BSZ1 vizsga

Balassa Ádám

# 1. Számelmélet alapjai

## Definíciók

* Oszthatóság
  + a | b ha létezik olyan c melyre a \* c = b (a b c egész számok)
  + Jelölés, a nem osztója b-nek jelölés
* Prímszám
  + p prímszám, ha |p| > 1, de nincs valódi osztója, vagyis p = a \* b, csak akkor ha a és b = 1 vagy -1
* Kongruencia
  + a kongruens b (mod m), ha a-t és b-t m-mel maradékosan osztva ugyanakkora maradékot kapunk
  + m: modulus (zárójelbe rakjuk)
  + m != 0

## Tételek

* Számelmélet alaptétele
  + Minden prím és összetett szám (minden szám ami != 0, 1, -1) felírható prímszámok szorzataként
  + Egyértelműen
  + Előjel és sorrendtől eltekintve
  + **BIZONYÍTÁS**
    - Felírjunk egy n számot a1, a2, … ak szorzataként
    - ha ezek prímek akkor megvagyunk
    - Ha valamelyik nem prím, azt helyettesítjük egy másik szorzatként
      * Ha az a szorzat is prímekből áll akkor megvagyunk, egyébként azt is tovább bontjuk
    - Mivel minden tényező > 2 és a szorzat hossza lépésenként nő, így az algoritmus le fog állni (log2n-nél kevesebb lépést végzünk)
* *Oszthatóság feltétele*
  + a kanonikus alakja p1^k1 \* p2^k2 \* … \* pn^kn, b-jé ugyanez csak l1, l2… ln hatványokkal
  + a | b akkor és csak akkor ha ki <= li minden i-re
  + TRIVIÁLIS
* *LNKO, LKKT*
  + (a, b) = p1 ^ min(k1, l1) \* p2 ^ min(k2, l2)… \* pn ^ min(kn, ln)
  + [a, b] = p1 ^ max(k1, l1) \* p2 ^ max(k2, l2)… \* pn ^ max(kn, ln)
* Végtelen prím van
  + Indirekt tegyük fel h véges sok prím van: p1, p2, p3, …, pn
  + p1 \* p2 \* p3 \*…\*pn + 1 nem osztható egyikkel sem, de a számelmélet alaptétele szerint felírható prímszorzatként, úgyhogy vagy egy új prím, vagy van egy olyan prímtényezője amit nem ismertünk => ellentmondás
* Prímek távolsága
  + Minden N-hez találunk olyan p és q prímeket, hogy köztük ne legyen más prímszám
  + N > 1
  + q – p > N
  + *BIZONYÍTÁS*
    - Vegyük azokat az a számokat melyek úgy állnak elő, hogy (N + 1)! + i, ahol i = 2, 3, 4, 5, .., N + 1
    - Ezek a számok szomszédosak, többen vannak mint N és mind összetettek, i minden értéke egyszer már jelen van az (N + 1)! szorzatban, így minden i-re ez a szám k \* i + i, ami osztható i-vel
* Nagy Prímszámtétel
  + pi(n) megadja, hány n-nél kisebb prím van
  + pi(n) = n / ln(n) elég nagy n-ekre
  + lim(n 🡪 végtelen) pi(n) / (n / ln(n)) = 1
* **a kongruens b mod m akkor és csak akkor, ha m | a – b**
  + a = k1 \* m + r, b = k2 \* m + r
  + a – b = k1 \* m – k2 \* m = (k1 – k2) \* m, vagiy osztható m-mel
* **Műveletek kongruenciákkal**
  + a kongruens b (m) és c kongruens d (m)
    - m | (a - b) és m | (c - d)
  + a + c kongruens b + d (m)
    - m | (a - b) + (c – d) vagyis m | (a + c) – (d + b)
  + a - c kongruens b - d (m)
    - m | (a - b) - (c – d) vagyis m | (a - c) – (d - b)
  + c\*a kongruens d\*b (m)
    - m | c(a - b) = ac – bc ill. m | b(c - d) = bc – bd
    - m | ac – bc + bc – bd = ac – bd
  + a ^ k kongruens b ^ k (m)
    - következik az előzőből ha c = a és d = b
  + a / c kongruens b / c (m / (m, c)), feltéve hogy c osztója a-nak és b-nek
    - c’ = c / (m, c) és m’ = m / (m, c)
    - m | c \* (a / c – b / c) 🡨🡪 m’ | c’ (a / c – b / c)
    - (c’, m’) = 1 (mert a legnagyobb közös osztóval vannak leosztva)
    - Emiatt m’ | a / c – b / c

