



MATEKING.HU

Képletgyűjtemény

DISZKRÉT MATEMATIKA tantárgy

Kiadás dátuma: 2026. 03. 27.

Tartalomjegyzék

Kombinatorika.....	2
Halmazok, rendezett párok, leképezések.....	4
Matematikai logika, ítéletkalkulus.....	6
Gráfelméleti alapok.....	8
Gráfok izomorfiaja és síkbarajzolhatósága.....	9
Gráfok bejárása és gráfalgoritmusok.....	11
Kromatikus szám, klikk, perfekt gráfok.....	13
Gráfparaméterek, párosítások.....	16
Hálózatok, maximális folyam, minimális vágás.....	18
Írányított gráfok, gráfalgoritmusok írányított gráfokban.....	20
Legkisebb négyzetek módszere, legjobb lineáris közelítés.....	21
Lineáris leképezések.....	22
Menger tételei, többszörös összefüggőség.....	24
Páros gráfok, párosítások.....	25
Sajátérték, sajátvektor, sajátfelbontás.....	26
Teljes indukció.....	30
Oszthatóság.....	31
Euklideszi algoritmus & Diofantoszi egyenletek.....	33
Kongruenciák.....	35
Mátrixok.....	38
Lineáris egyenletrendszerek.....	43
Determináns, adjungált, kvadratikus alakok.....	45
Komplex számok.....	51
Interpolációs polinomok.....	54
Csoportok, gyűrűk, testek.....	55

Kombinatorika

Egy adott n elemű halmaz elemeinek egy ismétlés nélküli permutációján az n különböző elem egy sorba rendezését értjük.

n darab különböző elem permutációinak száma:

$$1 \cdot 2 \cdot 3 \cdot \dots \cdot n = n!$$

[Megnézem a kapcsolódó epizódot](#)

n faktoriálisán az n -nél kisebb vagy egyenlő pozitív egész számok szorzatát értjük.

$$n! = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1$$

pl.:

$$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$

$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$$

$$1! = 1$$

Továbbá definíció szerint $0! = 1$.

[Megnézem a kapcsolódó epizódot](#)

Ha n db. egymástól különböző elem közül kiválasztunk k ($k \leq n$) db.-ot úgy, hogy a kiválasztott elemek sorrendje is számít, akkor az n elem k -ad osztályú ismétlés nélküli variációját kapjuk.

n darab különböző elemből kiválasztott k darab elem variációinak száma:

$$n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot (n-k+1) = \frac{n!}{(n-k)!}$$

[Megnézem a kapcsolódó epizódot](#)

Ha n különböző elem közül kiválasztunk k ($k \leq n$) db.-ot úgy, hogy a kiválasztott elemek sorrendjére nem vagyunk tekintettel, akkor n elem k -ad osztályú ismétlés nélküli kombinációját kapjuk.

n darab különböző elem közül kiválasztott k darab elem kombinációinak száma:

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

[Megnézem a kapcsolódó epizódot](#)

Ha n elem között van $k_1, k_2, \dots, k_r$ egymással megegyező, akkor az elemek egy sorba rendezését ismétléses permutációnak nevezzük.

n elem közötti $k_1, k_2, \dots, k_r$ egymással megegyező ismétléses permutációinak száma:

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

[Megnézem a kapcsolódó epizódot](#)

Ha n db. egymástól különböző elem közül kiválasztunk k db.-ot úgy, hogy a kiválasztott elemek sorrendje is számít és ugyanazt az elemet többször is választhatjuk, akkor az n elem k -ad osztályú ismétléses variációját kapjuk.

Az n elem k -ad osztályú ismétléses variációk száma: n^k .

[Megnézem a kapcsolódó epizódot](#)

Ha kör alakban helyezünk el n különböző elemet és azok sorrendjét vizsgáljuk, akkor ciklikus permutációról beszélünk.

n darab különböző elem ciklikus permutációinak száma $\frac{n!}{n} = (n - 1)!$

[Megnézem a kapcsolódó epizódot](#)

Halmazok, rendezett párok, leképezések

Vannak az A és B halmazok.

Az A és B halmazok uniója: Azon elemek halmaza, amelyek legalább az egyik halmazban benne vannak.

Jele: $A \cup B$

Az A és B halmazok metszete: Azon elemek halmaza, amelyek mindkét halmazban benne vannak.

Jele: $A \cap B$

Az A és B halmazok különbsége: Azon elemek halmaza, amelyek az A halmazba benne vannak, de a B halmazba nem.

Jele: $A \setminus B$

Az A halmaz komplementere a H alaphalmazon nézve: Az alaphalmaz azon elemeinek halmza, amelyek nincsenek benne az A -ban.

Jele: $\overline{A}$

[Megnézem a kapcsolódó epizódot](#)

A logikai szita formula két halmazra:

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

A logikai szita formula három halmazra:

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

[Megnézem a kapcsolódó epizódot](#)

Az első De Morgan azonosság azt mondja, hogy a metszet komplementere pont megegyezik a komplementrek uniójával:

$$\overline{A \cap B} = \overline{A} \cup \overline{B}$$

A második De Morgan azonosság pedig azt mondja, hogy az unió komplementere éppen megegyezik a komplementerek metszetével:

$$\overline{A \cup B} = \overline{A} \cap \overline{B}$$

[Megnézem a kapcsolódó epizódot](#)

Egy halmaz összes részhalmazainak halmazát hatványhalmaznak nevezzük.

Pl.: az $A = \{x, y, z\}$ halmaz hatványhalmaza:

$$P(A) = \{\emptyset, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, \{x, y, z\}\}$$

[Megnézem a kapcsolódó epizódot](#)

Az A és B halmazok szimmetrikus differenciája:

$$A \triangle B = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$$

Érdemes megjegyezni, hogy $A \triangle A = \emptyset$ és $A \triangle \emptyset = A$

[Megnézem a kapcsolódó epizódot](#)

Adott az $f : A \mapsto B$ függvény. A függvény értékkészlete azoknak az elemeknek a halmaza a B halmazban, amelyek hozzá vannak rendelve valamely A halmazbeli elemekhez.

Az értékkészlet jele az angol range szó alapján, ami azt jelenti, hogy kiterjedés: R_f vagy az akadálymentesített jelölése: É.K.

[Megnézem a kapcsolódó epizódot](#)

Egy kifejezés értelmezési tartományán azt a legbővebb halmazt értjük, ahol értelmezve van.

Függvény esetén azokat a szerencsés x -eket, amelyekhez a függvény hozzárendel egy y számot, a függvény értelmezési tartományának nevezzük.

A következőket érdemes megjegyezni:

$\sqrt[n]{\text{ez itt}} \geq 0$ $\sqrt[n]{\text{ez itt bármi}}$ $\log(\text{ez itt} > 0)$ tört nevező $\neq 0$

pl.: $f(x) = \frac{4x}{(x-3)^4}$ értelmezési tartománya $\forall x \in \mathbb{R} \setminus \{-3\}$, mert nincs gyök és nincs logaritmus, de tört van, tehát a nevező nem lehet nulla ($x \neq 3$)

[Megnézem a kapcsolódó epizódot](#)

Az A és B halmazok Descartes-szorzata úgy működik, hogy elkészítjük az összes lehetséges rendezett párt, aminek az első elemét A -ból, a második elemét pedig B -ből vesszük, és ezeket a rendezett párokat betesszük egy halmazba, amit az A és B halmazok Descartes-szorzatának hívunk.

$$A \times B = \{\langle x, y \rangle \mid x \in A, y \in B\}$$

[Megnézem a kapcsolódó epizódot](#)

Az f halmazt függvénynek nevezzük, ha minden eleme rendezett pár, és ha $\langle x_1, y_1 \rangle \in f$ és $\langle x_1, y_2 \rangle \in f$ akkor szükségképpen $y_1 = y_2$

[Megnézem a kapcsolódó epizódot](#)

Matematikai logika, ítéletkalkulus

Az univerzális kvantor egy jelölése a "minden" kifejezésnek.

Jele: $\forall$

[Megnézem a kapcsolódó epizódot](#)

Az egzisztenciális kvantor egy jelölése a "létezik" vagy "van olyan" kifejezésnek.

Jele: $\exists$

[Megnézem a kapcsolódó epizódot](#)

Az állítás negációja (vagy tagadása) egy egyváltozós művelet. Egy A kijelentés negációja az a kijelentés, amely akkor igaz, ha A hamis és akkor hamis, ha A igaz.

[Megnézem a kapcsolódó epizódot](#)

Az állítás (vagy kijelentés) olyan kijelentő mondat, amelyről egyértelműen eldönthetjük, hogy az igaz vagy hamis.

[Megnézem a kapcsolódó epizódot](#)

A konjunkció két állítás közti logikai művelet. Két kijelentés konjunkciója pontosan akkor igaz, ha mindkét kijelentés igaz, különben hamis.

Jele: $A \wedge B$

[Megnézem a kapcsolódó epizódot](#)

A diszjunkció két állítás közti logikai művelet. Két kijelentés diszjunkciója pontosan akkor igaz, ha legalább az egyik kijelentés igaz, különben hamis.

Jele: $A \vee B$

[Megnézem a kapcsolódó epizódot](#)

A "ha A , akkor B " kapcsolatnak megfelelő logikai műveletet nevezzük implikációnak. Az implikáció akkor hamis, ha A igaz és B hamis, minden más esetben igaz.

Jele: $A \Rightarrow B$

[Megnézem a kapcsolódó epizódot](#)

Az ekvivalencia egy olyan logikai művelet, amikor $A \Rightarrow B$ és $A \Leftarrow B$. Az ekvivalencia akkor igaz, ha A és B logikai értéke azonos, különben hamis.

Jele: $A \Leftrightarrow B$

[Megnézem a kapcsolódó epizódot](#)

$$\neg(A \wedge B) = \neg A \vee \neg B$$

$$\neg(A \vee B) = \neg A \wedge \neg B$$

$$\neg(A \Rightarrow B) = A \wedge \neg B$$

$$\neg(A \Leftrightarrow B) = A \Leftrightarrow \neg B$$

[Megnézem a kapcsolódó epizódot](#)

A diszjunktív normálforma, röviden DNF egy olyan alakja egy logikai formuláknak, ahol a művelet a változóinak vagy negáltjainak konjunkcióinak diszjunkciója.

[Megnézem a kapcsolódó epizódot](#)

Gráfelméleti alapok

A gráf csúcsokból és azokat összekötő élekből áll.

[Megnézem a kapcsolódó epizódot](#)

Egy gráf összefüggő, ha bármelyik csúcsából el lehet jutni bármelyik másik csúcsába élek mentén.

[Megnézem a kapcsolódó epizódot](#)

A gráf egy csúcsának fokszáma a gráf e csúcsában összefutó élek száma.

[Megnézem a kapcsolódó epizódot](#)

Egy gráfban körnek nevezünk egy olyan utat, amely csupa különböző csúcsokon és éleken haladva visszavezet a kiinduló csúcsába.

[Megnézem a kapcsolódó epizódot](#)

Ha egy gráfban nincs kör, de maga a gráf összefüggő, akkor fának nevezzük.

Egy n csúcsú fának mindig $n - 1$ darab éle van.

[Megnézem a kapcsolódó epizódot](#)

Azokat a gráfokat, ahol minden csúcs mindegyikkel össze van kötve, teljes gráfnak hívjuk.

Az n csúcsú teljes gráf éleinek a száma:

$$\frac{n(n-1)}{2}$$

[Megnézem a kapcsolódó epizódot](#)

Egy gráf egyszerű, ha nincs benne sem többszörös él, sem hurokél.

[Megnézem a kapcsolódó epizódot](#)

Egy gráf Euler-köre olyan zárt élsorozat, amely a gráf összes élet pontosan egyszer tartalmazza.

[Megnézem a kapcsolódó epizódot](#)

Gráfok izomorfiaja és síkbarajzolhatósága

A G gráf csúcsainak halmazát $V(G)$ -vel jelöljük. Itt a V az angol vertex = csúcs szóra utal.

A G gráf éleinek halmazát $E(G)$ -vel jelöljük. Itt E az angol edge = él.

A G gráf egy $(V(G), E(G))$ rendezett pár, ahol $V(G)$ egy nem üres halmaz, $E(G)$ pedig a $V(G)$ -ből képezhető párok egy halmaza.

[Megnézem a kapcsolódó epizódot](#)

Ha a gráf egy csúcsából elindulunk, és teszünk egy sétát a gráfon, akkor egy élsorozatot kapunk.

