x \nmid 2x$ de $2x \nmid x$

5.6. Tétel. Az elsőfokú polinomok bármely test felett irreducibilisek.

$f = \underset{\neq 0}{a}x + b = 0 \quad \alpha = -\frac{b}{a} \quad f(\alpha) = 0 \quad ax + b = a \cdot \left(x + \frac{b}{a}\right) \sim x - \left(-\frac{b}{a}\right) = x - \alpha$

5.7. Tétel. Ha $f \in T[x]$ irreducibilis és $\deg f \geq 2$, akkor f -nek nincs gyöke.

Bizonyítás. Tlh. f irr. $\exists \alpha \in T: f(\alpha) = 0$

Bérount: $f = \underbrace{(x - \alpha)}_{\substack{1 \\ \wedge \\ n}} \cdot \underbrace{(\dots)}_{\substack{n-1 \\ \wedge \\ n}}$ nemtriv. felb. $\nexists f$ irr.

□

5.8. Tétel. Ha $f \in T[x]$ és $2 \leq \deg f \leq 3$, akkor f pontosan akkor irreducibilis, ha nincs gyöke.

Bizonyítás. irr. $\Rightarrow \nexists$ gyöke.

$\nexists$ gyöke $\stackrel{?}{\Rightarrow}$ irr.

$f = g \cdot h$ nemtriv. felb.

$$\left. \begin{array}{l} 2 = \textcircled{1} + \textcircled{1} \times \\ 3 = \textcircled{1} + 2 \times \\ 3 = 2 + \textcircled{1} \times \end{array} \right\} \Rightarrow f \text{ irr.}$$

pl. $T = \mathbb{R}, f = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$

$f = (x^2 + 1) \cdot (x^2 + 1)$ nem irr, pedig $\nexists$ gyöke $\mathbb{R}$ -ben

□

5.9. Feladat. Bontsuk irreducibilis tényezők szorzatára az alábbi polinomot.

$$f = x^6 + 3x^4 - x^3 + 2x^2 + x - 1 \in \mathbb{Z}_5[x]. \quad \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

$$f(0) = -1 = 4 \neq 0$$

	1	0	3	-1	2	1	-1
1	1	1	4	3	0	1	0 = f(1)
1	1	2	1	4	4	0	
1	1	3	4	3	2		
2	1	4	4	2	3		
3	1	0	1	2	0		
3	1	3	0	2			
4	1	4	2	0			
4	1	3	4				

$$f = (x-1) \cdot (x^5 + x^4 + 4x^3 + 3x^2 + 1)$$

$$= (x-1)^2 \cdot (x^4 + 2x^3 + x^2 + 4x + 4)$$

$$= (x-1)^2 \cdot (x-3) \cdot (x^2 + x + 2)$$

$$f = (x-1)^2 \cdot (x-3) \cdot (x-4) \cdot (x^2 + 4x + 2)$$

nincs több
és az utolsó
⇒ irr.

5.10. Feladat. Bontsuk irreducibilis tényezők szorzatára az alábbi polinomot.

$$f = x^4 + x^2 + 1 \in \mathbb{Z}_2[x]. \quad \mathbb{Z}_2 = \{0, 1\}$$

pp. $f(0) = 1, f(1) = 1 + 1 + 1 = 1$

f -re, min möre

$$f = g \cdot h$$

$$4 = 1 + 3$$

$$4 = 3 + 1$$

$$4 = \underset{\substack{\uparrow \\ \text{irr.}}}{2} + \underset{\substack{\uparrow \\ \text{irr.}}}{2}$$

$$\left[\begin{array}{l} g = x^2 + 1 \quad g(0) = 1 \quad g(1) = 1 + 1 = 2 = 0 \\ = (x+1)^2 = x^2 + 2x + 1 \end{array} \right]$$

$$g = x^2 + x + 1 \quad g(0) = 1, g(1) = 1 + 1 + 1 = 1$$

$$h = x^2 + x + 1$$

$$f = (x^2 + x + 1)^2 = x^4 + x^2 + 1$$

5.11. Feladat. Bontsuk irreducibilis tényezők szorzatára az alábbi polinomot.

$$f = x^4 + x + 1 \in \mathbb{Z}_2[x].$$

$$f(0) = 1, f(1) = 1 \Rightarrow \text{ha nem irr, akkor}$$

$$f = (x^2 + x + 1)^2 \quad \nexists \Rightarrow f \text{ irr.}$$

6. Irreducibilis polinomok $\mathbb{C}$ felett, Viète-formulák

6.1. Tétel (az algebra alaptétele). Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.

6.2. Következmény. A komplex számok teste felett pontosan az elsőfokú polinomok irreducibilisek.

6.3. Következmény.

(1) Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik.

(2) Ha $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{C}[x]$ ($n \geq 1, a_n \neq 0$), akkor f -nek multiplicitással számolva pontosan n gyöke van.

(3) Ha ezek a gyökök $\alpha_1, \dots, \alpha_n$ (mindegyiket annyszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n \cdot (x - \alpha_1) \cdot \dots \cdot (x - \alpha_n)$. Ezt nevezzük a polinom **gyöktényezős felbontásának**.