# 2. Lineáris kongruenciák

## Tételek

* **ax kongruens b (m) akkor és csak akkor oldható meg, ha (a, m) | b. Ekkor a megoldások száma (a, m)**
  + Szükségesség (ha megoldható)
    - Ha megoldható akkor van egy x0 megodlás, melyre igaz, h ax0 kongruens b (m)
    - (a, m) osztója m-nek (így ax0 – b-nek is) és a-nak (tehát a \* x0-nak is)
    - Ebből (a, m) | ax0 – (ax0 – b) vagyis (a, m) | b
  + Elégségesség (ha b osztható)
    - (a, m) = 1
      * ekkor (a, m) | b-t triviálisan igaz
      * Ha a \* x-be x helyére behelyettesítjük az 1, 2, 3, 4, … m számokat
      * Ekkor minden ax különböző maradékot ad
        + Ha ugyanakkora maradékot adnának akkor igaz lenne az ax1 kongruens ax2 (m), így mivel (a, m) = 1 így az x1 kongruens x2 (m), ami lehetetlen, hiszen nem egyenlőek de 0 és m-közé kellene esniük
      * Ekkor viszont mivel m, legfeljebb m-féle maradékot adhat és találtunk mdb különböző maradékot, így az egyik jó megoldás lesz, az egyenlet megoldható
    - (a, m) > 1
      * Az alapfeltevésünk, hogy (a, m) | b-t, így leosztunk (a, m)-mel
      * A kapott kongruenciarenszer megoldható, mert az osztás után kapott a’ és m’ már relatív prímek, erre az esetre pedig már beláttuk az állítást
    - A megoldások száma (a, m)
      * Ha (a, m) = 1, akkor láttuk, hogy 1 megoldása van az egyenletnek
      * Másik esetben a megoldások az x = k \* m’ + x0, k < (a, m)
      * Ez épp (a, m) db megoldás
* *ax + by kongruens c (m) akkor oldható meg, ha (a, b) | c*
* az x kongruens a1 (m1) x kongruens a2 (m2) kongruenciarendszer akkor oldható meg, ha (m1, m2) | a2 – a1 és a megoldást mod [m1, m2] kapjuk meg
  + Az első egyenletből x = m1\*k + a1
  + a második egyenletbe helyettesítve m1\*k kongruens a2 – a1 (m2)
  + A feladatot k-ra rendezve, majd x-be helyettesítve egy m1 \* m2 / (m1, m2) modulusú megoldást kapunk ami épp [m1, m2]-vel egyezik meg
* **Euklideszi algoritmus** működik (rk = (a, m))
  + (m-met osztjuk a-val)
  + 1. lépés következménye: m kongruens r1 (a)
  + mivel ekkor viszont (m, a) = (a, r1)
  + Úgyhogy folytathatjuk az eukideszi algoritmust
* Az Euklideszi algoritmus hatékony
  + Legyen egy tetszőleges lépésben r1 = t \* r2 + r3
  + Ekkor tudjuk r1 > r2 >= r3
  + Vagyis mivel t >= 1 így r1 > r2 + r3 > 2 \* r3 🡪 két lépésenként feleződik a kapott maradék
  + a > 2r2 > 4r4 > … > 2^k \* r2k 🡪a-tól rk-ig log2(4) lépés van

# 3. Euler-Fermat tétel

## Definíciók

* Euler féle fi függvény
  + az 1, 2, 3, …, n számok közül az n-hez relatív prímek számát fi(n)-nel jelöljük
  + n >= 2
  + az f(n) = fi(n) függvény az Euler féle fi fv
* Redukált maradékrendszer
  + R = {c1, c2, c3… cfi(m)} egy redukált maradékrendszer modulo m, ha minden eleme relatív prím m-mel, bármely két eleme nem kongruens modulo m, így fi(m) eleme van

## Tételek

* Ha a kongruens b (m) igaz, akkor (a, m) = (b, m)
  + m | a – b 🡪 b = k\*m + a
  + (a, m) | a, m, így k\*m + a-t, vagyis b-t is
  + Ekkor tudjuk, hogy (a, m) <= (b, m), hiszen osztója b-nek és m-nek de az LNKO-juknál nem lehet nagyobb
  + a és b szerepe szimmetrikus, így (b, m) <= (a, m) vagyis egyenlőek
* fi(n) kiszámítása
  + fi(n) = (p^a1 – p^a1-1)(p^a2 – p^a2 -1)……
  + **BIZONYÍTÁS**
    - Ha n prímszám akkor fi(n) = p - 1, hiszen minden nála kisebb szám relatív prím hozzá
    - Ha n = p^a, vagyis egy prímszám hatványa, fi(n) = p^a – p^(a-1), hiszen minden szám (p^a db) relatív prím hozzá, kivéve p többszöröseit. Mivel minden p-edik szám p többszöröse így p^a / p db ilyen szám van így fi(n) = p^a – p^(a-1)
    - Mivel fi(n\*m) = fi(n)fi(m) így a tétel már triviális
* Ha R = {c1, c2, …ck} egy r.m.r. modulo m, akkor R’ = {a\*c1, a\*c2, …, a\*ck} is r.m.r mod m, ha (a, m) = 1
  + R’ minden eleme relatív prím m-hez, hiszen mind a, mind ci relatív prím m-hez minden i-re
  + R’ egyik eleme sem kongruens egy másikkal hiszen ha a\* ci kongruens lenne a\*cj (m) bármely i-re és j-re, akkor ci is kongruens lenne cj amiről tudjuk, hogy lehetetlen
  + R és R’ elemszáma triviálisan megegyezik
* Euler-Fermat tétel
  + Ha (a, m) = 1, akkor a^(fi(m)) kongruens 1 (m)
  + a és m >= 2
  + BIZONYÍTÁS
    - R és R’ redukált maradékrendszerek ci’ = a\*ci
    - Mivel R és R’ elemeit párokba lehet állítani az m-mel adott maradékuk szerint, így elemeik szorzata kongruens lesz egymással
    - Ekkor c1 \* c2 \* …\* ck kongruens ac1 \* ac2 \* … \* ack mod m és mivel minden ci relatív prím m-mel, így leoszthatunk c1\*c2\*…\*ck-val
    - a^(fi(m)) kongruens 1 (m)
* *Kis-Fermat tétel*
  + Ha p prímszám akkor minden a-ra a^p kongruens a (m)
  + BIZONYÍTÁS
    - Mivel p prím így a-val relatív prímek és p>=2
    - fi(p) = p – 1
    - Euler-Fermat tételt alkalmazzuk és felszorzunk a-val

