

**Összeállította: Csia Kitti**

**Bevezetés a számításelméletbe 1**

**Kidolgozott vizsgatételek**

**2017/2018.**

**Tartalomjegyzék**

[1. tétel: Számelmélet, kongruencia 2](#_Toc503789098)

[2. tétel: Lineáris kongruencia 7](#_Toc503789099)

[3. tétel: Euler-Fermat tétel 10](#_Toc503789100)

[4. tétel: Algoritmusok, nyilvános kulcsú titkosítás, RSA 13](#_Toc503789101)

[5. tétel: Térbeli koordinátageometria 21](#_Toc503789102)

[6. tétel: Alterek, lineáris függetlenség 25](#_Toc503789103)

[7. tétel: Bázis, dimenzió 31](#_Toc503789104)

[8. tétel: Gauss-elimináció, RLA 35](#_Toc503789105)

[9. tétel: Determináns 39](#_Toc503789106)

[10. tétel: Kifejtési tétel, mátrix 44](#_Toc503789107)

[11. tétel: Lineáris egyenletrendszer megoldhatósága 48](#_Toc503789108)

[12. tétel: Mátrix inverze, rangja 52](#_Toc503789109)

[13. tétel: Lineáris leképzés, transzformáció 59](#_Toc503789110)

[14. tétel: Magtér, képtér 63](#_Toc503789111)

[15. tétel: Bázistranszformáció 66](#_Toc503789112)

[16. tétel: Sajátvektor, karakterisztikus polinom 69](#_Toc503789113)

*Felhasznált irodalom:*

**Szeszlér Dávid - Bevezetés a számításelméletbe 1**

**Fleiner Tamás - A számítástudomány alapjai**

Talált **HIBA** esetén jelzés: nospatium@gmail.com

# **1. tétel: Számelmélet, kongruencia**



[**BACK**](#_top)

**Tételcím**

Oszthatóság, prímszámok, a számelmélet alaptétele (csak a felbonthatóság bizonyításával). Prímek száma, nagyságrendje (bizonyítás nélkül). Kongruencia fogalma, alapműveletek kongruenciákkal.

1. **Oszthatóság**
   * Definíció
     + osztója , ha létezik olyan , melyre
     + ugyanezt fejezzük ki, ha -t az *többszörös*ének mondjuk
   * Jelölés
     + ha osztója -nek:
     + ha nem osztója -nek:
     + *valódi osztó*ja, ha fennáll és
   * Példa
     + **igaz**: , , , , még hiszen bármilyen -re igaz
2. **Prímszám**
   * Definíció
     + prímszámnak nevezzük, ha és -nek nincs valódi osztója
       - kikötés a számok miatt kell, ugyanis ezek se nem prímek, se nem összetettek
     + tehát csak akkor lehetséges, ha vagy
     + ha és nem prím, akkor *összetett szám*
3. **Számelmélet alaptétele**
   * **Tétel**
     + **(1)** minden -től, -tól, () -től különböző szám felbontható prímek szorzatára
     + **(2)** ez a felbontás tényezők sorrendjétől, előjelétől eltekintve egyértelmű
       - pl. 100 felbontása lehet vagy
   * **Bizonyítás (1)**
     + *(felbonthatóság bizonyítása)*
     + tetszőleges felbontása *prímtényezők* szorzatára
     + eljárás végig fenntartja az egy (-től különböző) egészek szorzatára való bontását
     + ha , ahol mind prím eljárás megáll
     + ha tényezők között van összetett szám pl. van valódi osztója, így felírható: , ahol , helyettesíthető -vel eljárás folytatódik
     + felbontáskor tényezők száma mindig 1-gyel nő, tényező | | legalább 2 eljárás véges sok lépésben elvégezhető (max. tényezős szorzattal)
4. **Prímek számossága**
   * **Tétel**
     + prímek száma végtelen
   * **Bizonyítás**
     + TFI. prímek száma véges
     + az összes +p
     + prímtényezők szorzatára bomlik vagy maga is prím
     + nem osztható egyik -vel sem, mert +1 maradékot ad mindig, így minden prímtényezője hiányzik felsorolásból ellentmondás
5. **Szomszédos prímek**
   * **Tétel**
     + minden találhatóak olyan prímek, hogy és között nincs további prím és
   * **Bizonyítás**
     + be kell látni, hogy létezik db szomszédos összetett szám
       - ezeknél kisebb prímek közül a legnagyobb
       - ezeknél nagyobb prímek közül legkisebb
       - db
       - összetettek, mert minden esetén -nek valódi osztója nyilván osztható -t adva ismét -vel osztható számot kapunk
6. **Nagy prímszámtétel**
   * **Tétel**

vagyis

* + - értékére jó becslés abban az értelemben, hogy a becslés relatív hibája növekedtével 0-hoz konvergál

1. **Kongruencia**
   * Definíció
     + *kongruens* modulo , ha -t és -t -mel maradékosan osztva azonos maradékot kapunk
   * Jelölés
   * **Állítás**
     + fenti akkor és csak akkor igaz, ha
   * **Bizonyítás**
     + maradéka és maradéka -mel osztva
     + valamely , ahol
     + és szerep szimmetrikus :

* + - * maradék
    - akkor teljesül, ha ,
    - definíció szerint ez *ekvivalens* ezzel:

1. **Alapműveletek kongruenciákkal**
   * **Tétel**
     + TFH. és fennállnak tetszőleges

**(1)**

**(1)**

**(2)**

**(3)**

* + **Bizonyítás (1)**
    - előző definícióra alapozva
    - -mel osztható számok (+) és (-) is -mel osztható
      * definíció miatt ismét igaz
  + **Bizonyítás (2)**
    - mivel egy -mel osztható szám bármely többszöröse is -mel osztható, így
      * (hasonló ), tehát:
  + **Bizonyítás (3)**
    - Bizonyítás **(2)**-re alapozva, de itt most és
    - ekkora kapjuk:
    - újra alkalmazva előző bizonyítást kapjuk:
    - és ezt folytatva jutunk el:

1. **A kongruencia tétel**
   * **Tétel**
     + tetszőlegesek és
     + akkor, és csak akkor igaz, ha
   * **Bizonyítás**
     + és (, mert közös osztójuk)
     + ellenkező esetben egy -nél nagyobb közös osztó volna
     + kongruencia állítás:
       - ez ekvivalens azzal, hogy:
       - tovább ekvivalens

# **2. tétel: Lineáris kongruencia**



[**BACK**](#_top)

**Tételcím**

Lineáris kongruenciák: a megoldhatóság szükséges és elégséges feltétele, a megoldások száma. Euklideszi algoritmus, annak lépésszáma, alkalmazása lineáris kongruenciák megoldására is (konkrét, megadott példán).

1. **Eukleideszi algoritmus**
   * Definíció
     + input:
     + output:
     + **1. lépés:**
       - -et maradékosan osztjuk -val, megkapva a maradékot, felírjuk őket a következő módon:
     + **2. lépés:**
       - -t elosztjuk a kapott maradékkal:
     + **…. lépés:**
       - lépésben kapott maradékot elosztjuk -ben kapottal:
     + **utolsó lépés:**
       - akkor érünk el ide, ha , ekkor lesz az lnko
2. **Eukleideszi algoritmus**
   * **Állítás**
     + Eukleideszi algoritmus végrehajtása után
   * **Bizonyítás**
     + ha teljesül, akkor
       - ezt alkalmazva:

→

* + - legutolsó lépés szerint

1. **Eukleideszi algoritmus lépésszáma**
   * **Állítás**
     + Eukleideszi algoritmus *polinomiális idő*ben lefut
     + legfeljebb maradékos osztás után áll meg
   * **Bizonyítás**
     + vizsgáljuk meg az eljárás egy tetszőleges lépést:
       - , ahol a fentiek szerint
     + tehát:
       - miatt) következik:
       - ebből viszont
       - miatt
     + így az eljárás páros számú soraiból ezt kapjuk:
     + a választással
     + (TFI maradékkal még nem ért véget)
       - ellentmondást kapnánk
2. **Lineáris kongruenciák megoldhatósága**
   * **Tétel**
     + lineáris kongruencia akkor és csak akkor megoldható, ha
     + ha teljesül, akkor megoldásainak száma modulo egyenlő-val
   * **Bizonyítás**
     + *(szükségesség igazolása)*
       - ,
       - ha az megoldható, akkor
     + TFH. , azaz (modulust is)
     + mivel , így leosztás után
     + Eukleideszi algoritmus segítségével lnko előáll kiszámíthatunk olyan , amire
       - nem lehet közös prímosztója relatív prímek
     + megoldások modulo megadása
       - mivel , ezért minden szerinti *maradékosztály* pontosan db szerinti maradékosztály uniója
       - konkrét esetben:

vagy…

vagy…

…

# **3. tétel: Euler-Fermat tétel**



[**BACK**](#_top)

**Tételcím**

Euler-féle -függvény, képlet a meghatározására (csak prímhatvány esetre bizonyítva). Redukált maradékrendszer, Euler-Fermat-tétel, kis Fermat-tétel. Két kongruenciából álló kongruenciarendszer megoldása (konkrét, megadott példán).