6.4. Feladat. Határozzuk meg az alábbi polinom gyökeinek négyzetösszegét.

$$f = 3x^3 + 6x^2 + 24x + 18$$

Ha a gyökök $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{C}$, akkor

$$\begin{aligned} f &= 3x^3 + 6x^2 + 24x + 18 = 3 \cdot (x - \alpha_1) \cdot (x - \alpha_2) \cdot (x - \alpha_3) = \\ &= 3 \cdot (x^3 - \underbrace{(\alpha_1 + \alpha_2 + \alpha_3)}_{-2} x^2 + \underbrace{(\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3)}_8 x - \underbrace{\alpha_1 \alpha_2 \alpha_3}_{-6}). \end{aligned}$$

Ebből következik, hogy

$$\alpha_1 + \alpha_2 + \alpha_3 = -2 \quad \alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3 = 8 \quad \alpha_1 \alpha_2 \alpha_3 = -6$$

Ezekből ki tudjuk fejezni a gyökök négyzetösszegét:

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 \stackrel{pp.}{=} (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3) = (-2)^2 - 2 \cdot 8 = -12$$

$$(\alpha_1 + \alpha_2 + \alpha_3)^2 = \overbrace{\alpha_1^2 + \alpha_2^2 + \alpha_3^2} + 2(\alpha_1 \alpha_2 + \alpha_1 \alpha_3 + \alpha_2 \alpha_3)$$

6.5. Tétel (**Viète-formulák**). Legyenek az n -edfokú

$$f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{C}[x]$$

főpolinom komplex gyökei $\alpha_1, \dots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása). Ekkor fennállnak az alábbi összefüggések:

$$-a_{n-1} = \alpha_1 + \alpha_2 + \dots + \alpha_n;$$

$$a_{n-2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n;$$

$$-a_{n-3} = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \dots + \alpha_{n-2}\alpha_{n-1}\alpha_n;$$

$\vdots$

$$(-1)^{n-1}a_1 = \alpha_1\alpha_2 \dots \alpha_{n-2}\alpha_{n-1} + \alpha_1\alpha_2 \dots \alpha_{n-2}\alpha_n + \dots + \alpha_2\alpha_3 \dots \alpha_{n-1}\alpha_n;$$

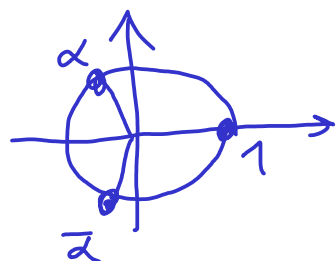
$$(-1)^n a_0 = \alpha_1\alpha_2\alpha_3 \dots \alpha_{n-1}\alpha_n.$$

6.6. Megjegyzés. A fenti képleteket **Viète-formuláknak** hívjuk. A k -adik sor bal oldalán $(-1)^k a_{n-k}$ áll, a jobb oldalon pedig az $\alpha_1, \dots, \alpha_n$ betűkből képezett összes k -tényezős szorzat összege, tehát egy $\binom{n}{k}$ -tagú összeg. Formálisan:

$$(-1)^k a_{n-k} = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} \alpha_{i_1} \cdot \alpha_{i_2} \cdot \dots \cdot \alpha_{i_k}.$$

6.7. Feladat. Bontsuk $\mathbb{C}$ és $\mathbb{R}$ felett irreducibilis tényezők szorzatára az $f = x^3 - 1$ polinomot.

PP- $x^3 - 1 = 0$ $x^3 = 1$ $x = \sqrt[3]{1}$ $\alpha = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ $\bar{\alpha} = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$



$\mathbb{C}$ felett: $f = (x-1) \cdot (x-\alpha) \cdot (x-\bar{\alpha}) =$

$$= (x-1) \cdot (x^2 - (\alpha + \bar{\alpha})x + \alpha \cdot \bar{\alpha}) =$$

$$= (x-1) \cdot (x^2 - 2\operatorname{Re}\alpha \cdot x + |\alpha|^2) =$$

$\mathbb{R}$ felett: $f = (x-1) \cdot (x^2 + x + 1)$

$\mathbb{R}$ $\mathbb{C}$

$$T_1 \subseteq T_2, f \in T_1[x] \subseteq T_2[x]$$

A: f irr. T_1 felett $\Rightarrow f$ irr. T_2 felett

B: f irr. T_2 felett $\Rightarrow f$ irr. T_1 felett ✓

C: "mindkettő" igaz -

D: "énig" van igaz.

7. Irreducibilis polinomok $\mathbb{R}$ felett

7.1. Tétel. A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \quad \forall z \in \mathbb{C}: f(z) = 0 \implies f(\bar{z}) = 0.$$

Bizonyítás.

$$\overline{f(z)} = \overline{a_n z^n + \dots + a_1 z + a_0} =$$

$$= \bar{a}_n \cdot \bar{z}^n + \dots + \bar{a}_1 \cdot \bar{z} + \bar{a}_0 =$$

$$\stackrel{\text{red circle}}{=} a_n \cdot \bar{z}^n + \dots + a_1 \cdot \bar{z} + a_0 = f(\bar{z})$$

$$\text{Tehát } \underbrace{\overline{f(z)}}_0 = \underbrace{f(\bar{z})}_0.$$

□

7.2. Következmény. Egy valós együtthatós polinom pontosan akkor irreducibilis a valós számok teste felett, ha elsőfokú, vagy olyan másodfokú polinom, melynek nincs valós gyöke. Tehát az $\mathbb{R}$ feletti irreducibilis polinomok a következők:

- $ax + b$ ($a, b \in \mathbb{C}, a \neq 0$); ✓
- $ax^2 + bx + c$ ($a, b, c \in \mathbb{C}, a \neq 0, b^2 - 4ac < 0$). ✓

Bizonyítás.

$$\text{Tfl. } \deg f \geq 3.$$

$$1) \text{ van valós gyök. } \alpha \in \mathbb{R}, f(\alpha) = 0 \implies f = (x - \alpha) \cdot (\dots) \\ \implies f \text{ nem ir.}$$

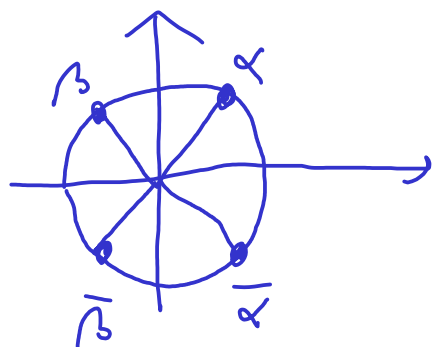
$$2) \text{ nincs valós gyök } \alpha \in \mathbb{C} \setminus \mathbb{R}, f(\alpha) = 0 \implies f(\bar{\alpha}) = 0 \implies$$

$$\alpha \neq \bar{\alpha}$$

$$\stackrel{\text{red circle}}{\implies} f = \underbrace{(x - \alpha) \cdot (x - \bar{\alpha})}_{\in \mathbb{R}[x]} \cdot (\dots) \\ = \underbrace{(x^2 - 2\operatorname{Re}(\alpha)x + |\alpha|^2)}_{\in \mathbb{R}[x]} \cdot (\dots) \\ \implies f \text{ nem ir.} \quad \square$$