Azokat az élsorozatotokat, amelyek a gráf semelyik pontján nem haladnak át többször, útnak nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Ha egy élsorozat ugyanabból a csúcsból indul, mint ahova érkezik, akkor körsétának nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Minden gráfban a csúcsok fokszámainak összege az élek számának a kétszerese:

$$\sum d(V_n) = 2e$$

[Megnézem a kapcsolódó epizódot](#)

Ha egy gráfban nincs kör, de maga a gráf összefüggő, akkor fának nevezzük.

Egy n csúcsú fának mindig $n - 1$ darab éle van.

[Megnézem a kapcsolódó epizódot](#)

A nem összefüggő körmentes gráfok neve erdő.

[Megnézem a kapcsolódó epizódot](#)

Egy gráf komplementere azt a gráfot jelenti, aminek csúcsai ugyanazok, mint az eredeti gráfnak, és két csúcs pontosan akkor szomszédos benne, ha az eredeti gráfban nem.

[Megnézem a kapcsolódó epizódot](#)

A $G(V(G), E(G))$ gráf izomorf a $G'(V(G'), E(G'))$ gráffal, ha van egy bijekció a $V(G)$ és $V'(G)$ között, amire teljesül, hogy G -ben pontosan akkor szomszédos két pont, ha G' -ben a nekik megfelelő pontok szomszédosak, és szomszédos pontpárok esetén ugyanannyi él fut közöttük.

[Megnézem a kapcsolódó epizódot](#)

Egy gráfban topologikusan ekvivalens átalakításnak nevezzük azt, ha egy élt egy másodfokú csúcs beiktatásával két éltre bontunk, vagy ha egy 2 fokú csúcsra illeszkedő éleket egybeolvasztunk, és a csúcsot elhagyjuk.

Két gráf akkor topologikusan izomorf, ha topologikusan ekvivalens lépések egymás utáni alkalmazásával el tudjuk érni, hogy a két gráf izomorf legyen.

[Megnézem a kapcsolódó epizódot](#)

A titkos recept gráfok izomorfijának vizsgálatához:

- 1) Fokszámok vizsgálata
- 2) Utak hossza
- 3) Van-e kör?
- 4) Milyen hosszúak a körök?
- 5) Élek vizsgálata

[Megnézem a kapcsolódó epizódot](#)

Egy gráf síkbarajzolható, ha lerajzolható úgy, hogy élei csak a csúcspontokban találkozzanak.

[Megnézem a kapcsolódó epizódot](#)

A Kuratowski-tétel szerint egy gráf pontosan akkor nem síkbarajzolható, ha tartalmaz $K_{3,3}$ -mal vagy K_5 -tel topológiailag izomorf részgráfot.

[Megnézem a kapcsolódó epizódot](#)

Azt mondja az Euler-féle poliéder-tétel, hogy ha egy konvex poliéder csúcsainak száma V , lapjainak száma F és éleinek száma E , akkor

$$V + F = E + 2$$

[Megnézem a kapcsolódó epizódot](#)

Ha egy egyszerű gráfban minden kör legalább k hosszú, akkor a síkbarajzolhatóság szükséges feltétele:

$$(k - 2) \cdot E \leq k \cdot V - 2k$$

[Megnézem a kapcsolódó epizódot](#)

Ha egy egyszerű gráf síkbarajzolható, akkor meg kell felelnie ennek a feltételnek:

$$E \leq 3V - 6$$

[Megnézem a kapcsolódó epizódot](#)

Gráfok bejárása és gráfalgoritmusok

Egy gráf feszítőfája a gráf minden csúcsát tartalmazó fa részgráf. Feszítőfából általában több is van.

[Megnézem a kapcsolódó epizódot](#)

A minimális feszítőfa egy gráfban a legkisebb élsúlyú feszítőfa.

[Megnézem a kapcsolódó epizódot](#)

A Kruskal algoritmus segítségével minimális feszítőfát lehet megtalálni.

Az első lépés, hogy keressük meg a gráfban a legkisebb súlyú élt. Ha több azonos súlyú él van, akkor válasszuk ki azt, amelyikhez kedvünk van.

Ezek után belépünk egy ciklusba, ahol minden lépésben az eddig még ki nem választott élekre alkalmazzuk az előző lépést úgy, hogy ne keletkezzen kör. Ha mégis kör keletkezne, akkor a legutolsó olyan élt, amelynek hozzávétele során a kört kapjuk, töröljük.

Ezt addig csináljuk, amíg kész nem vagyunk.

[Megnézem a kapcsolódó epizódot](#)

Gráfok egy adott pontjából való feltérképezésére alkalmas módszer a szélességi keresés (BFS = Breadth-first search).

Működése:

Elindulunk egy adott pontból, és megkeressük az összes szomszédos pontot. Ezek az 1 egység távolságra lévő szomszédok és mindegyikre ragasztunk egy 1-es címkét.

Most ezeknek keressük meg az 1 egység távoli szomszédjait. De csak azokat, akiken még nincsen címke.

Ők a kiinduló ponttól 2 egység távolságra vannak és 2-es címkét kapnak.

Ha valamelyik 2-es szomszédba több él is vezet, akkor csak az egyiket hagyjuk meg. Mindegy melyiket.

Az algoritmus aztán így folytatódik, és szép lassan végez.

[Megnézem a kapcsolódó epizódot](#)

A DFS (Depth-first search) algoritmus a gráf mélységi bejárása.

A DFS algoritmus lényege, hogy elindulunk egy úton, és megyünk, amíg csak tudunk.

Amikor elakadunk, mert már nem tudunk úgy továbbmenni, hogy olyan pontba jussunk, ahol még nem jártunk, akkor visszamegyünk egészen addig, ahonnan még lehet földerítetlen pontok felé haladni.

Amikor újra elakadunk, megint visszamegyünk, és ezt ismételjük, amíg az egész gráfot be nem jártuk.

[Megnézem a kapcsolódó epizódot](#)

A BFS és DFS algoritmusok végrehajtása során a gráfnak egy-egy feszítőfáját kapjuk. Ezeket nevezzük BFS és DFS fának.

[Megnézem a kapcsolódó epizódot](#)

Egy gráf csúcsainak bejárására van egy nagyon speciális módszer, amit Hamilton körnek nevezünk, és az a lényege, hogy egy olyan körön haladunk végig a gráfban, amely a gráf összes pontját tartalmazza.

Hamilton kör létezésének szükséges feltétele:

Ha egy gráfból k darab csúcsot kitörünk (a belőle kiinduló élekkel együtt), akkor a megmaradó gráfnak legfeljebb k darab komponense lehet.

[Megnézem a kapcsolódó epizódot](#)

A Hamilton út egy olyan út, amely a gráf minden csúcsát tartalmazza.

Hamilton út létezésének szükséges feltétele:

Ha egy gráfból k darab csúcsot kitörünk (a belőle kiinduló élekkel együtt), akkor a megmaradó gráfnak legfeljebb $k + 1$ darab komponense lehet.

[Megnézem a kapcsolódó epizódot](#)

A Dirac-tétel azt mondja ki, hogy ha egy G egyszerű, $n \geq 3$ csúcsú gráfban minden csúcs foka legalább $\frac{n}{2}$, akkor a gráfban van Hamilton kör.

[Megnézem a kapcsolódó epizódot](#)

Az Ore-tétel azt mondja, hogy ha egy G egyszerű, $n \geq 3$ csúcsú gráfban bármely V_i és V_j nem szomszédos csúcsra $d(V_i) + d(V_j) \geq n$ teljesül, akkor a gráfban van Hamilton kör.

[Megnézem a kapcsolódó epizódot](#)

Kromatikus szám, klikk, perfekt gráfok

A legkevesebb színt, amivel egy gráf csúcsait kiszínezzük úgy, hogy a szomszédos csúcsok ne legyenek egyforma színűek, a gráf kromatikus számának nevezzük.

Jele: $\chi(G)$.

[Megnézem a kapcsolódó epizódot](#)

Egy G egyszerű gráfban klikknek nevezzük azokat a részgráfokat, amelyek teljes gráfok.

[Megnézem a kapcsolódó epizódot](#)

Egy gráf klikkszám a gráfban található maximális klikk elemszáma.

A G gráf klikkszámát $\omega(G)$ -vel jelöljük.

Minden gráfban a klikkszám alsó becslés a kromatikus számra:

$$\omega(G) \leq \chi(G)$$

[Megnézem a kapcsolódó epizódot](#)

A G gráfban a G' részgráf feszített részgráf, ha bármely két csúcs a G' gráfban pontosan akkor szomszédos, ha G -ben is szomszédos.

[Megnézem a kapcsolódó epizódot](#)

Ha egy G gráf minden G' feszített részgráfjára igaz, hogy

$$\omega(G') = \chi(G')$$

akkor a G gráfot perfekt gráfnak nevezzük.

Ha egy gráf perfekt, akkor a kromatikus száma egyenlő a klikkszámával. Az állítás fordítva nem igaz, abból, hogy $\omega(G) = \chi(G)$ még nem következik, hogy a gráf perfekt.

[Megnézem a kapcsolódó epizódot](#)

$$\omega(G) \leq \chi(G) \leq \Delta(G) + 1$$

ahol $\omega(G)$ a gráf klikkszám, $\chi(G)$ a kromatikus száma és $\Delta(G)$ a maximális fokszáma.

[Megnézem a kapcsolódó epizódot](#)

A mohó színezés egy algoritmus a gráfok színezésére.

Lényege, hogy sorba rakjuk a gráf csúcsait, és elkezdjük színezni úgy, hogy minden csúcs színezéséhez a lehető legkisebb sorszámú színt használjuk. Ezt addig folytatjuk, amíg az összes csúcs ki nem lesz színezve, és így elhasználunk legfeljebb $\Delta(G) + 1$ darab színt.

[Megnézem a kapcsolódó epizódot](#)

Ha G nem teljes gráf, vagy páratlan csúcsú kör, akkor

$$\chi(G) \leq \Delta(G)$$

[Megnézem a kapcsolódó epizódot](#)

Egy G gráfban azt a legkisebb számot, amire a gráfnak már van jó élszínezése, a G gráf élkromatikus számának nevezzük.

Jele: χ_e

[Megnézem a kapcsolódó epizódot](#)

A Vizing-tétel a gráfok élkromatikus számára ad alsó és felső becslést:

$$\Delta(G) \leq \chi_e(G) \leq \Delta(G) + 1$$

Vagyis a G egyszerű gráfok két osztályba sorolhatók:

Első osztály: $\chi_e(G) = \Delta(G)$

Második osztály: $\chi_e(G) = \Delta(G) + 1$

[Megnézem a kapcsolódó epizódot](#)

Az intervallumgráf egy olyan gráf, melynek csúcsai megfeleltethetők a valós számok egy-egy intervallumának, és két csúcs között akkor vezet él, ha a nekik megfeleltethető két intervallum metszete nem üres.

Az intervallumgráfok mindig perfekt gráfok.

[Megnézem a kapcsolódó epizódot](#)

Egy G gráfot páros gráfnak nevezünk, ha csúcsainak a $V(G)$ halmaza felbontható az A és B diszjunkt részhalmazokra, úgy hogy A -n és B -n belül nem vezetnek élek.

A páros gráfok kromatikus száma 2, élkromatikus számukra pedig König Dénesnek van egy remek tétele:

Ha G páros gráf, akkor $\chi_e(G) = \Delta(G)$

[Megnézem a kapcsolódó epizódot](#)

Jan Mycielski lengyel matematikust nyugtalanította az a kérdés, hogy léteznek-e olyan gráfok, amelyeknek a kromatikus száma nagyon nagy, de a klikkszáma csak 2.

Létrehozott egy konstrukciót, amivel olyan gráfokat lehet alkotni, amelyek klikkszáma 2, a kromatikus számuk pedig bármilyen nagy lehet. Ezeket a gráfokat Mycielski-gráfoknak nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Gráfparaméterek, párosítások

A független ponthalmaz precíz definíciójára mindjárt kettő is van.

Íme az egyik:

Egy G gráfban független csúcshalmaznak nevezzük a csúcsoknak az $A \subset V(G)$ részhalmazát, ha nincs olyan él, amelynek mindkét végpontja A -ban van.

És itt jön a másik:

Egy G gráfban független csúcshalmaznak nevezzük a csúcsoknak az $A \subset V(G)$ részhalmazát, ha az A által feszített részgráf nem tartalmaz élt.

Egy G gráfban a független csúcsok maximális számát $\alpha(G)$ -vel jelöljük.