1. **Euler-féle -függvény**
   * Definíció:
     + ha , akkor az számok között -hez relatív prímek számát -nel jelöljük
2. **Euler-féle -függvény képlet**
   * **Tétel**
     + az kanonikus alakja , ekkor:
   * **Bizonyítás**
     + TFH. prímtényezős felbontásban csak 1 prím () van
     + (
     + ekkor , akkor és csak akkor igaz, ha
     + számok közül db nem relatív prím -hez
     + definíció szerint:
     + tehát igaz minden prímhatványra
3. **Redukált maradékrendszer**
   * Definíció
     + számhalmaz *redukált maradékrendszer* modulo , ha a következő feltételek teljesülnek:
       - **(1)** minden esetén
       - **(2)** bármely esetén
       - **(3)**
   * Példa
     + modulo 10 redmar. az
4. **Redukált maradékrendszer állítás**
   * **Állítás**
     + redmar. modulo , amely
     + szintén redmar. modulo
   * **Bizonyítás**
     + megmutatni, hogy -re is igaz, ami -re is
     + **(1)** (*1. tétel, Számelmélet alaptétel szerint)* és prímtényezős felbontásában nem lehet közös prím, ha külön -ban és -ben vagy -ben és -ben ᴓ
     + **(2)** bizonyításához TFH.:
     + mivel -re teljesül **(2)**, amely csak esetben fordulhat elő
     + mivel és ’ elemszáma , így **(3)** teljesül -re
5. **Euler-Fermat-tétel**
   * **Tétel**
     + ha az , akkor
   * **Bizonyítás**
     + tetszőleges redmar. modulo
     + mivel redmar. def. miatt
     + és ’ elemei párba állíthatók, párok kongruensek modulo
     + (*1. tétel, Alapműveletek kongruenciákkal (3) tulajdonságot használva*) és ’ elemeit összeszorozva modulo kongruens eredményeket kapunk:
       - mivel , ezért (*1. tétel, Számelmélet alaptétel következtében)* is igaz
       - osztással a modulus nem változik, így megkaptuk a tételt
6. **„Kis” Fermat-tétel**
   * **Tétel**
     + ha prím és , akkor
   * **Bizonyítás**
     + tétel állítása magától értetődő, ha
       - ekkor is igaz
     + ha is igaz
       - Euler-Fermat-tétel -ra és -re
       - miatt

# **4. tétel:** **Algoritmusok, nyilvános kulcsú titkosítás, RSA**

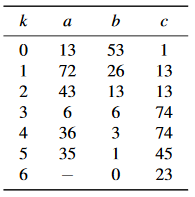


[**BACK**](#_top)

**Tételcím**

Polinomiális futásidejű algoritmus (vázlatos) fogalma. Számelmélet és algoritmusok: alapműveletek, hatványozás az egészek körében és modulo (ez utóbbi konkrét, megadott példán), ezek lépésszáma. Prímtesztelés, Carmichael számok. Nyilvános kulcsú titkosítás, megvalósítása RSA-kóddal.

1. **Polinomiális futásidejű algoritmus**
   * Definíció
     + az algoritmust *polinomiális futásidejű*nek tekintjük, ha méretű bemenethez tartozó függvényre, mely az *algoritmus lépésszám*át határozza meg
     + minden esetén fennáll:
2. **Számelméleti algoritmusok**
   * Összefoglaló (*számelméleti algoritmusok hatékonysága)*
     + bemenet méretét mindig a bemenetet adó számok összes számjegyének számával mérjük
     + algoritmus *hatékony*, ha:
       - jegyű számokon max vagy vagy lépést tesz meg
   * **Alapműveletek**
     + összeadás feladata:
       - bemenet:
       - kimenet:
       - ezzel analóg a kivonás, szorzás
     + maradékos osztás feladata:
       - *alsó egészrész*e, jelölés:
       - -nak szerint vett osztási maradéka, jelölése:
     + már alsó tagozatból ismert „írásbeli” algoritmusok megfelelőek erre
     + viszont, ha és jegyeinek száma és , akkor az algoritmusok lépésszáma a(z)…
       - írásbeli összeadás, kivonásnak:
       - szorzás, osztásnak:
       - összeadás, kivonás:
       - szorzás, osztás:
     + tehát: polinomiális futásidejű hatékony algoritmusok
     + hatványozás feladat:
       - bemenet:
       - kimenet:
     + ennek már nem adható hatékony algoritmus, mert a kimenet kiírása is túl sok ideig tart
       - pl. esetében jegyeinek száma
       - vagyis jegyeinek száma exponenciális függvénye
   * **Hatványozás modulo** 
     + nyilvános kulcsú titkosításhoz alapvető
     + kimenetet nem tudjuk kiszámítani a fentiek szerint, de annak adott szerinti maradékát meg tudjuk határozni
     + hatványozás feladat:
       - bemenet:
       - kimenet: vagyis osztási maradéka szerint
     + kiírási probléma megoldva, mert a kimenet
     + még mindig nem kiszámítható
     + szerinti maradékokat sorra kiszámoljuk
     + ez az eljárás szintén használhatatlanul lassú: db ilyen lépést kell tenni, ez exponenciális lépésszámú algoritmus
     + erre hatékony algoritmus: ***ismételt négyzetre emelések módszere***
     + példa: maradéka -tel osztva
     + ezzel a módszerrel -nak a -hatvány kitevőjű hatványait tudjuk meghatározni
     + a sort nem tudjuk tovább négyzetre emelni, így
     + részekre bontva:
     + végeredmény:
     + az algoritmus tehát meghatározza maradékát szerint minden -hatványra, vagyis kitevőkre, ahol
     + az így kapott maradékokból áll elő maradéka is
     + tehát a maradékok kiszámítását érdemes párhuzamosan végezni a négyzetre emelésekkel, teljes leírása:
   * **Ismételt négyzetre emelések módszere ( kiszámítására)**
     + bemenet: , (amelyekre teljesül, hogy
     + **lépés**
     + **lépés**
       - ha páratlan, akkor:
       - ha páros, akkor változatlan marad
     + **lépés**
     + **lépés**
       - ha akkor: PRINT „”, STOP
     + **lépés**
     + folytassuk az **lépésnél**
   * feladat újonnani végrehajtása ennek a módszernek a segítségével
   * *ciklus hányadszorra hajtódott végre, végeredmény*



* + sorra ugyanazok az értékek keletkeztek, mint amelyeket a korábbi számításban kaptunk

1. **Prímtesztelés, Fermat-teszt**
   * bemenet:
   * **lépés**
   * **lépés**
     + generáljunk véletlen számot és között
   * **lépés**
     + Euklideszi-algoritmussal számoljuk ki értékét
     + ha nem prím, STOP

**lépés**

* + - számítsuk ki értékét Ismételt négyzetre emelések módszerével
    - ha , nem prím, STOP
  + **lépés**
    - ha valószínűleg prím
  + **lépés**
    - vissza az **lépéshez**
  + fenti eljárás más szavakkal, krimis stílusban:
    - véletlen számokat sorban a tanúk padjára idézzük
    - vallomása az értéke
      * ha ez , akkor nem közöl információt prímségét illetően, ekkor ***cinkosa***
      * ha , akkor leleplezi összetettségét, tehát ***áruló***ja
        + nem szokás árulónak nevezni -t, ha
      * ha találunk olyan számot, melyre
        + ekkor az Eukleideszi algoritmus az egy valódi osztóját megtalálja
      * így további információkat ad ki -ről, tehát ***leleplező***je

1. **Fermat-teszt árulók száma**
   * **Tétel**
     + ha összetett szám és -nek van árulója, akkor az és közötti, -hez relatív prímszámoknak legalább a fele áruló
   * **Bizonyítás**
     + tetszőleges árulója -nek, az összes cinkosa
     + mutassuk meg, hogy számok páronként különböző árulói -nek
     + ebből következni fog, hogy az árulók száma legalább akkora, mint a cinkosok száma, amely ekvivalens a tétellel
     + mivel és miatt
     + így (*a 3. tétel, Euler-féle -függvény állítása szerint)* is igaz, mert
     + továbbá: -edik hatványra emelve:
     + ebből következik, hogy is áruló
     + végül megmutatjuk, hogy az árulók páronként különbözők
     + TFI valamely esetén
     + ez azonban miatt ellentmondás, így beláttuk
2. **Carmichael-számok**
   * Definíció
     + az összetett számot *univerzális álprím*nek más néven *Carmichael-szám*nak nevezzük, ha nincs árulója
     + vagyis minden esetén
3. **A nyilvános kulcsú titkosítás**
   * generálunk jegyű prímszámot:
   * ha csak -et ismerjük, nem fogjuk tudni megadni egy valódi osztóját
   * nyilvános kulcsú titkosítás alapfeladatát megoldó módszer
     + olyan kölcsönösen egyértelmű függvényeket keresünk, melyek
       - minden esetén , vagyis , egymás inverze
       - kód „tulajdonosa” értékét ki tudja számítani
       - kiszámítására vonatkozó eljárás nyilvánosságra hozható, -t nem lehet kiszámolni vele
   * tehát biztos sok számjegyű
   * függvénypár birtokában a kód tulajdonosa biztonságosan tud üzenetet fogadni kódegyeztetés nélkül
     + elküldi függvényt kiszámító eljárást, partner pedig üzenet helyett annak kódját küldi
     + tulajdonos-t -el ki tudja számolni
     + ha a két fél rendelkezik függvénypárral, akkor a kommunikáció teljesen biztonságos
   * RSA (Rivest-Shamir-Adleman) algoritmussal való megoldás a legszélesebb körű
   * *(ehhez szükséges állítás:)*
   * **Állítás**
     + különböző prímek és
     + ekkor tetszőleges és egészekre
   * **Bizonyítás**
     + ha , akkor az állítás következménye (*a 3. tétel, Euler-Fermat tételnek)*: állítást kapjuk
     + ha , akkor vagy
     + ha mindkettő teljesül, akkor , így a bizonyítandó állítás , magától értetődő
     + TFH vagy
     + mivel prím és , ezért , Euler-Fermat tétel miatt
     + ugyanez a kongruencia modulo és is fennáll
4. **RSA algoritmus**
   * előző dolgozva, és legyen , amelyre:
   * tegyük közzé a kódoló függvényünk
   * kiszámolható ismételt négyzetre emelések módszerével
   * D keresése hasonló módon:
   * -t úgy választjuk, hogy inverze legyen
   * ez akkor teljesül, ha minden esetén, ami
   * a fent említett állítás miatt
     + inverze lesz -nek, ha értékét sikerül úgy megválasztanunk, hogy teljesül valamely egészre
     + tehát a cél ezen kongruencia kielégítése
     + itt adottak, -re egy lineáris kongruencia feladat, amely megoldható, de kiszámítható Euklideszi algoritmussal is