7.3. Feladat. Bontsuk $\mathbb{C}$ és $\mathbb{R}$ felett irreducibilis tényezők szorzatára az $f = x^4 + 1$ polinomot.

pp. $x^4 + 1 = 0 \quad x = \sqrt[4]{-1}$



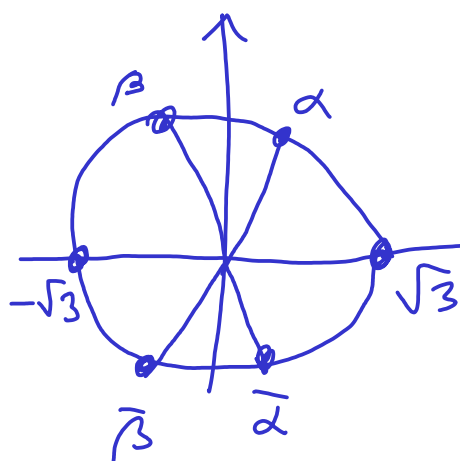
$$\alpha = \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i, \quad \beta = -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$$

$\mathbb{C}$ felett: $f = (x - \alpha) \cdot (x - \bar{\alpha}) \cdot (x - \beta) \cdot (x - \bar{\beta})$

$\mathbb{R}$ felett: $f = (x^2 - \sqrt{2}x + 1) \cdot (x^2 + \sqrt{2}x + 1)$

7.4. Feladat. Bontsuk $\mathbb{C}$ és $\mathbb{R}$ felett irreducibilis tényezők szorzatára az $f = x^6 - 27$ polinomot.

pp. $\sqrt[6]{27} \quad \alpha = \sqrt{3} \cdot \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) \quad \beta = \sqrt{3} \cdot \left(-\frac{1}{2} + \frac{\sqrt{3}}{2}i\right)$



$\mathbb{C}$ felett: $(x - \sqrt{3}) \cdot (x + \sqrt{3}) \cdot (x - \alpha) \cdot (x - \bar{\alpha}) \cdot (x - \beta) \cdot (x - \bar{\beta})$

$\mathbb{R}$ felett: $(x - \sqrt{3}) \cdot (x + \sqrt{3}) \cdot (x^2 - \sqrt{3}x + 3) \cdot (x^2 + \sqrt{3}x + 3)$

$\mathbb{Q}$ felett: $(x^2 - 3) \cdot (x^4 + 3x^2 + 9)$

ir. $\mathbb{Q}$ felett? $\checkmark$ ir. $\mathbb{Q}$ felett? $\checkmark$

$$\begin{aligned} a^3 - b^3 &= (a - b)(a^2 + ab + b^2) \\ x^6 - 27 &= (x^2)^3 - 3^3 = \\ &= (x^2 - 3) \cdot (x^4 + 3x^2 + 9) \end{aligned}$$

8. Irreducibilis polinomok $\mathbb{Q}$ felett

8.1. Példa ($\mathbb{Q}$ felett minden polinom asszociált egy $\mathbb{Z}$ felettihez).

$$\begin{aligned}\frac{15}{7}x^2 + \frac{45}{4}x + \frac{5}{2} &= \frac{60}{28}x^2 + \frac{315}{28}x + \frac{70}{28} = \\ &= \frac{1}{28}(60x^2 + 315x + 70) \sim 60x^2 + 315x + 70 \\ &= 5(12x^2 + 63x + 14) \sim 12x^2 + 63x + 14\end{aligned}$$

8.2. Feladat. Keressük meg az $f = 2x^5 + 3x^4 - 7x^3 - 3x^2 + 8x - 12$ polinom racionális gyökeit. $\alpha = \frac{p}{q}$ $\text{lcb}(p, q) = 1$

$$0 = f\left(\frac{p}{q}\right) = 2 \frac{p^5}{q^5} + 3 \frac{p^4}{q^4} - 7 \frac{p^3}{q^3} - 3 \frac{p^2}{q^2} + 8 \frac{p}{q} - 12 \quad | \cdot q^5$$

$$q^5 \mid \underbrace{2p^5 + 3p^4q - 7p^3q^2 - 3p^2q^3 + 8pq^4}_{p \mid} - 12q^5 \Rightarrow p \mid -12 \Rightarrow \text{lcb}(p, q) = 1$$

$$p = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12 \quad q = +1, +2$$

$$\frac{p}{q} = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm \frac{1}{2}, \pm \frac{3}{2}: \quad 16 \text{ lehetséges } \frac{p}{q} \text{-ra}$$

$$\text{rac. gyökök: } -2, -2, -\frac{3}{2}$$

Hogyan: $f = (x - (-2))^2 \cdot (x - \frac{-3}{2}) \cdot (2x^2 - 2x + 2) = (x+2)^2 \cdot (2x+3) \cdot (x^2+x+1)$
 az utolsó
 2-odjára
 $\Rightarrow$ irr $\mathbb{Q}$ felett

8.3. Tétel (Rolle(?) tétele). Legyen $f = a_n x^n + \dots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{p}{q}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz $p, q \in \mathbb{Z}$, $q \neq 0$ és $\text{Inko}(p, q) = 1$), akkor

$$f\left(\frac{p}{q}\right) = 0 \implies q \mid a_n \text{ és } p \mid a_0.$$

Speciálisan: egész együtthatós főpolinom racionális gyökei mindig egész számok.