# 4. Algoritmusok, RSA

## Definíciók

* Carmichael szám
  + Olyan m szám, melyhez nem létezik olyan a szám melyre a ^ m-1 kongruens 1 (m)
  + (a, m) = 1

## Tételek

* Ha m-nek létezik árulója, akkor legalább annyi árulója van mint cinkosa a hozzá relatív prímek között
  + Legyen c1, c2, c3…ck az m szám összes cinkosa, és a egy árulója és ai = (a \* ci modulo m)
  + Mivel ai kongruens a \* ci (m) így igaz, hogy (a, m) = 1, (ci, m) = 1, (a \* ci, m) = 1, (ai, m) = 1
  + Emeljük ezt a kongruenciát m – 1-edikre
  + ai^(m - 1) kongruens a^(m - 1)\*ci^(m - 1) (m)
  + Ebből a (m - 1)-ediken nem kongruens 1-gyel, mert a áruló, ci meg cinkos így a kongruencia jobb oldala nem 1
  + Tudjuk, hogy egyik ai sem egyezik meg egyik aj-vel sem, hiszen egyik ci sem egyezik meg egyik cj-vel

## Algoritmusok

* Ismételt négyzetreemelések módszere
  + Egy a számot modulo m hatványozunk k-adik kitevőjére
  + k felírható ilyenkor kettő hatványok szorzataként, így a^k is felírható kettőhatványú kitevőjű a-k szorzataként
  + Egyesével kiszámoljuk l = log2(k)-ig a^l mod(m) értékeit, majd ezek szorzata a hatvány modulo m
* Prímtesztelés
  + Van egy m szám amit vizsgálunk, és válasszunk 100 véletlen a számot
  + Megvizsgáljuk euklideszi algoritmussal, hogy (a, m) mennyi
  + Ismételt négyzetreemelések módszerével ellenőrizzük a^m-1 mod m értékét
  + Ha valamelyik (a, m) vagy a^m-1 mod m nem 1 akkor m értelemszerűen nem prím, ha nem, akkor sansz h prím
  + Ha m Carmichael szám akkor szopacs van, erre van a Miller-Rabin teszt ami jobban kikérdezi a tanúkat
    - Előre kitalálja melyik az a t >= 1 és c szám melyre m – 1 = 2^t \* c
    - Ekkor nem a^m-1 mod m-et ellenőrzi, hanem a^(2^i \* c) mod m értékeit minden i < t-re
* RSA
  + C(x): x 🡪 (x^c mod N) valamely (c, N) = 1 c-számra
  + D(y): y 🡪 y^d mod N ami = 1
    - Ehhez c \* d kongruens 1 (fi(N)) szükséges, hiszen (x^c mod N) ^ d kongruens kell legyen x-szel, vagyis x^(c\*d) kongruens kell legyen x-szel mod N
    - A fenti állítás az x^(k \* fi(m) + 1) kongruens x (mod N) tételt használja minden N = p \* q számra
  + Közzéteszik ehhez c-t és N-t, ám aki ismeri p-t és q-t az ki tudja számolni fi(N)-t, így Euklideszi algoritmussal d is.