# **5. tétel: Térbeli koordinátageometria**



[**BACK**](#_top)

**Tételcím**

Térbeli koordinátageometria: sík egyenlete, egyenes egyenletrendszerei. Skaláris szorzat fogalma és kiszámítása (bizonyítás nélkül); vektoriális szorzat fogalma és kiszámítása (bizonyítás nélkül). Adott térbeli vektorok lineáris függetlenségének, -beli generátorrendszer voltának, illetve bázis voltának geometriai feltétele.

1. **Térvektor tulajdonságok**
   * **Tétel**
     + és térvektorok,
2. **Skaláris szorzat**
   * Definíció
     + és *skaláris szorzatán* az alábbit értjük:
     + ha , akkor a szorzatösszeg
3. **Skaláris szorzat tétele**
   * **Tétel**
     + és térvektorok, ekkor:
4. **Egyenes**
   * Definíció
     + az egyenes paraméteres egyenletrendszere (*fenti Térvektor tulajdonságok tétel miatt*)
     + pont rajta van az egyenesen
     + *irányvektor*a
5. **Egyenes tétele**
   * **Tétel**
     + az egyenesnek pontja
     + irányvektora
     + tetszőleges pontjának nem paraméteres alakja:
   * **Bizonyítás**
     + , akkor igaz, ha paraméteres egyenletrendszerére értékére -t adja
     + ha , akkor a 3 egyenletből egy közös -ra kell jutnunk
     + ha , akkor megfelelő létezése azt jelenti, hogy és az első 2 egyenletből közös értéket kell kapnunk
     + ha csak , akkor az első két egyenlet egyértelmű, míg a 3. egyenlet mindig kielégíthető a választással
6. **Sík tétele**
   * **Tétel**
     + az adott síknak
     + normálvektora
     + ekkor akkor igaz, ha
   * **Bizonyítás**
     + , akkor igaz, ha -el
     + pedig akkor -el, ha merőleges -el ez akkor teljesül, ha skaláris szorzatuk 0
     + tétel szerint:
     + beszorzás és átrendezés után megkapjuk a tételben kimondott egyenletet
7. **Vektoriális szorzat**
   * Definíció
     + és vektorok *vektoriális szorzat*a az az -vel jelölt vektor, amelyre az alábbi feltételek fennállnak:
       - hossza:
       - merőleges és -re
     + *jobbsodrású rendszer*t alkotnak
     + ha valamelyik vektor ,akkor az eredmény is
8. **Vektoriális szorzat tétele**
   * **Tétel**
     + és vektorok, ekkor
9. **Vegyesszorzat**
   * Definíció
     + jelölt vektorok *vegyesszorzat*a

**10. Vegyesszorzat tétele**

* + **Tétel**
    - a vegyesszorzat kapcsolata a térfogattal az , által kifeszített paralelepipedon térfogata:
  + **Bizonyítás**
    - térfogatot a paralelogramma területének és magasságának szorzatából kapjuk
    - terület egyenlő az -vel
    - magasságot meg úgy kapjuk, hogy meghatározunk egy (*tetszőlegesen megbetűzött*) **OMW** háromszöget
      * **O**: origó
      * **M**: a W-ből az -re állított merőleges talppontja
      * **W**: végpontja
    - Pitagorasz tétel OM

# **6. tétel:** **Alterek, lineáris függetlenség**



[**BACK**](#_top)

**Tételcím**

és alterének a fogalma. Lineáris kombináció, generált altér (és ennek altér volta), generátorrendszer. Lineáris függetlenség (ennek kétféle definíciója és ezek ekvivalenciája). Az „újonnan érkező vektor” lemmája. F-G egyenlőtlenség.

* + Definíció
    - esetén az db valós számból álló *számoszlop*ok halmazát jelöli
    - ezen értelmezett összeadás és tetszőleges *skalárszoros*át az alábbi alapján értelmezzük:

és

1. tulajdonságok
   * **Tétel**
     + , és , ekkor igazak az alábbiak:
       - (
   * **Bizonyítás**
     + *triviális, mert mindegyike azonnal következik a valós számok műveleti tulajdonságaiból*
2. altere
   * Definíció
     + ᴓ, tehát az tér egy nemüres *részhalmaz*a
     + -t az *alteré*nek nevezzük, ha az alábbi két feltétel teljesül:
       - bármely esetén is igaz
       - bármely esetén is igaz
   * Jelölés
3. **Lineáris kombináció**
   * Definíció
     + vektorok és skalárok
     + vektort a vektorok skalárokkal vett *lineáris kombináció*ja
4. **Generált altér**
   * Definíció
     + vektorok, ezeknek a lineáris kombinációival kifejezhető -beli vektorok halmazát *generált altér*nek nevezzük
   * Jelölés
5. **Generátorrendszer**
   * Definíció
     + vektorok, ha , akkor a vektorhalmazt a altér *generátorrendszer*ének nevezzük
6. **Lineáris függetlenség, összefüggőség**
   * Definíció
     + a vektorrendszert akkor nevezzük *lineárisan független*nek, ha vektorok közül semelyik sem fejezhető ki a többi lineáris kombinációjaként
     + ha ez nem teljesül (*vagyis a vektorok között legalább egy olyan, amely kifejezhető a többi lineáris kombinációjaként),* akkor a vektorrendszert *lineárisan összefüggő*nek nevezzük
7. **Triviális lineáris kombináció**
   * **Tétel**
     + a vektorrendszer akkor és csak akkor lineárisan független, ha egyenlőség kizárólag abban az esetben teljesül, ha ezt nevezzük a triviális lineáris kombinációnak
   * **Bizonyítás**
     + („*akkor lineárisan független, ha…”)*
     + TFH. csak a triviális lineáris kombináció esetén teljesül
     + belátjuk, hogy lineárisan független
     + TFI.:
       - feltesszük, hogy ez mégsem lineárisan független
       - ha nem lineárisan független, akkor valamelyikük kifejezhető a többi lineáris kombinációjából: , ekkor

átrendezve

* + - * ez ellentmondás nemtriviális lineáris kombináció esetén is teljesül igazolva
    - („*csak akkor…”)*
    - feltesszük, hogy lineárisan független és megmutatjuk, hogy ekkor csak a esetben teljesül
    - TFI.:
      * TFH. , de a lambdák között van nemnulla
        + pl.:
      * ekkor átrendezés és -val való osztás után a következő alakot kapjuk:
      * ellentmondás, mégsem lineárisan független, mert kifejezhető a többiből lineáris kombinációval

1. **Újonnan érkező vektor lemmája (ÚÉVL)**
   * **Tétel**
     + TFH. az rendszer lineárisan független, de lineárisan összefüggő
     + ekkora tehát kifejezhető lineáris kombinációjaként
   * **Bizonyítás**
     + mivel lineárisan összefüggő, ezért lineáris függetlenség tétele alapján létezik nemtriviális lineáris kombináció, mely nullvektort adja végeredményül
     + ha a egyenletben azt jelenti, hogy a maradék egyenlet így néz ki ÉS a skalárok között van egy (vagy több) nemnulla tag
     + emiatt az eredeti rendszer lineárisan összefüggő ellentmondás
     + , és az ezzel való osztás után kapott egyenletből következik, hogy előállítható az rendszer lineáris kombinációjaként
2. **F-G egyenlőtlenség**
   * **Tétel**
     + altér, -beli vektorokból álló lineárisan független rendszer
     + pedig generátorrendszer -ben
   * **Bizonyítás**
     + ha , akkor -ben van a nullvektortól különb vektor (mert minden generátorrendszer legalább 1 elemű (üres halmaz esetén alteret generálja csak)
     + tétel esetén igaz
     + TFH. és már igaz -re igaz belátni -ra is
     + mivel generátorrendszer -ben, ezért minden -beli vektor is előáll ennek lineáris kombinációjaként:
       - lambdák között nemnulla, mert
       - megmutatjuk, hogy minden esetén az -hez található olyan skalár, hogy
       - felírható lineáris kombinációjaként:
     + ekkor megfelel:
       - együtthatója , így W-beli
     + megmutatjuk, hogy vektorok lineárisan függetlenek
     + vegyük egy -t adó lineáris kombinációjukat a skalárokkal
     + ezzel az egy -t adó lineáris kombinációját kaptuk
     + tudjuk, hogy ezek lineárisan független lineáris kombináció minden együtthatója 0 kell legyen
     + vagyis vektorok valóban lineárisan független

# **7. tétel: Bázis, dimenzió**



[**BACK**](#_top)

**Tételcím**

Bázis és dimenzió fogalma, a dimenzió egyértelműsége. Standard bázis, dimenziója. Koordinátavektor fogalma és annak egyértelműsége. Bázis létezése tetszőleges altérben.

