

Győri László

Diszkrét matematika 1

Kidolgozott tételek

A halmazelmélet elemei ()

• Elemi halmazelmélet:

- A halmaz fogalmát nem tudjuk definiálni, csak körülírni. $\rightarrow$ Bizonyos dolgok összessége.
- Egy halmazt akkor tekintünk adottnak, ha minden elemről meg tudjuk mondani, hogy hozzá tartozik -e a halmazhoz vagy sem.

- Jelölések:

- halmaz: $A, B, C, \dots$ vagy $A_1, A_2, A_3, \dots$
- elem: $a, b, c, \dots$ vagy $a_1, a_2, a_3, \dots$
- a eleme A -nak: $a \in A$
- a nem eleme A -nak: $a \notin A$

- Egy halmazt így adunk meg, hogy felsoroljuk az elemeit: $A = \{a, b, c, \dots\}$ vagy megadjuk, hogy az elemei milyen tulajdonságúak: $A = \{a \mid T(a)\}$.

- Az utóbbi esetben A elemei azon a elemek lesznek, amelyek rendelkeznek a T tulajdonsággal.

• Definíció:

Azt a halmazt, amelynek egyetlen eleme sincs, üres halmaznak nevezzük. Jele: $\emptyset$.

• Definíció:

Két halmazt ~~(pontosan)~~ akkor mondunk egyenlőnek, ha pontosan ugyanazok az elemek tartoznak mind a két halmazhoz.

• Jele: $A = B \Leftrightarrow (\forall x \in A \Rightarrow x \in B) \text{ és } (\forall x \in B \Rightarrow x \in A)$

// A és B akkor egyenlők, ha kölcsönösen részhalmazok egymásnak.

• Definíció:

Az A halmaz részhalmaza B -nek, ha A minden eleme B -hez tartozik. ($A \subseteq B$)

Természetesen minden halmaz önmaga részhalmaza. ($A \subseteq A$)

// Egy n elemű halmaznak 2^n darab részhalmaza van.

• Definíció:

Az A halmaz valódi részhalmaza B -nek, ha A részhalmaza B -nek, de $A \neq B$. ($A \subset B$)

- Az üres halmaz minden halmaznak a részhalmaza.

• Tétel:

Csak egy üres halmaz létezik.

- bizonyítás: Indirekt tegyük fel, hogy A és B is üres halmazok.

Ekkor $A \subset B$ és $B \subset A$ teljesül, így $A = B$, tehát csak egy üres halmaz létezik.

- Egy halmaz számosságát a következőképpen jelöljük: $|A| = n$, ahol $n \in \mathbb{N}$ és $n \geq 0$

• Definíció:

Egy A halmaz összes részhalmazából álló halmazt az A hatványhalmazának nevezzük.

- Jele: 2^A , illetve $P(A)$.

• Példa: $A = \{x, y\}$

$$2^A = \{\emptyset, \{x\}, \{y\}, \{x, y\}\}$$

• Definíció:

Halmazrendszernek nevezzük az olyan nem üres halmazt, amelynek elemei halmazok.

• Műveletek halmazok között: (A és B halmaz esetén)

• Únic: A vagy B vagy mindkettő eleme.

$$A \cup B = \{x \mid x \in A \text{ vagy } x \in B\}$$

• Metszet: A és B eleme.

$$A \cap B = \{x \mid x \in A \text{ és } x \in B\}$$

• Különbség: A eleme, de B nem eleme.

$$A \setminus B = \{x \mid x \in A \text{ és } x \notin B\}$$

• Szimmetrikus különbség: A és B únicjához eleme, de metszetüknek nem.

$$A \circ B = \{x \mid x \in A \cup B \text{ és } x \notin A \cap B\}$$

$$A \circ B = (A \setminus B) \cup (B \setminus A)$$

• Definíció:

Legyen X egy halmaz és A legyen X -nek valódi részhalmaza.

Ekkor az A halmaz X -re vonatkozó komplementerén az $X \setminus A$ halmazt értjük.

- Jele: $\bar{A}$ // $\bar{A} = \{a \in X \mid a \notin A\}$ (komplementer = kiegészítő halmaz)

• Definíció: (Ω = teljes halmaz esetén)

Az üreshalmaz komplementere a teljes halmaz. ($\bar{\emptyset} = \Omega$)

A teljes halmaz komplementere az üreshalmaz. ($\bar{\Omega} = \emptyset$)

Egy halmaz komplementerének komplementere maga a halmaz. ($\bar{\bar{A}} = A$)

Egy halmaz és komplementerének metszete az üreshalmaz. ($A \cap \bar{A} = \emptyset$)

Egy halmaz és komplementerének uniója a teljes halmaz. ($A \cup \bar{A} = \Omega$)

A halmazelmélet elemei ()

• Tétel:

$$A = B \Leftrightarrow \bar{A} = \bar{B}$$

• bizonyítás: Tegyük fel, hogy $A = B$. Ekkor $x \in \bar{A} \Leftrightarrow x \notin A \Leftrightarrow x \notin B \Leftrightarrow x \in \bar{B}$,
tehát $\bar{A}$ és $\bar{B}$ elemei megegyeznek, így $\bar{A} = \bar{B}$.

$$A \subset B \Leftrightarrow \bar{B} \subset \bar{A}$$

• bizonyítás: Tegyük fel, hogy $A \subset B$. Ekkor $x \in \bar{B} \Leftrightarrow x \notin B \Leftrightarrow x \notin A \Leftrightarrow x \in \bar{A}$,
tehát $\bar{B}$ elemei $\bar{A}$ -nek is elemei, azaz $\bar{B} \subset \bar{A}$.

$$\bar{\bar{A}} = A$$

• bizonyítás: $x \in \bar{\bar{A}} \Leftrightarrow x \notin \bar{A} \Leftrightarrow x \in A$, tehát $\bar{\bar{A}} = A$.

• Tétel:

Legyen X adott halmaz és $A, B, C \subset X$. Ekkor...

$$1., \left. \begin{array}{l} A \cup B = B \cup A \\ A \cap B = B \cap A \end{array} \right\} \text{Kommutatív}$$

$$2., \left. \begin{array}{l} (A \cup B) \cup C = A \cup (B \cup C) \\ (A \cap B) \cap C = A \cap (B \cap C) \end{array} \right\} \text{Asszociatív}$$

$$3., \left. \begin{array}{l} A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \end{array} \right\} \text{Disztributív}$$

$$4., \left. \begin{array}{l} A \cup A = A \\ A \cap A = A \end{array} \right\} \text{Idempotens}$$

$$5., \left. \begin{array}{l} A \cup \emptyset = A \\ A \cap \emptyset = \emptyset \end{array} \right\}$$

$$6., \left. \begin{array}{l} A \cup X = X \\ A \cap X = A \end{array} \right\}$$

$$7., \left. \begin{array}{l} \bar{\emptyset} = X \\ \bar{X} = \emptyset \end{array} \right\}$$

$$8., \left. \begin{array}{l} A \cup \bar{A} = X \\ A \cap \bar{A} = \emptyset \end{array} \right\}$$

$$9., A \cup B = A \Leftrightarrow B \subset A$$

$$10., A \cap B = A \Leftrightarrow A \subset B$$

• Bizonyítsuk be, hogy $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$

$$\begin{aligned} x \in A \cup (B \cap C) &\Leftrightarrow x \in A \text{ vagy } x \in (B \cap C) \Leftrightarrow x \in A \text{ vagy } (x \in B \text{ és } x \in C) \Leftrightarrow \\ &\Leftrightarrow (x \in A \text{ vagy } x \in B) \text{ és } (x \in A \text{ vagy } x \in C) \Leftrightarrow x \in (A \cup B) \text{ és } (A \cup C) \Leftrightarrow \\ &\Leftrightarrow x \in (A \cup B) \cap (A \cup C). \end{aligned}$$

• Tétel (De Morgan-féle azonosságok):

Legyen X egy adott halmaz, és $A, B \subset X$. Ekkor...

$$\overline{(A \cap B)} = \bar{A} \cup \bar{B}$$

$$\overline{(A \cup B)} = \bar{A} \cap \bar{B}$$

-bizonyítás:

$$x \in \overline{(A \cup B)} \Leftrightarrow x \notin (A \cup B) \Leftrightarrow x \notin A \text{ és } x \notin B \Leftrightarrow x \in \bar{A} \text{ és } x \in \bar{B} \Leftrightarrow x \in \bar{A} \cap \bar{B}.$$

$$x \in \overline{(A \cap B)} \Leftrightarrow x \notin (A \cap B) \Leftrightarrow x \notin A \text{ vagy } x \notin B \Leftrightarrow x \in \bar{A} \text{ vagy } x \in \bar{B} \Leftrightarrow x \in \bar{A} \cup \bar{B}.$$

• Tétel:

$$\overline{(\bar{A} \cap \bar{B})} = \overline{\bar{A}} \cup \overline{\bar{B}} = A \cup B.$$

$$\overline{(\bar{A} \cup \bar{B})} = \overline{\bar{A}} \cap \overline{\bar{B}} = A \cap B.$$

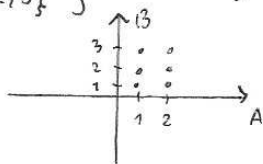
• Descartes-szorzat (direkt szorzat):

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

-rendezett pár: $(a, b) \ a \in A, b \in B$.

• példa:

$$\left. \begin{aligned} A &= \{1, 2\} \\ B &= \{1, 2, 3\} \end{aligned} \right\} A \times B = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$$



// Descartes-szorzat

$\mathbb{R}$ = valós számok halmaza (számegyenes, 1 dimenzió)

$\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ = valós számpárok halmaza (sík, 2 dimenzió)

$\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$ = valós számhármassok halmaza (tér, 3 dimenzió)

$A \times B$ általában nem egyenlő $B \times A$ -val, csak akkor, ha $A = B$.

$$(A \times B) \times C = \{(a, b), c) : a \in A, b \in B, c \in C\}$$

$$A \times (B \times C) = \{(a, (b, c)) : a \in A, b \in B, c \in C\}$$

} Asszociatív

Relációk ()

• Reláció: Valamilyen viszonyt fejez ki.

$$F \subseteq A \times B$$

↑

binár reláció
(kétváltozós)

Ha például $A = \{ \text{az összes vezetéknév} \}$

$B = \{ \text{az összes keresztnév} \}$,

akkor $A \times B = \{ \text{az összes lehetséges név} \}$

$F = \{ \text{M.O.-n anyakönyvezett tényleges nevek halmaza} \}$

• Tétel:

Legyenek A, B és C tetszőleges halmazok. Ekkor...

1. $A \times B = \emptyset \iff A = \emptyset \text{ vagy } B = \emptyset$
2. $(A \cup B) \times C = (A \times C) \cup (B \times C)$
3. $A \times (B \cup C) = (A \times B) \cup (A \times C)$
4. $(A \cap B) \times C = (A \times C) \cap (B \times C)$
5. $A \times (B \cap C) = (A \times B) \cap (A \times C)$
6. $(A \setminus B) \times C = (A \times C) \setminus (B \times C)$
7. $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$
8. $B \subset C \Rightarrow (A \times B) \subset (A \times C)$
9. $A \times B = B \times A \iff A = B$.

• Relációk tulajdonságai:

R reflexív, ha $(a, a) \in R$

R szimmetrikus, ha $(a, b) \in R \Rightarrow (b, a) \in R$

R tranzitív, ha $(a, b) \in R$ és $(b, c) \in R \Rightarrow (a, c) \in R$

R antiszimmetrikus, ha $(a, b) \in R$ és $(b, a) \in R \Rightarrow a = b$

R rendezési reláció, ha reflexív, antiszimmetrikus és tranzitív

R ekvivalencia reláció, ha reflexív, szimmetrikus és tranzitív.

• Ekvivalencia reláció:

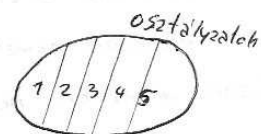
$$a \sim b = (a, b) \in F$$

$\sim$ relációt ekvivalencia relációnak nevezzük, ha reflexív, szimmetrikus és tranzitív.

• Példa:

$A = \{ \text{A Debreceni Egyetem elsőéves PTI BSC hallgatói} \}$

$a \sim b$, ha diskret matematikából azonos jegyet kaptak.



• Definíció:

Egy A halmazon osztályozásnak nevezzük az A halmaz felbontását párhelyes diszjunkt részhalmazokra.

- Az előző példa alapján: $A = A_1 \cup A_2 \cup A_3 \cup A_4 \cup A_5$

- ebben az esetben $A_n \cap A_m = \emptyset$, ha $n \neq m$, $n, m: 1, 2, 3, 4, 5$

• Állítás: Egy A halmazon egy ekvivalencia reláció osztályozást indukál.

Megfordítva: Minden osztályozás származtatható egy ekvivalencia relációból.

• Rendezési reláció:

Egy halmazon adott reláció rendezési reláció... ($\leq$ reláció)

ha $a \leq a$, $\forall a$

(reflexív)

ha $a \leq b$ és $b \leq c \Rightarrow a \leq c$

(transzitiv)

ha $a \leq b$ és $b \leq a \Rightarrow a = b$

(antiszimmetrikus)

} féligrendezési reláció

ha $a \leq b$ vagy $b \leq a$ teljesül $\Rightarrow$ rendezési reláció

Függvények ()

• Definíció:

$R \subset A \times B$ függvény, ha $(a, b) \in R$ és $(a, c) \in R$, akkor $b = c$

$R \rightsquigarrow f$

$(a, b) \in f \rightsquigarrow f(a) = b$

// Egy elemnek nem lehet 2 különböző képe.

// Egy ponthoz nem tartozhat 2 függvényérték.

$R \subset A \times B \rightarrow f \subset A \times B$

tartomány = $\text{dom}(f)$

$\text{dom } f = D_f = \{ a \in A \mid \exists b \in B: f(a) = b \}$

képzet = $\text{ran}(f)$

$\text{ran } f = R_f = \{ b \in B \mid \exists a \in A: f(a) = b \}$

• Megjegyzés:

Minden függvény reláció, de nem minden reláció függvény.