# 5. Koordináta geometria

## Tételek

* Műveletek térvektorokkal
  + Összeadás, kivonás, szorzás skalárral, skaláris szorzat
* **Egyenes egyenletrendszere**
  + v irányvektor: (a, b, c), P pont: (x0, y0, z0)
  + a, b, c != 0
    - (x – x0) / a = (y - y0) / b = (z – z0) / c
  + a = 0, b != 0, c != 0
    - x = x0, a többi marad
  + a = 0, b = 0, c != 0
    - x = x0, y = y0, a többi marad
  + BIZONYÍTÁS
    - P0 akkor eleme e egyenesnek ha létezik olyan lambda mellyel v-t szorozva P0-ból P-t kapjuk
    - Ezzel a lambda értékkel koordinátánként szorozzuk a vektorokat, ebből lambdát kifejezve közös értéket kell kapnunk
* **Sík egyenlete**
  + n normálvektor: (a, b, c), P0 pont: (x0, y0, z0)
  + P (x, y, z) akkor van rajta a síkon ha ax + by + cz = ax0 + by0 + cz0
  + BIZONYÍTÁS
    - P akkor van rajta a síkon ha a PP0 vektor merőleges n-re, vagyis skaláris szorzatuk 0
    - PP0 = (x – x0, y – y0, z – z0)
    - PP0 \* n = 0 = ax – ax0 + bx – bx0 + cx – cx0 = 0
* **Vektoriális szorzat**
  + v × u hossza v \* u \* sin(alpha), merőleges u-v síkjára (jobbsodrású rendszert alkot)
  + Ez egyenlő az (i u1 v1)(j u2 v2)(k, u3 v3) mátrix determinánsával
* R-ad3 generálása
  + Két közös síkra de nem közös egyenesre eső térvektor bázis azon a síkon (minden v vektor kifejezhető lineáris kombinációjukként)
  + 3 térvektor melyek közül egyik kettő sem esik közös síkra, bázis a térben
  + BIZONYÍTÁS
    - v O-ból mutasson P-be, vegyük fel azt a Q pontot, mely a metszéspontja az origóból a irányba és P-ből b irányba mutató egyeneseknek
    - Mivel v O-ból P-be mutat így kifejezhető OQ és QP vektorok összegeként, ahol OQ = alfa \* a és QP = beta \* b
  + BIZONYÍTÁS
    - Legyen R az a pont amely a és b síkját metszi P pontból c irányban
    - Ekkor v = OR + RP ahol OR az előző tétel alapján kifejezhető a-ból és b-ből, RP pedig gamma \* c

# 6. Rn beli vektorok

## Definíciók

* Műveletek vektorokkal
  + Rn beli vektorok n db valós számból álló számoszlopok
  + Összeg: olyan vektor melynek koordinátái a megfelelő koordináták összege
  + Skalárral vett szorzat: minden koordináta szorzódik az adott skalárral
* Altér
  + V <= Rn, ha zárt összeadásra és skalárral szorzásra
  + V vektoroknak olyan halmaza, melyben bármely két vektor összege, vagy szorzata bármely skalárral szintén eleme V-nek
* Lineáris kombináció
  + adottak v1, v2, v3… vk és lambda1, lambda2… lambdak skalárok
  + a v1\*lambda1 + … + vk\*lamdak vektor a v vektorok lambdák szerinti skaláris szorzata
* Generált altér
  + a v1, v2, … vk Rn beli vektorok lineáris kombinációjából kifejezhető vektorok a halmaza a v1, v2 … vk vektorok generált altere
  + <v1, v2, … vk>-val jelöljük (a vektorok ekkor generátorrendszerek az altérben)
* Lineáris függetlenség
  + v1, v2, v3… vk vektorok linárisan függetlenek, ha egyik sem fejezhető ki a többi lineáris kombinációjaként

## Tételek

* Vektor műveletek tulajdonságai
  + Összeadás kommutatív és asszociatív
  + Skalárral szorzás kommutatív és asszociatív
  + Skalárral szorzás disztributív vektorok összegére
  + Vektorral szorzás disztributív skalárok összegére
* A generált altér egy altér
  + Meg kell mutatni h zárt összeadásra és skalárral szorzásra
  + Összeadáskor kiemelünk v1-et v2-t stb. és belátjuk h az is egy lineáris kombináció
  + Skalárral szorzásnál meg… Azt sztem mindenki látja
* Lineáris függetlenség feltétele
  + v1, v2…, vk vektorok lineáris függetlensége ekvivalens azzal, h a vektorok nullvektort adó lineáris kombinációja a triviális lineáris kombináció
  + BIZONYÍTÁS
    - Ha ez csak a triviális lin.komb. akkor független
      * Indirekt feltesszük, hogy nem is függetlenek
      * Ekkor az egyik v (mondjuk v1) kifejezhető a többiből
      * Rendezzük ezt 0-ra, ekkor sikerült 0-t kapnunk úgy, hogy v1 együtthatója 1, vagyis ellentmondásra jutottunk
    - Ha független akkor csak a triv.lin.komb. a jó
      * Tegyük fel indirekt hogy lambda1 nem 0 mégis kifejeztük a nullvektort
      * Ekkor rendezzük az egyenletet v-re, vagyis osszunk le lambda1-gyel és vonjunk ki mindent
      * Ekkor kifejeztük v-t, vagyis ellentmondásra jutottunk
* Az újonnan érkező vektor lemmája
  + Ha f1, f2, … fk lineárisan független de fk+1-et hozzárakva már összefüggő, akkor fk+1 benne van f-ek generált alterében
  + BIZONYÍTÁS
    - fk+1 hozzádaása után vegyük azt a 0-t adó lin.komb.ot ahol nem minden együttható 0
    - Ekkor fk+1 együtthatója nem 0, mert különben eddig is összefüggő lett vna a rendszer
    - Ekkor rendezzük az egyenletet fk+1-re, leosztunk az együtthatójával és kifejeztük fk+1et
* Kicserélési lemma
  + Ha veszünk k-db független és m db generátor vektort egy altérben, akkor a független rendszer bármely vektorához találok a generátorrendszerből olyat, mellyel ha kicserélem, a függetlenség igaz marad
  + BIZONYÍTÁS
    - Tegyük fel indirekt, hogy ez nem igaz, tehát fi nem cserélhető ki
    - Ez azt jelenti, hogy kipróbálva g1, g2, g3 stb. vektorokat az eddig független rendszer összefüggővé vált, így az újonnan érkező vektor lemmája szerint f-ek fi nélkül generálják a generátorrendszer összes elemét
    - Ez azt jelentené, hogy akkor generálják a teljes alteret, ami lehetetlen, hisz fi is eleme az altérnek, és azt tudjuk, hogy nem generálják, tehát ellentmondásra jutottunk
* **F-G egyenlőtlenség**
  + Ha egy altérben van egy k elemű független rendszer és egy m elemű generátorrendszer, akkor k <= m
  + BIZONYÍTÁS
    - A kicserélési lemmát alkalmazzuk a független rendszer összes elemére
    - Ekkor kiválasztottunk kdb különböző elemet g-ből (hiszen független elemeket választottunk), vagyis m-ből legalább kdb kiválasztható volt így m >= k