1. **Bázis**
   * Definíció
     + altér
     + -beli vektorokból álló rendszert *bázis*nak nevezzük -ben, ha
       - a rendszer *lineárisan független*
       - *generátorrendszer*t alkot
2. **Bázis egyértelműsége**
   * **Tétel**
     + TFH. a altérben a rendszer és a rendszer egyaránt bázisok →
   * **Bizonyítás**
     + mindkét rendszer bázis, ezért -ben
       - lineárisan független
       - generátorrendszer

mivel egyszerre igazak, így

* + - * (*6. tétel, F-G egyenlőtlenséget tétel miatt)*
    - ennek fordítottját is kimondhatjuk, így -ben
      * generátorrendszer
      * lineárisan független
      * *(ismét F-G miatt)*

1. **Dimenzió**
   * Definíció
     + *altér*ben rendszer bázis
     + ekkor *dimenzió*ja
   * Jelölés
2. **Standard bázis** 
   * Definíció
     + jelölje minden esetén azt az -beli vektort, melynek (felülről) az -edik koordinátája
     + ekkor bázis az -ben ez a *standard bázis*
   * Jelölés
   * **Bizonyítás**
     + *lineáris kombinációja* skalárokkal
     + látszik, hogy generátorrendszer -ben, hiszen lineáris kombinációjukként tetszőleges vektor előállhat
     + ha *nullvektor*t akarjuk kifejezni, akkor csak a triviális lineáris kombináció esetén fog az előállni
     + tehát a rendszer lineárisan független tényleg bázist alkot az -ben
     + fenti állításból következik, hogy
     + viszont csak az egyike az „ dimenziós tereknek” és minden -nek van -dimenziós altere
3. **Bázis tétele**
   * **Tétel**
     + altérben a vektorok akkor és csak akkor alkotnak bázist, ha minden egyértelműen, azaz pontosan egyféleképpen fejezhető ki lineáris kombinációjukként
   * **Bizonyítás**
     + *(„csak akkor” alkotnak bázist… kifejtése)*
     + akkor bázis, ha -ben generátorrendszer és lineárisan független (bázis tételből)
     + *(„akkor” … kifejtése)*
     + minden kifejezhető lineáris kombinációjaként
     + TFI. valamely kétféleképpen kifejezhető:

és

* + - kettő különbségét véve:

tehát kifejezhető a nemtriviális lineáris kombinációjaként, hiszen , ez ellentmondás

1. **Koordinátavektor**
   * Definíció
     + , bázis -ben, tetszőleges vektor
     + azt mondjuk, hogy vektor a vektor szerinti *koordinátavektor*a, ha
   * Jelölés
     + nem csak -től függ:
       - ugyanannak a vektornak más-más bázis esetén más-más koordinátavektorok felelnek meg
2. **Bázis létezése tétele**
   * **Tétel**
     + altér,  -beli vektorokból álló lineárisan független rendszer
     + kiegészíthető véges sok további vektorral úgy, hogy a kapott rendszer bázis legyen
   * **Bizonyítás**
     + igaz, hogy , mivel altér
       - ha , akkor generátorrendszer, így bázis -ben tétel belátva
       - ha , akkor létezik egy , vektor
         * *újonnan érkező vektor lemmája* szerint ekkor , lineárisan független
         * ha ez már generátorrendszer -ben, akkor kész
         * különben be kell látni, hogy ez a folyamat leáll egy idő után F-G egyenlőtlenség igénybevétele
         * ez alapján -nél nagyobb elemszámú lineárisan független rendszer ᴓ -ben, de létezik elemű generátorrendszer ebben a térben
         * az eljárás tehát lépés után biztos megáll
       - minden altérben van bázis létezik
     + ha , akkor az üres halmaz bázis-ben
     + ha tartalmaz egy , akkor -re alkalmazva a fenti tételt kapunk egy -beli bázist

# **8. tétel: Gauss-elimináció, RLA**

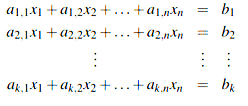


[**BACK**](#_top)

**Tételcím**

Lineáris egyenletrendszer megoldása Gauss-eliminációval. Megoldhatóság, a megoldás egyértelműségének feltétele. Lépcsős alak és redukált lépcsős alak fogalma. Kapcsolat az egyenletek és ismeretlenek száma, illetve a megoldás egyértelműségé között.

1. **Lineáris egyenletrendszer**
   * Definíció
     + egy egyenletből álló változós röviden: -es *lineáris egyenletrendszer*
     + *kettős indexelésű együtthatók* bevezetése:
       - -edik egyenletben a -edik változó együtthatója minden:
         * esetén
       - konstans tag
     + lineáris egyenletrendszer „hagyományos” alakja:



* + - *kibővített együtthatómátrix*os alakja



* + - *(fontos elméleti következmény:)*
    - TFH. adott egy egyenletből álló, ismeretlenes lineáris egyenletrendszer
    - megoldhatóságával kapcsolatos következmények, ha csak és relációját ismerjük
      * *nem igaz*, hogy ha , akkor biztosan van megoldás
      * *nem igaz*, hogy ha , akkor biztosan végtelen sok megoldás van
      * *nem igaz*, hogy ha , akkor biztosan nincs megoldás ellenpélda lásd (lentebb): *Lineáris rendszer megoldhatóság* tétele

1. **Elemi sorekvivalens lépések**
   * Definíció
     + kibővített együtthatómátrixával adott lineáris egyenletrendszer esetén *elemi sorekvivalens* lépésnek nevezzük alábbiakat
     + ( skalár esetén):
       - **(1)** a mátrix -edik sorának (tagonként való) megszorzása -val
       - **(2)** a mátrix -edik sorának helyettesítése sajátmagának és a -edik sor -szorosának (tagonként vett) összegével
       - **(3)** az -edik és -edik sor felcserélése
       - **(4)** egy csupa nulla elemeket tartalmazó sor elhagyása
2. **Gauss elimináció**
   * **Állítás**
     + előző definícióban felsorolt lépések ekvivalens átalakítások
     + egyenletrendszer megoldásait nem változtatják meg
     + (*részletesebben: ha az számok kielégítik az egyenletrendszert egy lépés megtétele előtt, akkor annak megtétele után is, és fordítva is)*
   * **Bizonyítás**
     + *(csak a* **(** *lépésre bizonyítva…)*
     + ha kielégítik az egyenletrendszert, akkor:

fentihez adva

* + - * tehát az új -edik egyenlet teljesül
    - megfordítva: ha megoldása a rendszernek a **(** lépés megtétele után, akkor a és egyenletek igazak
    - ebből kivonva -szorosát egyenletét kapjuk
    - tehát lépés megtétel előtt is teljesül

1. **Lépcsős alak, redukált lépcsős alak**
   * Definíció
     + egy kibővített együtthatómátrixával adott lineáris egyenletrendszert *lépcsős alakú*nak *(LA)* mondunk, ha az alábbiak teljesülnek:
       - a mátrix minden sorában van nemnulla elem és (balról) az első nemnulla elem egy -es, úgynevezett *vezéregyes*
         * (*Vezéregyeseket nem tartalmazó oszlopok szabad paramétereknek felelnek meg. A sorok adják meg átrendezés után, hogy a többi változó hogyan fejezhető ki a szabad paraméterekből.*)
       - ha , akkor az -edik sorban álló vezéregyes kisebb sorszámú oszlopban van, mint a -edik sor vezéregyese
       - a vezéregyesekkel egy oszlopban, azok alatt álló minden elem 0
     + *redukált lépcsős alak*únak *(RLA)* mondjuk a mátrixot, ha még az alábbi is teljesül:
       - vezéregyesekkel egy oszlopban, azok fölött álló minden elem 0
2. **Gauss elemináció tétel**
   * **Tétel**
     + tetszőleges, kibővített együtthatómátrixával adott lineáris egyenletrendszer esetén a Gauss-eleminációt futtatva az alábbi esetek közül pontosan az egyik valósul meg
       - az első fázis . lépésének végrehajtásakor az eljárás „tilos sort” talál az egyenletrendszer nem megoldható
       - az algoritmus RLA-ra hozza a kibővített együtthatómátrixot, amelynek minden oszlopában van vezéregyes az egyenletrendszer egyértelműen megoldható
       - az algoritmus RLA-ra hozza a kibővített együtthatómátrixot, de annak nem minden oszlopában van vezéregyes az egyenletrendszernek végtelensok megoldása van
     + a második és harmadik esetben a megoldások a RLA-ból közvetlenül kiolvashatóak
3. **Lineáris egyenletrendszer megoldhatóság**
   * **Tétel**
     + ha egy egyenletből álló, ismeretlenes lineáris egyenletrendszer egyértelműen megoldható, akkor
   * **Bizonyítás**
     + lefuttatjuk a Gauss-eliminációt az egyenletrendszerre
     + megoldható (tehát nincs *tilos sor*), az algoritmus egy RLA-t hoz létre
     + ebben a sorok száma:
     + nyilván , mert az algoritmus csökkentheti a sorok számát (első fázis lépésben), de nem növelheti
     + mivel az egyenletrendszer egyértelműen megoldható, ezért RLA minden oszlopa tartalmaz vezéregyest
     + ezeket összevetve: , ezzel a tétel belátva

# **9. tétel: Determináns**

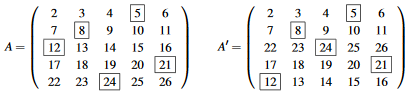


[**BACK**](#_top)

**Tételcím**

Determináns definíciója, alaptulajdonságai, kiszámítása.