Bizonyítás. Tegyük fel, hogy $\frac{p}{q}$ gyöke f -nek ($\text{Inko}(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \dots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n -nel:

$$0 = \underbrace{a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1}}_{p \mid} + \underbrace{a_0 q^n}_{p \mid} \implies p \mid a_0$$

Hasonlóan:

$$q \mid a_n \iff \underbrace{a_n p^n}_{q \mid} + \underbrace{a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n}_{q \mid} = 0 \quad \square$$

8.4. Feladat. Bontsuk $\mathbb{Q}$ felett irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = 2x^7 + 5x^6 + 4x^5 + 13x^4 + 54x^3 + 84x^2 + 54x + 12$$

ROLLE: $q \mid 12$; $p \mid 12$

$$q = 1, 2 \quad ; \quad p = \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$$

$$\frac{p}{q} : \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12, \pm \frac{1}{2}, \pm \frac{3}{2}$$

	2	5	4	13	54	84	54	12
-1	2	3	1	12	42	42	12	0
-1	2	1	0	12	30	12	0	
-1	2	-1	1	11	19	-7		
-1/2	2	0	0	12	24	0		
-1/2	2	-1	1/2	4 1/4	15 1/8			

$$f = (x - (-1))^2 \cdot (x - \frac{-1}{2}) \cdot (2x^4 + 12x + 24)$$

min ra. nide
im.?

$$f = (x+1)^2 \cdot (2x+1) \cdot (x^4 + 6x + 12)$$

im. ? $\checkmark$ $5-2$ 12
 $p=3$ 11
 $\dots + 6d$

$$x^4 + 6x + 12 = (x^2 + ax + b) \cdot (x^2 + cx + d) = x^4 + \dots$$

8.5. Tétel (Gauss-lemma). Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor $\mathbb{Q}$ felett sem bomlik így fel, és viszont.

Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

(1) $\exists g, h \in \mathbb{Z}[x] : f = gh$ és $0 < \deg g, \deg h < n$;

A: (1) $\Rightarrow$ (2) triviális ✓

B: (2) $\Rightarrow$ (1) triviális

(2) $\exists g, h \in \mathbb{Q}[x] : f = gh$ és $0 < \deg g, \deg h < n$.

C: Minkább triviális.

D: Egyszerűesen triviális.

8.6. Példa.

$$\begin{aligned}
 & 72x^5 - 102x^4 - 2244x^3 + 208x^2 - 1036x - 280 = \\
 & = \left(\frac{15}{7}x^2 + \frac{45}{4}x + \frac{5}{2}\right) \cdot \left(\frac{168}{5}x^3 - 224x^2 + \frac{448}{5}x - 112\right) = \\
 & = \frac{5}{28}(12x^2 + 63x + 14) \cdot \frac{56}{5}(3x^3 - 20x^2 + 8x - 10) = \\
 & = \frac{5}{28} \frac{56}{5} \cdot (12x^2 + 63x + 14)(3x^3 - 20x^2 + 8x - 10) = \\
 & = 2 \cdot (12x^2 + 63x + 14)(3x^3 - 20x^2 + 8x - 10) = \\
 & = (24x^2 + 126x + 28) \cdot (3x^3 - 20x^2 + 8x - 10)
 \end{aligned}$$

8.7. Definíció. Azt mondjuk, hogy a p prímszám **pontos osztója** az a egész számnak, ha a osztható p -vel, de p^2 -tel már nem. Jelölés: $p \parallel a$.

8.8. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n, \quad p \mid a_{n-1}, \dots, p \mid a_1, \quad p \parallel a_0,$$

akkor f irreducibilis a racionális számok teste felett.

8.9. Következmény. Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n -edfokú polinom.

Bizonyítás. $p=2$ $x^n + 2$ $p=2$: $2 \nmid 1, 2 \mid 0, \dots, 2 \mid 0, 2 \parallel 2$

□

8.10. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám, amelyre

$$p \parallel a_n, \quad p \mid a_{n-1}, \dots, p \mid a_1, \quad p \nmid a_0,$$

akkor f irreducibilis a racionális számok teste felett.

8.11. Feladat. Bontsuk $\mathbb{Q}$ felett irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = 5x^8 - 5x^7 + 4x^2 - 2x - 2$$

ROLTE: $q|5, p|-2 \Rightarrow \frac{p}{q}: \pm 1, \pm 2, \pm \frac{1}{5}, \pm \frac{2}{5}$

rac. mól: 1

LEPKEP: $(x-1) \cdot (5x^7 + 4x + 2) = f$
 im. im. S-E: $p=2$

8.12. Feladat. Bontsuk $\mathbb{Q}$ felett irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = 2x^{100} - 3x^{73} + 69x - 12$$

ROLTE: $q|2, p|-12 \quad \frac{p}{q}: \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm \frac{1}{2}, \pm \frac{3}{2}$

S-E $p=3 \Rightarrow f$ irred.

8.13. Feladat. Bontsuk $\mathbb{Q}$ felett irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = x^6 - 27$$

ROLTE: $q|1, p|27 \quad \frac{p}{q}: \pm 1, \pm 3, \pm 9, \pm 27$

rac. mól min

$\mathbb{C}: \dots$

$\mathbb{R}: (x-\sqrt{3}) \cdot (x+\sqrt{3}) \cdot (x^2 - \sqrt{3}x + 3) \cdot (x^2 + \sqrt{3}x + 3)$

$\mathbb{Q}: (x^2 - 3) \cdot (x^4 + 3x^2 + 9)$

8.14. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n, \quad p \mid a_{n-1}, \dots, p \mid a_2, \quad p \mid a_1, \quad p \nmid a_0,$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás. Tfh. van megfelelő p prímszám, de f mégsem irreducibilis $\mathbb{Q}$ felett. Ekkor, a Gauss-lemma szerint léteznek olyan **egész** együtthatós g, h polinomok, amelyekre $f = gh$ és $1 \leq \deg g, \deg h < n$. Legyen

$$g = b_k x^k + b_{k-1} x^{k-1} + \dots + b_2 x^2 + b_1 x + b_0 \in \mathbb{Z}[x] \quad \deg g = k < n$$