# 7. Bázisok

## Definíciók

* Bázis
  + Egy V altérben b1, b2, … bk vektorokat bázisnak nevezzük, ha lineárisan függetlenek és generálják V-t
* Dimenzió
  + Egy altér dimenziója a bázisainak elemszáma
  + Vagyis ha b1, b2…, bk egy bázis akkor dimV = k
* Koordinátavektor
  + B legyen egy V-beli bázisvektorok halmaza.
  + v egy x vektor B szerinti koordinátabektora, ha x b-vel vett lineáris kombinációjában b1 együtthatója v1, b2-jé v2 stb.

## Tételek

* **Két bázis elemszáma megegyezik**
  + F-G egyenlőtlenségből triviális (b1, b2, …bk és c1,… ck bázisokból először az egyikre megmutatjuk h kisebbegyenlő elemszámú aztán a másikra)
* **Standard bázis**
  + Rn-ben azon n vektor halmaza, melyeknek felülről az i-edik 1-es elemén kívül minden eleme 0 (0 < i <= n) egy bázis Rn-ben
  + Belátjuk, hogy független és hogy generátorrendszer
* b1, b2, … bk vektorok akkor és csak akkor bázisok egy altérben, ha az altér összes vektora egyféleképpen fejezhető ki lináris kombinációjukként
  + Ha egyféleképpen akkor bázis
    - Generátorrendszernek értelemszerűen az, hiszen egyféleképp minden kifejezhető
    - Függetlennek is, mert a nullvektor is egyféleképpen fejezhető ki
  + Ha bázis akkor egyféleképpen
    - Indirekt tegyük fel, hogy az egyik vektor kétféleképpen is kifejezhető
    - A két lineáris kombináció különbsége: 0 = (alfa1 – beta1)b1 + … +(alfak + betak)bk
    - Mivel bázis, így alfai – betai = 0 hiszen független, vagyis alfa mégis = beta
* Bázis létezése
  + Adott egy V altér és benne f1 f2 f3,… fk független rendszer. Ekkor ez kiegészíthető véges sok fk+1, fk+2 stb. vektorral, hogy a kapott rendszer bázis legyen
  + BIZONYÍTÁS
    - Legyen W a független rendszer generált altere. W <= V hiszen minden f eleme V-nek
    - Ha W = V akkor készen vagyunk, egyébként vegyünk egy v vektort mely nem eleme W-nek de eleme V-nek
    - Ezzel a vektorral az újonnan érkező vektor lemmája szerint a rendszer független marad. Ezt ismételgetjük
    - Az eljárás megáll hiszen V <= Rn, legfeljebb n elemű bázisa lehet, így az F-G egyenlőtlenségből adódik, hogy legfeljebb n-k lépést kell végeznünk
  + KÖVETKEZMÉNY
    - Minden altérben van bázis, hiszen, veszünk egy vektort az altérben és addig egészítjük ki az előző tétel alapján amíg egy bázist nem kapunk
    - Ha V = {0} akkor a bázis az üres halmaz

# 8. Gauss elimináció

## Definíciók

* Sorekvivalens lépések
  + Mátrix i-edik sorának szorzása skalárral
  + Mátrix i-edik sorának j skalárszorosával vett összege
  + i-edik és j-edik sor felcserélése
  + Csupa nulla sor elhagyása
* Lépcsős alak
  + Minden sorban a legbaloldalibb nem nulla elem egy egyes
  + Minden sorra igaz ha i < j, akkor az i-edik sor vezéregyese balrább van mint a j-ediké
  + (Minden vezéregyes alatt álló összes elem 0)
* Redukált lépcsős alak
  + Olyan lépcsős alakú mátrix, ahol a vezéregyesek fölött álló összes elem is 0