[Megnézem a kapcsolódó epizódot](#)

Egy G gráfban a $T \subset V(G)$ ponthalmaz lefogó ponthalmaz, ha G minden élének legalább az egyik végpontja T -ben van.

Egy gráfban a minimális méretű lefogó ponthalmaz elemszámát $\tau(G)$ -vel jelöljük.

A maximális lefogó ponthalmaz pedig a gráf összes csúcsa, és elemszáma éppen $|V(G)| = n$.

[Megnézem a kapcsolódó epizódot](#)

Ha vesszük egy gráfban a maximális számú független pontokat és a minimális számú lefogó pontokat, akkor épp megkapjuk a gráf összes pontját.

Ezt hívjuk első Gallai tételnek:

$$\tau(G) + \alpha(G) = n$$

[Megnézem a kapcsolódó epizódot](#)

Egy G gráf éleinek M részhalmaza független élhalmaz, ha M semelyik két elemének nincs közös végpontja.

Egy gráf független éleinek maximális számát $\nu(G)$ -vel jelöljük.

[Megnézem a kapcsolódó epizódot](#)

Egy G gráf éleinek R részhalmaza lefogó élhalmaz, ha a gráf minden csúcsa valamelyik R -beli él végpontja.

Egy G gráfban a lefogó élek minimális számát $\rho(G)$ -vel jelöljük.

[Megnézem a kapcsolódó epizódot](#)

Ha vesszük egy gráfban a minimális számú lefogó éleket, és a maximális számú független éleket, akkor a gráf minden pontjához pontosan egy él fog tartozni.

Ez Gallai második tétele:

Ha egy n csúcsú gráf nem tartalmaz izolált pontot, akkor

$$\rho(G) + \nu(G) = n$$

[Megnézem a kapcsolódó epizódot](#)

$$\alpha(G) \leq \rho(G) \quad \nu(G) \leq \tau(G)$$

[Megnézem a kapcsolódó epizódot](#)

Egy G gráf akkor és csak akkor páros, ha minden G -ben szereplő kör páros hosszúságú.

[Megnézem a kapcsolódó epizódot](#)

Egy G gráfban az $E(G)$ élhalmaznak egy M részhalmazát párosításnak nevezzük, ha M semelyik két elemének nincs közös végpontja.

[Megnézem a kapcsolódó epizódot](#)

Egy G gráfban az $e_1, e_2, e_3, \dots, e_n$ élsorozat az M párosítás javító útja, ha

1) a megadott élsorozat egy páratlan hosszú út G -ben

2) az élek felváltva elemei M -nek:

$$e_{2k} \in M \text{ és } e_{2k+1} \notin M$$

3) az út kezdő és végpontja nem illeszkedik semelyik M -beli élre sem

[Megnézem a kapcsolódó epizódot](#)

Azokat a párosításokat nevezzük teljes párosításoknak, ami a gráf összes csúcsát lefedi.

[Megnézem a kapcsolódó epizódot](#)

Egy gráfban akkor és csakis akkor létezik teljes párosítás, ha bárhogyan hagyunk el a gráfból néhány pontot, a megmaradt gráfban a páratlan komponensek száma nem több az elhagyott pontok számánál.

[Megnézem a kapcsolódó epizódot](#)

Hálózatok, maximális folyam, minimális vágás

Legyen X a $V(G)$ -nek egy olyan részhalmaza, ami S -t tartalmazza. Ekkor az X -ből a $V(G) - X$ -be vezető éleket (S, T) vágásnak nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Egy (S, T) vágás kapacitása, a vágásban szereplő élek kapacitásainak összege.

[Megnézem a kapcsolódó epizódot](#)

A Ford-Fulkerson algoritmus egy olyan algoritmus, amit a maximális folyam megkeresésére használunk. Az algoritmus lényege pedig az a javító gráf, amit az eredeti hálózat alapján készítünk el. A javító gráf megmutatja nekünk, hogy milyen útvonalon tudjuk növelni a meglévő folyamat.

[Megnézem a kapcsolódó epizódot](#)

Legyen G egy irányított gráf és értelmezzünk a gráf élein egy $E \rightarrow R_0^+$ függvényt, ami minden élhez hozzárendeli a $c(e)$ nem negatív számot, amit az él kapacitásának nevezünk.

[Megnézem a kapcsolódó epizódot](#)

Legyen G egy irányított gráf és értelmezzünk a gráf élein egy $E \rightarrow R_0^+$ függvényt, ami minden élhez hozzárendeli a $c(e)$ nem negatív számot, amit az él kapacitásának nevezünk.

Van továbbá két kitüntetett pont a gráfban, S (source = forrás) és T (target = cél).

Ekkor a (G, S, T, c) egy hálózat.

[Megnézem a kapcsolódó epizódot](#)

A hálózatban folyamnak nevezünk egy olyan $f(e) E \rightarrow R_0^+$ függvényt, amire teljesül, hogy bármely e élre $0 \leq f(e) \leq c(e)$ és bármely T -től és S -től különböző V csúcsra:

$$\sum_{Vbe} f(e) - \sum_{Vki} f(e) = 0$$

[Megnézem a kapcsolódó epizódot](#)

Egy folyam értékének az

$$m_f = \sum_{Ski} f(e) - \sum_{Sbe} f(e)$$

számot nevezzük.

[Megnézem a kapcsolódó epizódot](#)

A Ford-Fulkerson tétel azt mondja ki, hogy egy hálózatban a maximális folyam mindig megegyezik a minimális vágással.

[Megnézem a kapcsolódó epizódot](#)

Mindig létezik egy olyan út, ami csak azokon a pontokon halad át, ahol a tartalékidő nulla, és az út hossza megegyezik a teljes folyamat hosszával. Ezt az utat kritikus útnak nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Irányított gráfok, gráfalgoritmusok irányított gráfokban

A DFS algoritmusnak az a lényege, hogy kiindulunk egy csúcsból, és megyünk ameddig tudunk.

Az, hogy merre megyünk, teljesen a véletlen műve.

Egyszer aztán elérkezünk egy olyan pontba, ahonnan már nincs tovább.

Innen már csak olyan csúcsba tudnánk továbblépni, ahol korábban már jártunk.

Ekkor visszaugrunk egészen addig, ahonnan még vezet út bejáratlan csúcsba.

Ha már minden csúcshoz eljutottunk, akkor a DFS algoritmus véget ér.

[Megnézem a kapcsolódó epizódot](#)

A DFS algoritmus eredményeként kapjuk a DFS-fát.

Hogyha a DFS-fába berajzoljuk az eredeti gráf többi élét is, akkor ezek az élek három típusba sorolhatóak. Vannak olyan élek, amelyek képesek lerövidíteni egy utat a DFS fában. Ezeket az éleket úgy hívjuk, hogy "előre-él". Ha az eredeti gráfban van fordított irányú él, akkor ezt az élt "vissza-él"-nek nevezzük. Hogyha az eredeti gráfban van u -ból v -be vezető él, akkor ezt az élt "kereszt-él"-nek nevezzük.

[Megnézem a kapcsolódó epizódot](#)

A BFS-algoritmus lényege, hogy kiindulunk egy csúcsból, aztán megkeressük a közvetlen szomszédjait. Innen folytatódik az algoritmus, és az új csúcsoknak keressük meg a szomszédjait. Ha több él is vezet egy szomszéd felé, mindegy melyiket választjuk. Az algoritmust addig ismételjük, amíg minden csúcsot meg nem találtunk.

[Megnézem a kapcsolódó epizódot](#)

A BFS algoritmus eredményeként kapjuk a BFS-fát.

Hogyha a BFS-fába berajzoljuk az eredeti gráf többi élét is, akkor ezek az élek három típusba sorolhatóak.

Vannak "előre-él"ek, "vissza-él"ek és "kereszt-él"ek.

[Megnézem a kapcsolódó epizódot](#)

A Dijkstra algoritmus képes megtalálni a gráf egy adott csúcsából a többi csúcsba vezető legrövidebb utat.

Az algoritmus lényege, hogy kiválasztunk egy pontot, és ebből a pontból kiindulva csúcsról csúcsra haladva felderítjük az egész gráfot.

[Megnézem a kapcsolódó epizódot](#)

Legkisebb négyzetek módszere, legjobb lineáris közelítés

Gauss-féle normálegyenletek:

$$n \cdot b_0 + b_1 \cdot \sum x_i = \sum y_i$$

$$b_1 \cdot \sum x_i^2 + b_0 \cdot \sum x_i = \sum x_i y_i$$

Ahol n a megfigyelések száma.

[Megnézem a kapcsolódó epizódot](#)

Az $A\underline{x} = \underline{b}$ egyenletrendszer optimális megoldásai megegyeznek az

$$A^T \cdot A \cdot \underline{x} = A^T \cdot \underline{b}$$

egyenletrendszer megoldásaival.

[Megnézem a kapcsolódó epizódot](#)

Ha egy egyenletrendszernek nincs megoldása, akkor az optimális megoldás megadja a legjobb közelítést.

Az $A\underline{x} = \underline{b}$ egyenletrendszer optimális megoldásai megegyeznek az

$$A^T \cdot A\underline{x} = A^T \cdot \underline{b}$$

egyenletrendszer megoldásaival.

[Megnézem a kapcsolódó epizódot](#)

Az $A\underline{x} = \underline{b}$ egyenletrendszer Gauss-féle normálegyenlete:

$$A^T \cdot A\underline{x} = A^T \cdot \underline{b}$$

[Megnézem a kapcsolódó epizódot](#)

Egy $\underline{b}$ vektort nem csak merőlegesen vetíthetjük, hanem ferdén is. Viszont egyedül a merőleges vetítés rendelkezik a legjobb közelítés tulajdonságával.

A $\underline{b}$ vektor legjobb közelítése a W altérben egy olyan $\underline{b}'$ vektor, amire $|\underline{b} - \underline{b}'|$ minimális.

[Megnézem a kapcsolódó epizódot](#)

Lineáris leképezések

A φ leképezést lineáris leképezésnek nevezzük, ha bármely $\underline{v}_1, \underline{v}_2 \in V_1$ vektorokra és $\lambda \in R$ számra teljesül, hogy

$$\varphi(\underline{v}_1 + \underline{v}_2) = \varphi(\underline{v}_1) + \varphi(\underline{v}_2)$$

$$\varphi(\lambda \cdot \underline{v}) = \lambda \cdot \varphi(\underline{v})$$

[Megnézem a kapcsolódó epizódot](#)

A $V_1 \rightarrow V_2$ lineáris leképezésnél V_2 -nek azt a részét, amely a leképezés során előáll, a leképezés képterének nevezzük és $Im\varphi$ -vel jelöljük.

[Megnézem a kapcsolódó epizódot](#)

A nullvektorból minden lineáris leképezés nullvektort csinál, vagyis $\underline{0}$ képe mindig $\underline{0}$, de előfordulhat, hogy más V_1 -beli [vektorok](#) képe is nullvektor lesz. Ezen [vektorok](#) halmazát nevezzük a leképezés magterének és $Ker\varphi$ -vel jelöljük.

[Megnézem a kapcsolódó epizódot](#)

A képtér és a magtér dimenziója összesen éppen kiadja V_1 dimenzióját.

Ezt az összefüggést dimenziótételnek nevezzük:

$$\dim(Ker\varphi) + \dim(Im\varphi) = \dim(V_1)$$

[Megnézem a kapcsolódó epizódot](#)

Minden lineáris leképezést jellemezhetünk egy mátrixszal. Valójában mindegyiket végtelen sok mátrixszal jellemezhetjük, ezek a [mátrixok](#) pedig úgy keletkeznek, hogy veszünk egy tetszőleges bázist V_1 -ben és a bázis[vektorok](#) képeit egymás mellé írjuk.

[Megnézem a kapcsolódó epizódot](#)

A φ leképezésben minden vektor képét így kapjuk:

$$\varphi(\underline{v}) = (\varphi)_b \cdot \underline{v}$$

[Megnézem a kapcsolódó epizódot](#)

Egy leképezésnek pontosan akkor létezik inverze, ha a $(\varphi)_b$ mátrixnak létezik inverze, és az inverz leképezés mátrixa:

$$\varphi^{-1} \text{ mátrixa } (\varphi)_b^{-1}$$

[Megnézem a kapcsolódó epizódot](#)

A $\varphi \circ \mu$ leképezés mátrixa:

$$(\varphi \circ \mu)_b = (\varphi)_b \cdot (\mu)_b$$

[Megnézem a kapcsolódó epizódot](#)

Ha egy $n \times n$ -es mátrixnak van n darab független sajátvektora, akkor létezik a mátrixnak egy úgynevezett diagonális alakja.