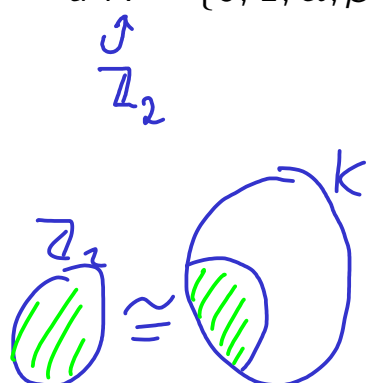
$$h = c_\ell x^\ell + c_{\ell-1} x^{\ell-1} + \dots + c_2 x^2 + c_1 x + c_0 \in \mathbb{Z}[x] \quad \deg h = \ell < n$$

Vizsgáljuk az $f = gh$ egyenlőséget együtthatónként: $(k + \ell = n)$

$$\begin{aligned} x^0 \text{ e.l.: } a_0 &= b_0 c_0 \xRightarrow{p \nmid a_0} p \nmid b_0 \vee p \nmid c_0 \\ x^1 \text{ e.l.: } a_1 &= b_1 c_0 + b_0 c_1 \xRightarrow{p \mid a_1} p \mid b_1 c_0 \xRightarrow{p \nmid b_0} p \mid c_1 \\ x^2 \text{ e.l.: } a_2 &= b_2 c_0 + b_1 c_1 + b_0 c_2 \xRightarrow{p \mid a_2} p \mid b_2 c_0 \xRightarrow{p \nmid b_0} p \mid c_2 \\ &\vdots \\ x^i \text{ e.l.: } a_i &= b_i c_0 + \dots \xRightarrow{p \mid a_i} p \mid b_i c_0 \xRightarrow{p \nmid b_0} p \mid c_i \\ x^n \text{ e.l.: } a_n &= b_n c_\ell \xRightarrow{p \nmid a_n} p \nmid b_n \vee p \nmid c_\ell \end{aligned}$$

9. Egyszerű algebrai bővítés, véges testek

9.1. Példa. Az $m = x^2 + x + 1 \in \mathbb{Z}_2[x]$ polinomnak nincs gyöke $\mathbb{Z}_2$ -ben, ezért irreducibilis $\mathbb{Z}_2$ felett (hiszen csak másodfokú). Bővítsük ki a $\mathbb{Z}_2 = \{0, 1\}$ testet a $K = \{0, 1, \alpha, \beta\}$ testté:



+	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$GF(4) = K = \mathbb{Z}_2(\alpha)$
 $\alpha^2 + \alpha + 1 = 0$

·	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

$\beta + \alpha + 1 = 0$

Ebben a testben már van gyöke az m polinomnak: $m(\alpha) = \alpha^2 + \alpha + 1 = 0$.

A K test izomorf a $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$ testtel; hogy ezt lássuk, csak be kell vezetni a $0 := \bar{0}$, $1 := \bar{1}$, $\alpha := \bar{x}$, $\beta := \overline{x+1}$ jelöléseket:

+	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

·	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{0}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

$$m(\alpha) = m(\bar{x}) = \overline{x^2 + x + 1} = \overline{x^2 + x + 1} = \bar{m} = \bar{0}$$

9.2. Tétel. A $T[x]/\langle m \rangle$ maradékosztály-gyűrű akkor és csak akkor test, ha az $m \in T[x]$ polinom irreducibilis T felett. $\mathbb{Z}_m \text{ test} \Leftrightarrow m \text{ pr}$

9.3. Tétel. Legyen T test, $m \in T[x]$ irreducibilis polinom, $\deg f = n$. Ekkor a $K = T[x]/\langle m \rangle$ maradékosztály-gyűrű olyan test, amelyben az m polinomnak van gyöke. A K test minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0} \quad (a_{n-1}, \dots, a_0 \in T)$$

alakban. Ha $T = \mathbb{Z}_p$, akkor $|K| = p^n$.

Bizonyítás. $\alpha = \bar{x}$

$$m(\alpha) = m(\bar{x}) = \overline{m(x)} = \bar{m} = \bar{0}, \text{ hiszen } m \equiv 0 \pmod{m}$$

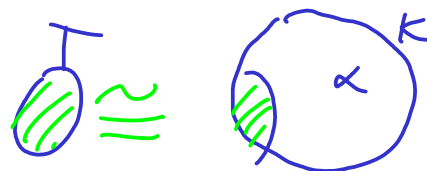
□

9.4. Következmény. Tetszőleges T test és $m \in T[x]$ irreducibilis polinom esetén létezik olyan K test, amelyre

- (1) K **bővítése** T -nek, azaz $K \supseteq T$;
- (2) létezik olyan $\alpha \in K$ elem, amely gyöke m -nek;
- (3) K elemei egyértelműen előállnak $a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0$ ($a_{n-1}, \dots, a_0 \in T$) alakban, ahol $n = \deg f$.

Bizonyítás. Legyen $K = T[x]/\langle m \rangle$.

$$\bar{a} = a$$



- (1) K -ban $\{ \bar{a} : a \in T \subseteq T[x] \}$ egy T -vel izomorf résztest.
- (2) Legyen $\alpha = \bar{x}$, ekkor $m(\alpha) = m(\bar{x}) = \overline{m(x)} = \bar{0}$, hiszen $m \equiv 0 \pmod{m}$.
- (3) K elemei egyértelműen előállnak így ($a_{n-1}, \dots, a_0 \in T$ együtthatókkal):

$$\begin{aligned} \overline{a_{n-1}x^{n-1} + \dots + a_1x + a_0} &= \overline{a_{n-1}}\bar{x}^{n-1} + \dots + \overline{a_1}\bar{x} + \overline{a_0} = \\ &= a_{n-1}\bar{x}^{n-1} + \dots + a_1\bar{x} + a_0 = \\ &= a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0. \end{aligned} \quad \square$$

9.5. Definíció. Azt mondjuk, hogy a K test T -ből az α elem **adjungálásával** keletkezik (jelölés: $K = T(\alpha)$), és az ilyen módon előálló testeket T **egyszerű algebrai bővítéseinek** nevezzük.