## Tételek

* **Egy kibővített együtthatómátrixon végzett sorekvivalens lépés nem változtatja meg a megoldáshalmazt**
  + Mind a 4 átalakításra megmutatjuk h a kapott egyenletrendszer ekvivalens a kezdetivel
* *Ha az algoritmus végzése során a 3.lépésben i < k, akkor i-nél lejjebbi sorok vonaltól balra lévő elemei 0-k*
  + *A 3. lépésbe akkor lép csak be, ha i = k, vagy j = n. Ezesetben j = n történt meg értelemszerűen*
  + *Mivel j-t egyesével növelgettük, és minden növeléskor az iediknél nagyobb sorszámú sorokban a j-edik tagokat kinulláztuk (az 1. lépésben)*
* A Gauss elimináció-nak 3 féle kimenetele lehet
  + Tilos sort találunk így nincs megoldás
  + Minden oszlopban van vezéregyes vagyis az egyenletrendszer egyértelműen megoldható
  + Nincs minden oszlopban vezéregyes vagyis az egyenletrendszernek végtelen sok megoldása van
* Ha egy k egyenletű n ismeretlenes lineáris egyenletrendszer egyértelműen megoldható, akkor k >= n
* **Egy lineáris egyenletrendszer akkor és csak akkor egyértelműen megoldható, ha együtthatómátrixának determinánsa != 0**
  + Gauss eliminációt végezve a determináns értéke változhat, de 0 volta nem
  + Ha tilos sort, vagy csupa 0 sort találunk, akkor fordulhat elő, hogy nem egyértelműen megoldható, mindkét esetben 0 a determináns
  + Ha egyértelműen megoldható akkor a lépcsős alakjában minden oszlopban van vezéregyes vagyis a determinánsa 1

## Algoritmusok

* Gauss elimináció
  + i = 1, j = 1
  + 1. lépés
    - ha aij = 0
      * Ha van olyan lejjebbi sor melynek j-edik eleme nem 0, akkor cseréljük őket fel
      * Egyébként, ha j = n akkor i-- és 3.lépés
      * Egyébként j++
    - Osszuk le az i-edik sor minden elemét a j-edikkel
    - Vonjuk ki az összes lejjebbi t sorból az i-edik sor atj-szeresét
    - Ha j = n akkor 3. lépés
    - i++, j++ 1.lépés
  + 3. lépés
    - Ha i = k akkor lépcsős alakú a mátrixunk
    - Egyébként ha van olyan t > i melyre bt != 0 akkor tilos sort találtunk
    - Egyébként elhagyjuk az i alatti sorokat és lépcsős alakú a mátrixunk

# 9. Determináns

## Definíciók

* Permutáció inverziószáma
  + A permutációban inverzióban lévő elemek száma
  + Inverzióban van két elem ha i < j de pii > pij
* Bástyaelhelyezés
  + Egy négyzetes mátrix minden sorából és oszlopából pontosan egy elemet választunk ki
  + Ez megfeleltethető egy permutációnak, ahol a permutáció pik-adik tagja a mátrix k-adik sorából kiválasztott elem sorszáma
* Determináns
  + Egy négyzetes mátrix determinánsa az összes bástyaelhelyezésben vett elemek szorzatának előjeles összege
  + Az előjelet a bástyaelhelyezéshez rendelhető permutáció inverziószámának paritása határozza meg, ha páros akkor pozitív, ha páratlan akkor negatív

## Tételek

* Egy permutációban két elem felcserélésével megváltozik az inverziószám paritása
  + Egymás mellett álló elemek esetén
    - Mivel egymáshoz képest semelyik másik elemmel való viszonyuk nem változott, így az inverziószám pontosan 1-gyel változott
  + Egyéb esetben
    - pii-t egyesével lépegetve addig cserélgetjük a mellette álló elemekkel amíg j mellé nem került. Az eddig végzett cserék száma legyen t
    - Most pii-t és pij-t felcseréljük
    - pij-vel visszalépegetünk pii helyére
    - 2t + 1 cserét végeztünk, vagyis páratlan száma paritásváltás történt
* Determináns értékei
  + Ha van csupa 0-sora a mátrixnak, akkor detA = 0
  + Ha a mátrix felsőháromszög mátrix, akkor detA a főátló elemeinek szorzata
* Segéd lemma
  + Ha X Y Z négyzetes mátrixok i-edik soraiktól eltekintve megegyeznek és Z ideik sorára zij = xij + yij minden j-re, akkor detZ = detX + detY
  + BIZONYÍTÁS
    - Írjuk fel Z determinánsát definíció szerint, és az i-edik sorából választott elem helyére írjuk, hogy xij + yij
    - Mivel minden más k sorára igaz, hogy zkj = xkj = ykj így a zárójelet felbontva megkapjuk X és Y determinánsa felírásának összegét
* **Determináns kiszámítása**
  + Ha egy A mátrix i-edik sorát lambdával szorozzuk, akkor a kapott A’ mátrixra detA’ = detA \* lambda
  + Ha egy A mátrix i-edik és j-edik sorát felcseréljük akkor a kapott A’ mátrixra detA’ = -detA
  + Ha egy A mátrix i-edik sorához j-edik sorának lambdaszorosát adjuk attól a determinánsa nem változik
  + BIZONYÍTÁS
    - Írjuk fel A determinánsát
    - Ekkor ha egy sorát lambdával szorozzuk az összeg minden tagjából ki lehet emelni lambdát
    - Ha két sorát felcseréljük, akkor az összegek az előjelüktől eltekintve megegyeznek, és minden előjel az ellentettjére változott (ez következik abból, hogy egy permutációban két elem cseréjekor megváltozik az inverziószám paritása)
    - A harmadik állítás bizonyításához a segédlemmát használjuk
      * Z = A’ X = A és Y = az a mátrix melynek j-edik sorában A i-edik sorának lambdaszorosa áll
      * Legyen Y’ az a mátrix, melynek j-edik sorában A i-edik sora áll (vagyis az i-edik és j-edik sora megegyezik)
      * Ekkor detY = lambda detY’
      * det Y’ = - detY’ hiszen ha két sorát felcseréljük, a determináns ellentettjére változik, ám az a két sora megegyezik, vagyis detY’ = 0 így detY is 0