1. **Determináns**
   * Definíció
     + egy adott mátrix
     + minden *bástyaelhelyezés*re szorozzuk össze az azt alkotó elemet
     + szorzathoz adjunk előjelet következő szabály szerint:
       - ha a bástyaelhelyezésnek megfelelő *permutáció* inverziószáma páros, akkor az előjel pozitív
       - ha páratlan, akkor az előjel negatív
     + az így kapott db, tényezős szorzat összegét az *determináns*ának nevezzük
   * Jelölés
     + vagy
2. **Determináns alaptulajdonságai (1)**
   * **Tétel**
     + -es mátrix
     + ha annak van csupa 0 elemet tartalmazó sora vagy oszlopa, akkor
     + ha felsőháromszög mátrix vagy alsóháromszög mátrix, akkor a determinánsa a főátlóbeli elemek szorzata:
   * **Bizonyítás**
     + csupa 0 állítás azonnal következik a determináns definíciójából:
       - mivel mind az db szorzat tartalmaz elemet abból a sorból/oszlopból, amelyiknek minden tagja 0, ezért minden szorzat értéke és ezek összege is 0 lesz
     + (*második állítás bizonyítása*)
     + vegyük *felsőháromszög-mátrix*ot
     + a bástyaelhelyezések akkor nem tartalmaznak 0 elemet, ha az első oszlopból az első elemet, a második oszlopból a második elemet, választjuk ki (többit nem lehetne) és így tovább…
     + a kapott permutáció *inverziószám*a 0, így pozitív előjelű ez a tag, és mivel ez az egyetlen tag, amiben nem szerepel 0, ezért ez lesz az előjeles összeg eredménye
     + ezt megismételve (*fent az oszlop és a sor szavak megcserélésével*) megkapjuk ugyanezt a bizonyítást *alsóháromszög-mátrix*ra is
3. **Determináns alaptulajdonságai (2)**
   * **Tétel**
     + -es mátrix, skalár,
     + **(1)** ha egy sorát megszorozzuk -val, akkor a kapott ’ mátrix determinánsa -szorosa -énak:
     + **(2)** ha két sorát felcseréljük, akkor a kapott ’ mátrix determinánsa ellentétje -énak:
     + **(3)** ha -edik sorát helyettesítjük sajátmagának és a -edik sor -szorosának összegével, akkor a kapott ’ mátrix determinánsa megegyezik -éval:
     + oszlopokra igaz ugyanez
   * **Bizonyítás (*egy hosszú bizonyítás következik… készülj fel rá lelkileg*)**
     + **(1)** TFH. -t az -edik sor szorzásával kaptuk
     + hasonlítsuk össze és determinánsának definíció szerinti kiszámítását:
     + mivel minden bástyaelhelyezés pontosan egy elemet tartalmaz az -edik sorból, ezért az kiszámítása közben keletkező szorzatok mindegyikében egy tényező a -szorosára változik, amikor -t számítjuk
     + maga a szorzat értéke is a -szoros lesz, előjel nem változik
     + mindegyik összeadandó a -szorosára változik, ezért ezek (előjeles) összege, vagyis a determináns értéke is
     + bizonyítás érvényes a -edik oszlopra is
     + **(2)** példán keresztüli bemutatása:



* + - *a és az sor felcserélésével kaptuk -t*
    - *-ban bekeretezett rész a bástyaelhelyezés*
    - ennek megfelelő permutáció , ennek inverziószáma keletkező szorzat negatív előjelet kap
    - kiszámításánál ugyanez, különbség a tényezők sorrendjében, és a bástyaelhelyezésben
    - ekkor inverziószám már 6, előjel pozitív
    - -ből és felcserélésével kapjuk
    - ugyanígy és
    - tehát: bástyaelhelyezés szorzatok sorrendtől eltekintve azonosak, előjelük ellentétes
    - oszlopcserénél lényegében azonos
    - **(3)** lemmával/segédtétellel bizonyítjuk:

**Determináns alaptulajdonságai lemma**

* + **Tétel**
    - TFH. az -es mátrixok az -edik soraiktól eltekintve elemről elemre megegyeznek
    - -edik soraikra viszont fennáll, hogy minden esetén
    - a -edik sora épp az és az -edik sorának (tagonkénti) összege
    - ekkor
    - az állítás érvényes oszlopokra is
  + **Lemma bizonyítása**
    - vegyünk egy tetszőleges *bástyaelhelyezés*t -ben
    - feleljen meg a permutációinak, ebből keletkező szorzat tehát:
    - a behelyettesítéssel:
    - felbontva a zárójelet, és felhasználva, hogy minden esetén :
    - mivel minden bástyaelhelyezésre összegezve definíció szerint és )-t kapjuk, a lemmát belátva
    - (oszlopok esetén bizonyítás lényegében azonos)
  + **Bizonyítás**
    - **(3)** **folytatás…**
    - lemma alkalmazható az mátrixra, hiszen abban az -edik sor minden eleme egy kéttagú összeg:
    - minden -ra
    - lemmát alkalmazva: és pedig az a mátrix, amely az -edik sorától eltekintve azonos -val
    - az -edik sorában pedig az -edik sorának -szorosa áll:
    - lemmát ezekre alkalmazva:
    - már csak bizonyítása kell
    - -edik sorára alkalmazható a tétel (már bebizonyított) ***(1*** állítás:
    - ha jelöli azt a mátrixot, amely az -edik sorától eltekintve azonos -nal (és így -val), az -edik sorában pedig az -edik sorának másolata áll
      * vagyis minden -ra, akkor ***(1***-bőlkövetkezik
    - -re pedig a tétel ***(2*** állítását alkalmazzuk:
    - ha -ben felcseréljük az -edik és -edik sort, akkor a determináns az ellentétjére változik, és változatlan is marad (hiszen -n a sorcsere „nem látszik”, annak -edik és -edik sora azonos)
    - , tétel bizonyítva
    - oszlopokra ismét változtatás nélkül elmondható

1. **Determináns kiszámolása – Gauss eliminációval**
   * Bemenet: - es mátrix
   * **0. lépés**
   * **1. lépés**
     + ha , akkor folytassuk a **2. lépés**nél
     + szorozzuk meg -edik sort -vel
     + ha , akkor PRINT STOP
     + minden esetén adjuk a -edik sorhoz az -edik sor -szeresét
   * **2. lépés**
     + ha , és van olyan , melyre , akkor:
       - cseréljük fel az -edik sort a -edikkel
       - folytassuk az **1. lépés**nél
     + PRINT STOP
2. **Sarrus-szabály, speciális**
   * csak - as mátrixoknál működik

# **10. tétel: Kifejtési tétel, mátrix**

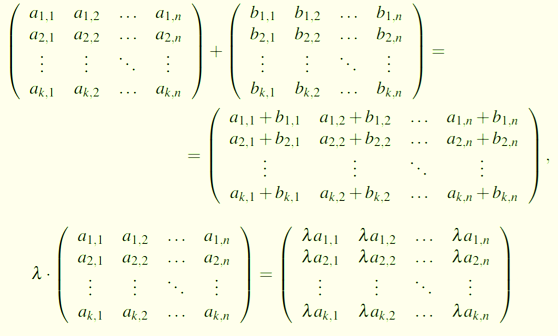


[**BACK**](#_top)

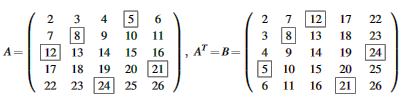
**Tételcím**

A determinánsok kifejtési tétele (bizonyítás nélkül). Műveletek mátrixokkal (összeadás, skalárral szorzás, transzponálás), ezek tulajdonságai. A transzponált determinánsa. Determinánsok szorzástétele (bizonyítás nélkül).

1. **Kifejtési tétel**
   * **Tétel**
     + az -es mátrix valamelyik sorának vagy oszlopának minden elemét megszorozzuk a hozzá tartozó előjeles aldetermináns értékével
     + a kapott db kéttényezős szorzatot összeadjuk determináns értékét kapjuk
2. **Mátrix**
   * Definíció
     + adott egy -es egészek esetén -es mátrixnak nevezzük egy sorból, és oszlopból álló táblázatot
     + minden cellájában valós szám áll
     + -es mátrixok halmazát jelöli
     + mátrix -edik sorának és -edik oszlopának kereszteződésében álló elemet jelöli
     + -en értelmezett, -al jelölt összeadást és tetszőleges esetén -tal jelölt skalárral való szorzást tudjuk értelmezni



1. **Mátrixműveletek**
   * **Tétel**
     + és
     + ekkor igazak az alábbiak:
       - **(1)**
       - **(2)** (
       - **(3)**
       - **(4)**
       - **(5)**
2. **Transzponált**
   * Definíció
     + egy -es mátrixának nevezzük az -as mátrixot, ha teljesül minden és esetén
   * Jelölés
3. **Mátrixszorzás**
   * Definíció
     + a -es -es mátrixok szorzatának nevezzük
     + -vel jelöljük azt a -es mátrixot, melyre minden és esetén
     + **Állítás**
       - ha azésmátrixokraszorzat létezik, akkor is létezik és
4. **Transzponált determinánsa**
   * **Tétel**
     + minden négyzetes mátrixra
   * **Bizonyítás**
     + (*példán mutatjuk be, felhasználva a 9. tételben látott mátrixokat:*)