9.6. Példa. Mivel az $x^2 + 1$ polinom irreducibilis $\mathbb{R}$ felett, a $K := \mathbb{R}[x]/\langle x^2 + 1 \rangle$ maradékosztály-gyűrű test.

- elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$);
- számolási szabály: $\overline{x^2 + 1} = \bar{0}$.

$$\mathbb{C} = \mathbb{R}(i)$$

Menjünk le alfába...

- elemek: $a + b\alpha$ ($a, b \in \mathbb{R}$);
- számolási szabály: $\alpha^2 + 1 = 0$.

$$\alpha^2 = -1 \quad \alpha = i$$

9.7. Példa. Mivel $m := x^3 - 2$ irreducibilis $\mathbb{Q}$ felett, a $K := \mathbb{Q}[x]/\langle x^3 - 2 \rangle$ maradékosztály-gyűrű test.

- elemek: $\overline{a + bx + cx^2}$ ($a, b, c \in \mathbb{Q}$);
- számolási szabály: $\overline{x^3 - 2} = \overline{0}$.

Euklideszi algoritmussal kiszámítottuk, hogy $\overline{x^2 - 2x + 1}^{-1} = \overline{5 + 4x + 3x^2}$.

Menjünk le alfába...

$$= a + b\sqrt[3]{2} + c\sqrt[3]{4} \quad \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$$

- elemek: $a + b\alpha + c\alpha^2$ ($a, b, c \in \mathbb{Q}$);
- számolási szabály: $\alpha^3 - 2 = 0$. $\alpha^3 = 2$

A fenti inverz alfás felírása: $(\alpha^2 - 2\alpha + 1)^{-1} = 5 + 4\alpha + 3\alpha^2$.

$$\alpha = \sqrt[3]{2}$$

$$\frac{1}{\sqrt[3]{4} - 2\sqrt[3]{2} + 1} = 5 + 4\sqrt[3]{2} + 3\sqrt[3]{4}$$

9.8. Tétel. Akkor és csak akkor létezik q -elemű test, ha q prímszám.

Bizonyítás.

- **akkor:** Ha $q = p^n$, akkor $K := \mathbb{Z}_p[x]/\langle m \rangle$ jó lesz tetszőleges $m \in \mathbb{Z}_p[x]$ irreducibilis n -edfokú polinom esetén. (Nem triviális, hogy van ilyen!)
- **csak akkor:** Ha K egy véges test, akkor a legkisebb részteste izomorf $\mathbb{Z}_p$ -vel valamilyen p prímszámra (nem triviális!), és K vektorteret alkot ezen test felett, így $|K| = p^n$, ahol $n = \dim K$. $\square$

9.9. Megjegyzés. Tetszőleges q prímszám esetén izomorfia erejéig egyetlen q -elemű test létezik. Jelölés: $\text{GF}(q)$. Galois field

9.10. Példa.

- $\text{GF}(2) \cong \mathbb{Z}_2$
- $\text{GF}(3) \cong \mathbb{Z}_3$
- $\text{GF}(4) \cong \mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle$
- $\text{GF}(5) \cong \mathbb{Z}_5$
- $\text{GF}(6)$ nem létezik
- $\text{GF}(7) \cong \mathbb{Z}_7$
- $\text{GF}(8) \cong \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle \cong \mathbb{Z}_2[x]/\langle x^3 + x^2 + 1 \rangle$

pp.

$$x^3 + x^2 + x + 1$$

10. Lagrange-iterpoláció

10.1. Tétel. Egy test feletti nemnulla polinomnak nem lehet több gyöke, mint amennyi a fokszáma.

Bizonyítás. $\alpha_1, \dots, \alpha_r$ ^{kül.} ~~gyök~~ f -nek $\Rightarrow$

$$\Rightarrow (x - \alpha_1) \cdot \dots \cdot (x - \alpha_r) \mid f \Rightarrow r \leq \deg f \quad \square$$

10.2. Következmény. Ha az $f, g \in T[x]$ polinomok legfeljebb n -edfokúak, és $n + 1$ különböző helyen ugyanaz a helyettesítési értékük, akkor $f = g$.

Bizonyítás. A $h := f - g$ polinom legfeljebb n -edfokú és legalább $n + 1$ gyöke van, ezért a fenti tétel szerint $h = 0$. $\square$

10.3. Következmény. Ha a T test végtelen, akkor két T feletti polinom akkor és csak akkor egyenlő, ha a hozzájuk tartozó polinomfüggvények megegyeznek.

10.4. Megjegyzés. Ha a T test véges, akkor viszont mindig találhatók különböző T feletti polinomok, amelyekhez ugyanaz a polinomfüggvény tartozik, pl. ha $T = \{a_1, \dots, a_q\}$, akkor az $f = 0$ és $g = (x - a_1) \cdot \dots \cdot (x - a_q)$ polinomokhoz ugyanaz a polinomfüggvény tartozik (konstans nulla).

10.5. Tétel (Lagrange-iterpoláció). Tetszőleges $a_1, \dots, a_{n+1}$ páronként különböző és $b_1, \dots, b_{n+1}$ (nem feltétlenül különböző) T -beli elemekhez létezik pontosan egy $f \in T[x]$ legfeljebb n -edfokú polinom, amelyre $f(a_i) = b_i$ teljesül $i = 1, \dots, n + 1$ esetén.