# 10. Mátrixok

## Definíciók

* Előjeles aldetermináns
  + Egy A négyzetes mátrix aij eleméhez tartozó előjeles aldetermináns alatt az A i-edik sorát és j-edik oszlopát elhagyva kapott mátrix determinánsának (-1)^(i + j)-szeresét értjük
* Mátrixműveletek
  + Összeadás: elemenkénti összeadás
  + Skalárral szorzás: minden elem szorzása a skalárral
  + Transzponálás: A n x k mátrix transzponáltja az az AT = B k x n-es mátrix melynél aij = bji minden i-re és j-re
  + Mátrixszal szorzás: A n x k és B k x m szorzatán azt a C n x m mátrixot értjük, melynek cij eleme A i-edik sorának és B j-edik oszlopának skaláris szorzata
* Egységmátrix
  + Négyzetes mátrix melynek a főátlójában 1-esek, máshol 0-sok vannak
  + EA = AE

## Tételek

* **Kifejtési tétel**
  + Ha egy mátrix egyik sorának minden elemét megszorozzuk a hozzá tartozó előjeles aldetermináns értékével, detA-t kapjuk
  + BIZONYÍTÁS\*\*\*\*\*
    - Ha kiemeljük a determináns felírásából az adott szorzat i-edik sorában lévő elemet, a zárójelben a hozzá aldetermináns értéke lesz
* Mátrixműveletek tulajdonságai
  + Összeadás és skalárralszorzás kommutatív és asszociatív
  + Skalárral szorzás az összeadásra nézve disztributív
  + Mátrixszorzás asszociatív (skalárral szorzással is), és az összeadásra disztributív
    - Legyen X = A x B, ekkor definíció szerint lambda \* A x B-nél felbontható a zárójel és a többi a szorzás asszociativitásából adódik
    - Disztributivitás: X = A x B, Y = A x C ekkor X + Y összegéből kiemelhető minden aij, ezzel az állítást beláttuk
    - Asszociativitás: Belátjuk, hogy bárhogy csoportosítva ugyanakkora mátrixokat kapunk, majd hogy ha X = A x B akkor X x C átcsoportosítható
  + (A x B)T = BT x AT
    - X = A x B és Y = BT x AT, ebből xij = ai1 b1j + ai2 b2j… yji = b1j ai1 … vagyis ugyanaz
* detAT = detA
  + A-ra vett minden bástyaelhelyezésnek megtaláljuk a transzponáltján vett ugyanolyan bástyaelhelyezést, vagyis az összegben lévő szorzatok egyenlőek
  + A tényezők előjelei is megegyeznek, mert egy permutáció inverziószáma megegyezik az inverz permutáció inverziószámával
    - pii legyen k és pij = l. k és l akkor vannak inverzióban, ha i < j, de k > l
    - az inverz pi’ permutációban pi’k = i és pi’l = j, vagyis akkor állnak inverzióban, ha k < l, de i > j
    - Vagyis pii és pij inverziója ekvivalens azzal, hogy i és j inverzióban vannak pi’-ben
* detAB = detA\*detB

# 11. Tételek mátrixokról

## Tételek

* **Lineáris egyenletrendszer egyértelmű megoldhatósága**
  + Egy n x n-es lineáris egyenletrendszer akkor és csak akkor megoldható, ha az együtthatókból alkotott kibővített együtthatómátrix determinánsa nem 0
  + Egy lineáris egyenletrendszer akkor és csak akkor nem oldható meg egyértelműen ha baloldalon van olyan sor melyen minden elem 0, ez ekvivalens azzal, hogy a Gauss elimináció után determináns 0
* Lineáris egyenletrendszer megoldhatósága
  + Az a1 a2… ak vektorokból oszloponként alkotott mátrix legyen A és egy adott b vektor. Ekkor az alábbi állítások ekvivalensek
  + Megoldható az Ax = b mátrixegyenlet
  + Az (A|b) együtthatómátrixú lineáris egyenletrendszer megoldható
  + b eleme <a1, a2, … ak>
  + BIZONYÍTÁS
    - I. = II.: Ax i-edik koordinátája ai,1x1 + ai,2x2 + ai,3x3… = bi. Ez épp a lineáris egyenletrendszer
    - II. = III.: Ha b eleme A oszlopai által generált altérnek, akkor felírható azok lináris kombinációjaként. Ekkor x1, x2, … xn-t választva a1, a2, … lináris kombinációjának együtthatóiként
* Lineáris függetlenség feltétele
  + Ax = 0 egyetlen megoldása az x = 0
  + A oszlopai lineárisan függetlenek
    - Ez a felső kettő k x n-es mátrixra is igaz
  + A sorai lineárisan függetlenek
  + detA != 0
  + BIZONYÍTÁS
    - Tudjuk h csak akkor függetlenek vektorok ha 0-t adó lineáris kombinációja csak 0 együtthatókkal igaz. Ekkor ha x koordinátáit választjuk együtthatóknak, az állítások ekvivalenciája triviális
    - Az előző tételből tudjuk, hogy az Ax = 0 megoldhatósága ekvivalens az (A|0) egyenletrendszer megoldhatóságával, ami a determináns 0 voltával egyenlő