* + - determinánsának definíció szerinti kiszámításakor is megjelenik ez a szorzat
    - itt a megfelelő permutáció , amelynek az inverziószáma „véletlenül” szintén 5, előjel marad negatív
    - tetszőleges -es mátrix és
    - bizonyítjuk, hogy kiszámításakor ugyanazok a szorzatok keletkeznek, ugyanolyan előjellel
    - tetszőleges permutáció
    - ennek kiszámításakor előjelezett szorzat felel meg
    - mivel minden és esetén, ezért ugyanez a szorzat (egyelőre előjeltől eltekintve) megjelenik -ben is   
       alakban
    - ezért permutáció, amiben az és a -edik helyen, a 2 és a -edik helyen stb. az és a -edik helyen áll
    - ekkor -t inverzének hívjuk
      * ugyanis permutációt olyan kölcsönösen egyértelmű függvénynek fogjuk fel, amely az számokhoz rendre értékeket rendel
      * függvénytani értelemben inverze, és is permutáció
    - elemeiből készített szorozat alakban írható fel, így előjelet kapja
    - meg kell mutatni, hogy igaz minden permutációra és annak a inverzére
    - permutációban , ekkor a inverz permutációban
    - és tagok -ben definíció szerint akkor állnak inverzióban, ha
    - definíció szerint ez azt jelenti, hogy -ben az tagok állnak inverzióban, hiszen , de
    - összefoglalva:
      * -ben , akkor és csak akkor állnak inverzióban, ha -ben állnak inverzióban
    - így -ben inverzióban álló elempárok kölcsönösen egyértelműen megfeleltethetők a -ben inverzióban álló elempároknak
    - valóban következik

1. **Determinánsok szorzástétele**
   * **Tétel**
     + bármely és -es mátrixokra:

# **11. tétel:** **Lineáris egyenletrendszer megoldhatósága**



[**BACK**](#_top)

**Tételcím**

-es lineáris egyenletrendszer egyértelmű megoldhatóságának jellemzése a determináns segítségével. Kapcsolat a lineáris egyenletrendszerek, az -beli generált altérhez tartozás kérdése, illetve a mátrixszorzáson alapuló mátrixegyenletek között. Kapcsolat négyzetes mátrix determinánsa, illetve a sorok és az oszlopok lineáris függetlensége között.

1. **Lineáris egyenletrendszer megoldhatósága**
   * **Tétel**
     + egy változós, egyenletből álló lineáris egyenletrendszer kibővített együtthatómátrixa
     + az egyenletrendszer akkor és csak akkor egyértelműen megoldható, ha
   * **Bizonyítás**
     + futtassuk -re Gauss-eliminációt
     + az algoritmus által megtett sorekvivalens lépések az együtthatómátrix determinánsát megváltoztatják ugyan, de annak nulla/ nemnulla mivoltán nem változtatnak
     + Gauss-elimináció az alábbi három lehetőség valamelyikével ér véget:
       - tilos sor: egyenletrendszer nem megoldható
       - egyenletrendszernek végtelen sok megoldása van:
         * kevesebb sor, mint oszlop (és fordítva), mivel eredetileg -es volt
         * az első fázis lépésében keletkeznie kellett csupa sornak, emiatt eredetileg is
       - egyenletrendszer megoldása egyértelmű:
         * RLA, determinánsa
         * főátlóban csupa
         * mindenhol máshol
         * mivel determináns végül nem , ezért eredetileg sem volt
2. **-n ekvivalens állítások**
   * **Tétel**
     + vektorok és -k egyesítésével keletkező -es mátrix
     + az alábbi állítások ekvivalensek:
       - **(1)** megoldható „mátrixegyenlet”
       - **(2)** megoldható az kibővített együtthatómátrixú lineáris egyenletrendszer
       - **(3)**
   * **Bizonyítás**
     + **(2)** és **(3)** állítás ekvivalens
     + **(3)** állítás teljesülése azt jelenti, hogy létezik a lineáris kombináció
     + vektor -edik koordinátája minden esetén
     + tehát az alsó és a felső egyenlet ekvivalens, és ezzel lineáris egyenletrendszert kapjuk
     + **(1)** és **(2)** ekvivalenciájához azt kell észrevennünk, hogy csak -beli oszlopvektor lehet
     + -edik koordinátája minden esetén -vel jelölve az szorzat -edik koordinátája a mátrixszorzás definíciója szerint
     + ezért azzal ekvivalens, hogy teljesül minden esetén ismét lineáris egyenletrendszert kapjuk
   * **Következmény:**
     + vektorok és -k egyesítésével keletkező -es mátrix
     + az alábbi állítások ekvivalensek:
       - lineáris egyenletrendszernek az egyetlen megoldása
       - vektorok lineárisan függetlenek
   * **Bizonyítás**
     + akkor és csak akkor lineárisan független, ha , triviális lineáris kombináció esetén
       - vagyis:
     + ez ekvivalens azzal, hogy lineáris egyenletnek egyetlen megoldása az, hogy minden változó értéke
3. **Sor/oszlopvektor lineáris függetlenség**
   * **Tétel**
     + -es mátrix
     + az alábbi állítások ekvivalensek:
       - **(1)** oszlopai, mint -beli vektorok, lineárisan függetlenek
       - **(2)**
       - **(3)** sorai, mint hosszú sorvektorok lineárisan függetlenek
   * **Bizonyítás**
     + **(1)** állítás az előző következmény miatt azzal ekvivalens, hogy az kibővített együtthatómátrixú lineáris egyenletrendszer egyértelműen megoldható
     + mivel négyzetes mátrix, ezért a lineáris egyenletrendszer megoldhatósága tétel szerint, akkor és csak akkor teljesül, ha (***(1)*** *és* ***(2)*** *állítás bizonyítva*)
     + **(2)** és **(3)** állítás közötti ekvivalenciához transzponáltjára alkalmazzuk az **(1)** és **(2)** állítás közötti, már bizonyított ekvivalenciát
     + mivel oszlopai megegyeznek soraival, és fordítva, ezért sorai akkor és csak akkor lineárisan függetlenek, ha
     + azonban transzponált-determináns tétel miatt ezért ez valóban ekvivalens feltétellel

# **12. tétel: Mátrix inverze, rangja**



[**BACK**](#_top)

**Tételcím**

Mátrix inverze, létezésének szükséges és elégséges feltétele, az inverz kiszámítása. Mátrix rangja, rangfogalmak egyenlősége, rang meghatározása.

1. **Inverz mátrix**
   * Definíció
     + egy -es *mátrix inverz*ének nevezzük az -es mátrixot, ha teljesül:
   * Jelölés
2. **Inverz mátrix létezése**
   * **Tétel**
     + -es mátrixnak akkor és csak akkor létezik inverze, ha
     + ha létezik, akkor az egyértelmű
   * **Bizonyítás**
     + TFH. létezik
     + megmutatjuk, hogy
     + definíció szerint egyenlet mindkét oldalának determinánsát véve: , ahol
       - alkalmazzuk szorzástételt:
3. **Inverz mátrix létezés lemmája**
   * **Tétel**
     + ha és akkor egyértelműen létezik mátrix, hogy
   * **Bizonyítás**
     + fenti szorzás ekvivalens, mátrixszorzás szerint a következővel:
     + az lineáris egyenletrendszer, amely úgy jelölhető, hogy
     + mivel ezért ez az egyenletrendszer egyértelműen megoldható
     + beláttuk a lemmát: a keresett -edik oszlopa a rendszer egyértelmű megoldása minden esetén
   * **Inverz kiszámítása Gauss-eliminációval**
     + egymás mellé felírjuk az -es mátrixot, valamint az -es egységmátrixot
     + lefuttatjuk a Gauss-eliminációt az -n, úgy, hogy sorekvivalens lépéseket megismételjük, az -n is
     + addig folytatjuk a Gauss-eliminációt, amíg az RLA-ban nem lesz
     + ekkor az
4. **Négyzetes részmátrix**
   * Definíció
     + -es mátrix és
     + válasszuk ki tetszőlegesen sorai és oszlopai közül - db
     + ekkor kiválasztott sorok és oszlopok kereszteződéseiben kialakuló -es mátrixot egy négyzetes *részmátrix*ának nevezzük
5. **Rang (1)**
   * Definíció
     + tetszőleges mátrix, azt mondjuk, hogy
       - ***oszloprang***ja , ha oszlopai közül kiválasztható db úgy, hogy a kiválasztott oszlopok lineárisan függetlenek, de már nem válaszható ki így
       - ***sorrang***ja , ha sorai közül kiválasztható db úgy, hogy a kiválasztott sorok lineárisan függetlenek, de már nem válaszható ki így
       - ***determinánsrang***ja , ha -nak van nemnulla determinánsú -es részmátrixa, de -es nemnulla determinánsú már nincs
6. **Rangfogalmak egyenlősége**
   * **Tétel**
     + minden mátrixra
   * **Bizonyítás**
     + elég belátni, hogy igaz minden mátrixra
     + mivel oszlopai megegyeznek soraival, ezért , valamint
     + mivel az -ből válaszható négyzetes részmátrixok az -ból választhatók transzponáltjai
     + legnagyobb nemnulla determinánsú is ugyanazon méretű
     + ha az állítást minden mátrixra, így -ra is igaznak feltételezzük, akkor összesítve az egyenlőséget kapjuk
     + csak -t kell bizonyítani:
     + először megmutatjuk, hogy , majd, hogy
     + TFH.
     + meg kell mutatnunk, hogy , vagyis, hogy oszlopai közül kiválasztható db lineárisan független
     + -ból miatt kiválasztható egy -es nemnulla determinánsú részmátrix
     + -nak abból az oszlopából álló mátrixa, amelyeket az készítésekor választunk ki
     + ekkor tehát sorai sorainak részhalmaza, és oszlopairól állítjuk, hogy lineárisan függetlenek
       - ha nem így volna, akkor (*a 11-es tételben levő következmény miatt*) lineáris egyenletrendszernek volna egy megoldása
       - ekkor azonban megoldása volna az lineáris egyenletrendszernek is, hiszen az utóbbi rendszert az előbbiből kapjuk
       - tehát oszlopai lineárisan összefüggők volnának, ami a sorvektor lineáris függetlenség tétele miatt (*előző tétel)* ellentmondana annak, hogy
       - így valóban igaz
     + ezt lemmával bizonyítjuk