• Függvények tulajdonságai:

- Monotonitás:

- monoton növekvő / csökkenő

- szigorúan monoton növekvő / csökkenő

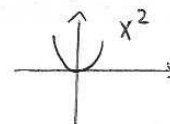
- lokálisan monoton növekvő / csökkenő

- globálisan monoton növekvő / csökkenő

- Paritás:

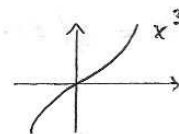
- páros, ha a függvény az y -tengelyre szimmetrikus,

$$f(-x) = f(x) \quad | \quad (-x)^2 = x^2$$



- páratlan, ha a függvény az origóra szimmetrikus,

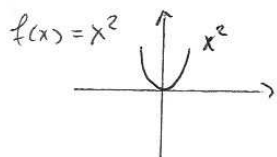
$$f(-x) = -f(x) \quad | \quad (-x)^3 = (-1)^3 \cdot x^3 = -x^3$$



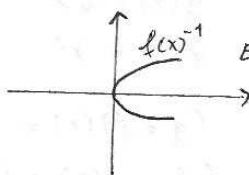
- Invertálhatóság:

• Definíció:

Egy függvényt invertálhatónak nevezük, ha az inverze is függvény.



x^2 inverze $\rightarrow$

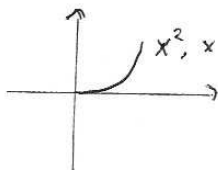


Ez nem függvény.

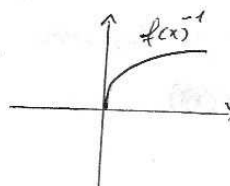
$\Rightarrow$ Tehát x^2 nem invertálható!

Azonban megszorítással invertálhatóvá válik egy adott intervallumon.

$$f(x) = x^2, \quad x \in [0, 1]$$



$x^2, x \in [0, 1] \rightarrow f(x)$ inverze $\rightarrow$



Ez függvény.

Tehát megfelelő megszorítással az x^2 függvény is invertálható.

- Injektivitás:

Egy függvény (f) ~~invertálható, azaz~~ injektív, ha bármely $b \in B$ f esetén egyértelműen létezik ősképe (értelmezési tartomány), azaz $a \in A$, hogy $f(a) = b$.

- Szürjektivitás:

Egy függvény (f) szürjektív, ha minden $b \in B$ -hez létezik ősképe.

$$f: \mathbb{N} \rightarrow \mathbb{N}, \quad f(n) = 2n + 4 \rightarrow \text{injektív}$$

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad f(x) = (x+3)^2 - 1 \rightarrow \text{egyik sem}$$

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad f(x) = 2 \cdot \sqrt{x} - 1 \rightarrow \text{injektív}$$

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad f(x) = \begin{cases} \frac{x}{2}, & x < 0 \\ x^2, & x \geq 0 \end{cases} \rightarrow \text{injektív és szürjektív}$$

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad f(x) = \log_2 x \rightarrow \text{injektív és szürjektív}$$

$$f: \mathbb{R} \rightarrow \mathbb{R}, \quad f(x) = \cos x \rightarrow \text{egyik sem, de } 1\pi \text{ szakaszon invertálható!}$$

• Függvények kompozíciója:

$$f: A \rightarrow B$$

$$g: R_f \subset B \rightarrow C$$

$$(g \circ f)(x) = g(f(x)) \leftarrow g \text{ és } f \text{ kompozíciója}$$

$$D_{g \circ f} = A$$

$$R_{g \circ f} = C$$

• Példa:

$$g(x) = \sin x$$

$$f(x) = x + 3$$

$$(g \circ f)(x) = \sin(x+3)$$

$$(f \circ g)(x) = \sin x + 3$$

$$g(x) = \sqrt{x}$$

$$f(x) = x^2$$

$$(g \circ f)(x) = \sqrt{x^2} = |x|$$

$$(f \circ g)(x) = (\sqrt{x})^2 = x$$

• Tétel:

Legyenek $f: A \rightarrow B$ és $g: B \rightarrow C$ függvények.

Ekkor $\supset g \circ f$ reláció is függvény.

- Jelölés: $(g \circ f)(x) = g(f(x))$

- bizonyítás:

Ha $(x, z) \in (g \circ f)$, akkor definíció szerint létezik olyan $y \in B$, melyre

$(x, y) \in f$ és $(y, z) \in g$. Mivel f függvény, így $y = f(x)$ egyértelműen

létezik, és ehhez az egyértelműen létező y -hoz egyértelműen tartozik

$z = g(y) = g(f(x))$, mert g is függvény. Eszerint bármely $x \in A$ esetén

egyértelműen létezik $z \in C$ így, hogy $z = (g \circ f)(x)$, azaz $(x, z) \in (g \circ f)$,

tehát $g \circ f$ is függvény.

Természetes számok ()

• Definíció:

A természetes számoknak adható egy axiómarendszere, amely egyértelműen megadja ezt a fogalmat, mi azonban ezt az axiómarendszert csak fogalempontosságra használjuk.

- Jele: $\mathbb{N} = \{1, 2, 3, \dots\}$

• Peano-axiómák:

- (1) Az 1 természetes szám,
- (2) minden természetes számnak van egy rákövetkezője, ami ugyancsak természetes szám
 n rákövetkezője n' ,
- (3) Az 1 egyetlen természetes számnak sem rákövetkezője
- (4) Ha $n' = m' \Rightarrow n = m$
- (5) A teljes indukció axiómája:

Ha a természetes számok egy részhalmazának az 1 eleme és abból, hogy az $(n = n')$ n eleme, az következik, hogy az n' is eleme, úgy a részhalmaz tartalmazza az összes természetes számot.

Azaz a teljes indukció azt jelenti, ha T teljesül 1-re, teljesül n -re, így $n+1$ -re is, akkor T teljesül minden természetes számra.

• Tétel:

A természetes számok halmaza rendelkezik a következő két tulajdonsággal:

(1) $\mathbb{N} \subset \mathbb{R}$ felől nem korlátos.

(2) Archimedeszi tulajdonság:

$$\forall x \in \mathbb{R}, x \geq 0 \text{ és } \forall y \in \mathbb{R} \text{ esetén } \exists n \in \mathbb{N}, y < n \cdot x.$$

• Teljes indukció elve:

• Lényege: Egyes megfigyelésekből törvényszerűségekre következtethetünk.

- (1) Ellenőrizni, hogy az állítás a legkisebb számmal teljesül-e.
- (2) Feltesszük, hogy az állítás igaz minden, valamilyen n vagy annál kisebb természetes számokra. (Indukciós feltevés)
- (3) Igazoljuk, hogy az állítás igaz $n+1$ -re, így a fentiekre is.

$$1 + 2 + 3 + \dots + n = \frac{n \cdot (n+1)}{2}$$

$$(1) \quad 1 = \frac{1 \cdot (1+1)}{2} \Rightarrow 1 = \frac{1 \cdot 2}{2} \Rightarrow 1 = \frac{2}{2} \Rightarrow 1 = 1 \quad \checkmark$$

$$(2) \quad n \quad \checkmark$$

$$(3) \quad \underbrace{1 + 2 + 3 + \dots + n}_{\frac{n \cdot (n+1)}{2}} + n + 1 = \frac{(n+1) \cdot ((n+1)+1)}{2} \Rightarrow \frac{n \cdot (n+1)}{2} + n + 1 = \frac{(n+1) \cdot (n+2)}{2} \Rightarrow$$
$$\Rightarrow \frac{n}{2} + 1 = \frac{n+2}{2} \Rightarrow \frac{n+2}{2} = \frac{n+2}{2}$$

• Műveletek természetes számok között:

Az összeadás és a szorzás elvégezhető velük.

$$\text{Ha } a, b \in \mathbb{N}, \text{ akkor } \left. \begin{array}{l} a+b=c \\ a \cdot b=d \end{array} \right\} c, d \in \mathbb{N}$$

• Definíció:

$$\left. \begin{array}{l} n+1=n' \\ n+m'=(n+m)' \\ 1 \cdot m=m \\ n \cdot m=n \cdot m+m \end{array} \right\} \begin{array}{l} \text{Az összeadás pontosan definiálható} \\ \parallel (n+m) \cdot r = n \cdot r + m \cdot r \end{array} \left. \begin{array}{l} \text{Tehát a } +, * \\ - \text{ asszociatív,} \\ - \text{ kommutatív,} \\ - \text{ disztributív.} \end{array} \right\} \text{felcsoport}$$

Az osztás és a kivonás azonban nem minden esetben végezhető el.

• Biner művelet:

$$f: A \times A \rightarrow A \text{ függvény biner művelet.}$$

- példa:

$$\left. \begin{array}{l} f(a, b) = a + b \\ f(a, b) = a \cdot b \end{array} \right\} \text{biner műveletek (egy számhoz és egy másik számhoz egy harmadik számot rendelünk.)}$$

Egész számok ()

• Definíció:

Azokat a valós számokat, amelyek előállnak két természetes szám különbségeként, egész számoknak nevezzük.

- Jele: $\mathbb{Z} = \{x \mid x \in \mathbb{R}, \exists m, n \in \mathbb{N} : x = m - n\}$.

$$\mathbb{Z} = \{-\infty \dots -2, -1, 0, 1, 2 \dots\}$$

A természetes számok halmaza'n nem tudjuk minden esetben maradéktalanul elvégezni a kivonást és az osztást.

Ha (n, m) pár, ahol $n, m \in \mathbb{N}$ reprezentálja $(n-m)$ -et, akkor

ha $(n, m) = (q, r)$ akkor $n+r = q+m$.

↑ Ekvivalencia reláció, hiszen osztályozást indukál.

Egy osztály egy egész szám.

- példa:

$$\begin{aligned} -3 \text{ osztálya: } & \left. \begin{aligned} (1, 4) &= 1-4 = -3 \\ (2, 5) &= 2-5 = -3 \\ (3, 6) &= 3-6 = -3 \end{aligned} \right\} \text{ Tehát } (1, 4), (2, 5) \text{ és } (3, 6) \text{ egy} \\ & \text{osztályba tartoznak.} \end{aligned}$$

• Definíció:

$$(n_1, m_1) + (n_2, m_2) \stackrel{\text{def.}}{=} (n_1 + n_2, m_1 + m_2)$$

$$(n_1, m_1) \cdot (n_2, m_2) \stackrel{\text{def.}}{=} (n_1 \cdot n_2 + m_1 \cdot m_2, m_1 \cdot n_2 + n_1 \cdot m_2)$$

$\Rightarrow$ Az összeadás kommutatív és asszociatív.

$\Rightarrow$ A szorzás is kommutatív és asszociatív.

$\Rightarrow$ Az összeadás és a szorzás disztributív.

• Félcsoport:

Egy G nem üres halmazt félcsoportnak nevezünk, ha értelmezett rajta egy asszociatív művelet.

- például: $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, \cdot)$

• Abel-féle félcsoport:

Legyen a halmazon értelmezett művelet kommutatív.

Ekkor G félcsoportot csoportnak nevezzük, ha $\exists$ neutrális elem és minden elemnek van inverze.

↑

A nullelem és az egységelem.

$$\forall a : a + 0 = a \quad \forall a : a \cdot 1 = a$$

• Definíció:

Inverz elem:

$$\forall a \exists a^{-1} \Rightarrow a \cdot a^{-1} = 1 \quad (\text{Egy elem és reciprokának szorzata 1.})$$

$$\forall a \exists -a \Rightarrow a + (-a) = 0 \quad (\text{Egy elem és negáltjának összege 0.})$$

$\Rightarrow$ Az összeadás additív

$\Rightarrow$ A szorzás multiplikatív

• Tétel:

$(\mathbb{I}, +)$ Az egész számok halmaza összeadás szerint csoport. (és asszociatív is)

• Gyűrű:

$R: +, \cdot$ $(R, +)$ kommutatív csoport
 $\uparrow$
ring $\Rightarrow$ A szorzás asszociatív
 $\Rightarrow$ A szorzás és az összeadás disztributív

• Példa:

$(\mathbb{I}, +, \cdot)$ Az egész számok összeadása és szorzása gyűrű.
-kommutatív, létezik egységelem, nullasztőmentes

Maradékos osztás ()

Legyen $a, b \in \mathbb{I}$, $a \geq 0$ és $b > 0$

$$a = r_1 \cdot b + r_2, \text{ ahol } r_1, r_2 \in \mathbb{I}, r_1, r_2 \geq 0 \text{ és } r_2 < b$$

$r_2 =$ maradék

$r_1 =$ hányados

-magyarázat: Ha $b > a$, akkor $a = 0 \cdot b + a$
Ha $a \geq b$, akkor addig vonjuk le, amíg $a < b$ nem lesz.

• Definíció:

$a \mid b$, ha $b = c \cdot a$, ahol $c \in \mathbb{I}$.

Ha $a, b \in \mathbb{I}$, $a \geq 0$ és $b \geq 0$,

Ha $b \mid a$ és $b > a$, akkor $a = 0$.

-bizonyítás:

$$a = q \cdot b \quad \text{Ha } 1 \mid 1 \quad a \neq 0, \text{ akkor } q \geq 1$$

$$1 \leq q \mid \cdot b$$

$$b \leq b \cdot q = a, \text{ ami ellentmond } b > a\text{-nak.}$$

Maradékos osztás ()

• Tétel:

$$a, b \geq 0, a, b \in \mathbb{I}$$

$$b \neq 0.$$

Ekkor egyértelműen $\exists q$ és $r \in \mathbb{I}$, hogy $a = q \cdot b + \underset{\substack{\uparrow \\ \text{maradék}}}{r}$ és $q \geq 0, 0 \leq r < b$

- bizonyítás:

Ilyen felírás létezik az első magyarázat alapján.

$$\left. \begin{array}{l} a = q_1 \cdot b + r_1 \\ a = q_2 \cdot b + r_2 \end{array} \right\} b > r_2 \quad (q_1 - q_2) \cdot b = \underbrace{r_1 - r_2}_{b > r_1 - r_2 \geq 0}$$

$$b \mid r_1 - r_2$$

$$b > r_1 - r_2$$

$$r_1 - r_2 = 0$$

$$r_1 = r_2$$

$$q_1 = q_2$$

Számrendszerek ()

Legyen b egy rögzített pozitív egész szám.