Bizonyítás. Tekintsük az alábbi $f_i \in T[x]$ polinomokat ($i = 1, \dots, n + 1$):

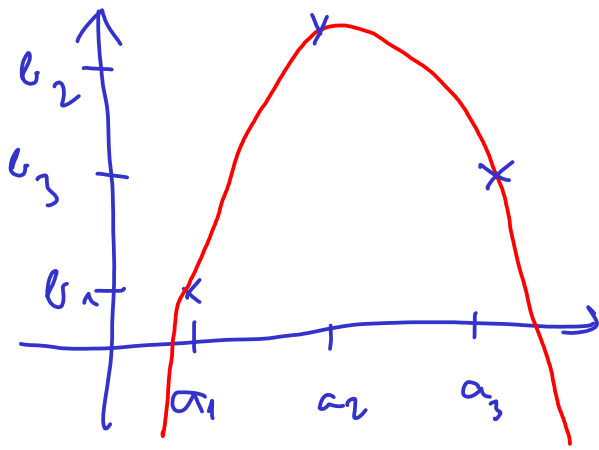
$$f_i := b_i \cdot \frac{(x - a_1) \cdot \dots \cdot (x - a_{i-1}) \cdot (x - a_{i+1}) \cdot \dots \cdot (x - a_{n+1})}{(a_i - a_1) \cdot \dots \cdot (a_i - a_{i-1}) \cdot (a_i - a_{i+1}) \cdot \dots \cdot (a_i - a_{n+1})}.$$

Ekkor f_i értéke az a_j helyen:

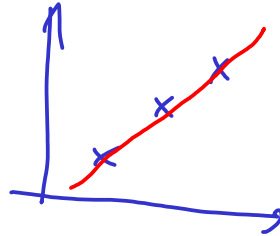
$$f_i(a_j) = \begin{cases} 0, & \text{ha } i \neq j; \\ b_i, & \text{ha } i = j. \end{cases}$$

Tehát az $f = f_1 + \dots + f_{n+1}$ polinom megfelelő lesz:

$$\begin{aligned} f(a_j) &= f_1(a_j) + \dots + f_{j-1}(a_j) + f_j(a_j) + f_{j+1}(a_j) + \dots + f_{n+1}(a_j) = \\ &= 0 + \dots + 0 + b_j + 0 + \dots + 0 = b_j. \end{aligned} \quad \square$$



$$f \in \mathbb{R}[x]$$



$$\begin{array}{c} a_1 \quad a_2 \quad a_3 \\ \hline \end{array}$$

$$f: \quad b_1 \quad b_2 \quad b_3$$

$$f_1: \quad b_1 \quad 0 \quad 0$$

$$f_2: \quad 0 \quad b_2 \quad 0$$

$$f_3: \quad 0 \quad 0 \quad b_3$$

$$f_1 = b_1 \cdot \frac{(x-a_2)(x-a_3)}{(a_1-a_2)(a_1-a_3)}$$

$$f_2 = b_2 \cdot \frac{(x-a_1)(x-a_3)}{(a_2-a_1)(a_2-a_3)}$$

$$f_3 = b_3 \cdot \frac{(x-a_1)(x-a_2)}{(a_3-a_1)(a_3-a_2)}$$

$$f = f_1 + f_2 + f_3$$

$$f(a_1) = f_1(a_1) + f_2(a_1) + f_3(a_1) = b_1 + 0 + 0 = b_1$$

$$\deg f \leq 2$$

11. Derivált, többszörös gyökök

11.1. Definíció. Az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinom **deriváltján** az $f' = n a_n x^{n-1} + \dots + 2 a_2 x + a_1$ polinomot értjük.

Jelölés. A k -adik deriváltat $f^{(k)}$ jelöli, az $f^{(1)} = f'$ és $f^{(0)} = f$ megállapodással.

11.2. Tétel. Tetszőleges $f, g \in T[x]$ polinomokra és k pozitív egész számra érvényesek az alábbi deriválási szabályok:

$$(1) (f + g)' = f' + g';$$

$$(2) (f \cdot g)' = f' \cdot g + f \cdot g';$$

$$(3) (f^k)' = k \cdot f^{k-1} \cdot f'.$$

11.3. Tétel. Ha az α komplex szám k -szoros gyöke az $f \in \mathbb{C}[x]$ polinomnak, akkor $(k-1)$ -szeres gyöke f' -nek. (Ha $k=1$, akkor α nem gyöke f' -nek.)

Bizonyítás. Tízh. $f = (x-\alpha)^k \cdot g$ és $g(\alpha) \neq 0$.

$$f' = k \cdot (x-\alpha)^{k-1} \cdot g + (x-\alpha)^k \cdot g' = (x-\alpha)^{k-1} \cdot \underbrace{(k \cdot g + (x-\alpha) \cdot g')}_{x=\alpha \text{ helyen:}}$$

$$\neq k \cdot g(\alpha) = k \cdot g(\alpha) + (\alpha-\alpha) \cdot g'(\alpha) \quad \square$$

11.4. Megjegyzés. Az előző tétel megfordítása nem igaz: f' -nek lehetnek olyan gyökei is, amelyekért nem f többszörös gyökei a „felelősek”.

11.5. Következmény. Az $f \in \mathbb{C}[x]$ polinom α gyökének multiplicitása nem más, mint a legkisebb olyan k nemnegatív egész, amelyre $f^{(k)}(\alpha) \neq 0$, azaz α akkor és csak akkor k -szoros gyök, ha

$$f(\alpha) = f'(\alpha) = \dots = f^{(k-1)}(\alpha) = 0, \text{ de } f^{(k)}(\alpha) \neq 0.$$

11.6. Feladat. Hányszoros gyöke $\alpha = 2$ az $f = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8$ polinomnak?

$$\begin{array}{l} f = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8 \\ f' = 5x^4 - 20x^3 + 21x^2 - 4x + 4 \\ f'' = 20x^3 - 60x^2 + 42x - 4 \\ f''' = 60x^2 - 120x + 42 \end{array} \quad \left. \begin{array}{l} f(2) = 0 \\ f'(2) = 0 \\ f''(2) = 0 \\ f'''(2) = 42 \end{array} \right\} \alpha = 2 \text{ 3-szoros gyök}$$

11.7. Feladat. Határozzuk meg az $a, b \in \mathbb{R}$ együtthatókat úgy, hogy teljesüljön az alábbi oszthatóság.

pp.