**Mátrix oszlopok lineáris függetlenség lemmája**

* + **Tétel**
    - -es mátrix, amelynek az oszlopai (mint -beli vektorok) lineárisan függetlenek
    - ha , akkor sorai közül kiválasztható egy úgy, hogy ezt a sort elhagyva a kapott -es mátrix oszlopai szintén lineárisan függetlenek
  + **Bizonyítás**
    - oszlopai , az ezek által generált -beli altért
    - mivel -ben van elemű generátorrendszer, és F-G egyenlőtlenség miatt nem lehet benne elemű lineárisan független rendszer
    - -beli standard bázis vektorai között van olyan, amelyik nem tartozik -hez
    - ilyen, állítjuk, hogy -edik sora teljesíti a lemma feltételeit:
      * az elhagyásával a kapott mátrix oszlopai lineárisan függetlenek
    - TFI nem így van
      * lineáris egyenletrendszernek van egy megoldása
      * ekkor , mert oszlopai lineárisan függetlenek
      * mivel szorzat abban különbözik -től, hogy az utóbbiba a -edik helyre „beszúródik” a -edik sorának és a -nak a skaláris szorzata
      * ezért oszlopvektor -edik koordinátája egy szám, többi 0
      * következik, hogy
      * ez ellentmond annak, hogy
        + viszont ez ellentmond a 11.tétel Mátrixszorzás tételének
      * mely szerint a oszlopainak az kombinációja épp -t adja vissza, lemma bizonyítva
    - bizonyítás folytatása:
    - és válasszunk oszlopai közül lineárisan függetlent alkossák ezek mátrixot
    - mutassuk meg, hogy
    - sorainak számát -val jelölve oszlopai -beli vektorok, így az F-G egyenlőtlenség miatt
    - , akkor a fenti lemmát -re alkalmazva kapjuk a -es mátrixot, amelynek az oszlopai továbbra is lineárisan függetlenek
    - ha , akkor ismét alkalmazhatjuk a lemmát -re és ezt folytathatjuk egészen amíg lépés után egy -es mátrixot kapunk
    - (*11. tétel Sorvektor lineáris függetlenség tétel miatt*)
    - mivel az -nak -es részmátrixa, ezért ez bizonyítja , és a tételt is

1. **Rang (2)**
   * Definíció
     + az mátrix rangjának nevezzük az közös értékét
   * Jelölés
2. **Rang kiszámolása (1)**
   * **Tétel**
     + -es mátrix és az oszlopai legyenek
     + ekkor
   * **Bizonyítás**
     + válasszuk ki oszlopai közül a legtöbbet úgy, hogy ezek lineárisan függetlenek legyenek
     + oszloprang definíció szerint ekkor
     + állítjuk, hogy bázist alkot a altérben
     + be kell látni, hogy generátorrendszer -ben
     + , lássuk be, hogy
     + esetén lineárisan összefüggő, mivel -ból lineárisan független oszlopot nem lehet kiválasztani
     + az Újonnan érkező vektor lemmája szerint ekkor , tehát mind -beli
     + mivel altér, ezért minden -beli, tehát vektorokból lineáris kombinációval kifejezhető vektor is -beli kell, hogy legyen
     + bizonyítottuk, hogy
3. **Rang kiszámolása (2)**
   * **Tétel**
     + az elemi sorekvivalens lépések a mátrix rangját nem változtatják meg
     + a LA mátrix sorainak a száma egyenlő a mátrix rangjával
   * **Bizonyítás**
     + (*elemi sorekvivalens lépések bizonyítása)*
     + válasszunk ki oszlopai közül tetszőleges néhányat, ezek együtt az
     + oszlopai az előző tétel Következménye miatt akkor és csak akkor lineárisan független, ha az lineáris egyenletrendszernek az egyetlen megoldása
     + amikor -ra alkalmazzuk valamelyik elemi sorekvivalens lépést, akkor ugyanezt alkalmazzuk az kibővített együtthatómátrixra is
     + egyrészt sorai az sorainak részei, másrészt, ha a jobb oldalakon csupa 0 áll, akkor ezt a tulajdonságot mindegyik elemi sorekvivalens lépés fenntartja
     + azonban -n végzett lépések az lineáris egyenletrendszer megoldásait nem változtatják meg
     + -n végzett elemi sorekvivalens lépések nem változtatnak azon, hogy oszlopai lineárisan függetlenek-e
     + így oszlopai közül kiválasztható legnagyobb lineárisan független rendszer mérete, vagyis az oszloprang se változik
     + (*LA mátrix sorainak száma egyenlő a… bizonyítás)*
     + ha a LA mátrix sorainak száma , akkor -ból az összes sor és a vezéregyeseket tartalmazó oszlopok kiválasztásával keletkező négyzetes részmátrix egy felsőháromszög-mátrix
     + ennek főátlójában minden elem 1 (vezéregyesek)
     + így vagyis -nak van -as, nemnulla determinánsú négyzetes részmátrixa
     + ennél nagyobb nyilván nincs, mert -nak csak sora van
     + tehát determináns rangja valóban

# **13. tétel:** **Lineáris leképzés, transzformáció**



[**BACK**](#_top)

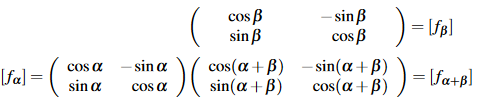
**Tételcím**

Lineáris leképzés fogalma, mátrixa. Szükséges és elégséges feltétel egy függvény lineáris leképzés voltára. Lineáris leképzések szorzata, szorzat mátrixa. Következmény: addíciós tételek a sinus és cosinus függvényekre. Lineáris transzformáció invertálhatósága.

1. **Lineáris leképzés**
   * Definíció
     + *lineáris leképzés*nek hívjuk, ha
       - létezik olyan -es mátrix, melyre minden
       - esetben -et *lineáris transzformáció*nak is nevezzük
       - ha leképzésnek és minden -re, akkor mátrixa
   * Jelölés
     + *(3. állítás jelölése)*
2. **Lineáris leképzés feltétele**
   * **Tétel**
     + függvény akkor és csak akkor lineáris leképzés, ha:
       - **(1)** igaz minden
       - **(2)** igaz minden és esetén
     + ha teljesíti ezt a 2 tulajdonságot, akkor:
       - egyértelmű
       - és azonos azzal a -es mátrixszal, melynek minden esetén az -edik oszlopa
   * **Bizonyítás**
     + (*szükségesség belátása*)
     + TFH. lineáris leképzés és
     + *(10. tétel, Mátrixműveletek tétel, Megjegyzések: mátrixszorzás összeadásra nézve disztributivitás miatt:)*
     + *(10. tétel, Mátrixműveletek tétel, Megjegyzések: mátrixszorzás asszociativitás miatt:)*
     + (*egyértelműség belátása*)
     + -nek egyik mátrixa, -nak -edik oszlopa minden -re
     + *(10. tétel, Mátrixszorzás definíció miatt:)*
     + ebből miatt:, amely bizonyítja egyértelműségét
       - csak az a mátrix lehet, amelynek -edik oszlopa , vagyis csak
     + (*elégségesség bizonyítása*)
     + ha az első 2 tulajdonság teljesül, akkor lineáris leképzés
     + mutassunk olyan mátrixot, amelyre: minden
     + mátrix -edik oszlopa minden -re, jelölje
     + ekkor: teljesül vektorokra
     + belátjuk, hogy (1) tagú összegekre is teljesül
       - vagyis egymás után alkalmazva az (1)
     + tetszőleges -edik koordinátáját jelölje: , ekkor:

((

1. **Lineáris leképzés szorzata**
   * **Tétel**
     + és lineáris leképzések
     + ezeknek a szorzata is lineáris leképzés, melyre
   * **Bizonyítás**
     + , minden -re,
     + , minden -re,
     + alkalmazzuk a függvényt tetszőleges -re
       - tehát
2. **Addíciós tételek**
   * **Tétel**
     + tetszőleges és szögekre teljesülnek az alábbi összefüggések
   * **Bizonyítás**
     + a síkban az origó körüli szöggel való elforgatás
     + ezek lineáris leképzések
     + alkalmazzuk a fenti *Lineáris leképzés szorzata tételt*
     + igaz, hogy az origó körüli szögű elforgatással
       - hiszen egy tetszőleges -t először , majd szöggel elforgatva ugyanazt kapjuk, mintha szöggel forgattuk volna
     + és lineáris transzformációk mátrixa kiolvasható az állításból, ezekre lineáris leképzés szorzata fennáll:



1. **Lineáris transzformáció invertálhatósága**
   * **Tétel**
     + lineáris transzformáció akkor és csak akkor invertálható, ha
     + ha ez a feltétel fennáll, akkor , vagyis az inverz transzformáció mátrixa az mátrixnak az inverze
   * **Bizonyítás**
     + , vagyis minden
     + (*szükségesség bizonyítása)*
     + ha invertálható, akkor
     + TFI , ekkor (*8. tétel, Lineáris egyenletrendszer megoldhatósága tétel miatt)* oszlopai lineárisan összefüggők, ellentmond annak, hogy invertálható
     + (*elégségesség bizonyítása)*
     + ha , akkor invertálható
     + mivel , ezért (*12. tétel, Inverz mátrix tétel miatt)* létezik inverz mátrix
     + tetszőleges esetén azt jelenti, hogy
     + tehát függvény azonos az inverzével

# **14. tétel: Magtér, képtér**



[**BACK**](#_top)

**Tételcím**

Lineáris leképzések magtere, képtere, ezek altér volta. Dimenziótétel.