Ekkor tetszőleges 2 pozitív szám egyértelműen írható le az alábbi alakba:

$$A = a_n \cdot b^n + a_{n-1} \cdot b^{n-1} + \dots + a_1 b^1 + a_0,$$

ahol $0 \leq a_0, a_1, \dots, a_n < b$

- bizonyítás:

$$A = q_1 \cdot b + a_0 \quad \leftarrow \text{Ez egyértelmű}$$

$$q_1 = q_2 \cdot b + a_1 \quad \parallel b > 1$$

$$q_2 = q_3 \cdot b + a_2 \quad A > q_1 > q_2 > \dots \geq 0$$

• Ismert és gyakran használt számrendszerek:

- bináris
- oktális
- decimális
- hexadecimális

Oszthatóság ()

• Tétel:

$$a, b \in \mathbb{I}$$

$$a = b \cdot c, \text{ tehát } b \mid a$$

- Állítás:

Ha $b \mid a$, akkor $b \mid c \cdot a$, ahol $c \in \mathbb{I}$,

ha $a \mid b$ és $b \mid c$, akkor $a \mid c$,

ha $a \mid b$ és $b \mid a$, akkor $a = \pm b$.

Legyen $b, a > 0$.

Ha $a \neq 0$, akkor $b \leq a$.

Az osztó nem lehet nagyobb, mint a szám, kivéve ha a nullát osztjuk.

$$0 \leq b \leq a$$

• Tétel:

Minden, nullától különböző egész számnak csak véges sok osztója van.

- bizonyítás: Elegendő csak a pozitív egészek körébe vizsgálni.

Oszthatósági szabályok ()

$$A = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0$$

$$a_0, a_1, \dots, a_n \in \{0, 1, 2, \dots\}$$

$$2 \mid A \Leftrightarrow 2 \mid a_0$$

$$4 \mid A \Leftrightarrow 4 \mid 10 \cdot a_1 + a_0$$

$$A = a_n \cdot (10 - 1) + a_{n-1} \cdot (10 - 1) + \dots + a_1 \cdot (10 - 1) + (a_n + a_{n-1} + \dots + a_1 + a_0)$$

$$3 \mid A \Leftrightarrow 3 \mid (a_n + a_{n-1} + \dots + a_0)$$

$$9 \mid A \Leftrightarrow 9 \mid (a_n + a_{n-1} + \dots + a_0)$$

Legnagyobb közös osztó ()

c a és b legnagyobb közös osztója, ha $c \mid a$ és $c \mid b$, továbbá, hogy ha valamely szám osztója mind az a -nak, mind a b -nek, akkor osztható c -vel is.

- Állítás: Bármely 2 egész számnak létezik legnagyobb közös osztója.

A pozitív egészek körében a legnagyobb közös osztó egyértelmű.

Euklideszi algoritmus ()

A legnagyobb közös osztó létezését beláthatjuk az Euklideszi algoritmus alkalmazásával.

• Működési elve:

Egy egész szám osztóját osztjuk mindig a maradékkal, amíg a maradék nulla nem lesz.
Ez a maradék adja meg a szám és az osztó legnagyobb közös osztóját.

Lineáris diophantosi egyenletek ()

• Lényege: Megoldásait az egészek között keressük.

Olyan egyenletek, amelyeknél az együtthatók egészek és a megoldás is az egészes számok halmazán található.

• Tétel:

$$ax + by = c \quad \text{megoldható} \Leftrightarrow \text{Inko}(a, b) \mid c$$

- bizonyítás:

• Tegyük fel, hogy megoldható, ekkor...

(1) $\text{Inko}(a, b)$ osztható c -vel, a -val, b -vel, ax -vel, by -al és $ax+by$ -al is.

(2) $\text{Inko}(a, b) = ax_1 + by_1 \quad / \cdot d$

$$c = a \cdot \underbrace{x_1 d}_x + b \cdot \underbrace{y_1 d}_y \quad // \text{Inko}(a, b) = c$$

Legkisebb közös többszörös ()

Két egész szám legkisebb közös többszörösét így kapjuk meg, hogy összeszorozzuk azokat a prímtenyezőikkel, amelyek legalább az egyikben szerepel és az előforduló prímtenyezők közül is a legnagyobb hatványon levőket.

- példa:

$$a = 2^3 \cdot 5^4 \cdot 11^2$$

$$\text{lkkt}(a, b) = 2^3 \cdot 5^8 \cdot 11^2$$

$$b = 2^1 \cdot 5^8 \cdot 11^2$$

$$\text{Inko}(a, b) = 2^1 \cdot 5^4$$

$$a \cdot b = \text{Inko}(a, b) \cdot \text{lkkt}(a, b)$$

$$\text{lkkt}(a, b) = a \cdot b / \text{Inko}(a, b)$$

• Definíció:

A számelméletben két vagy több pozitív egész szám legkisebb közös többszörösén azt a legkisebb pozitív egész számot értjük, amely az adott számok mindegyikével osztható.

Prímszámok ()

• Tétel:

$p > 1$ prímszám egész, ha csak 1-gyel és önmagával osztható.

• Eratosthenesi szita:

- Definíció szerint a nulla nem prímszám, de az egy prímszám.
- felírjuk az 1-nél nagyobb, pozitív egész számokat
- kijelöljük a kettes számot, majd az öt követő 2-vel osztható számokat kivesszük a listából,
- kijelöljük a hármas számot, majd az öt követő 3-mal osztható számokat kivesszük a listából,
- a négyes számot már kivettük a listából, mert osztható 2-vel,
- ezen az elven megszámlálhatatlan végtelen lépésből megkapjuk a prímszámok halmazát.

• Állítás:

A prímszámok száma végtelen.

-bizonyítás:

Indirekt tegyük fel, hogy csak véges számú prímszám van.

$p_1, p_2, \dots, p_n$ • Mi a prímtényező felbontása a -nak?

$a = p_1 p_2 \dots p_{n+1} \leftarrow a$ -nak egyetlen prímszám sem prímtényezője $\Rightarrow$ ~~X~~ ellentmondás!

Tehát a nem osztható p_1 -el, mert hozzáadtunk 1-et, ami a maradék.

• Állítás:

A prímszámok sorozatában tetszőleges hosszú hízag található.

$$M < p^{\text{prim}}$$

• Tétel:

$$p \text{ prim} \Leftrightarrow p \mid a \cdot b \Rightarrow p \mid a \text{ vagy } p \mid b.$$

$$\left. \begin{array}{l} 2 \cdot 3 \cdot 4 \cdot \dots \cdot p+2 \\ -11-+3 \\ \vdots \\ -11-+p \end{array} \right\} \text{ Ezeket a számokat hozzáadva a} \\ \text{szám már nem lesz prímszám.}$$

• Aritmetika alaptétele: (Egyértelmű prímfaktorizáció)

Minden pozitív, egész számnak van prim osztója.

Minden pozitív, egész szám egyértelműen felírható: $a = p_1^{d_1} \cdot p_2^{d_2} \cdot \dots \cdot p_r^{d_r}$

- Jelmagyarázat:

- példa: $12 = 2^2 \cdot 3^1$

$p_1, p_2, \dots, p_r =$ különböző prímek

$d_1, d_2, \dots, d_r =$ pozitív egészek

• Relatív prímek:

A és B szám relatív prím, ha az $|1|$ -en kívül nincs más közös osztójuk.

Minden prímszám tetszőleges másik prímszámmal relatív prím.

Egy prímszámmal minden nála kisebb természetes szám relatív prím.

• Kongruencia:

A kongruencia egy reláció, amelyet az egész számok halmazán értelmezünk. Egy ilyen reláció kifejezi, hogy 2 szám adott számmal vett osztási maradéka egyenlő-e.

Legyen a, b tetszőleges, m pozitív egész szám.

Azt mondjuk, hogy a kongruens b -vel modulo m , azaz a és b egészeit m -mel vett osztási maradéka egyenlő, ha $m \mid (a - b)$, azaz $\exists k \in \mathbb{Z} : a = k \cdot m + b$

Ha a nem kongruens b -vel modulo m , azt mondjuk, hogy inkongruens vele.

Ha $a \equiv b \pmod{0} \Rightarrow a = b$ $7 \equiv 4 \pmod{3}$ ($7 \% 3 = 1, 4 \% 3 = 1$)

• Definíció:

A kongruencia reláció ekvivalencia és művelettartó, azaz szorozható és összeadható.

$$\left. \begin{array}{l} 7 \equiv 4 \pmod{3} \\ 11 \equiv 8 \pmod{3} \\ 18 \equiv 12 \pmod{3} \\ 74 \equiv 32 \pmod{3} \end{array} \right\} \begin{array}{l} \swarrow \\ \downarrow + \\ \swarrow \end{array}$$

• Maradékosztályok: (2-re vett maradékosztály esetén)

2 eset létezik: $\{\text{páros}\}, \{\text{páratlan}\}$
 $x \% 2 = 0 \quad x \% 2 = 1$

- 2-re vett maradék osztályok teste:

+	0	1
0	0	1
1	1	0

•	0	1
0	0	0
1	1	1

- kommutatív
- asszociatív
- disztributív
- van nullelem (0)
- van egységelem (1)

- 0 additív inverze $\Rightarrow 0 + \underline{0} = 0$
- 1 additív inverze $\Rightarrow 1 + \underline{1} = 0$

$$T = \{0, 1\}$$

$(T, +, \cdot)$ test

Tehát a 2-re vett maradék osztály egy 2 elemű, véges elemszámú test.

Ha $m > 1$ egész $\rightarrow \pmod{m}$ maradékosztályai:

$$\{0\}, \{1\}, \{2\}, \dots, \{m-1\}$$

Tehát m maradékosztály van.

Maradek osztályok (mod m)

• Műveletek maradékosztályokkal:

$$\{a\} + \{b\} = \{a+b\}$$

$$\{a\} \cdot \{b\} = \{a \cdot b\}$$

Az $+$ és $\cdot$ a reprezentánsaként működik.

$$\{0+1\} = \{1\}$$

$$\{3+4\} = \{7\} = \{1\}$$

$$\{0 \cdot 1\} = \{0\}$$

$$\{3 \cdot 4\} = \{12\} = \{0\} \quad (12 \% 3 = 0)$$

A maradékosztályok gyűrűt alkotnak.

• Definíció:

Ha m prím $\Rightarrow (\text{mod } m)$ maradékosztályok testet alkotnak.

$$\{a\} \cdot \{x\} = \{1\}$$

$$a \cdot x = y \cdot m + 1$$

$$a \cdot x - y \cdot m = 1 \Leftrightarrow \text{Inko}(a, m) \mid 1 \quad (\text{hiszen a prímszámoknak csak az 1 közös osztója})$$

• megjegyzés:

Teljes maradékhrendszer: minden maradékosztályból 1-1 reprezentáns.

Az Euler-féle φ -függvény ()

• Definíció:

$\varphi(m) = \# \{0, 1, 2, \dots, m-1\}$ halmazban az m -hez relatív prímek számát adja meg.

• Állítás:

φ multiplikatív, $\varphi(a, b) = \varphi(a) \cdot \varphi(b) \Leftrightarrow a$ és b relatív prím ($\text{Inko}(a, b) = 1$)

• A φ -függvény alkalmazása:

$$\varphi: \mathbb{N} \rightarrow \mathbb{N}$$

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_r}\right)$$

$$\varphi(15300) = 3840$$

- levezetés:

15300	2
7650	2
3825	3
1275	3
425	5
85	5
17	17
1	

$$\begin{aligned} \varphi(15300) &= 15300 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{17}\right) = \\ &= 15300 \cdot (0,5) \cdot \left(\frac{2}{3}\right) \cdot \left(\frac{4}{5}\right) \cdot \left(\frac{16}{17}\right) = \underline{\underline{3840}} \end{aligned}$$

Euler-tétel ()

• Definíció:

$$a^{\varphi(m)} \equiv 1 \pmod{m} \Leftrightarrow a \text{ és } m \text{ relatív prím}$$

- példa:

$$5^{\varphi(12)} \equiv 1 \quad \varphi(12) = \underline{4}$$

$$5^4 = 625 = \underline{1}$$

$$625 : 12 = 52$$

$$\begin{array}{r} 25 \\ 1 \\ \hline \end{array}$$

Fermat-tétel ()

• Definíció: (kis Fermé-tétel)

$$a^{p-1} \equiv 1 \pmod{p} \Leftrightarrow p \text{ prím és } a \text{ nem osztható } p\text{-vel.}$$

- Euler: $a^{\varphi(p)} \equiv 1 \pmod{p} \Leftrightarrow a \text{ és } p \text{ relatív prím}$

$\Downarrow$

$$a^{p-1} \quad // \text{ Euler tételének egyszerű következménye a kis Fermé-tétel}$$

- példa:

$$4^{\varphi(3)} \equiv 1 \pmod{3}$$

$$4^2 \equiv 1 \pmod{3}$$

$$\underline{1} = 1$$

$$\begin{array}{r} 16 : 3 = 5 \\ \underline{1} \end{array}$$

Racionális számok ()

• Definíció:

Azokat a valós számokat, amelyeket előállnak 2 egész szám hányadosaként, racionális számoknak nevezzük.

- Jele: $\mathbb{Q} = \{x \mid x \in \mathbb{R}, \exists p, q \in \mathbb{Z}, q \neq 0 : x = \frac{p}{q}\}$

• Definíció:

Az $\mathbb{R} \setminus \mathbb{Q}$ halmaz elemeit irracionális számoknak nevezzük, ezek végtelen, nem szakaszos törték.

A racionális számok halmaza így néz ki: $\mathbb{Q} = \{\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \dots\}$

$(a_1, b_1) \sim (a_2, b_2)$ ha $a_1 \cdot b_2 = a_2 \cdot b_1$ ← ekvivalencia reláció, ami osztályozást indukál.

• Definíció:

Egy racionális szám nem más, mint a fenti ekvivalencia egy osztálya.