$$(x+2)^2 \mid x^4 + ax^3 + bx^2 + 4$$

↑↑

-2 legalább kétszeres gyöke f -nek és $(x+2)^3 \nmid f$

↑↑

$f(-2) = 0$ és $f'(-2) \neq 0$ és $f'(-2) \neq 0$

$$f = x^4 + ax^3 + bx^2 + 4 \quad f(-2) = 16 - 8a + 4b + 4 = 0 \quad (1)$$

$$f' = 4x^3 + 3ax^2 + 2bx \quad f'(-2) = -32 + 12a - 4b = 0 \quad (2)$$

$$\begin{cases} (1) & 8a - 4b = 20 \\ (2) & 12a - 4b = 32 \end{cases} \quad a = 3, b = 1$$

$$f = (x-\alpha) \cdot (x-\beta) \cdot (x-\gamma)^2 \cdot (x-\delta)^5 \cdot (x-\varepsilon)^5$$

$$f' = (x-\gamma) \cdot (x-\delta)^4 \cdot (x-\varepsilon)^4 \cdot (x-\zeta) \cdot (x-\eta)^3$$

$$(f, f') = (x-\gamma) \cdot (x-\delta)^4 \cdot (x-\varepsilon)^4$$

$$\frac{f}{(f, f')} = (x-\alpha) \cdot (x-\beta) \cdot (x-\gamma) \cdot (x-\delta) \cdot (x-\varepsilon)$$

11.8. Következmény. Az α komplex szám akkor és csak akkor többszörös gyöke az $f \in \mathbb{C}[x]$ polinomnak, ha gyöke $\text{Inko}(f, f')$ -nak.

11.9. Következmény. Bármely legalább elsőfokú $f \in \mathbb{C}[x]$ polinomra az $\frac{f}{\text{Inko}(f, f')}$ polinom gyökei ugyanazok, mint f gyökei, de mindegyik egyszeres gyök.

11.10. Következmény. Ha T számtest, azaz $T \leq \mathbb{C}$, és $f \in T[x]$ irreducibilis T felett, akkor f -nek minden komplex gyöke egyszeres.

11.11. Feladat. Határozzuk meg az $f = x^5 - 10x^3 - 20x^2 - 15x - 4 \in \mathbb{C}[x]$ polinom (többszörös) gyökeit és a gyökök multiplicitását.

$$f' = 5x^4 - 30x^2 - 40x - 15 \sim x^4 - 6x^2 - 8x - 3$$

$$(f, f') = ? \quad f / (f, f') = ?$$

$$\begin{array}{r} \overbrace{(x^5 - 10x^3 - 20x^2 - 15x - 4)}^f : \overbrace{(x^4 - 6x^2 - 8x - 3)}^{f'/5} = x \\ x^5 - 6x^3 - 8x^2 - 3x \\ \hline -4x^3 - 12x^2 - 12x - 4 \sim x^3 + 3x^2 + 3x + 1 \sim (f, f') = (x+1)^3 \end{array}$$

$$(x^4 - 6x^2 - 8x - 3) : (x^3 + 3x^2 + 3x + 1) = x - 3$$

$$\begin{array}{r} x^4 + 3x^3 + 3x^2 + x \\ \hline -3x^3 - 9x^2 - 9x - 3 \\ \hline -3x^3 - 9x^2 - 9x - 3 \\ \hline 0 \end{array}$$

$\Downarrow$
-1 f-nek 4-nak

$$f = (x+1)^4 \cdot (\dots)$$

$$f / (f, f') = x^2 - 3x - 4 = (x+1) \cdot (x-4)$$

pp-

$$f = (x+1)^4 \cdot (x-4)^2$$

...(HÖRNER)...

$$f = (x+1)^4 \cdot (x-4)^2$$

2.5. Feladat. Határozzuk meg az $a, b \in \mathbb{R}$ együtthatók értékét úgy, hogy teljesüljön az oszthatóság $\mathbb{R}[x]$ -ben.

- (a) $(x-1)(x+2) \mid ax^3 + x^2 + bx + 3$;
- (b) $(x-2)(x+1) \mid ax^3 - x^2 + bx + 4$; $= f$
- (c) $(x-2)(x-3) \mid ax^3 + bx^2 + x - 4$;
- (d) $(x+1)(x+2) \mid x^3 + ax^2 + bx - 1$.

$$(b) \quad (x-2) \cdot (x+1) \mid f \Leftrightarrow f(2) = f(-1) = 0$$

$$f(2) = 8a - 4 + 2b + 4 = 0 \quad (1)$$

$$f(-1) = -a - 1 - b + 4 = 0 \quad (2)$$

$$\left. \begin{array}{l} (1) \quad 8a + 2b = 0 \\ (2) \quad a + b = 3 \end{array} \right\} \quad a = -1, b = 4$$

$$f \in \mathbb{C}[x]$$

2.10. Feladat. Adjunk meg minimális fokszámú $f \in \mathbb{R}[x]$ polinomot, amelynek

- (a) a 2 kétszeres, a -1 és a $2+i$ egyszeres gyöke;
- (b) az i háromszoros, a $3+i$ egyszeres gyöke;
- (c) az $1+i$ háromszoros, a -2 kétszeres, az i egyszeres gyöke.

$$(c) \quad f = (x - (1+i))^3 \cdot (x - (-2))^2 \cdot (x - i) \in \mathbb{R}[x]$$

$$\begin{aligned} f &= \underbrace{(x - (1+i))^3 \cdot (x - (1-i))^3}_{(x^2 - 2x + 2)^3} \cdot (x - (-2))^2 \cdot (x - i) \cdot (x - (-i)) \\ &= (x^2 - 2x + 2)^3 \cdot (x + 2)^2 \cdot (x^2 + 1) \end{aligned}$$

$$(x - \alpha) \cdot (x - \bar{\alpha}) = (x^2 - 2\operatorname{Re}\alpha \cdot x + |\alpha|^2)$$