A diagonális alak így néz ki:

$$\text{diag}(A) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

a főatlóban vannak a sajátértékek és az összes többi elem nulla.

A diagonális alakot a következő módon állítjuk elő:

$$\text{diag}(A) = X^{-1} \cdot A \cdot X$$

$$\text{itt } X = (\underline{v}_1 \quad \underline{v}_2 \quad \dots \underline{v}_n)$$

[Megnézem a kapcsolódó epizódot](#)

A φ lineáris leképezésnek a $\underline{b}_1 \quad \underline{b}_2 \quad \dots \quad \underline{b}_n$ bázisban felírt mátrixát úgy kapjuk meg, hogy a bázisvektorok képeit egymás mellé írjuk:

$$(\varphi)_b = (\varphi(\underline{b}_1) \quad \varphi(\underline{b}_2) \quad \varphi(\underline{b}_3) \quad \dots \quad \varphi(\underline{b}_n))$$

Bármilyen bázist is választunk is V_1 -ben, a leképezés mátrixa mindig egy $n \times n$ -es mátrix lesz. Ha ennek a mátrixnak van n darab független sajátvektora, akkor ezek a sajátvektorok szintén egy bázist alkotnak V_1 -ben, amit sajátbázisnak nevezünk.

[Megnézem a kapcsolódó epizódot](#)

A $V_1 \rightarrow V_2$ lineáris leképezést másnéven homomorfizmusnak is nevezzük. Ezek a homomorfizmusok és azok mátrixai maguk is egy vektorteret alkotnak, ezt a vektorteret $\text{Hom}(V_1, V_2)$ -nek nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Ha A és B olyan mátrixok, hogy létezik egy C mátrix úgy, hogy

$$A = C^{-1} \cdot B \cdot C$$

akkor a két mátrix egymáshoz hasonló.

[Megnézem a kapcsolódó epizódot](#)

Menger tételei, többszörös összefüggőség

Egy G gráf k -szorosan élösszefüggő, ha bárhogyan hagyunk el belőle k -nál kevesebb élt, a maradék gráf összefüggő marad.

[Megnézem a kapcsolódó epizódot](#)

Egy G gráf k -szorosan pontösszefüggő, ha legalább $k + 1$ pontja van és bárhogyan hagyunk el belőle k -nál kevesebb pontot, a maradék gráf összefüggő marad.

[Megnézem a kapcsolódó epizódot](#)

Egy G irányított gráfban az u -ból v -be vezető élidegen utak maximális száma megegyezik az u -ból v -be vezető utakat lefogó élek minimális számával.

Egy G gráfban az u -ból v -be vezető élidegen utak maximális száma megegyezik az u -ból v -be vezető utakat lefogó élek minimális számával.

Egy G irányított gráfban u és v legyen két különböző nem szomszédos csúcs. Ekkor az u -ból v -be vezető pontidegen utak maximális száma megegyezik az u -ból v -be vezető utakat lefogó (u -tól és v -től különböző) pontok minimális számával.

Egy G gráfban u és v legyen két különböző nem szomszédos csúcs. Ekkor az u -ból v -be vezető pontidegen utak maximális száma megegyezik az u -ból v -be vezető utakat lefogó (u -tól és v -től különböző) pontok minimális számával.

[Megnézem a kapcsolódó epizódot](#)

Páros gráfok, párosítások

Legyen $G(A, B, E)$ páros gráf és X pedig A -nak egy tetszőleges részhalmaza. Az X -ben lévő csúcsok B -beli szomszédjainak halmazát hívjuk $N(X)$ -nek. A G gráfnak akkor és csak akkor van A -t fedő párosítása, ha bármely X halmazra

$$|X| \leq |N(X)|$$

[Megnézem a kapcsolódó epizódot](#)

A $G(A, B, E)$ páros gráfban akkor és csak akkor létezik teljes párosítás, ha

$$|A| = |B| \text{ és}$$

$$|X| \leq |N(X)| \text{ minden } X \subseteq A \text{ ponthalmazra.}$$

[Megnézem a kapcsolódó epizódot](#)

Sajátérték, sajátvektor, sajátfelbontás

Az A $n \times n$ -es [mátrix](#) sajátértéke egy olyan λ valós szám, amelyhez van valami $\underline{v}$ nem nullvektor, hogy $A \cdot \underline{v} = \lambda \cdot \underline{v}$

A sajátérték lényege, hogy vannak olyan [mátrixok](#), és olyan [vektorok](#), hogyha a mátrixot megszorozzuk a vektorral, akkor az eredeti vektornak egy számszorosát kapjuk. Az egységmátrixpéldául ilyen: ha az egységmátrixszal megszorozunk egy tetszőleges vektort, akkor ugyanazt a vektort kapjuk. Ilyenkor minden vektor sajátvektor és a sajátérték 1, mert minden vektorból az 1-szerese lesz.

A saját[vektorok](#) és sajátértékek egyik legfontosabb alkalmazása a geometriai transzformációk, amelyek szintén mátrixokkal írhatók le. A síkbeli tükrözés az x tengelyre például egy geometriai transzformáció, aminek a mátrixa két sajátértékkel rendelkezik. Az x tengelyen lévő vektorokkal a tükrözés hatására nem történik semmi. Ezek tehát saját maguk 1-szeresei lesznek. Az y tengelyen lévő [vektorok](#) viszont az x tengelyre történő tükrözéskor "megfordulnak" vagyis beszorzódnak -1-gyel. A tükrözés mátrixának tehát ezek lesznek a sajátértékei. Az 1 és a -1. Mindez sokkal érthetőbb lesz, ha megnézed a kapcsolódó epizódot.

[Megnézem a kapcsolódó epizódot](#)

Az A $n \times n$ -es [mátrix](#) sajátvektora egy olyan $\underline{v}$ nem nullvektor, amelyhez van valami λ valós szám, hogy $A \cdot \underline{v} = \lambda \cdot \underline{v}$

A sajátvektor lényege, hogy vannak olyan [mátrixok](#), és olyan [vektorok](#), hogyha a mátrixot megszorozzuk a vektorral, akkor az eredeti vektornak egy számszorosát kapjuk. A saját[vektorok](#) és sajátértékek egyik legfontosabb alkalmazása a geometriai transzformációk, amelyek szintén mátrixokkal írhatók le.

Vegyük például a síkbeli tükrözést az x tengelyre. Ez egy geometriai transzformáció. Az x tengelyen lévő vektorokkal a tükrözés hatására nem történik semmi. Ezek tehát saját maguk 1-szeresei lesznek. Vagyis ezek a [vektorok](#) egytől egyig saját[vektorok](#), mert teljesítik azt amit egy sajátvektornak tudnia kell: ha megszorozzuk a mátrixot a vektorral, akkor az eredeti vektor számszorosát kapjuk. Itt most éppen az eredeti vektor 1-szeresét kapjuk. Az y tengelyen lévő [vektorok](#) szintén saját[vektorok](#), mert az x tengelyre történő tükrözéskor "megfordulnak" vagyis beszorzódnak -1-gyel. Vagyis ezek a [vektorok](#) saját maguk -1-szeresei lesznek. A tükrözés mátrixának tehát ezek lesznek a sajátvektorai: az x tengely és az y tengely vektorai. Az x tengelyen lévő sajátvektorokhoz tartozó sajátérték az 1, míg az y tengelyen lévő sajátvektorokhoz tartozó sajátérték a -1. Mindez sokkal érthetőbb lesz, ha megnézed a kapcsolódó epizódot.

[Megnézem a kapcsolódó epizódot](#)

A karakterisztikus egyenlet a sajátértékek kiszámolásához szükséges egyenlet:

$$\det(A - \lambda \cdot I) = 0$$

A karakterisztikus egyenlet segít nekünk kiszámolni egy [mátrix](#) sajátértékeit. A sajátértékeket úgy kapjuk, hogy a karakterisztikus polinomot egyenlővé tesszük nullával. Így egy egyenletet kapunk, és ennek az egyenletnek a megoldásai a sajátértékek. Az egyenletet karakterisztikus egyenletnek is szokás nevezni, és egyetlen bökkenő vele, hogy egy $n \times n$ -es [mátrix](#) karakterisztikus egyenlete n -edfokú. Vagyis 2-nél és 3-nál még valahogyan meg tudjuk oldani az egyenletet, de mondjuk egy 5×5 -ös mátrixnál már ötödfokú egyenletet kapunk, amivel adódhatnak gondok.

[Megnézem a kapcsolódó epizódot](#)

A karakterisztikus polinom:

$$\det(A - \lambda \cdot I)$$

A karakterisztikus polinom segít nekünk kiszámolni egy [mátrix](#) sajátértékeit. A sajátértékeket úgy kapjuk, hogy a karakterisztikus polinomot egyenlővé tesszük nullával. Így egy egyenletet kapunk, és ennek az egyenletnek a megoldásai a sajátértékek. Vagyis a sajátértékek mindig a karakterisztikus polinom gyökei. Előfordul, hogy egy sajátérték többszörös gyök, és az is megeshet, hogy komplex gyökei vannak a karakterisztikus polinomnak.

Azt az egyenletet, amikor a karakterisztikus polinomot egyenlővé tesszük nullával karakterisztikus egyenletnek is szokás nevezni, és egyetlen bökkenő vele, hogy egy $n \times n$ -es [mátrix](#) karakterisztikus egyenlete n -edfokú. Vagyis 2-nél és 3-nál még valahogyan meg tudjuk oldani az egyenletet, de mondjuk egy 5×5 -ös mátrixnál már ötödfokú egyenletet kapunk, amivel adódhatnak gondok.

[Megnézem a kapcsolódó epizódot](#)

Ha egy $n \times n$ -es mátrixnak van n darab független sajátvektora, akkor létezik a mátrixnak egy úgynevezett diagonális alakja.

A diagonális alak így néz ki:

$$\text{diag}(A) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

a főatlóban vannak a sajátértékek és az összes többi elem nulla.

A diagonális alakot a következő módon állítjuk elő:

$$\text{diag}(A) = X^{-1} \cdot A \cdot X$$

$$\text{itt } X = (\underline{v}_1 \quad \underline{v}_2 \quad \dots \underline{v}_n)$$

[Megnézem a kapcsolódó epizódot](#)

Ha egy $n \times n$ -es mátrixnak van n darab független sajátvektora, akkor létezik a mátrixnak egy úgynevezett diagonális alakja.

A diagonális alak így néz ki:

$$\text{diag}(A) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

a főatlóban vannak a sajátértékek és az összes többi elem nulla.

A diagonális alakot a következő módon állítjuk elő:

$$\text{diag}(A) = X^{-1} \cdot A \cdot X$$

$$\text{itt } X = (\underline{v}_1 \quad \underline{v}_2 \quad \dots \underline{v}_n)$$

[Megnézem a kapcsolódó epizódot](#)

Ha egy $n \times n$ -es mátrixnak van n darab független sajátvektora, akkor létezik a mátrixnak egy úgynevezett diagonális alakja.

A diagonális alak így néz ki:

$$\text{diag}(A) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

a főatlóban vannak a sajátértékek és az összes többi elem nulla.

A diagonális alakot a következő módon állítjuk elő:

$$\text{diag}(A) = X^{-1} \cdot A \cdot X$$

$$\text{itt } X = (\underline{v}_1 \quad \underline{v}_2 \quad \dots \underline{v}_n)$$

[Megnézem a kapcsolódó epizódot](#)

Ha az A mátrix egy $n \times n$ -es diagonalizálható mátrix, akkor a sajátfelbontása:

$$A = X \cdot \text{diag}(A) \cdot X^{-1}$$

Itt $X = (\underline{v}_1 \quad \underline{v}_2 \quad \dots \quad \underline{v}_n)$ vagyis egyszerűen úgy keletkezi, hogy a sajátvektorokat fogjuk, és leírjuk egymás mellé és

$$\text{diag}(A) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

A spektrálfelbontás segítségével könnyebben hatványozhatunk:

$$A^n = X \cdot (\text{diag}(A))^n \cdot X^{-1}$$

[Megnézem a kapcsolódó epizódot](#)

Teljes indukció

A teljes indukció olyan állítások bizonyítására alkalmas, melyek n pozitív egész számtól függenek.

A teljes indukciós bizonyítás lépései:

1. lépés: Igazoljuk, hogy az állítás $n = 1$ esetén vagy az első néhány n -re igaz.

2. lépés: Igazoljuk, hogy ha az állítás n -re igaz, akkor $n + 1$ esetén is igaz.

Ezzel az állítást minden n pozitív egész számra belátjuk.