$(\mathbb{Q}, +)$ A racionális számok halmaza Abel-csoport

Hiszen az összeadás asszociatív, van nullelem, van additív inverz és kommutatív.)

$$(a, b) + (c, d) \stackrel{\text{def.}}{=} (ad + bc, bd) \quad \parallel \quad 0 + 0 = 0$$

$(\mathbb{Q}, +, \cdot)$ A racionális számok halmaza test

Hiszen az összeadás Abel-csoport és a szorzás asszociatív, kommutatív, van egységelem, van multiplikatív inverz és disztributív.

$$(a, b) \cdot (c, d) \stackrel{\text{def.}}{=} (a \cdot c, b \cdot d)$$

• Definíció:

$T \neq \emptyset$ test, ha van rajta 2 biner művelet: $+$ és $\cdot$

$(T, +)$ Abel-csoport

$$T = \{0, 1\}$$

$+$	0	1
0	0	1
1	1	0

$1 + 1 = 0$
Páratlan + páratlan = páros

$\cdot$	0	1
0	0	0
1	0	1

$1 \cdot 0 = 0$
Páratlan $\cdot$ páros = páros

• megjegyzés: Sem a természetes, sem az egész számok nem alkotnak testet!

• Tétel:

A racionális számok nem teljes rendezett testet alkotnak.

- például:

A teljesség nem teljesül, ha

$\{a \in \mathbb{Q} : a \leq \sqrt{2}\}$ felülről korlátos, de $\sup \notin \mathbb{Q}$.

Rendezés ()

• Definíció:

Ha $a \in \mathbb{N}$, akkor ha $a > 0 \stackrel{\text{def.}}{\iff} a \in \mathbb{N}$

$\frac{a}{b} \in \mathbb{Q}$, akkor ha $a > 0 \stackrel{\text{def.}}{\iff} a > 0$ és $b > 0$ vagy $a < 0$ és $b < 0$.

Ha $c, d \in \mathbb{Q}$, akkor $c > d \stackrel{\text{def.}}{\iff} c - d > 0$

Ha $c, d \in \mathbb{Q}$, akkor $c \geq d \stackrel{\text{def.}}{\iff} c > d$ vagy $c = d$

• Állítás:

$\geq$ reláció rendezési reláció (reflexív, antiszimmetrikus, tranzitív és lineáris) $\mathbb{Q}$ -n.

$(\mathbb{Q}, +, \cdot, \leq)$ rendezett test, akkor $(\mathbb{Q}, +, \cdot)$ test $\leq$ rendezés, és:

ha $a \leq b$, akkor $a + c \leq b + c$

ha $a \leq b$ és $c \geq 0$, akkor $a \cdot c \leq b \cdot c$

• Archimédész törvény:

$r > 0$ és $s > 0$ racionális szám, akkor, ha $\exists k \in \mathbb{N}$, hogy $s < kr$.

• Tétel (tizedes tört alak):

A racionális számok véges vagy végtelen szakaszos tizedestört alakban is felírhatók.

Van nem racionális szám is!

- például:

Minden, nem teljes négyzetből vent gyök.

$\sqrt{2}$ $\rightarrow$ nem racionális

$\sqrt{2} = \frac{a}{b} \rightarrow 2b^2 = a^2$ (redukált alak)

$2b^2 = a^2$ (a és b relatív prím)

2^x

Valós számok ()

Definíció:

Legyen adott egy $\mathbb{R}$ halmaz és legyen rajta értelmezve 2 művelet:

$$f_1: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}, f_1(x, y) = x + y \quad \forall x, y \in \mathbb{R}$$

$$f_2: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}, f_2(x, y) = x \cdot y \quad \forall x, y \in \mathbb{R}$$

Azt mondjuk, hogy $(\mathbb{R}, +, \cdot)$ test, ha teljesíti az alábbi tulajdonságokat, az úgynevezett testaxiómákat:

1. kommutativitás

$$x + y = y + x \quad \forall x, y \in \mathbb{R}$$

$$x \cdot y = y \cdot x \quad \forall x, y \in \mathbb{R}$$

2. asszociativitás

$$(x + y) + z = x + (y + z) \quad \forall x, y, z \in \mathbb{R}$$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z) \quad \forall x, y, z \in \mathbb{R}$$

3. disztributivitás

$$x \cdot (y + z) = x \cdot y + x \cdot z \quad \forall x, y, z \in \mathbb{R}$$

4. létezik zéruselem (0)

$$\exists 0 \in \mathbb{R} : x + 0 = x \quad \forall x \in \mathbb{R}$$

5. létezik additív inverz

$$\forall x \in \mathbb{R} \text{ esetén } \exists (-x) \in \mathbb{R} : x + (-x) = 0$$

6. létezik egységelem (1)

$$\exists 1 \in \mathbb{R}, 1 \neq 0 : x \cdot 1 = x \quad \forall x \in \mathbb{R}$$

7. létezik multiplikatív inverz

$$\forall x \in \mathbb{R}, x \neq 0 \text{ esetén } \exists (x^{-1}) \in \mathbb{R} : x \cdot (x^{-1}) = 1$$

Definíció:

Legyen adva az $\mathbb{R}$ testen egy $\leq$ rendezési reláció: $\leq \subset \mathbb{R} \times \mathbb{R}$.

Azt mondjuk, hogy $(\mathbb{R}, +, \cdot, \leq)$ rendezett test, ha teljesül az alábbi két tulajdonság:

1, ha $x, y \in \mathbb{R}$ és $x \leq y$, akkor $x + z \leq y + z \quad \forall z \in \mathbb{R}$,

2, ha $x, y \in \mathbb{R}$ és $x \geq 0, y \geq 0$, akkor $x \cdot y \geq 0$.

• Definíció:

Az $(\mathbb{R}, +, \cdot, \leq)$ rendezett test teljes, ha bármely felülről korlátos nemüres részhalmazának létezik pontos felső korlátja.

A valós számok halmazának nevezzük egy teljes rendezett testet.

• Tétel:

- $\mathbb{R}$ -ben az egységelem és a nullelem egyértelműen létezik,
- minden $\mathbb{R}$ -beli elemnek egyértelműen létezik additív inverze,
- minden nem nulla valós számnak létezik multiplikatív inverze.

• Tétel (Egyszerősítési szabály):

- 1, Ha $x, y, z \in \mathbb{R}$, $x + y = x + z$, akkor $y = z$.
- 2, Ha $x, y, z \in \mathbb{R}$, $x \neq 0$, $x \cdot y = x \cdot z$, akkor $y = z$.

• Tétel (Kivonási és osztási szabály):

- 1, Bármely $x, y \in \mathbb{R}$ esetén egyértelműen létezik $z_1 \in \mathbb{R}$, amelyre $x = y + z_1$.
 z_1 jele: $x - y$.
- 2, Bármely $x, y \in \mathbb{R}$, $y \neq 0$ esetén egyértelműen létezik $z_2 \in \mathbb{R}$, amelyre $x = y \cdot z_2$.
 z_2 jele: $\frac{x}{y}$.

• Definíció:

Legyen $x \in \mathbb{R}$. Ekkor x abszolút értékét az alábbi módon definiáljuk:

$$|x| = \begin{cases} x, & \text{ha } x \geq 0, \\ -x, & \text{ha } x < 0. \end{cases}$$

• Az abszolút érték tulajdonságai:

- 1, $|-x| = |x|$
- 2, $|x \cdot y| = |x| \cdot |y|$
- 3, $\left| \frac{x}{y} \right| = \frac{|x|}{|y|}$
- 4, $|x + y| \leq |x| + |y|$
- 5, $||x| - |y|| \leq |x - y|$

Valós számok ()

• Tétel:

Bármely $x \in \mathbb{R}$, $x \geq 0$ és $n \in \mathbb{N}$ esetén egyértelműen létezik $y \in \mathbb{R}$ és $y \geq 0$, melyre $y^n = x$. $\parallel x^0 \stackrel{\text{def.}}{=} 1$

• Definíció:

Legyen $x \in \mathbb{R}$, $x \geq 0$ és $n \in \mathbb{N}$. Azt az egyértelműen létező $y \in \mathbb{R}$ nem negatív számot, melyre $y^n = x$ teljesül, az x valós szám n -edik gyekének nevezzük.

- Jele: $\sqrt[n]{x} = y$ vagy $x^{\frac{1}{n}} = y$.

• Definíció:

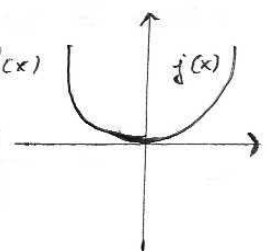
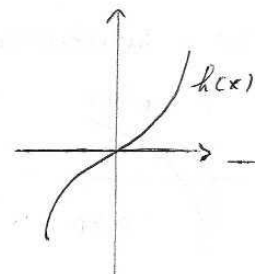
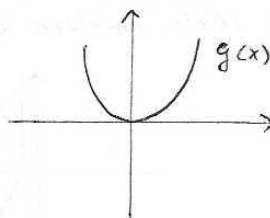
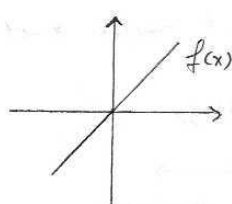
Ha $S \subset \mathbb{R}$ felülről nem korlátos, akkor $\sup S = \infty$ és ha $S \subset \mathbb{R}$ alulról nem korlátos, akkor $\inf S = -\infty$. Ha ezzel a két szimbólummal kibővítjük a valós számok halmazát, akkor az így kapott halmazt a bővített valós számok halmazának nevezzük.

$$\mathbb{R}_b = \mathbb{R} \cup \{\infty\} \cup \{-\infty\}$$

$\mathbb{R}_b$ azonban nem test!

Valós függvények ()

- $f(x) = x$
- $g(x) = x^2$
- $h(x) = x^3$
- $j(x) = x^4$



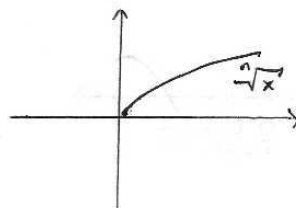
• Megjegyzés:

- páros hatványon a függvény lefutása $\cup$ irányú,
- páratlan hatványon a függvény lefutása $/$ vagy $\backslash$ irányú,
- a páros hatványú függvények csak a $[0, \infty]$ intervallumon invertálhatóak,
- a páratlan hatványú függvények invertálhatóak.

• Definíció:

$n \in \mathbb{N}$, $x \geq 0$, $\exists z \geq 0$, hogy $z^n = x$. z az x n -edik gyöke.

- Jele: $\sqrt[n]{x}$



Definíció:

$x \geq 0$ valós szám

$$x^{\frac{m}{n}} \stackrel{\text{def.}}{=} (\sqrt[n]{x})^m, \quad n, m \in \mathbb{N}$$

$$x^{-a} \stackrel{\text{def.}}{=} \frac{1}{x^a} \quad a \text{ racionális szám és nagyobb, mint nulla.}$$

$\Rightarrow$ Ezzel az eljárással tetszőleges racionális hatványt definiáltunk.

$$x^a \quad \underbrace{x \in \mathbb{R}}_{\text{valós}}, \underbrace{a \in \mathbb{Q}}_{\text{racionális}}, \quad x > 0$$

$$\begin{aligned} // x^{a+b} &= x^a \cdot x^b \\ // x^{a \cdot b} &= (x^a)^b \end{aligned}$$

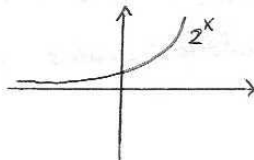
Exponenciális és logaritmus függvény ()

$$f(x) = a^x, \quad a > 0, \quad a \neq 1$$

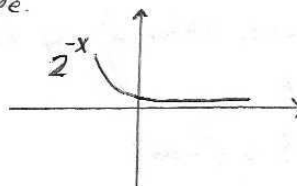
$$f(x) = 2^x$$

$$f(x) = \left(\frac{1}{2}\right)^x = 2^{-x}$$

a^x és $\left(\frac{1}{a}\right)^x$
egymásnak tükörképe.



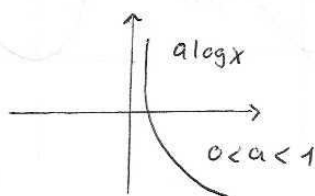
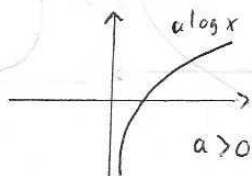
- szigorúan monoton nő
- folytonos
- invertálható



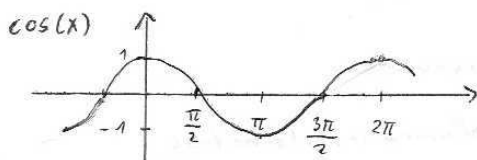
- szigorúan monoton csökken
- folytonos
- invertálható

$$f(x) = a^x, \quad a > 0, \quad a \neq 1 \text{ inverze } a \log x.$$

$a \log x \stackrel{\text{def.}}{=} \text{Az a hatványkitevőt jelöli, amelyre a-t emelve x-et kapom.}$

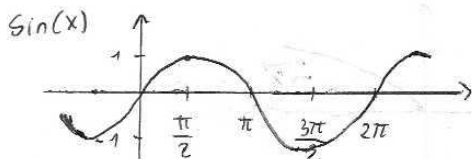


Trigonometrikus függvények ()



• Cosinus: Azon egységvektor első koordinátája, amelynek fergősszöge x .

• Sinus: Azon egységvektor második koordinátája, amelynek fergősszöge x .



- arc cos x : $\cos x \in [0; \pi]$ inverze

- tg : $\frac{\sin}{\cos}$ - ctg : $\frac{\cos}{\sin}$

komplex számok ()

• Definíció:

Tekintsük a valós számokból képzett (a, b) számpárok halmazát. Ezen a halmazon értelmezzük a szorzás és az összeadás műveletét az alábbi módon:

$$(a, b) + (c, d) \doteq (a + c, b + d)$$

$$(a, b) \cdot (c, d) \doteq (a \cdot c - b \cdot d, b \cdot c + a \cdot d)$$

A valós számpárok halmazát ezen két művelettel ellátva komplex számoknak nevezzük.

Ha $z \in \mathbb{C}$ és $z = (a, b)$, akkor a $\operatorname{Re}(z) \doteq a$ számot a komplex szám valós részének nevezzük, és az $\operatorname{Im}(z) \doteq b$ számot pedig a komplex szám képzetes (imaginárius) részének nevezzük.

$\Rightarrow$ két komplex szám csak akkor egyenlő, ha a valós és képzetes részük is megegyezik.