1. **Magtér, képtér**
   * Definíció
     + lineáris leképzés
     + *magter*e:
       - jelölés:
       - azon -beli vektorok halmazát (, melyeknek a képe az -beli
     + *képter*e:
       - jelölés:
       - azon -beli vektorok halmazát (, melyek megkaphatók (legalább) 1 alkalmas -beli vektor -fel vett képeként
2. **Mag - és képtér altér volta**
   * **Tétel**
     + lineáris leképzés, ekkor
       - , vagyis altér -ben
       - , vagyis altér -ban
   * **Bizonyítás**
     + *bizonyítása)*
     + *(6. tétel, alterei definíció miatt)* meg kell mutatnunk, hogy bármely és esetén
       - teljesülnek
     + ha , akkor és
     + *(13. tétel, Lineáris leképzés feltétele tétel tulajdonság (1) miatt)*
     + *(13. tétel, Lineáris leképzés feltétele tétel tulajdonság (2) miatt)*
       - nem lehet üres, hiszen definíció szerint mindig igaz
     + *bizonyítása)*
     + ha , akkor definíció szerint azokból az vektorokból áll, melyek kifejezhetők alakban
     + *(11. tétel, Mátrixszorzás tétel szerint)* ez ekvivalens , ahol oszlopait -k jelölik
     + generált altér
3. **Dimenziótétel**
   * **Tétel**
     + ha lineáris leképzés, akkor
   * **Bizonyítás**
     + , válasszunk egy tetszőleges bázist -ben, amely lineárisan független
     + *(7. tétel, Bázis létezése tétel szerint)* ez a rendszer kiegészíthető egy bázisává
     + mivel , kellenek további vektor szükséges:
     + megmutatjuk, hogy rendszer bázis -ben
     + lássuk be: generátorrendszer -ben
     + tetszőleges, ekkor valamely
     + mivel generátorrendszer -ben, ezért kifejezhető lineáris kombinációjukként
       - utolsó lépésben felhasználjuk, hogy
       - tetszőlegesen választott kifejezhető lineáris kombinációja
     + most belátjuk, hogy lineárisan független
     + TFH.
     + meg kell mutatnunk, hogy *(7. tétel, Standard bázis tétele miatt)* ekkor
     + ebből definíció szerint → kifejezhető lineáris kombinációjaként
       - azonban lineárisan független
       - triviális lineáris kombinációja adhatja
       - megmutattuk, hogy lineárisan független, így bázis is

# **15. tétel: Bázistranszformáció**



[**BACK**](#_top)

**Tételcím**

Bázistranszformáció fogalma, lineáris transzformáció mátrixa adott bázis szerint, annak kiszámítása.

1. **Bázistranszformáció**
   * **Tétel**
     + lineáris transzformáció és egy -es mátrix, melynek oszlopai bázist alkotnak -ben
     + az a függvény, mely minden esetén -hez -t rendel
     + ekkor is lineáris transzformáció, melynek mátrixa
   * **Bizonyítás**
     + oszlopai akkor és csak akkor alkotnak bázist, ha
     + alteres következmény szerint bázisai az tagú lineárisan független rendszerek
     + *(11. tétel, Sorvektor lineáris függetlenség tétel miatt)* oszlopainak lineáris függetlensége ekvivalens
     + *(12. tétel, Inverz mátrix létezése tétel miatt)* inverz mátrix valóban létezik
     + folytatáshoz lemmát használunk
     + folytatva a tételt a lenti lemma segítségével:
     + függvény azonos függvénnyel
     + ha -re alkalmazzuk -t, akkor -et kapjuk, erre -et alkalmazva -et kapjuk, végül erre -et alkalmazva -t kapjuk
     + *(13. tétel, Lineáris leképzés szorzata tétel miatt)*  valóban lineáris transzformáció, mátrixa:
2. **Bázistranszformáció lemmája**
   * **Tétel**
     + az a függvény, mely minden esetén -hez -et rendel
     + ekkor lineáris transzformáció, melynek mátrixa
   * **Bizonyítás**
     + -re koordinátavektor -edik koordinátája minden esetén
     + ekkor
     + *(10. tétel, Mátrixszorzás definíciója szerint)* azonos oszlopaiból koordinátáival, mint együtthatókkal képzett lineáris kombinációval
     + így , amely mutatja, hogy a függvény lineáris transzformáció, melynek mátrixa
     + mivel , ezért *(13. tétel, Lineáris transzformációk invertálhatósága tétel szerint)* inverz transzformáció is létezik, mátrixa:
     + ez minden esetén -hez -et rendel
3. **Lineáris transzformáció adott bázis szerint**
   * Definíció
     + *lineáris transzformáció* és bázis -ben
     + ekkor lineáris transzformáció mátrixát az transzformáció bázis szerinti mátrixának nevezzük
   * Jelölés
4. **Lineáris transzformáció kiszámítása adott bázis szerint**
   * **Tétel**
     + ! lineáris transzformáció
     + egy -es mátrix, melynek oszlopai bázist alkotnak -ben
     + ekkor mátrixra alábbiak teljesülnek:
       - **(1)** minden -re
       - **(2)**
       - **(3)** -edik oszlopa egyenlő koordinátavektorral minden esetén
   * **Bizonyítás**
     + **(2)** már beláttuk az előző tétel bizonyításában
     + **(1)** *közvetlenül következik a Lineáris transzformáció adott bázis szerinti definíciójából és annak tételéből*
       - mivel annak a lineáris transzformációnak a mátrixa, amely minden -re -t rendel, az állítás igaz
     + **(3)** *(13. tétel, Lineáris leképzés feltétele tétel következménye)*:
       - mivel a lineáris transzformáció mátrixa, ezért -edik oszlopa -vel egyenlő minden -re
       - *(7. tétel, Koordinátavektor definíciója szerint)* éppen koordinátavektora
       - vagyis:

# **16. tétel:** **Sajátvektor, karakterisztikus polinom**



[**BACK**](#_top)

**Tételcím**

Négyzetes mátrixok sajátértékei és sajátvektorai, ezek meghatározása. Karakterisztikus polinom. A sajátértékek és sajátvektorok kapcsolata lineáris transzformáció valamely bázis szerinti mátrixának diagonalitásával.

1. **Sajátérték, sajátvektor**
   * Definíció
     + -es mátrix
     + ***sajátérték***
       - olyan skalár
       - ha létezik olyan vektor, melyre
     + ***sajátvektor***
       - olyan vektor
       - ha létezik olyan skalár, melyre
     + röviden:
       - ha , akkor sajátértéke, sajátvektora -nak
2. **Sajátérték meghatározása**
   * **Tétel**
     + négyzetes mátrixnak a skalár akkor és csak akkor sajátértéke, ha
   * **Bizonyítás**
     + definíció szerint akkor sajátérték, ha , van megoldása
     + írhatunk helyett
     + *(10. tétel, Mátrixműveletek tétel (1) szerint)*
     + egyenletet átrendezve, majd *(Mátrixműveletek tétel (2) szerint):*
     + akkor és csak akkor sajátértéke -nak, ha az lineáris egyenletrendszernek van megoldása
     + *a következmény szerint* ekvivalens mátrix oszlopai lineárisan összefüggőek
     + *(11. tétel, Sorvektor lineáris függetlenség tétel szerint)* valóban azzal ekvivalens, hogy
3. **Karakterisztikus polinom**
   * Definíció
     + -es mátrix *karakterisztikus polinom*jának nevezzük a determináns értékét, ahol változó
   * Jelölés
   * (*sajátérték definíciója átfogalmazva az előző tétel és definíció felhasználásával:* 
     + *mátrix sajátértékei a karakterisztikus polinom gyökei, tehát egyenlet megoldásai*
     + *algebra egyik tétele szerint tehát -edfokú polinomnak legfeljebb gyöke lehet* -*es mátrixnak legfeljebb sajátértéke van)*
4. **Diagonális mátrix**
   * Definíció
     + -es mátrix akkor nevezzük *diagonális mátrix*nak, ha minden esetén teljesül
5. **Kapcsolat sajátérték és lineáris leképzések közt**
   * { tetszőleges bázis
   * TFH. mátrix diagonális, a főátlóban álló elemeket jelölje sorba
   * -edik oszlopa -vel egyenlő
   * ebből kifolyólag , ez viszont azt jelenti, hogy

, vagyis

* + összefoglalva:
    - akkor lesz diagonális, ha minden tagjára teljesül valamilyen skalárral