[Megnézem a kapcsolódó epizódot](#)

Oszthatóság

Az a és b szám legnagyobb közös osztója az a d pozitív szám, amire $d \mid a$ és $d \mid b$, és e közös osztók közül ez a legnagyobb.

Jelölés: $d = (a, b)$

[Megnézem a kapcsolódó epizódot](#)

a és b relatív prímek, ha $(a, b) = 1$

[Megnézem a kapcsolódó epizódot](#)

Ha $a \mid c$ és $b \mid c$ és $(a, b) = 1$ akkor $ab \mid c$

Ha $c \mid ab$ és $(a, c) = 1$ akkor $c \mid b$

[Megnézem a kapcsolódó epizódot](#)

Azokat a számokat, amelyeknek az egységszorzón és önmagukon kívül nincsen más pozitív egész osztója, prímeknek nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Ha két egymást követő páratlan szám prímszám, akkor azokat ikerprímeknek nevezzük.

A 3-nál nagyobb ikerprímek $6k - 1$ és $6k + 1$ alakúak, ahol $k \in \mathbb{Z}^+$.

[Megnézem a kapcsolódó epizódot](#)

A nullától és az egységszorzóktól különböző összes n egész szám felbontható prímek szorzatára a sorrendtől és az egységszeresektől eltekintve egyértelműen.

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k} \text{ ahol } k \in \mathbb{Z}^+$$

Itt k a felbontásban szereplő különböző prímek száma.

[Megnézem a kapcsolódó epizódot](#)

Egy p szám prím, ha

$$p \mid ab \Rightarrow p \mid a \text{ vagy } p \mid b$$

[Megnézem a kapcsolódó epizódot](#)

Egy q szám felbonthatatlan, ha nem létezik olyan egységtől különböző a és b szám, hogy $q = ab$

[Megnézem a kapcsolódó epizódot](#)

A legkisebb közös többszörös megtalálásának lépései:

1. Elkészítjük a prímtényezős felbontást
2. Vesszük az összes prímet a két prímtényezős felbontásból
3. Mindegyik prím a nagyobbik kitevőt kapja.

[Megnézem a kapcsolódó epizódot](#)

Minden négyzetszám 4-gyel osztva nulla, vagy egy maradékot ad.

Minden négyzetszám 3-mal osztva nulla, vagy egy maradékot ad.

Minden négyzetszám 5-tel osztva nulla, vagy egy vagy négy maradékot ad.

[Megnézem a kapcsolódó epizódot](#)

Minden négyzetszám 4-gyel osztva nulla, vagy egy maradékot ad.

Minden négyzetszám 3-mal osztva nulla, vagy egy maradékot ad.

Minden négyzetszám 5-tel osztva nulla, egy vagy négy maradékot ad.

[Megnézem a kapcsolódó epizódot](#)

$$a - b \mid a^n - b^n$$

$$a + b \mid a^n + b^n \text{ ha } n \text{ páratlan}$$

[Megnézem a kapcsolódó epizódot](#)

Euklideszi algoritmus & Diofantoszi egyenletek

Az euklideszi algoritmus egy formányos módszer két szám legnagyobb közös osztójának kiszámolására.

a és b számokra így néz ki az algoritmus:

$$a = q_1 \cdot b + r_1$$

$$b = q_2 \cdot r_1 + r_2$$

$$r_1 = q_3 \cdot r_2 + r_3$$

$\vdots$

$$r_{n-2} = q_n \cdot r_{n-1} + r_n$$

$$r_{n-1} = q_{n+1} \cdot r_n + 0$$

A legnagyobb közös osztó az utolsó nem 0 maradék (r_n).

Az euklideszi algoritmussal továbbá a két szám legnagyobb közös osztója kifejezhető a két szám segítségével:

$$D = \alpha \cdot a + \beta \cdot b$$

Itt D a legnagyobb közös osztó.

[Megnézem a kapcsolódó epizódot](#)

A Diofantoszi egyenletek így néznek ki:

$$ax + by = c$$

ahol $a, b, c \in \mathbb{Z}$ és $x, y \in \mathbb{Z}$

Megoldásukat azzal kezdjük, hogy kiszámoljuk a és b legnagyobb közös osztóját: D , és ezzel végig osztjuk az egyenletet, így kapjuk az

$$Ax + By = C$$

egyenletet, ahol $(A, B) = 1$.

A második lépés, hogy az euklideszi algoritmus segítségével kifejezzük A és B legnagyobb közös osztóját, ami az 1, így

$$\alpha \cdot A + \beta \cdot B = 1$$

egyenletet kapunk.

Ezt az egyenletet beszorozva C -vel megkapunk egy megoldást:

$$(\alpha \cdot C) \cdot A + (\beta \cdot C) \cdot B = C$$

Az általános megoldásokat a következő alakban kapjuk meg:

$$x = \alpha \cdot C + k \cdot B$$

$$y = \beta \cdot C - k \cdot A$$

[Megnézem a kapcsolódó epizódot](#)

Kongruenciák

Ha a és b ugyanazt a maradékot adja m -mel osztva, akkor azt mondjuk, hogy a és b kongruensek modulo m , és ezt a tényt így jelöljük:

$$a \equiv b \pmod{m}$$

[Megnézem a kapcsolódó epizódot](#)

Reflexív:

$$a \equiv a \pmod{m}$$

Szimmetrikus:

$$a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$$

Tranzitív:

$$a \equiv b \pmod{m} \text{ és } b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$$

Összefüggés összeadásra:

$$a \equiv b \pmod{m} \text{ és } c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}$$

Összefüggés szorzásra:

$$a \equiv b \pmod{m} \text{ és } c \equiv d \pmod{m} \Rightarrow a \cdot c \equiv b \cdot d \pmod{m}$$

[Megnézem a kapcsolódó epizódot](#)

Legyenek a és b egész számok és m pozitív egész szám.

Ekkor

$$a \equiv b \pmod{m}, \text{ ha } m \mid a - b$$

[Megnézem a kapcsolódó epizódot](#)

$$a \equiv b \pmod{m} \Rightarrow a \cdot c \equiv b \cdot c \pmod{m}$$

$$a \cdot c \equiv b \cdot c \pmod{m} \Rightarrow a \equiv b \pmod{m} \quad (m, c) = 1$$

[Megnézem a kapcsolódó epizódot](#)

Egy adott m modulus esetén az a -val kongruens elemek halmazát az a által reprezentált maradékosztálynak nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Egy mod m modulus esetén az m -hez relatív prím elemekből álló maradékosztályokat redukált maradékosztálynak nevezzük.

A redukált maradékosztályok számát a $\varphi(m)$ számelméleti függvény írja le.

[Megnézem a kapcsolódó epizódot](#)

Az euler féle φ függvény azt adja meg, hogy hány m -nél nem nagyobb, m -hez relatív prím pozitív szám létezik.

Ha p prím, akkor

$$\varphi(p) = p - 1$$

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

És ha

$$m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$$

akkor

$$\varphi(m) = (p_1^{\alpha_1} - p_1^{\alpha_1-1}) \cdot \dots \cdot (p_n^{\alpha_n} - p_n^{\alpha_n-1})$$

Továbbá

$$\varphi(ab) = \varphi(a) \cdot \varphi(b)$$

[Megnézem a kapcsolódó epizódot](#)

$$a^{\varphi(m)} \equiv 1 \pmod{m} \text{ ha } (a, m) = 1$$

[Megnézem a kapcsolódó epizódot](#)

$$a^p \equiv a \pmod{p} \text{ ha } p \text{ prím}$$

[Megnézem a kapcsolódó epizódot](#)

A lineáris kongruenciák így néznek ki:

$$ax \equiv b \pmod{m}$$

És érdemes megjegyezni, hogy csak akkor oldhatók meg, ha $(a, m) \mid b$.

[Megnézem a kapcsolódó epizódot](#)

A lineáris kongruenciák így néznek ki:

$$ax \equiv b \pmod{m}$$

Megoldás csak akkor létezik, ha $(a, m) \mid b$.

A megoldás menete a következő:

1. lépés: Redukálunk

$$a_1 x \equiv b_1 \pmod{m}$$

2. lépés: Leosztunk a_1 -gyel, de b_1 -et lélekben fel kell erre készíteni

A megoldások száma: (a, m)

[Megnézem a kapcsolódó epizódot](#)

Az RSA lényege, hogy a titkosítás kulcsa nyilvános, vagyis azt bárki ismerheti. Csak a dekódolás kulcsa az, ami titkos.

Az alapötlete a következő:

Veszünk két jó nagy prímet, p -t és q -t amit csak mi ismerünk, ezek titkosak.

Elkészítjük az $N = p \cdot q$ számot és $\varphi(N)$ -et, amit csak mi ismerünk.

Ha p és q többszázjegyű prímek, akkor N prímfelbontása a jelenlegi számítógépekkel több ezer évig tartana, és így $\varphi(N)$ kiszámolása is lehetetlen.

Végül már csak egy dolog kell, egy e kitevő, amire teljesül, hogy $(e, \varphi(N)) = 1$

Ezt követően jön a titkosítás.

A visszafejtéshez pedig az Euler-Fermat tétel kell, aminek segítségével megalkotjuk ad megfejtő kulcsot.

[Megnézem a kapcsolódó epizódot](#)

Mátrixok

Egy $n \times k$ -as [mátrix](#) tulajdonképpen nem más, mint egy táblázat, aminek n darab sora és k darab oszlopa van.

$$\text{pl.: } A = \begin{pmatrix} 2 & 3 & 1 \\ 5 & 1 & 1 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Ha egy mátrixot egy számmal szorzunk, akkor a [mátrix](#) összes elemét meg kell szorozni a számmal.

$$\text{pl.: } 3 \cdot \begin{pmatrix} 5 & 7 & -2 \\ 2 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 15 & 21 & -6 \\ 6 & 6 & 3 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Ha egy mátrixot osztunk egy számmal, akkor a [mátrix](#) minden elemét osztani kell a számmal.

$$\text{pl.: } \frac{\begin{pmatrix} 6 & 9 & -12 \\ 3 & 3 & 15 \end{pmatrix}}{3} = \begin{pmatrix} 2 & 3 & -4 \\ 1 & 1 & 5 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Két [mátrix](#) összeadásakor összeadjuk az ugyanazon pozícióban lévő elemeket. Két mátrixot csak akkor lehet összeadni, ha ugyanannyi soruk és oszlopuk van.

$$\text{pl.: } \begin{pmatrix} 2 & 4 & 7 \\ 1 & 5 & 3 \end{pmatrix} + \begin{pmatrix} 1 & 7 & -2 \\ 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 11 & 5 \\ 5 & 7 & 4 \end{pmatrix}$$

A [mátrixok](#) összeadása kommutatív, azaz

$$A + B = B + A$$

És asszociatív, azaz

$$(A + B) + C = A + (B + C)$$

[Megnézem a kapcsolódó epizódot](#)

Két [mátrix](#) kivonásakor kivonjuk az ugyanazon pozícióban lévő elemeket. Két mátrixot csak akkor lehet kivonni egymásból, ha ugyanannyi soruk és oszlopuk van.

$$\text{pl.: } \begin{pmatrix} 2 & 4 & 7 \\ 1 & 5 & 3 \end{pmatrix} - \begin{pmatrix} 1 & 7 & -2 \\ 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -3 & 9 \\ -3 & 3 & 2 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Két [mátrix](#) szorzata akkor létezik, ha a bal oldali [mátrix](#) oszlopainak száma megegyezik a jobb oldali [mátrix](#) sorainak számával.

Ha az A [mátrix](#) $m \times n$ -es a B [mátrix](#) pedig $n \times k$ -s, akkor az eredmény [mátrix](#) $m \times k$ -s lesz.

Az eredmény [mátrix](#) i -edik sorának j -edik elemét úgy kapjuk, hogy a bal oldali [mátrix](#) i -edik sorát skalárisan szorozzuk a jobb oldali [mátrix](#) j -edik oszlopával. (Tehát az első elemet az elsővel, a másodikat a másodikkal stb. szorozzuk, majd összeadjuk)

$$\text{pl.: } \begin{pmatrix} 3 & 4 \\ 1 & 5 \end{pmatrix} \cdot \begin{pmatrix} 2 & 4 & 7 \\ 1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 10 & 32 & 33 \\ 7 & 29 & 22 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Két mátrixot csak akkor adhatunk össze, ha ugyanannyi soruk és oszlopuk van.