• Tétel:

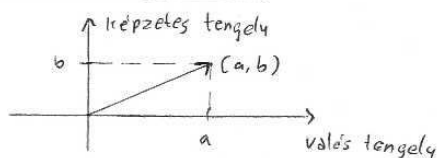
$\mathbb{C}$ test, hiszen additív, kommutatív, asszociatív, létezik nullaelem és létezik additív inverz, multiplikatív, valamint disztributív.

• Definíció:

- Algebrai alak:

$$Z = a + i \cdot b, \quad a, b \in \mathbb{R}$$

- Gauss-féle számsík:



$$(3 + 4i) + (2 + 2i) = (3 + 2) + (4 + 2) \cdot i$$

$$(3 + 4i) - (2 + 2i) = (3 - 2) + (4 - 2) \cdot i$$

$$(2 + 3i) \cdot (4 - 5i) =$$

$$= (2 \cdot 4 - 3 \cdot (-5)) + (3 \cdot 4 + 2 \cdot (-5)) \cdot i$$

• Tétel:

$$i^2 = -1$$

- bizonyítás:

$$(0, 1) \cdot (0, 1) = (0 - 1, 0 + 0) = (-1, 0) = -1 (+0 \cdot i)$$

$$\Rightarrow \text{Ebből következően } \sqrt{-1} = i$$

• Definíció:

Egy $z \in \mathbb{C}$, $z = a + i \cdot b$ szám konjugáltja: $\bar{z} \doteq a - i \cdot b$.

A konjugált képzés felcserélhető a többi művelettel: $\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2$

• Definíció:

Egy komplex szám abszolút értéke éppen a vektor hossza.

$$|z| = \sqrt{a^2 + b^2} \Rightarrow (\sqrt{a^2 + b^2})^2 = a^2 + b^2$$

$$(a + b \cdot i) \cdot (a + b \cdot i) = a^2 + a \cdot b \cdot i + a \cdot b \cdot i + b \cdot i^2 = a^2 + 2abi + b \cdot i^2 = \underline{\underline{a^2 + 2abi - b^2}}$$

Egy $z \in \mathbb{C}$ szám abszolút értéke a $|z| = \sqrt{z \cdot \bar{z}}$ nem negatív valós számot értjük.
Ekkor $|z| = \sqrt{a^2 + b^2}$

• Tétel:

Az abszolút érték tulajdonságai:

1., $0 \leq |z|$ és $|z| = 0 \Leftrightarrow z = 0$,

2., $|\bar{z}| = |z|$,

3., $|z \cdot w| = |z| \cdot |w|$,

4., $|\operatorname{Re}(z)| \leq |z|$,

5., $|\operatorname{Im}(z)| \leq |z|$,

6., $|z + w| \leq |z| + |w|$.

Műveletek komplex számokkal ()

• Összeadás: $(a, b) + (c, d) = (a + c, b + d)$

• Szorzás: $(a, b) \cdot (c, d) = (a \cdot c - b \cdot d, b \cdot c + a \cdot d)$

• Kivonás: $(a, b) - (c, d) = (a - c, b - d)$

• Osztás:

• A nulla komplex szám

• $z_2 \neq 0$

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \bar{z}_2}{z_2 \cdot \bar{z}_2} = \frac{z_1 \cdot \bar{z}_2}{|z_2|^2}$$

- példa:

$$\frac{2-3i}{1+4i} = \frac{(2-3i) \cdot (1-4i)}{(1+4i) \cdot (1-4i)} = \frac{2-3i-8i-12}{1^2+4^2} = \frac{-10-11i}{17} = \underline{\underline{-\frac{10}{17} - \frac{11}{17}i}}$$

A tételt bővítsük a nevező konjugáltjával!

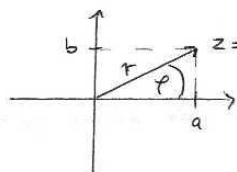
Komplex számok ()

• Definíció:

- Trigonometrikus alak:

$$Z = |z| \cdot (\cos \varphi + i \sin \varphi)$$

$$0 \stackrel{\text{def.}}{=} (0, \varphi = \text{akármennyi})$$



$$r = |z|$$

$$a = r \cdot \cos \varphi$$

$$b = r \cdot \sin \varphi$$

↳ Nullvektor esetén nem számít a forgásszög.

A trigonometrikus alak összeadásra és kivonásra nem jó, de szorzásra, osztásra, gyökvételre és hatványozásra igen!

Műveletek trigonometrikus alakkal ()

Komplex számok szorzásakor az abszolút értékek szorozódnak, az argumentumok összeadódnak.

$$Z = (r, \varphi) = (r, \varphi + 2 \cdot k \cdot \pi), \text{ ahol } k \text{ lehet } 0, \pm 1, \pm 2, \dots$$

Argumentum (a valós tengellyel bezárt szög)

Abszolút érték

$$\text{Legyen } Z = |z| \cdot (\cos \varphi + i \sin \varphi)$$

$$W = |w| \cdot (\cos \psi + i \sin \psi)$$

$$Z \cdot W = |z| \cdot |w| \cdot [\cos(\varphi + \psi) + i \sin(\varphi + \psi)]$$

$$\frac{Z}{W} = \frac{|z|}{|w|} \cdot [\cos(\varphi - \psi) + i \sin(\varphi - \psi)]$$

• Komplex számok hatványozása:

$$Z^1 \stackrel{\text{def.}}{=} Z$$

$$Z^{n+1} \stackrel{\text{def.}}{=} Z^n \cdot Z, \text{ ahol } n \text{ természetes szám}$$

$$Z^3 \stackrel{\text{def.}}{=} Z \cdot Z \cdot Z$$

$$Z^n \stackrel{\text{def.}}{=} \underbrace{Z \cdot Z \cdot \dots \cdot Z}_{n \text{ db-szor}}$$

$$Z^{-n} \stackrel{\text{def.}}{=} \frac{1}{Z^n}, \text{ ahol } n \text{ természetes szám és } Z \neq 0$$

$$Z^0 \stackrel{\text{def.}}{=} 1$$

$$\text{Legyen } Z = r \cdot (\cos \alpha + i \sin \alpha)$$

$$Z^n = r^n (\cos n \cdot \alpha + i \sin n \cdot \alpha)$$

Gyökvenés komplex számokból ()

• Definíció:

Legyen $z = r \cdot (\cos \alpha + i \cdot \sin \alpha)$

$$\sqrt[n]{z} = \sqrt[n]{r} \cdot \left(\cos \frac{\alpha}{n} + i \cdot \sin \frac{\alpha}{n} \right)$$

• Egyseggyökök:

$$[r \cdot (\cos \alpha + i \cdot \sin \alpha)]^n = 1 \quad (\text{Az 1 komplex szám } n\text{-edik gyökeit } n\text{-edik egyseggyökeinek nevezzük})$$

$$r^n = 1 \rightarrow r = 1$$

$$n \cdot \alpha = 2 \cdot k \cdot \pi \quad k = 0, \pm 1, \pm 2, \dots$$

$$\alpha = \frac{2 \cdot k \cdot \pi}{n} \quad k = 0, 1, 2, \dots, n-1$$

Pontosan n darab n -edik egyseggyök van és ezek $k = 0, 1, 2, \dots, n-1$

• Definíció:

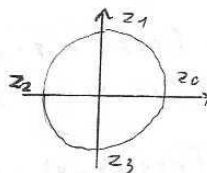
$$\sqrt[n]{1} = \sqrt[n]{|1|} \cdot \left[\cos \left(\frac{0 + 2 \cdot k \cdot \pi}{n} \right) + i \cdot \sin \left(\frac{0 + 2 \cdot k \cdot \pi}{n} \right) \right] = \left(\cos \frac{2k\pi}{n} + i \cdot \sin \frac{2k\pi}{n} \right)$$

$\epsilon_{n,k} \rightarrow n$ -edik egyseggyök

$$\epsilon_{n,k} = \cos \frac{k \cdot \pi}{2} + i \cdot \sin \frac{k \cdot \pi}{2} \quad k = 0, 1, 2, 3$$

Az egysegkörbe mindig egy szabályos n -szög rajzolódik ki.

A szög első csúcsa mindig 1.



• Gyökvenés tetszőleges komplex számból az egyseggyökök segítségével:

$$z \neq 0 \quad \sqrt[n]{z} = ?$$

$$z = r \cdot (\cos \alpha + i \cdot \sin \alpha)$$

$$\sqrt[n]{z} = \sqrt[n]{r} \cdot \left(\cos \frac{\alpha}{n} + i \cdot \sin \frac{\alpha}{n} \right)$$

$$\sqrt[n]{r} \cdot \left(\cos \frac{\alpha}{n} + i \cdot \sin \frac{\alpha}{n} \right) \cdot \left(\cos \frac{2k\pi}{n} + i \cdot \sin \frac{2k\pi}{n} \right) = \sqrt[n]{r} \cdot \left(\cos \frac{\alpha + 2k\pi}{n} + i \cdot \sin \frac{\alpha + 2k\pi}{n} \right)$$

$\frac{W}{z_0}$ jelölje $\sqrt[n]{z}$ -t!

$$\frac{W}{z_0} = ?$$

$z_0 = n$ -edik gyöke z -nek

$$\left(\frac{W}{z_0} \right)^n = \frac{z}{z} = 1$$

$$(z_0)^n = z$$

$$(\sqrt[n]{z})^n = z$$

n darab, $k = 0, 1, 2, \dots, n-1$

n darab, különböző n -edik

gyöke van minden nem

nulla komplex számnak.

• Primitív egyseggyökök:

Olyan egyseggyökök, amelynek hatványai kiadja az összes egyseggyököt. (például: $\frac{2\pi}{n}$)

• Exponenciális alak:

$$e^{i \cdot \alpha} \stackrel{\text{def}}{=} \cos \alpha + i \cdot \sin \alpha, \quad \alpha \in \mathbb{R}$$

$$r \cdot \cos \alpha + i \cdot r \cdot \sin \alpha = (r, \varphi) = r \cdot e^{i \cdot \alpha}$$

// r = alap

// φ = argumentum

Algebrai struktúrák ()

• Definíció:

Algebrai struktúrának egy olyan S halmazt értünk, amely legalább 1 művelettel el van látva.

• Egyműveletes struktúrák:

- Félcsoport:

Legyen G egy halmaz, értelmezzünk G halmazon egy szorzás műveletet. Ekkor...

$(G, \cdot)$ félcsoport, ha a $\cdot$ művelet asszociatív (zárosiként)

- ha a G halmazon értelmezett szorzás kommutatív, akkor $\rightarrow$ kommutatív félcsoport

- Csoport:

A G halmazt csoportnak nevezzük, ha létezik minden elemnek inverze:

$\forall a \in G$ -hez $\exists$ olyan b elem, hogy: $a \cdot b = b \cdot a = 1$, ekkor

b -t a inverzenek nevezzük és a^{-1} szimbólummal jelöljük.

- Abel-csoport:

A G csoportot Abel-csoportnak (vagy kommutatívnak) nevezzük, ha

$$\forall a, b \in G: a \cdot b = b \cdot a$$

- Például:

$$(\mathbb{Z}, +) \quad a^{-1} \rightarrow -a$$

$$(\mathbb{Z}, \cdot) \quad a^{-1} = \frac{1}{a} \leftarrow 1\text{-en kívül más elemnek nincs inverze } \mathbb{Z}\text{-n!}$$

• Kétműveletes struktúrák:

• Cayley-táblázat:

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\} \quad // 5+4=9=6+3 \Rightarrow 5+4=3$$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$(\mathbb{Z}_6, +)$ maradékosztály-gyűrű

$(\mathbb{R}, +, \cdot)$ gyűrű, ha $(\mathbb{R}, +)$ Abel-csoport
és $(\mathbb{R}, \cdot)$ félcsoport

// Ha $(\mathbb{R}, \cdot)$ egységelemes $\rightarrow \mathbb{R}$ egységelemes gyűrű

A gyűrű disztributív tulajdonságú.

$$a \cdot (b+c) = a \cdot b + a \cdot c, \quad a, b, c \in \mathbb{R}.$$

• Definíció:

$a \in R$ nilpotens, ha $a \neq 0$, de $a^n = 0$, valamely $n \geq 2$ -re.

- példa:

$(\mathbb{Z}_6, +, \cdot)$ -ban zérusosztó = 2 és 3 ($2 \cdot 3 = 0$)
- mégis benne nilpotens elem.

$(\mathbb{Z}_8, +, \cdot)$ -ban zérusosztó = 2 és 4 ($2 \cdot 4 = 0$)
- van benne nilpotens elem = 2 $\Rightarrow 2^3 = 0$.

- Gauss-egész gyűrűje:

$G = \{a + b \cdot i \mid a, b \in \mathbb{Z}\}$ (nem lehet test, mert nem invertálhatók az elemek)

- Polinomok gyűrűje:

$$\mathbb{R}[x] = \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \mid a_i \in \mathbb{R}\}$$

- Integritás tartomány:

$(R, +, \cdot)$ Integritás tartomány, ha $(R, +)$ kommutatív, egységelemes, zérusosztómentes,

- például: Gauss-egész gyűrűje valamint ha $(R, +, \cdot)$ gyűrűt alkot.

$$G = \{a + b \cdot i \mid a, b \in \mathbb{Z}\},$$

vagy $(\mathbb{Z}, +, \cdot)$.

- Test:

Ha R $(R, +)$ és $(R, \cdot)$ is Abelcsoport, akkor test.

- például: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$

• Tétel:

$\mathbb{Z}_n$ test, ha n prim.

- bizonyítás:

$$n \text{ prim} \leadsto p \equiv n$$

$$\mathbb{Z}_p = \{0, 1, \dots, p-1\}$$

$$(a, p) = 1 \text{ (lnk)} \quad \forall a \in \mathbb{Z}_p$$

$\Rightarrow$ Elegendő azt kell belátni, hogy a invertálható.

$$\text{Ha } \exists a^{-1}: 1 = a \cdot a^{-1} = x + y \cdot p = a \cdot a^{-1} + y \cdot p$$

$\Rightarrow (a, p) = 1$ miatt tehát megoldható $\rightarrow \mathbb{Z}_p$ test!

$$a \cdot x + b \cdot y = c, \text{ ahol } a, b, c \text{ egész szám}$$

$\Rightarrow$ a megoldás is egész szám lesz

$\Rightarrow$ kétváltozós diophantosi egyenlettel megoldható

$\Downarrow$

$$\text{Ha } (a, b) \mid c$$

$\Rightarrow$ végtelen sok megoldás

Kombinatorika ()

• Definíció:

n darab különböző elem lehetséges sorrendjét n elem permutációjának nevezzük.

$$1! \stackrel{\text{def.}}{=} 1$$

$$(n+1)! \stackrel{\text{def.}}{=} n! \cdot (n+1)$$

$$0! \stackrel{\text{def.}}{=} 1$$

• Állítás:

n darab különböző elem permutációjának száma $n!$

- bizonyítás: (A fa szerkezet segítségével)



Az elágazásokat követően minden ág saját ágja 1-gyel csökken, míg nem elérkezünk odáig, hogy minden ághoz csak 1 elem tartozik. Ezek az elemek összesen $n!$ db.