A [mátrix](#) összeadás kommutatív:

$$A + B = B + A$$

És asszociatív:

$$(A + B) + C = A + (B + C)$$

[Megnézem a kapcsolódó epizódot](#)

A mátrixszorzás nem kommutatív, azaz:

$$A \cdot B \neq B \cdot A$$

De asszociatív, azaz:

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

[Megnézem a kapcsolódó epizódot](#)

A kvadratikus [mátrix](#) négyzetes [mátrix](#) vagyis ugyanannyi sora van, mint oszlopa.

$$\text{pl.: } \begin{pmatrix} 2 & 3 & 5 \\ 1 & 4 & 1 \\ 2 & 1 & 1 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

A diagonális [mátrix](#) olyan kvadratikus [mátrix](#), aminek a főátlóján kívüli elemek nullák.

$$\text{pl.: } \begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Az egység mátrix olyan mátrix, ami azt tudja, hogy bármely A mátrixra $A \cdot I = A$.

Az egység mátrixok olyan diagonális mátrixok, aminek minden főátló-eleme egy.

$$\text{pl.: } I_{2 \times 2} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Az inverz mátrix jele A^{-1} és ez egy olyan mátrix, ami azt tudja, hogy

$$A \cdot A^{-1} = I \text{ (jobb inverz)}$$

$$A^{-1} \cdot A = I \text{ (bal inverz)}$$

[Megnézem a kapcsolódó epizódot](#)

A transzponált a mátrix sorainak és oszlopainak felcserélése. Jele A^T vagy A^*

pl.:

$$A = \begin{pmatrix} 2 & 3 & 5 \\ 1 & 4 & 1 \\ 2 & 5 & 7 \end{pmatrix} \Rightarrow A^T = \begin{pmatrix} 2 & 1 & 2 \\ 3 & 4 & 5 \\ 5 & 1 & 7 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Azokat a mátrixokat, melyek transzponáltjuk önmaga, szimmetrikus mátrixnak nevezzük.

$$\text{pl.: } A = \begin{pmatrix} 5 & 1 & 7 \\ 1 & 4 & 2 \\ 7 & 2 & 6 \end{pmatrix} \Rightarrow A^T = \begin{pmatrix} 5 & 1 & 7 \\ 1 & 4 & 2 \\ 7 & 2 & 6 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Vektort egy számmal úgy szorzunk, hogy a vektor minden koordinátáját megszorozzuk a számmal.

$$\text{Pl.: } 3 \cdot \begin{pmatrix} 1 \\ 3 \\ 5 \end{pmatrix} = \begin{pmatrix} 3 \\ 9 \\ 15 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Vektort egy számmal úgy osztunk, hogy a vektor minden koordinátáját leosztjuk a számmal.

$$\text{Pl.: } \frac{\begin{pmatrix} 3 \\ 6 \\ 15 \end{pmatrix}}{3} = \begin{pmatrix} 1 \\ 2 \\ 5 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Két vektort úgy adunk össze, hogy minden egyes koordinátájukat külön-külön össze adjuk.

$$\text{Pl.: } \begin{pmatrix} 2 \\ 4 \\ -1 \end{pmatrix} + \begin{pmatrix} 4 \\ 2 \\ 7 \end{pmatrix} = \begin{pmatrix} 6 \\ 6 \\ 6 \end{pmatrix}$$

Tulajdonságok:

$$\text{kommutatív: } \underline{a} + \underline{b} = \underline{b} + \underline{a}$$

$$\text{asszociatív: } (\underline{a} + \underline{b}) + \underline{c} = \underline{a} + (\underline{b} + \underline{c})$$

[Megnézem a kapcsolódó epizódot](#)

Két vektort úgy vonunk ki egymásból, hogy minden egyes koordinátájukat külön-külön kivonjuk egymásból.

$$\text{Pl.: } \begin{pmatrix} 2 \\ 4 \\ -1 \end{pmatrix} - \begin{pmatrix} 4 \\ 2 \\ 7 \end{pmatrix} = \begin{pmatrix} -2 \\ 2 \\ -8 \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

A [skaláris szorzat](#) két vektor közti művelet, ami csinál belőlük egy számot.

$$\text{Pl.: } \underline{a} = \begin{pmatrix} 3 \\ 2 \\ 5 \end{pmatrix} \quad \underline{b} = \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}$$

$$\underline{a}^T \cdot \underline{b} = 3 \cdot 4 + 2 \cdot 1 + 5 \cdot 2 = 24$$

Tulajdonságok:

$$\text{kommutatív: } \underline{a}^T \cdot \underline{b} = \underline{b}^T \cdot \underline{a}$$

$$\text{nem asszociatív: } (\underline{a}^T \cdot \underline{b})^T \cdot \underline{c} \neq \underline{a}^T \cdot (\underline{b}^T \cdot \underline{c})$$

[Megnézem a kapcsolódó epizódot](#)

Két vektor diadikus szorzata egy [mátrix](#). Lássuk milyen.

$$\text{Pl.: } \underline{a} = \begin{pmatrix} 3 \\ 2 \\ 5 \end{pmatrix} \quad \underline{b} = \begin{pmatrix} 4 \\ 1 \\ 2 \end{pmatrix}$$

$$\underline{a} \cdot \underline{b}^T = \begin{pmatrix} 12 & 3 & 6 \\ 8 & 2 & 4 \\ 20 & 5 & 10 \end{pmatrix}$$

Tulajdonságok:

nem kommutatív

nem asszociatív

[Megnézem a kapcsolódó epizódot](#)

Ha egy mátrixot beszorzunk az $\underline{I} = \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}$ vektorral, akkor az szépen összeadja a mátrixunk soraiban lévő

elemeket.

[Megnézem a kapcsolódó epizódot](#)

Ha egy mátrixot beszorzunk az $\underline{I}^T = (1 \quad 1 \quad \dots \quad 1)$ vektorral, akkor az szépen összeadja a mátrixunk oszlopaiban lévő elemeket.

[Megnézem a kapcsolódó epizódot](#)

Ha egy mátrixot megszorozunk jobbról egy $\underline{e}_i$ egységvektorral, akkor megkapjuk a [mátrix](#) i-edik oszlopát.

[Megnézem a kapcsolódó epizódot](#)

Ha egy mátrixot megszorozunk balról egy $\underline{e}_i$ egységvektorral, akkor megkapjuk a [mátrix](#) i-edik sorát.

[Megnézem a kapcsolódó epizódot](#)

Lineáris egyenletrendszerek

Egy egyenletrendszer együtthatómátrixa az x -ek együtthatóiból álló [mátrix](#).

[Megnézem a kapcsolódó epizódot](#)

A Gauss-elimináció egy lineáris egyenletrendszerek megoldására használt algoritmus.

Az elimináció lényege, hogy egyenletrendszerünket visszavezetjük vagy valamely háromszög- vagy átlós [mátrix](#) alakra.

A Gauss-elimináció megengedett lépései:

- Két sort (egyenletet) felcserélhetünk
- Egy sort (egyenletet) nem nulla számmal szorozhatunk
- Egyik sorhoz (egyenlethez) hozzáadhatjuk egy másik sor (egyenlet) nem nulla számszorosát

[Megnézem a kapcsolódó epizódot](#)

Az elemi bázistranszformáció (Szuper-Gauss) a lineáris egyenletrendszerek megoldásának egy algoritmikus módja.

1. lépés: a generáló elem választása

Csak x -es oszlopból és e -s sorból választhatunk generáló elemet, nullát nem választhatunk és lehetőleg 1-et vagy mínusz 1-et érdemes.

2. lépés: a bázistranszformáció

A generáló elem sorát osztjuk a generáló elemmel, oszlopát elhagyjuk.

A többi elemből kivonjuk a generáló elem neki megfelelő sorában és oszlopában lévő számok szorzatát, osztva a generálóelemmel.

3. lépés: megint generáló elem választás

Újra és újra végrehatjuk a bázistranszformációt, amíg az összes oszlop el nem tűnik

4. lépés: az utolsó transzformáció és a megoldás

[Megnézem a kapcsolódó epizódot](#)

Az elemi bázistranszformáció (Szuper-Gauss) a lineáris egyenletrendszerek megoldásának egy algoritmikus módja.

1. lépés: a generáló elem választása

Csak x -es oszlopból és e -s sorból választhatunk generáló elemet, nullát nem választhatunk és lehetőleg 1-et vagy mínusz 1-et érdemes.

2. lépés: a bázistranszformáció

A generáló elem sorát osztjuk a generáló elemmel, oszlopát elhagyjuk.

A többi elemből kivonjuk a generáló elem neki megfelelő sorában és oszlopában lévő számok szorzatát, osztva a generálóelemmel.

3. lépés: megint generáló elem választás

Újra és újra végrehatjuk a bázistranszformációt, amíg az összes oszlop el nem tűnik

4. lépés: az utolsó transzformáció és a megoldás

[Megnézem a kapcsolódó epizódot](#)

Négyzetes [mátrixok](#) inverzét a Gauss-elimináció segítségével úgy állíthatjuk elő, hogy megoldjuk az $Ax = b$ egyenletrendszert úgy, hogy a b helyére beírjuk az egységmátrixot. Az eliminációs lépéseket addig kell végezni, amíg az egységmátrixot nem kapjuk az A helyén, a b helyén keletkezett [mátrix](#) pedig az A [mátrix](#) inverze lesz.

[Megnézem a kapcsolódó epizódot](#)

Négyzetes [mátrixok](#) inverzét a bázistranszformáció segítségével úgy állíthatjuk elő, hogy megoldjuk az $Ax = b$ egyenletrendszert úgy, hogy a b helyére beírjuk az egységmátrixot.

[Megnézem a kapcsolódó epizódot](#)

Négyzetes [mátrixok](#) inverzét a Gauss-Jordan elimináció segítségével úgy állíthatjuk elő, hogy megoldjuk az $Ax = b$ egyenletrendszert úgy, hogy a b helyére beírjuk az egységmátrixot.

[Megnézem a kapcsolódó epizódot](#)

Az inverz kiszámolása rettentő egyszerű dolog. Mindössze annyit kell tennünk, hogy felírjuk a mátrixot a szokásos táblázatba, és mellé írjuk az egységmátrixot. Ezek után jön a bázistranszformáció. Ha nem tudjuk mindegyik x -et levinni, akkor nincs inverz. Ha mindet le tudjuk vinni, akkor van.

[Megnézem a kapcsolódó epizódot](#)

Determináns, adjungált, kvadratikus alakok

Ha az A egy $n \times n$ -es [mátrix](#), akkor determinánsa

$$\det(A) = \sum_{\forall p} (-1)^{I(p)} \cdot \prod_{i=1}^n a_{ip(i)}$$

ahol p az oszlopindexek permutációi, $I(p)$ pedig ezen permutációk inverziószáma.

[Megnézem a kapcsolódó epizódot](#)

Egy 2×2 -es [mátrix](#) determinánsa:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \det(A) = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = a \cdot d - b \cdot c$$

[Megnézem a kapcsolódó epizódot](#)

A 3×3 -as [mátrixok](#) determinánsának kiszámolására van egy szabály, ami szarrusz szabály néven ismert. A szabály lényege, hogy fogjuk a mátrixot és leírjuk saját maga mögé még egyszer, majd vesszük a főátlókat és a mellékátlókat, így

$$\det(A) = -a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32}$$

[Megnézem a kapcsolódó epizódot](#)

Ha az A egy $n \times n$ -es [mátrix](#), akkor determinánsa

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

$$\det(A) = \sum_{j=1}^n (-1)^{i+j} a_{ij} \cdot \det(A_{ij})$$

Itt $\det(A_{ij})$ az a_{ij} elemhez tartozó aldetermináns.

[Megnézem a kapcsolódó epizódot](#)

Az A [mátrix](#) determinánsa nulla, ha

- van csupa nulla sora
- van két azonos sora
- egyik sora a másik sor számszorosa
- egyik sora más sorok lineáris kombinációja
- mindez sor helyett oszlopra is elmondható

Determinánsok szorzási tétele:

$$\det(A \cdot B) = \det(A) \cdot \det(B)$$

$$\det(A^k) = \det(A)^k$$

[Megnézem a kapcsolódó epizódot](#)

Azokat a mátrixokat nevezzük szingulárisnak, amelyek determinánsa nulla.

Az A [mátrix](#) szinguláris:

- $\det(A) = 0$
- Nem létezik A^{-1} inverz [mátrix](#)
- $\text{RANG} < n$
- Az A [mátrix](#) oszlopvektoraiból álló vektorrendszer lineárisan összefüggő
- Az $A \cdot \underline{x} = \underline{b}$ egyenletrendszernek vagy végtelen sok megoldása van vagy nincs megoldása
- Az $A \cdot \underline{x} = \underline{0}$ homogén lineáris egyenletrendszernek végtelen sok megoldása van

[Megnézem a kapcsolódó epizódot](#)

Azokat a mátrixokat nevezzük regulárisnak, amelyek determinánsa nem nulla.

Az A [mátrix](#) reguláris:

- $\det(A) \neq 0$
- Létezik A^{-1} inverz [mátrix](#)
- $\text{RANG} = n$
- Az A [mátrix](#) oszlopvektoraiból álló vektorrendszer lineárisan független
- Az $A \cdot \underline{x} = \underline{b}$ egyenletrendszernek csak egy megoldása van
- Az $A \cdot \underline{x} = \underline{0}$ homogén lineáris egyenletrendszernek csak egy megoldása van (a triviális megoldás)

[Megnézem a kapcsolódó epizódot](#)

A Cramer szabály szerint az $A \cdot \underline{x} = \underline{b}$ egyenletrendszer megoldásai a következőképp állnak elő:

$$x_k = \frac{\det(A_k)}{\det(A)}$$

ahol $\det(A_k)$ annak a mátrixnak a determinánsát jelenti, hogy az A [mátrix](#) k -edik oszlopát kicseréljük a $\underline{b}$ vektorral.

[Megnézem a kapcsolódó epizódot](#)

Itt egy 3x3-as [mátrix](#).

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Adjungáltja pedig ez lesz.

$$\text{adj}(A) = \begin{pmatrix} +\det \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} & -\det \begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} & +\det \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix} \\ -\det \begin{pmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{pmatrix} & +\det \begin{pmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{pmatrix} & -\det \begin{pmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{pmatrix} \\ +\det \begin{pmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{pmatrix} & -\det \begin{pmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{pmatrix} & +\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \end{pmatrix}^T$$

[Megnézem a kapcsolódó epizódot](#)

Itt egy 2x2-es [mátrix](#).

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Adjungáltja pedig ez lesz.

$$\text{adj}(A) = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

[Megnézem a kapcsolódó epizódot](#)

Az adjungált egyik legnagyobb haszna, hogy segítségével meg tudunk alkotni egy képletet a négyzetes [mátrixok](#) inverzére.

Itt is van:

$$A^{-1} = \frac{\text{adj}(A)}{\det(A)}$$

[Megnézem a kapcsolódó epizódot](#)

Az egyenletrendszerek megoldására is megalkothatunk egy új képletet az adjungált segítségével.

$$A \cdot \underline{x} = \underline{b}$$

Legalábbis abban az esetben, hogyha az A nxn-es invertálható [mátrix](#).

Az egyenletrendszer megoldását úgy kapjuk meg, hogy beszorzunk az A [mátrix](#) inverzével...

$$\underline{x} = \frac{1}{\det(A)} \cdot \text{adj}(A) \cdot \underline{b}$$

[Megnézem a kapcsolódó epizódot](#)

Az $x_1, x_2, \dots, x_n$ elemek által generált Vandermonde-determináns első sorában x_1 hatványai szerepelnek, aztán a második sorában x_2 hatványai jönnek, és így tovább.

A Vandermonde-determinánst ezzel az egyszerű képlettel ki tudjuk számolni:

$$V(x_1, x_2, \dots, x_n) = \det \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \dots & x_3^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix} = \prod_{j < i} (x_i - x_j)$$

[Megnézem a kapcsolódó epizódot](#)

Egy [mátrix](#) sarok főminor mátrixai a [mátrix](#) bal felső sarkától kezdődő sarok [mátrixok](#) determinánsai.

$$\text{Pl.: } A = \begin{pmatrix} 2 & 3 & 5 & 1 \\ 4 & 7 & 2 & 1 \\ 2 & 1 & 14 & \\ 3 & 5 & 1 & 7 \end{pmatrix}$$

első sarokfőminora a 2-es

második sarokfőminora a bal felső 2x2-es determináns

$$\det \begin{pmatrix} 2 & 3 \\ 4 & 7 \end{pmatrix} = 2 \cdot 7 - 3 \cdot 4 = 2$$

és így tovább

[Megnézem a kapcsolódó epizódot](#)

Egy [mátrix](#) főminor mátrixai a [mátrix](#) bal felső sarkától kezdődő sarok [mátrixok](#) determinánsai.

$$\text{Pl.: } A = \begin{pmatrix} 2 & 3 & 5 & 1 \\ 4 & 7 & 2 & 1 \\ 2 & 1 & 14 & \\ 3 & 5 & 1 & 7 \end{pmatrix}$$

első főminora a 2-es

második főminora a bal felső 2x2-es determináns

$$\det \begin{pmatrix} 2 & 3 \\ 4 & 7 \end{pmatrix} = 2 \cdot 7 - 3 \cdot 4 = 2$$

és így tovább

[Megnézem a kapcsolódó epizódot](#)

Az A $n \times n$ -es [mátrix](#) pozitív definit, ha minden λ sajátérték: $\lambda > 0$.

Vagy ha minden sarokfőminor pozitív.

[Megnézem a kapcsolódó epizódot](#)

Az A $n \times n$ -es [mátrix](#) negatív definit, ha minden λ sajátérték: $\lambda < 0$.

Vagy ha a sarokfőminorok váltakozva $- + - +$ de mínusszal indul.

[Megnézem a kapcsolódó epizódot](#)

Az A $n \times n$ -es [mátrix](#) pozitív szemidefinit, ha minden λ sajátérték: $\lambda \geq 0$.

2x2-es mátrixoknál, ha az első sarokfőminor pozitív, a második nulla.

[Megnézem a kapcsolódó epizódot](#)

Az A $n \times n$ -es [mátrix](#) negatív szemidefinit, ha minden λ sajátérték: $\lambda \leq 0$.

2x2-es mátrixoknál, ha az első sarokfőminor negatív, a második nulla.

[Megnézem a kapcsolódó epizódot](#)

Az A $n \times n$ -es [mátrix](#) indefinit, ha van λ_1 és λ_2 sajátérték, hogy $\lambda_1 > 0$ és $\lambda_2 < 0$.

Ha $\det(A) \neq 0$ és nem pozitív vagy negatív definit, akkor indefinit.

[Megnézem a kapcsolódó epizódot](#)

Ha A $n \times n$ -es szimmetrikus [mátrix](#) és $\underline{x}$ egy vektor R^n -ben, akkor a

$$Q(\underline{x}) = \underline{x}^* \cdot A \cdot \underline{x}$$

kifejezést kvadratikus alaknak nevezzük.

Azért hívjuk kvadratikusnak vagyis négyzetesnek, mert ez mindig egy homogén másodfokú kifejezés.

[Megnézem a kapcsolódó epizódot](#)

A $Q(\underline{x}) = \underline{x}^* \cdot A \cdot \underline{x}$ kvadratikus alak

pozitív definit, ha minden $\underline{x} \neq \underline{0}$ vektorra $Q(\underline{x}) > 0$

negatív definit, ha minden $\underline{x} \neq \underline{0}$ vektorra $Q(\underline{x}) < 0$

pozitív szemidefinit, ha minden $\underline{x} \neq \underline{0}$ vektorra $Q(\underline{x}) \geq 0$

negatív szemidefinit, ha minden $\underline{x} \neq \underline{0}$ vektorra $Q(\underline{x}) \leq 0$

indefinit, ha van olyan $\underline{x} \neq \underline{0}$ és $\underline{y} \neq \underline{0}$, hogy $Q(\underline{x}) < 0$ és $Q(\underline{y}) > 0$

[Megnézem a kapcsolódó epizódot](#)

Komplex számok

Van itt két komplex szám: $z_1 = a + bi$, $z_2 = c + di$

A két komplex szám összege:

$$z_1 + z_2 = (a + c) + (b + d)i$$

A két komplex szám különbsége:

$$z_1 - z_2 = (a - c) + (b - d)i$$

[Megnézem a kapcsolódó epizódot](#)

Van itt két komplex szám: $z_1 = a + bi$, $z_2 = c + di$

A két komplex szám szorzata:

$$z_1 \cdot z_2 = (a + bi) \cdot (c + di) = a \cdot c - b \cdot d + (a \cdot d + b \cdot c)i$$

[Megnézem a kapcsolódó epizódot](#)

A [komplex számok](#) egy valós és egy imaginárius (képzetes) számból épülnek föl. A valós számok a szokásos x tengelyen helyezkednek el, míg az imaginárius számok egy erre merőleges y tengelyen, amit imaginárius tengelynek, vagy képzetes tengelynek nevezünk. Az imaginárius tengely egysége az i , ami olyan, mint a valós tengelyen az 1, csak éppen egy meglehetősen furcsa dolgot tud. Az imaginárius egység egy olyan komplex szám, aminek a négyzete -1 és i -vel jelöljük, azaz

$$i^2 = -1$$

[Megnézem a kapcsolódó epizódot](#)

A komplex számokat azért hívjuk "komplex"-nek, mert két részből tevődnek össze. Egy valós és egy imaginárius (képzetes) számból épülnek föl. A valós számok a szokásos x tengelyen helyezkednek el, míg az imaginárius számok egy erre merőleges y tengelyen, amit imaginárius tengelynek, vagy képzetes tengelynek nevezünk. A [komplex számok](#) egy valós számból és egy imaginárius számból tevődnek össze:

$$z = a + bi$$

Itt a és b valós számok, az i pedig az imaginárius egység, ami azt tudja, hogy $i^2 = -1$.

Magukat a valós számokat és az imaginárius számokat is komplex számnak tekinthetjük. A valós számok olyan [komplex számok](#), amelyeknek az imaginárius része nulla, míg az imaginárius számok olyan [komplex számok](#), amelyeknek a valós része nulla. A [komplex számok](#) egy síkon, az úgynevezett komplex számsíkon helyezkednek el. Kicsit olyanok, mint a koordináta geometriában a kétdimenziós sík vektorai, ahol az i és j bázisvektorkat szokás használni, az x tengelynél az i és az y tengelynél a j vektorral. Ennek az analógiának köszönhetően vannak, akik az imaginárius számokat nem is i -vel, hanem j -vel jelölik. Bár ez segíthet erősíteni az analógiát a sík vektoraival, de mégis zavaró, mivel aki komolyabban is foglalkozik a komplex számokkal, a hivatalos jelöléssel fog találkozni, ahol az imaginárius tengelyen i -k vannak.

[Megnézem a kapcsolódó epizódot](#)

A valós számokat úgy érdemes elképzelni, mint egy koordináta-rendszer x tengelyét. És minden helyet ki is töltenek a valós számok ezen a számegyenesen. A [komplex számok](#) egy valós és egy imaginárius (képzetes) részből épülnek föl, és szemléltetésükhöz nem egy, hanem két koordinátatengelyre van szükség. Az x tengelyen vannak a valós számok, az y tengelyen pedig az imaginárius, vagyis a képzetes számok. A valós számok tengelyén az egység a szokásos 1, míg az imaginárius számok tengelyén az egység az i . A két tengely által kifeszített síkot nevezzük komplex számsíknak, vagy másként Gauss-féle számsíknak.