- példa ismétlés nélküli permutációra:

Egy kártyapakli megkeverése a 32 lap egy permutációja, és $32! \approx 2,63 \cdot 10^{35}$ számú különböző sorrend létezik.

• Definíció:

Tegyük fel, hogy van n darab elemünk, amelyek közül $k_1, k_2, \dots, k_n$ rendre egyforma is előfordulnak. Ekkor az n elem lehetséges sorrendjeit ismétléses permutációnak nevezzük.

• Állítás:

Legyen n elemünk, amelyek közül $k_1, k_2, \dots, k_n$ rendre egyforma, ekkor a lehetséges sorrendek száma:

$$\frac{n!}{k_1! \cdot k_2! \cdot \dots \cdot k_n!}$$

- bizonyítás:

Legyen x a lehetséges sorrendek száma,

- az egyforma elemeket átmenetileg számozással megkülönböztetjük egymástól,

- így minden egyes sorrendet át tudunk rendezni olyan módon, hogy az egyforma elemeket megcseréljük egymással.

$$\text{Ekkor } x \cdot k_1! \cdot k_2! \cdot \dots \cdot k_n! = n!$$

$$x = \frac{n!}{k_1! \cdot k_2! \cdot \dots \cdot k_n!}$$

} Tehát x a lehetséges sorrendek száma

- példa ismétléses permutációra:

Ha úgy keverünk össze egy kártyapaklit, hogy csak a színeket vesszük figyelembe, akkor négyféle lap lesz és mindegyikből 8 darab van a pakliban.

Ez a 32 lap ismétléses permutációja, és az összes különböző sorrend száma: $\frac{32!}{8! \cdot 8! \cdot 8! \cdot 8!}$

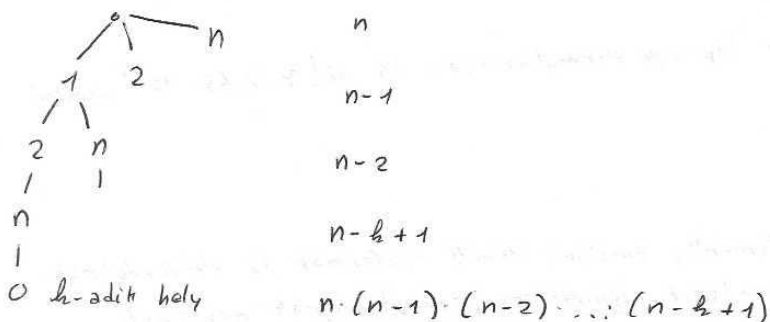
• Definíció:

n darab különböző elemből válasszunk ki k darab elemet úgy, hogy a sorrend számít. Ekkor az n elem k -ad osztályú ismétlés nélküli variációját kapjuk.

• Állítás:

Az összes lehetséges ismétlés nélküli k -ad osztályú variációk száma n különböző elem esetén: $\frac{n!}{(n-k)!} = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+1)$

- bizonyítás: (A fa szerkezet segítségével)



- bizonyítás: (Vezessük vissza a permutációt)

$$\underbrace{1 \ 2 \ 3 \ 4 \ \dots \ k}_{k} \underbrace{\dots}_{n-k} \quad \begin{aligned} x \cdot (n-k)! &= n! \Rightarrow x = \frac{n!}{(n-k)!} = \\ &= \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1) \cdot \cancel{(n-k)} \cdot \cancel{(n-k-1)} \cdot \dots \cdot 2 \cdot 1}{\cancel{(n-k)} \cdot \cancel{(n-k-1)} \cdot \dots \cdot 2 \cdot 1} \end{aligned}$$

- példa ismétlés nélküli variációra:

Ha egy futóversenyen 10 ember áll rajthoz, akkor az első három helyezett a 10 ember 3-ad osztályú ismétlés nélküli variációja, és összesen 10 · 9 · 8 felekeppén állhatnak fel a dobogóra a versenyzők.

Kombinatorika ()

• Definíció:

Ha n darab különböző elemből úgy választunk ki k darabot, hogy egy elemet többször is választathatunk és a sorrend számít, akkor az n elem egy k -ad osztályú ismétléses variáció-ját kapjuk.

• Állítás:

Az összes lehetséges k -ad osztályú ismétléses variációk száma n különböző elem esetén: n^k .

- bizonyítás: (Teljes indukcióval)

$$k=1 \Rightarrow n^k = 1$$

Tegyük fel, hogy k -ra igaz.

$$k+1 \Rightarrow$$

Az első k hűzős feljegyzése

n -féle lehet

k $k+1$

$$n^k \cdot n = \underline{n^{k+1}} \rightarrow \text{tehát igaz } k\text{-ra is!}$$

- példa ismétléses variációra:

A totó-szelvény kitöltése 3 darab elem $(13+1)$ -ed osztályú ismétléses variáció, ami összesen 3^{14} -féleképpen tölthető ki.

• Definíció:

Ha n darab különböző elemből visszatérés nélkül választunk ki k darab elemet úgy, hogy a sorrend számít, az n elem k -ad osztályú kombináció-ját kapjuk.

• Állítás:

Az összes lehetséges k -ad osztályú ismétlés nélküli kombináció n elem esetén:

$$\frac{n!}{k!(n-k)!} = \binom{n}{k}$$

Az $\binom{n}{k}$ számokat binomiális együtthatóknak nevezzük.

- bizonyítás:

Az n elem ismétlés nélküli k -ad osztályú variációi között $k!$ számú van, melyekben ugyanazok az elemek szerepelnek, csak más sorrendben.

Ezek mind ugyanazt a kombinációt állítják elő.

- bizonyítás: (Vezessük vissza variációra)

Legyen x a kombinációk száma,

k különböző elem van kiválasztva, a sorrend nem számít,

$$x = \frac{n!}{k! \cdot (n-k)!} = \binom{n}{k}$$

- példa ismétlés nélküli kombinációra:

Az ötös lottón 90 számból kell 5 számot kiválasztanunk úgy, hogy egyik számot sem választhatunk kétszer. Ekkor a lehetséges kiválasztások száma:

$$\binom{90}{5} = \frac{90 \cdot 89 \cdot 88 \cdot 87 \cdot 86}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5} = 8\,489\,853\,600$$

• Definíció:

Ha n darab elemből úgy választunk ki k darabot, hogy a sorrend nem számít, és egy elemet többször is választhatunk, akkor n elem egy k -ad osztályú ismétléses kombinációját kapjuk.

• Állítás:

Az összes lehetséges k -ad osztályú ismétléses kombinációk száma n elem esetén:

$$\binom{n+k-1}{k}$$

- bizonyítás:

Megmutatjuk, hogy n elem k -ad osztályú ismétléses kombinációjának halmaza és $n+k-1$ elem k -ad osztályú ismétlés nélküli kombinációjának a halmaza között kölcsönösen egyértelmű megfeleltetés létezik, azaz

$$C_{n, \text{ism.}}^k = C_{n+k-1}^k$$

- példa ismétléses kombinációra:

Ha ötféle csokoládét lehet kapni a boltban, és mi 10 darabot veszünk, akkor ez az 5 csokoládé 10-ed osztályú ismétléses kombinációja, és összesen $\binom{5+10-1}{10}$ -féleféppen választhatunk.

A binomiális tétel ()

• Definíció:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} \cdot a^k \cdot b^{n-k} = \\ = \binom{n}{0} \cdot a^0 \cdot b^n + \binom{n}{1} \cdot a^1 \cdot b^{n-1} + \dots + \binom{n}{n-1} \cdot a^{n-1} \cdot b^1 + \binom{n}{n} \cdot a^n \cdot b^0$$

• Definíció:

$$\binom{n}{0} = \frac{n!}{0! \cdot n!} = 1 \quad \binom{n}{n} = \frac{n!}{n! \cdot (n-n)!} = 1$$

$$\binom{n}{n} = \frac{n!}{n! \cdot 0!} = 1 \quad \binom{n}{k} = \binom{n}{n-k} \text{ ugyanaz ...}$$

$$\binom{n}{k} = \binom{n}{n-k} \quad \binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} \quad \binom{n}{n-k} = \frac{n!}{(n-k)! \cdot (n-(n-k))!} \\ \text{egyenlőek}$$

• Tétel:

$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k} \quad \text{bizonyítás!}$$

$$\underline{\underline{\binom{n}{k+1} + \binom{n}{k} = \frac{n!}{(k+1)! \cdot (n-k-1)!} + \frac{n!}{k! \cdot (n-k)!} = \frac{n!}{k! \cdot (n-k-1)!} \cdot \left(\frac{1}{(k+1) \cdot 1} + \frac{1}{1 \cdot (n-k)} \right) = \\ = \frac{(n+1)!}{(k+1)! \cdot (n-k)!} = \binom{n+1}{k+1}}}$$

• A binomiális tétel alkalmazása:

$$\text{Mennyivel egyenlő } \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} = (1+1)^n = 2^n$$

Hány részhalmaza van egy n elemű halmaznak? $\Rightarrow 2^n$

$$\text{-bizonyítás: } \binom{n}{0} = 1$$

$$\binom{n}{1} = n$$

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} = \underline{\underline{2^n}}$$

• A binomiális együtthatók tulajdonságai:

$$1, \binom{n}{k} = \binom{n}{n-k}, \text{ ha } 0 \leq k \leq n,$$

$$2, \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}, \text{ ha } 0 \leq k \leq n,$$

$$3, \binom{n+1}{k+1} = \binom{n}{k} + \binom{n-1}{k} + \dots + \binom{k+1}{k} + \binom{k}{k}, \text{ ha } 0 \leq k \leq n,$$

$$4, \binom{n+1}{k+1} = \frac{n+1}{k+1} \cdot \binom{n}{k}, \text{ ha } 0 \leq k \leq n.$$

A multinomiális tétel ()

• Definíció:

Legyen $a_1, a_2, \dots, a_k \in \mathbb{R}$ és $n \in \mathbb{N}$. Ekkor...

$$(a_1 + a_2 + \dots + a_k)^n = \sum_n \left(\frac{n!}{s_1! \cdot s_2! \cdot \dots \cdot s_k!} \right) a_1^{s_1} \cdot a_2^{s_2} \cdot \dots \cdot a_k^{s_k}.$$

Az összegzés azon nem negatív egész $s_1, s_2, \dots, s_k$ számokra terjed ki, amelyek összege n .

Pascal-háromszög ()

• Definíció:

Az $(a+b)^n$ kifejezésben szereplő együtthatókat $n=2, \dots$ esetén egymás alá elhelyezzük:

$$\begin{array}{ccccccc} n=0 & & & & & & \binom{0}{0} \\ n=1 & & & & & \binom{1}{0} & \binom{1}{1} \\ n=2 & & & \binom{2}{0} & & \binom{2}{1} & \binom{2}{2} \\ n=3 & & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} \\ n=4 & \binom{4}{0} & \binom{4}{1} & \binom{4}{2} & \binom{4}{3} & \binom{4}{4} \end{array}$$

Az $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$ képlet alapján látható, hogy abban, az úgynevezett Pascal-háromszögben szereplő értékek a közvetlenül felettük szereplő két érték összegeként kaphatók meg. Ez is mutatja, hogy $\binom{n}{k}$, $0 \leq k \leq n$, pozitív egész.

• A Pascal-háromszögben szereplő számok:

$$\begin{array}{ccccccc} & & & & 1 & & & \\ & & & & 1 & & 1 & \\ & & & 1 & & 2 & & 1 \\ & & 1 & & 3 & & 3 & & 1 \\ & 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

$$(a+b)^4 = 1a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + 1b^4$$

$$(a+b)^3 = 1a^3 + 3a^2b + 3ab^2 + 1b^3$$

Számosságok ()

• Definíció:

Az A és B halmaz egyenlő számosságú, ha létezik egy olyan $f: A \rightarrow B$ kölcsönösen egyértelmű, -ra való leképezés, hogy A és B között bijektív a leképezés.

$\Rightarrow$ Az A és B halmaz egyenlő számosságú, ha létezik közöttük bijektív leképezés.
- Jele: $A \sim B$

• Definíció:

Az A halmaz számossága nagyobb, mint B halmaz számossága, ha számosságuk nem egyenlő, és létezik olyan C halmaz, melynek számossága egyenlő B számosságával és $C \subset A$.

• Definíció:

Az A halmaz végtelen számosságú, ha nem véges a számossága.

$\Rightarrow$ Az A halmaz megszámlálhatóan végtelen, ha $A \sim \mathbb{N}$.

Ennek a számosságnak $\aleph$ (alef) a jele.

$\Rightarrow$ A megszámlálhatóan végtelen halmazok is megszámlálhatóak.

• Definíció:

Az üres halmaz is véges számosságú.

- példa a kölcsönös egyértelműségre:

$$\{1, 2, 3, \dots\} \sim \{2, 4, 6, \dots\} \quad 1 \mapsto 2i \quad (-\text{ra való leképezés})$$

• Tétel:

$|A|$ (számossága) végtelen $\Leftrightarrow$ ha van A -nak megszámlálhatóan véges részhalmaza.

- bizonyítás:

Legyen A végtelen, azaz nem véges.

$a_1 \in A$ ← még nem merült ki a halmaz, tehát több eleme is van (végtelen)

$a_2 \in A \setminus \{a_1\}$

$a_3 \in A \setminus \{a_1, a_2\}$ Ha végtelen, mindig van megszámlálható részhalmaza.

Mindig marad eleme...

• Tétel:

Legyen A egy halmaz.

A végtelen $\Leftrightarrow$ ha ekvivalens valamelyik valódi részhalmazzal.

-bizonyítás:

Legyen A végtelen.

$$A = \underbrace{(A \setminus \{a_1, a_2, \dots\})}_{\text{megszámlálható}} \cup \{a_1, a_2, \dots\} \rightarrow A \setminus \{a_1, a_3, a_5\}$$

$\downarrow$
 $a_i \rightarrow a_{2i}$

Számosságok ()

• Tétel:

A természetes számok halmaza megszámlálhatóan végtelen.

Minden elemnek létezik rákövetkezője (aritmia).

• Tétel:

Az egész számok halmaza megszámlálhatóan végtelen.

$$|\mathbb{Z}| = |\mathbb{N}| \quad (\mathbb{N} \subsetneq \mathbb{Z})$$

-bizonyítás:

$\mathbb{Z}$	$\mathbb{N}$
-3	0
-2	1
-1	2
0	3
1	4
2	5
3	6

$$\text{Ha } a = 0 \Rightarrow a \rightarrow 0,$$

$$\text{ha } a > 0 \Rightarrow a \rightarrow 2a,$$

$$\text{ha } a < 0 \Rightarrow 2 \cdot |a| - 1.$$

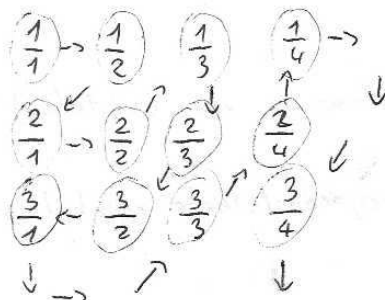
Tehát képesek vagyunk bijektív leképezést készíteni.

• Tétel:

A racionális számok halmaza megszámlálhatóan végtelen.

$$|\mathbb{Q}| = |\mathbb{N}| \quad (\mathbb{N} \subsetneq \mathbb{Q})$$

-bizonyítás:



Ebben az esetben is

képesek vagyunk megszámlálni

az elemeket, tehát a halmaz

megszámlálhatóan végtelen.

Számosságok ()

• Tétel:

A valós számok számossága nagyobb, mint a racionális számok számossága.
 $|R| > |N|$

- bizonyítás:

Tegyük fel, hogy bármely valós szám felírható 2-es számrendszerben.

$\Rightarrow$ Azonban $0,1 = 0,0\bar{9}$, tehát létezik több olyan szám is, amelyet ugyanúgy kellene ábrázolni.

$\Rightarrow$ A felírás csak akkor lenne egyértelmű, ha kikötjük, hogy j_k index, hogy $a_{k-1} = 1$, $\forall j \geq 0$.

Tehát a valós számok számossága nagyobb, mint a racionális számoké.

• Definíció:

A valós számok, illetve a vele ekvivalens halmazok számosságát kontinuum számosságnak nevezzük.

• Definíció:

$$|P(R)| > |R|$$

A valós számok összes részhalmazának halmaza.

• Megjegyzés:

$$|N| < |P(N)| < |P(P(N))| < |P(P(P(N)))| < \dots$$

$$\begin{array}{ccccccc} R_0 & & R_1 & & R_2 & & R_3 \\ & \swarrow & & \swarrow & & \swarrow & \\ & & & & & & \end{array}$$

$\rightarrow$ szürreális számok: $R_0 + \pi$.

Szita formula ()

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

- példa:

Egy társaságban 64 ember van. Közülük 44 beszél angolul, 35 németül, és 23 mindkét nyelvet. Hányan nem tudnak se németül, se angolul?

$$64 = 44 + 35 - 23 + X$$

$$64 = 59 + X$$

$$X = 8$$

$\hookrightarrow$ Azok száma, akik egyik nyelvet sem beszélnek.

Rekurzív sorozatok ()

• Definíció:

A rekurzió egy olyan művelet, mely végrehajtáskor a saját maga által definiált műveletet hajtja végre, ezáltal önmagát ismétli.

A rekurzió lényege, hogy egy adott probléma megoldható úgy, hogy először megnezzük van-e megoldás.

- Ha van, a probléma meg van oldva,

- ha nincs, felbontjuk részproblémákra és ismételjük a fenti eljárást.

A lépéssort a szükséges lépésszámmig ismételve, előbb utóbb eljutunk a végző megoldáshoz - feltéve, hogy az adott probléma a használt algoritmussal rekurzívan kezelhető.

• Hanoi - tornyai:

T_n : Az n korong esetén szükséges lépések száma.

$$T_1 = 1$$

$$T_2 = 3$$

$$T_3 = 4$$

$$T_n = 2^n - 1 \quad (T_{n-1} = 2^{n-1} - 1)$$

$$T_n = T_{n-1} + 1 + T_{n-1} = 2 \cdot T_{n-1} + 1$$

$$2 \cdot (2^{n-1} - 1) + 1 = \underline{\underline{2^n - 1}}$$

• Nyúlás:

$$F(n+1) = F(n) + F(n-1)$$

$f(n+2) = a_1 \cdot f(n+1) + a_2 \cdot f(n)$ $\forall n$ és $f(1)$ és $f(2)$ adott, a_1 és a_2 fix szám.
Legyen f_1 és f_2 megoldás $\Rightarrow$ akkor ezek lineáris kombinációja is megoldás.

$$A \cdot f_1(n) + B \cdot f_2(n)$$

$$A \cdot f_1(n+2) + B \cdot f_2(n+2) \stackrel{?}{=} a_1 \cdot (A \cdot f_1(n+1) + B \cdot f_2(n+1)) + a_2 \cdot (A \cdot f_1(n) + B \cdot f_2(n))$$

• Fibonacci - számok:

• Definíció:

$$F_0 = 1$$

$$F_1 = 1$$

$$F_n = F_{n-1} + F_{n-2}$$

$$\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \phi \quad (\text{aranymetszes} = \frac{1+\sqrt{5}}{2} \approx 1,618 \dots)$$

↑
Határértéke.

- Fibonacci számok: 1, 1, 2, 3, 5, 8, 13, 21, 34, ...

• Aranymetszés:



$$\frac{a+b}{a} = \frac{a}{b} \quad (\text{Ez az aranymetszés aránya.})$$

$$\phi = \frac{a+b}{a} = \frac{\frac{a}{b} + 1}{\frac{a}{b}} = \frac{\phi + 1}{\phi} = \phi \quad // \text{ Az egész hossz úgy aránylik a hosszabb részhez, mint a hosszabb rész a rövidebbhez.}$$

$$\phi = \frac{\phi + 1}{\phi}$$

$$\phi^2 = \phi + 1$$

$$\phi^2 - \phi - 1 = 0$$

$$\phi_{1,2} = \frac{1 \pm \sqrt{5}}{2}$$

• Binet-formula:

Az n -edik Fibonacci-számot adja eredményül, de nem teljesen pontosan.

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5} \cdot 2^n}$$

• Két paraméteres rekurzió:

- Pascal-háromszög:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

- példa:

$$\binom{5}{3} = \binom{5-1}{3-1} + \binom{5-1}{3}$$

$\underbrace{\quad}_{10} \quad \underbrace{\quad}_6 \quad \underbrace{\quad}_4$

$$\begin{array}{cccccc} & & \binom{0}{0} & & & n=0 \\ & \binom{1}{0} & & \binom{1}{1} & & n=1 \\ & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & n=2 \\ \binom{3}{0} & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & n=3 \\ \binom{4}{0} & \binom{4}{1} & & \binom{4}{2} & & \binom{4}{3} & \binom{4}{4} & n=4 \end{array}$$

• Karakterisztikus egyenlet:

$$X^2 = a_1 X + a_2 \quad // \text{ Ha } r \text{ az egyenlet megoldása, akkor } f(n) = r^n \text{ a megoldás.}$$

- bizonyítás:

$$r^{n+2} \stackrel{?}{=} a_1 \cdot r^{n+1} + a_2 \cdot r^n$$

$$r^n \cdot \underbrace{(r^2 - a_1 r - a_2)}_0 \stackrel{?}{=} \underline{\underline{0}}$$

• Általános megoldás:

$$\underline{\underline{A f_1(n) + B f_2(n) = A r^n + B \cdot n \cdot r^{n-1}}}$$

Polinomok ()

• Definíció:

Legyen x egy szimbólum, T pedig egy test ($\mathbb{Z}$, $\mathbb{R}$ vagy $\mathbb{Q}$). Ekkor...

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \quad a_n, a_{n-1}, \dots, a_0 \in T$$

egy egyhatározatlan polinom, ha

- $a_n \neq 0$, n = fokszáma a polinomnak,
- $a_0, a_1, \dots, a_n$ együtthatók.

• Műveletek polinomok között:

$$p(x) = a_n x^n + \dots + a_0$$

$$g(x) = b_n x^n + \dots + b_0$$

$$p(x) \pm g(x) = (a_n \pm b_n) x^n + \dots + (a_1 \pm b_1) x + (a_0 \pm b_0)$$

$$p(x) \cdot g(x) = a_n \cdot b_n \cdot x^{2n} + (a_n \cdot b_{n-1} + a_{n-1} \cdot b_n) \cdot x^{2n-1} + \dots$$

• Tétel:

A polinomok az összeadásra és a szorzásra tekintve gyűrűt alkotnak.

Polinomok $(+, \cdot)$ gyűrű

- nullem: 0
 - egységelem: 1
 - kommutatív
 - nullszorzómentes
- } Integritási tartomány

• Az algebra alaptétele:

Minden komplex együtthatós, legalább elsőfokú polinomnak van gyöke a komplex számok között.

$$p(x) = (x - x_0) \cdot f(x) + c$$

$$0 = p(x_0) = (x - x_0) \cdot f(x) + c \rightarrow c = 0, \text{ azaz } p(x) = (x - x_0) \cdot f(x)$$

$$\Rightarrow \text{Ha } p \text{ fokú } n \Rightarrow f \text{ fokú } (n-1)$$

• Állítás:

Minden n -edfokú, komplex együtthatós polinom felírható

$$p(x) = (x - x_1)^{d_1} \cdot (x - x_2)^{d_2} \cdot \dots \cdot (x - x_k)^{d_k} \quad \text{ahol } d_1 + d_2 + \dots + d_k = n$$

$\downarrow$
 x_1 multiplicitása

$\Rightarrow$ Minden n -edfokú komplex együtthatós polinomnak n darab gyöke van, ha számoljuk a gyök multiplicitásait is!

• Tétel:

$$ax^2 + bx + c = 0, \quad a \neq 0$$

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$\Rightarrow$ Mindig van megoldás a komplex számok halmazán.

$$ax^3 + bx^2 + cx + d = 0$$

$$ax^4 + bx^3 + cx^2 + dx + e = 0 \quad \left. \vphantom{ax^4 + bx^3 + cx^2 + dx + e = 0} \right\} \text{ Ezekre még felírható gyökképlet}$$

• Galois:

Negyedfoknál nagyobb fokszámú egyenletekre nem írható fel megoldóképlet.

• Polinomok osztása:

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

$$-(4x^4 - 2x^3 + 2x^2)$$

$$-2x^2 - 2x + 4$$

$$-(-2x^2 + 4 - 1)$$

$$-3x + 5 \Leftarrow \text{Maradék}$$

$$\underbrace{(4x^4 - 2x^3 + 0 \cdot x^2 - 2x + 4)}_{p(x)} = \underbrace{(2x^2 - x + 1)}_{g(x)} \cdot \underbrace{(2x^2 + 0x - 1)}_{f(x)} + \underbrace{(-3x + 5)}_{R(x)}$$

$$p(x) = g(x) \cdot f(x) + R(x)$$

• Definíció:

Egy polinom akkor irreducibilis, ha komplex gyökei vannak, vagy ha már elsőfokú. Komplex gyökök csak párban fordulnak elő, tehát minden páratlan fokú polinom lehet irreducibilis.

• Vale's együtthato's polinomok gyökei:

$$\text{Ha } p(x) = 0 \text{ akkor } p(\bar{x}) = 0.$$

$$a_n \bar{x}^n + \dots + a_1 \bar{x} + a_0 = \bar{0}, \quad p(x) = (x - x_0) \cdot (x - \bar{x}_0) \cdot f(x).$$

Ha x_0 gyök, akkor $\bar{x}_0$ is ugyanannyiszoros gyök.
 $\hookrightarrow$ konjugát

$$p(x) = a_n \cdot [(x - x_1) \cdot (x - x_2) \cdot (x - \bar{x}_2) \dots] \cdot [(x - x_3) \cdot (x - x_{3+1}) \cdot \dots \cdot (x - x_t)]$$

$$x^2 - (x_1 + \bar{x}_1) \cdot x + x_1 \cdot \bar{x}_1 = \text{vale's együtthato's, másodfokú polinom}$$

Minden vale's együtthato's polinom felírható, mint első és másodfokú polinom szorzata.

Polinomok ()

• Egész együtthatós polinomok gyökei:

Ha $a \geq 0$ és $b > 0$ egészek, akkor $a = b \cdot r + s$, ahol $r \geq 0$ egész és $b > s \geq 0$.

// Maradékos osztás

• Horner-eljárás:

A polinom helyettesítési értékét lehet vele kiszámolni, illetve az elsőfokú polinommal való osztás hányadosát és maradékát.

- példa:

$$x^6 - 3x^5 + 4x^3 - 2x^2 - 5x + 1$$

$$p(3) = \underline{\underline{76}} \quad \downarrow$$

	1	-3	0	4	-2	-5	1
3	1	0	0	4	-10	25	76

$$p(x) = (x-3) \cdot (x^5 + 0 \cdot x^4 + 0 \cdot x^3 + 4x^2 + 10x + 25) + 76$$

- példa:

$$2x^4 - 4x^3 + 2x - 3 : (x+1) = \underline{\underline{2x^3 - 6x^2 + 6x - 4}}$$

	2	-4	0	2	-3
-1	2	-6	6	-4	1

$$2x^4 - 4x^3 + 2x - 3 = (x+1) \cdot (2x^3 - 6x^2 + 6x - 4) + 1$$

• Parciális törtekre bontás:

$\frac{f(x)}{g(x)}$ parciális tört, ha $\deg f < \deg g$ és $g(x)$ irreducibilis.