[Megnézem a kapcsolódó epizódot](#)

Van itt ez a komplex szám:

$$z = a + bi$$

Komplex számoknak van ilyenje, hogy imaginárius egység:

$$i^2 = -1$$

[Komplex számok](#) konjugáltja:

$$\bar{z} = a - bi$$

[Megnézem a kapcsolódó epizódot](#)

Van itt ez a komplex szám: $z = a + bi$

Ennek a komplex számnak az abszolútértéke:

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

[Megnézem a kapcsolódó epizódot](#)

A $z = a + bi$ komplex szám trigonometrikus alakja:

$$z = r(\cos \theta + i \sin \theta), \text{ ahol}$$

$$r = \sqrt{a^2 + b^2} \quad \cos \theta = \frac{a}{r}$$

[Megnézem a kapcsolódó epizódot](#)

Van itt két komplex szám trigonometrikus alakban: $z_1 = r_1(\cos \theta_1 + i \sin \theta_1)$, $z_2 = r_2(\cos \theta_2 + i \sin \theta_2)$

[Komplex számok szorzása](#) trigonometrikus alakban:

$$z_1 z_2 = r_1 r_2 (\cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2))$$

[Komplex számok osztása](#) trigonometrikus alakban:

$$\frac{z_1}{z_2} = \frac{r_1}{r_2} (\cos(\theta_1 - \theta_2) + i \sin(\theta_1 - \theta_2))$$

[Megnézem a kapcsolódó epizódot](#)

Van itt ez a komplex szám trigonometrikus alakban: $r(\cos \theta + i \sin \theta)$

Ekkor ennek a komplex számnak az n -edik hatványa:

$$z^n = r^n (\cos n\theta + i \sin n\theta)$$

[Megnézem a kapcsolódó epizódot](#)

Van itt ez a komplex szám trigonometrikus alakban: $z = r(\cos \theta + i \sin \theta)$

Ekkor ennek a komplex számnak az n -edik gyöke:

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

[Megnézem a kapcsolódó epizódot](#)

Van itt két komplex szám exponenciális alakban: $z_1 = r_1 e^{i\theta_1}$, $z_2 = r_2 e^{i\theta_2}$

[Komplex számok szorzása](#) exponenciális alakban:

$$z_1 z_2 = r_1 r_2 e^{i(\theta_1 + \theta_2)}$$

[Komplex számok osztása](#) exponenciális alakban:

$$\frac{z_1}{z_2} = \frac{r_1}{r_2} e^{i(\theta_1 - \theta_2)}$$

[Megnézem a kapcsolódó epizódot](#)

Van itt ez a komplex szám exponenciális alakban: $z = r e^{i\theta}$

Ekkor ennek a komplex számnak az n -edik hatványa:

$$z^n = r^n e^{ni\theta}$$

[Megnézem a kapcsolódó epizódot](#)

Van itt ez a komplex szám exponenciális alakban: $z = r e^{i\theta}$

Ekkor ennek a komplex számnak az n -edik gyöke:

$$\sqrt[n]{z} = \sqrt[n]{r} e^{i \frac{\theta + 2k\pi}{n}}$$

[Megnézem a kapcsolódó epizódot](#)

Interpolációs polinomok

Az interpoláció egy közelítő módszer, amely a függvény ismert értékei alapján ad közelítést a nem ismert értékeire.

[Megnézem a kapcsolódó epizódot](#)

A Lagrange-féle interpolációs polinom megadja azt a polinomot, amely x_1 -ben y_1 -et, x_2 -ben y_2 -t és így tovább x_n -ben y_n értéket vesz föl. Általánosan így tudjuk leírni:

$$P(x) = \sum_{j=1}^n \prod_{k \neq j} \frac{x - x_k}{x_j - x_k} \cdot y_j$$

[Megnézem a kapcsolódó epizódot](#)

A Newton interpoláció első lépése, hogy elkészítjük a Newton-együtthatókat:

$$N_1 = \frac{y_2 - y_1}{x_2 - x_1} \quad N_2 = \frac{y_3 - y_2}{x_3 - x_2} \quad N_3 = \frac{y_4 - y_3}{x_4 - x_3}$$

$$N_4 = \frac{N_2 - N_1}{x_3 - x_1} \quad N_5 = \frac{N_3 - N_2}{x_4 - x_2}$$

$$N_6 = \frac{N_5 - N_4}{x_4 - x_1}$$

A polinomot pedig így kapjuk meg:

$$P(x) = y_1 + N_1(x - x_1) + N_4(x - x_1)(x - x_2) + N_6(x - x_1)(x - x_2)(x - x_3)$$

[Megnézem a kapcsolódó epizódot](#)

A Hermite interpoláció abban különbözik a Lagrange és Newton féle interpolációtól, hogy az $x_1, x_2, \dots, x_n$ helyeken nem csak az eredeti polinom-függvény értékeit, hanem a deriváltjait is nézzük.

A keresett polinomfüggvény mindig egyel kisebbfokú lesz, mint az interpolációs pontok száma k és a következő alakban keressük:

$$f(x) = a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \dots + a_1x + a_0$$

A polinom együtthatóit úgy kapjuk meg, hogy az ismert adatokat behelyettesítjük és egy egyenletrendszert alkotunk belőle, amit pl. Gauss eliminációval megoldhatunk.

[Megnézem a kapcsolódó epizódot](#)

Ha az f függvény $n + 1$ -szer deriválható az $x_1, x_2, \dots, x_n$ és x által kifeszített I intervallumon, akkor az interpoláció hibája:

$$E_n(x) = \frac{f^{(n+1)}(\xi_x)}{(n+1)!} \cdot \prod_{i=1}^n (x - x_i) \quad \xi_x \in I$$

[Megnézem a kapcsolódó epizódot](#)

Csoportok, gyűrűk, testek

Azokat a nem üres halmazokat, amelyekben értelmezve van egy művelet, és ez a művelet asszociatív, létezik benne egységelem, és minden elemnek létezik benne inverze, csoportnak nevezzük.

[Megnézem a kapcsolódó epizódot](#)

A kommutatív csoportokat Abel-csoportnak nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Azt az elemet, amely a művelet elvégzése során mindenkit változatlanul hagy, egységelemnek nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Egy elem akkor lesz inverz, ha azt tudja, hogy a művelet elvégzése során az eredeti elemből egységelemet csinál.

Például ha vesszük az 5-öt és a szorzás műveletet, akkor az 5-nek a szorzás műveletre vett inverze az $\frac{1}{5}$, mert $5 \cdot \frac{1}{5} = 1$, vagy ha vesszük a 2-öt és az összeadás műveletet, akkor a 2-nek az összeadás műveletre vett inverze a -2 , mert $2 + (-2) = 0$.

[Megnézem a kapcsolódó epizódot](#)

Ha egy csoportban az elemeknek nincs inverze, és nincs egységelem sem, akkor félcsoportnak nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Egy csoportot ciklikus csoportnak nevezünk, ha előáll egyetlen elemének egész kitevős hatványaiból.

[Megnézem a kapcsolódó epizódot](#)

Egy elem rendje azt a legkisebb pozitív egész kitevőt jelenti, amelyre emelve az egységelemeket kapjuk.

A rend jele: σ (ordó)

[Megnézem a kapcsolódó epizódot](#)

Egy nem üres halmazt gyűrűnek nevezünk, ha értelmezve van benne egy összeadás és egy szorzás művelet.

Az összeadásnak azt kell tudnia, hogy asszociatív és kommutatív.

$$(a + b) + c = a + (b + c)$$

$$a + b = b + a$$

Van egységelem. Az összeadás egységelemét nullelemnek hívjuk.

Minden elemnek van inverze, amit ellentettnek hívunk.

A szorzásnak pedig mindössze annyit kell tudnia, hogy asszociatív.

$$(ab)c = a(bc)$$

A két művelet pedig egymásra nézve disztributív:

$$a(b + c) = ab + ac$$

$$(a + b)c = ac + bc$$

Példák gyűrűre: egész számok, $(n \times n)$ -es [mátrixok](#), mod m maradékosztályok

[Megnézem a kapcsolódó epizódot](#)

A kommutatív nullosztómentes gyűrűket nevezzük integritási tartománynak.

[Megnézem a kapcsolódó epizódot](#)

Az R gyűrűben az I részhalmazt ideálnak nevezzük, ha I részgyűrű R -ben és minden $r \in R$ és $i \in I$ elemre $r \cdot i \in I$

És mivel a szorzás nem feltétlenül kommutatív, léteznek bal és jobb ideálok.

Bal ideál:

Az R gyűrűben az I részhalmaz bal ideál, ha I részgyűrű R -ben és $\forall r \in R$ és $i \in I$ elemre $r \cdot i \in I$

Jobb ideál:

Az R gyűrűben az I részhalmaz jobb ideál, ha I részgyűrű R -ben és $\forall r \in R$ és $i \in I$ elemre $i \cdot r \in I$

[Megnézem a kapcsolódó epizódot](#)

Az egy elem által generált ideált főideálnak nevezzük.

[Megnézem a kapcsolódó epizódot](#)

Azokat a gyűrűket, amelyben minden ideál főideál, úgy hívjuk, hogy főideálgyűrű.

Használatos rájuk a PIR rövidítés is (Principal Ideal Ring).

[Megnézem a kapcsolódó epizódot](#)

Azokat a komplex számokat, ahol a és b egész szám Gauss egészeknek nevezzük.

$$z = a + b \cdot i$$

[Megnézem a kapcsolódó epizódot](#)

A [komplex számok](#) abszolútértékének mintájára bevezetünk egy fogalmat, amit normának hívunk:

$$N(z) = |z|^2 = a^2 + b^2$$

Ha z_1 és z_2 Gauss egészek, akkor

$$z_1 \mid z_2 \Rightarrow N(z_1) \mid N(z_2)$$

Az állítás megfordítása nem igaz:

$$N(z_1) \mid N(z_2) \nRightarrow z_1 \mid z_2$$

[Megnézem a kapcsolódó epizódot](#)

A Gauss egészek gyűrűt alkotnak az összeadás és szorzás műveletekkel.

A Gauss egészek tudják az oszthatóságot is, egy Gauss egész akkor oszt egy másikat, ha az osztás eredménye is Gauss egész.

A Gauss egészek körében négy darab egység van: $1, -1, i, -i$

[Megnézem a kapcsolódó epizódot](#)

A Gauss egészek gyűrűjében prímek azok a p_1 és p_2 Gauss egészek, amelyek szorzata $4k + 1$ alakú prím:

$$p_1 \cdot p_2 = p$$

[Megnézem a kapcsolódó epizódot](#)

Az n szám akkor és csak akkor áll elő két négyzetszám összegeként

$$n = x^2 + y^2$$

ha kanonikus alakjában

$$n = 2^\gamma \cdot p_1^{\alpha_1} p_2^{\alpha_2} \dots q_1^{\beta_1} q_2^{\beta_2} \dots \quad p_i = 4k - 1 \quad q_i = 4k + 1$$

minden $4k - 1$ alakú prím kitevője páros.

[Megnézem a kapcsolódó epizódot](#)

Azokat a gyűrűket, amikben működik az Euklideszi algoritmus úgy hívjuk, hogy Euklideszi gyűrű.

Minden Euklideszi gyűrű egyben főideálgyűrű.

Euklideszi gyűrű például az egész számok gyűrűje, vagy éppen a Gauss egészek gyűrűje.

[Megnézem a kapcsolódó epizódot](#)

Azokat a gyűrűket, melyeknek van additív inverze, és a 0-tól eltekintve minden elemének van multiplikatív inverze is, testnek nevezzük.

[Megnézem a kapcsolódó epizódot](#)

9 test-axióma van, ezek:

1. Az összeadás asszociatív
2. Az összeadás kommutatív
3. Létezik nullelem az összeadás műveletben
4. Minden elemnek van additív inverze
5. A szorzás asszociatív
6. A szorzás kommutatív
7. Létezik egységelem a szorzás műveletben
8. Minden elemnek van multiplikatív inverze, kivéve a nullelemet
9. Az összeadás és szorzás művelet disztributív

[Megnézem a kapcsolódó epizódot](#)

A rendezés reláció négy fontos tulajdonságát rendezési axiómának nevezzük.

1. Trichotómia: Bármely a és b valós számra, az $a < b$, az $a = b$ és az $a > b$ állítások közül pontosan egy igaz.
2. Transzitivitás: Bármely a, b és c valós számra, ha $a < b$ és $b < c$ akkor $a < c$.
3. Bármely a, b és c valós számra ha $a < b$ akkor $a + c < b + c$.
4. Bármely a, b és $c > 0$ valós számra, ha $a < b$ akkor $ac < bc$.

[Megnézem a kapcsolódó epizódot](#)

Minden számnál van nagyobb természetes szám. Ezt az állítást Arkhimédészi-axiómaként szokás emlegetni.

$$\forall x \in \mathbb{R} \quad \exists n \in \mathbb{N} \quad n > x$$

Az Arkhimédészi-axióma átfogalmazható úgy is, hogy bármely a és b pozitív számokra létezik olyan n természetes szám, hogy $an > b$

Sőt, átfogalmazható így is:

Bármely a és b pozitív számokra létezik olyan n természetes szám, hogy $\frac{a}{b} > \frac{1}{n}$

Ez pedig azt jelenti, hogy bármely pozitív számra létezik olyan n természetes szám, hogy az $\frac{1}{n}$ kisebb ennél a számnál.

[Megnézem a kapcsolódó epizódot](#)

A Cantor-axióma azt mondja, hogy egymásba skatulyázott zárt intervallumok végtelen sorozatának metszete nem üres.

Ha $a_1 \leq a_2 \leq \dots \leq a_n$ és $b_1 \geq b_2 \geq \dots \geq b_n$ akkor $\exists x \in \mathbb{R}$

$$x \in \bigcap_{i=1}^{\infty} [a_i, b_i]$$

[Megnézem a kapcsolódó epizódot](#)