- $\forall$ gyöke valós és egyszeres: $\frac{f(x)}{(x-1) \cdot (x+3)} = \frac{A}{(x-1)} + \frac{B}{(x+3)}$

- $\forall$ gyöke valós, de van többszörös gyöke is: $\frac{f(x)}{(x+2)^2} = \frac{A}{(x+2)} + \frac{B}{(x+2)^2}$

- $\exists$ komplex gyök is, de egyszeres: $\frac{f(x)}{x^2+1} = \frac{Ax+B}{x^2+1}$

- $\exists$ többszörös komplex gyök: $\frac{f(x)}{(x^2+1)^2} = \frac{Ax+B}{(x^2+1)} + \frac{Cx+D}{(x^2+1)^2}$

Események ()

• Definíció:

A valószínűségszámítás véletlen tömegjelenségekkel foglalkozik, azaz olyanokkal, amelyek sokszor ismétlődnek azonos körülmények között.

• Definíció:

A véletlen azt jelenti, hogy előre nem tudjuk megmondani, hogy mi lesz egy kísérlet kimenetele. A való's számok törvényszerűségei azért léteznek, hiszen sok végrehajtás esetén jó közelítést adnak. A való's számok a statisztika elvi alapozását adják.

• Definíció:

Legyen k egy véletlen kísérlet és n független kísérletet végzünk el egymás után. A adja meg az eredményt.

Ekkor A relatív gyakorisága $\frac{k_A}{n} = \frac{A \text{ hányados}}{n}$

Ebből kiderül, hogy a relatív gyakoriság sok esetben jól stabilizálódik az érték körül.

• Definíció:

$$\frac{k_A}{n} \approx P(A) = A \text{ valószínűsége}$$

• Tétel:

Dobjunk fel 8-szor egy érmét, majd írjuk le az eredményeket egymás után sorban.

1, F, F, 1, 1, 1, F, F

$A =$ fejek

$$\frac{k_A}{n} = \frac{0}{1}, \frac{1}{2}, \frac{2}{3}, \frac{2}{4}, \frac{2}{5}, \frac{2}{6}, \frac{3}{7}, \frac{4}{8} \leftarrow 8 \text{ értékből } 4 \text{ fej.}$$



$$P(A) \approx \frac{k_A}{n} \geq 0$$

A relatív gyakoriság nagyon ingadozik.

// A és B kizáró esemény, egyszerre nem lehet fej és írás is!

• A valószínűség axiómái:

$$P(A) \geq 0 \quad \forall A \text{ esemény}$$

$$P(\Omega) = 1 \quad \text{biztos esemény}$$

$$P(A+B) = P(A) + P(B)$$

• Definíció:

$A, B_1, B_2, \dots$ eseményeket teljes eseménynek nevezzük.

• Kolmogorov-féle valószínűségű mező:

Ω = eseményter

$\omega \in \Omega$ = elemi esemény

• $\mathcal{A}$ az események családja, ami azt jelenti, hogy $\mathcal{A} \subseteq 2^\Omega$.

Ha $A \in \mathcal{A}$, akkor $A \subseteq \Omega$.

• Legyen $\mathcal{A}$ σ -algebra, azaz

- $\Omega \in \mathcal{A}$

- ha $A \in \mathcal{A}$, akkor $\bar{A} \in \mathcal{A}$

- ha $A_1, A_2, \dots \in \mathcal{A}$, akkor $A_1 \cup A_2 \cup \dots \in \mathcal{A}$

$\parallel (A \in \mathcal{A}) = A$ esemény

• $P: \mathcal{A} \rightarrow \mathbb{R}$

- $P(A) \geq 0 \quad \forall A \in \mathcal{A}$

- $P(\Omega) = 1$

- $P(A_1 \cup A_2 \cup \dots) = P(A_1) + P(A_2) + \dots, \quad \forall A_1, A_2, \dots$ páronként kizáró eseményre

- Következmény:

$$P(\emptyset) = 0, \text{ ugyanis } 1 = P(\Omega) = P(\Omega \cup \emptyset \cup \emptyset \cup \dots) = P(\Omega) + \underbrace{P(\emptyset) + P(\emptyset) + \dots}_{P(\emptyset) = 0}$$

• $\mathcal{A}$ σ -additivitásból következik a véges additivitás:

Legyenek $A_1, A_2, \dots, A_n$ páronként kizáró események,

$$P(A_1 \cup A_2 \cup A_3 \cup \dots \cup A_n) = \underbrace{P(A_1) + P(A_2) + \dots + P(A_n)}_0 + \underbrace{P(\emptyset)}_0$$

$$P(\Omega) = P(\Omega) + P(\emptyset) + \dots$$

$$\text{Ha } P(\emptyset) = 0.$$

• Definíció:

$A, B_1, B_2, \dots$ eseményeket teljes eseményrendszernek nevezzük, ha ezen események páronként kizáróak és együtt a teljes eseményteret adják vissza.

• Állítás:

Ha $B_1, B_2, \dots$ teljes eseményrendszer, akkor $p_i = P(B_i), i = 1, 2, \dots$

- $p_i \geq 0, \forall i$

- $\sum_{i=1}^{\infty} p_i = 1$ } diszkrét eloszlást alkotnak

- Bizonyítás: $p_i = P(B_i) \geq 0$, mert valószínűség

$$\sum p_i = \sum P(B_i) = P\left(\bigcup_{i=1}^{\infty} B_i\right) = P(\Omega) = 1, \text{ hiszen ez az események összege } 1.$$

Események ()

- Feltételes valószínűség:

Legyen egy k kísérlet n -szer megismételve.

$$p(B) > 0$$

Menyi A relatív gyakorisága, ha B bekövetkezik?

$$\begin{array}{ccccccccccc} B & \overline{13} & 13 & \overline{13} & \overline{13} & 13 & 13 & 13 & \dots & 13 \\ A & & A & & & \overline{A} & \overline{A} & A & \dots & A \end{array}$$

- a feltételes valószínűség: $\frac{h_{A \cap B}}{h_B} = \frac{\frac{h_{A \cap B}}{n}}{\frac{h_B}{n}} \sim \frac{P(A \cap B)}{P(B)}$

- Definición:

$$P(A|B) = \frac{P(A \cdot B)}{P(B)} \quad \Leftarrow \text{A-nak B-re vonatkozó feltételes valószínűsége.}$$

Fix β esetén ez is egy valószínűség.

- pe'lda:

n : dia'keh s'za'ma

1-: abhayan irnath

A: legjobb tanuló is

13: legrossabb tanuló ír

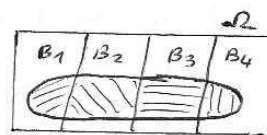
$$P(A|B) = \frac{P(A \cdot B)}{P(B)} = \frac{\frac{\binom{n-2}{r-2}}{\binom{n}{r}}}{\frac{\binom{n-1}{r-1}}{\binom{n}{r}}} = \frac{\binom{n-2}{r-2}}{\binom{n-1}{r-1}}$$

* A teljes valószínűség tétele:

Legyen $B_1, B_2, \dots$ teljes eseményrendszer, $P(B_i) > 0$, $\forall i$.

Legyen A esemény.

Erkorr $P(A) = \underline{P(A|B_1) \cdot P(B_1) + P(A|B_2) \cdot P(B_2) + \dots}$



- bizen yita's:

$$P(A) = P((A \cap B_1) \cup (A \cap B_2) \cup \dots) = P(A \cdot B_1) + P(A \cdot B_2) + \dots$$

$$P(A \cdot B_i) = P(A|B_i) \cdot P(B_i)$$

- Bayes-formula:

$$P(B|A) = \frac{P(B \cdot A) \cdot P(B)}{P(A)} \quad \begin{matrix} P(A) > 0 \\ P(B) > 0 \end{matrix}$$

◦ Bayes-tétel (Az okok valószínűségének tetele - előtétel):

Ha $B_1, B_2, \dots$ teljes eseményrendszer és $P(B_i) > 0$, $\forall i$ és $P(A) > 0$,

akkor...

$$P(B_j | A) = \frac{P(A | B_j) \cdot P(B_j)}{\sum_{i=1}^{\infty} P(A | B_i) \cdot P(B_i)}$$

- bizonyítás: (teljes valósz. tetele)

$$P(B_3 | A) = \frac{P(A | B_3) \cdot P(B_3)}{P(A | B_1) \cdot P(B_1) + P(A | B_2) \cdot P(B_2) + P(A | B_3) \cdot P(B_3)}$$

◦ Definíció:

Egy esemény független a másiktól, ha az nem befolyásolja a bekövetkezésének valószínűségét.

A független B-től, ha $P(A) = P(A | B)$, ha $P(B) > 0$, $P(A) \cdot P(B) = P(A \cdot B)$

B független A-tól, ha $P(B) = P(B | A)$, ha $P(A) > 0$, $P(B) \cdot P(A) = P(B \cdot A)$

◦ Definíció:

Azt mondjuk, hogy A és B független egymástól, ha $P(A \cdot B) = P(A) \cdot P(B)$.

- A pénz és kockafeldobási játékokban függetlenség szerepel.

- Azonban az olyan szerencsejátékokban, ahol nem állítják vissza a kezdeti állapatra, nem szerepel a függetlenség.

- példa:

◦ Pénzfeldobás:

A: fejs lesz az első feldobás eredménye.

B: írás lesz a második feldobás eredménye.

$$P(A) = \frac{1}{2} \quad P(B) = \frac{1}{2} \quad P(A \cdot B) = \frac{1}{4} = P(A) \cdot P(B)$$

◦ Kockadobás:

A: az első dobás páros szám.

B: a második dobás 2-nél nagyobb szám.

$$P(A) = \frac{1}{2} \quad P(B) = \frac{4}{6} \quad P(A \cdot B) = \frac{3 \cdot 4}{6 \cdot 6} = P(A) \cdot P(B)$$

Diszkrét valószínűségi változók ()

• Definíció:

Legyen Ω egy véletlen kísérlet.

$\mathcal{A}$ kimeneteli, események.

$\mathcal{A}$ olyan kimeneteli, amelyeket csak egyfeltehetően következhetnek be: elemi események.

- példa (pénzfeldobás):

- elemi események: fej, írás

- eredmények: $\{\text{fej}\}$, $\{\text{írás}\}$

- Ω : biztos esemény, eseménytér (az összes lehetséges kimenetel halmaza)

- $\emptyset$: lehetetlen esemény

Az események így tekinthetők, mint elemi eseményekből álló halmazok.

• Műveletek események között:

$$A \text{ vagy } B = A \cup B$$

$$A \text{ és } B = A \cap B$$

A ellentettje $\bar{A}$, azaz A nem következik be.

• Definíció:

$$\text{relatív gyakoriság} = \frac{\#A}{n} \approx P(A)$$

• Definíció:

Azt mondjuk, hogy A és B esemény kizáró, ha egyszerre nem következhetnek be, azaz $A \cap B = \emptyset$.

• A valószínűség axiómái:

$$P(A) \geq 0$$

$$P(\Omega) = 1$$

$$P(A \cup B) = P(A) + P(B), \text{ ha } A \cap B = \emptyset \text{ (additív)}$$

-következmény:

$$A \cup \bar{A} = \Omega \text{ és } A \cap \bar{A} = \emptyset \Rightarrow P(A) + P(\bar{A}) = P(\Omega) = 1, \text{ azaz } P(\bar{A}) = 1 - P(A),$$

$$P(A_1 \cup A_2 \cup \dots \cup A_n) = P(A_1) + P(A_2) + \dots + P(A_n), \text{ ha } A_1, A_2, \dots, A_n \text{ páronként kizáróak,}$$

$$P(A \cup B) = P(A) + P(B) - P(A \cap B)$$

$$P(A \cup B \cup C) = P(A) + P(B) + P(C) - P(A \cap B) - P(A \cap C) - P(B \cap C) + P(A \cap B \cap C)$$

↑
Szita formula!

• Definíció:

Legyen $p_1, p_2, p_3, \dots, p_n$ adott tetszőleges, $p_i \geq 0, \forall i, \sum_{i=1}^n p_i = 1$

Legyen $\Omega = \{\omega_1, \omega_2, \dots, \omega_n\}, p(A) = \sum_{\omega_i \in A} p_i, \forall A \subseteq \Omega$ esetén.

↑
Véges valószínűségű mező!

• Speciális eset (klasszikus valószínűségű mező):

Azt írja le, amikor minden kimenetel azonos valószínűségű.

Például szabályos kocka esetén az 1, 2, 3, 4, 5, 6 azonos valószínűséggel következik be.

- példa: (Pénzérme feldobása)

$$\Omega = \{\text{fej}, \text{írás}\}$$

$$\mathcal{A} = 2^\Omega \text{ (esemény)}$$

$$P(\text{Fej}) = P(\text{írás}) = \frac{1}{2}$$

$$P(\Omega) = 1$$

$$P(\emptyset) = 0$$

• Hipergeometrikus eloszlás (visszatelés nélküli mintavétel):

Legyen egy urnában sok-sok piros és fehér golyó.

n golyót húzunk ki az urnából.

m db. piros }
 $n-m$ db. fehér } összesen n darab

$$p(k \text{ piros}) = \frac{\binom{M}{k} \cdot \binom{N-M}{n-k}}{\binom{N}{n}} \quad // \text{ Sorrend nem számít, kombináció}$$

• Binomiális eloszlás (visszateléses mintavétel):

Az előző példa mintájára...

$$P(k \text{ piros}) = \frac{M^k \cdot (N-M)^{n-k}}{N^n} + \dots + \dots = \binom{n}{k} \cdot \frac{M^k \cdot (N-M)^{n-k}}{N^n} = \binom{n}{k} p^k \cdot (1-p)^{n-k}$$

$$\underbrace{000\dots0}_{k} \underbrace{00000}_{n-k} + \underbrace{0}_{1} \underbrace{00\dots0}_{k} \underbrace{000\dots0}_{n-k-1}$$

$$// p = \frac{M}{N}, k = 0, \dots, n$$

$$\sum_{k=0}^n \binom{n}{k} p^k \cdot (1-p)^{n-k} = 1 = \underbrace{(p + (1-p))}_1^n$$

• Definíció:

$A_1, A_2, \dots, A_n$ teljes eseményrendszer, ha $\bigcup_{i=1}^n A_i = \Omega$ és páronként kizáróak.

Ha $A_1, A_2, \dots, A_n$ teljes eseményrendszer, akkor $\sum_{i=1}^n p(A_i) = 1$