# 12. Mátrix rangja

## Definíciók

* Egy A négyzetes mátrix inverze az B mátrix melyre A x B = E
  + A-1-gyel jelőljük
* Négyzetes részmátrix
  + A egy n x k-s mátrix. Kiválasztunk r db (r < n, k) oszlopot és r db sort, ezek kereszteződésében álló elemek alkotják A egy négyzetes részmátrixát
* Rangok
  + o(A) Oszloprang: értéke r ha kiválasztható r független oszlopa, de r + 1 nem
  + s(A) Sorrang: értéke r ha kiválasztható r független sora, de r + 1 nem
  + d(A) Determinánsrang: ha egy r x r-es négyzetes részmátrixának determinánsa nem 0, de bármely (r + 1) x (r + 1)-es négyzetes részmátrixának determinánsa 0
  + r(A) mátrix rangja: s(A) o(A) d(A)

## Tételek

* **Egy A n x n mátrix akkor és csak akkor invertálható, ha detA != 0. Ekkor az inverz egyértelmű**
  + Ha létezik akkor detA != 0
    - Mivel detE = 1 és A x B = E, akkor det(A x B) = det E = detA x detB, ahol detB értelemszerűen nem lehet 0
  + Ha detA != 0 akkor létezik olyan egyértelmű X melyre A x X = E
    - Értelmezzük az A x X = E szorzatot oszlopvektoraiként
      * A\*x1 = e1, … A\*xn = en
    - Korábbi tételből tudjuk,. hogy ezek az egyenletek egyértelmű megoldhatósága ekvivalens azzal, hogy detA != 0, vagyis van egyértelmű megoldásunk
  + Ha A x X = E-re X létezik akkor X x A = E
    - Legyen X inverze Y (Y létezik hiszen detX != 0)
    - Y = E x Y = (A x X) x Y = A x (X x Y) = A x E = A (mátrixszorzás asszociatív)
      * Y = A
* s(A) = o(A) = d(A)
  + d(A) meghatározásakor legyen M a kiválasztott részmátrix és Am az a mátrix melynek oszlopait választottuk A-ból M készítésekor
    - Ekkor Am-nek r db oszlopa van, melyek függetlenek, ha nem lennének akkor M oszlopai is összefüggőek volnának, és a determinánsa nem lehet 0
    - Ebből tudjuk, hogy o(A) >= d(A)
  + Segéd Lemma: Ha van egy C k x n-es mátrix, melyre k > n és oszlopai függetlenek, akkor választható olyan sor melyet elhagyva a kapott mátrix oszlopai függetlenek maradnak
    - Tudjuk, hogy az Ek egységmátrix egyik oszlopa nincs benne a C által generált altérben (F-G egyenlőtlenségből következik) legyen ez ej
    - Ekkor ha elhagyjuk C j-edik sorát és indirekt feltesszük, hogy a kapott C’ sorai lineárisan összefüggnek, az azt jelenti, hogy C’a = 0 egyenletben a lehet más mint nullvektor
    - Ekkor viszont tudjuk, hogy Ca != 0. Ha a j-edik koordinátája alfa, akkor viszont Ca / alfa = ej, ami ellentmondás (ez azért igaz, mert C és C’ csak a j-edik sorukban különböznek, a többi sorban a megoldás 0)
  + Ekkor válasszunk A oszlopai közül r db függetlent (ezt tudjuk hogy lehetséges) és hagyogassunk el addig sorokat amíg r x r-es mátrixot kapunk. Ekkor annak is függetlenek az oszlopai és determinánsa már nem 0, vagyis o(A) <= d(A)
  + Ebből o(A) = d(A) ami = s(A), mert A transzponáltjának d(A)-ja ugyanaz, amelynek s(A)-ja A o(A)-ja
* Egy mátrix rangja egyenlő az oszlopai által generált altér dimenziójával
  + Válasszuk ki a mátrix r-db oszlopát, ezek függetlenek. Az általuk generált altér U, kiválasztás előtt generált altér W
  + U <= W triviális
  + Az újonnan érkező vektor lemmájából tudjuk, hogy mivel a rang definíciójából r + 1 oszlop már összefüggő, így a mátrix minden ki nem választott oszlopa benne van U-ban
  + Ebből U = W triviális
* **Sorekvivalens lépések a mátrix rangját nem változtatják meg, lépcsős alakú mátrix rangja a sorainak száma**
  + I.
    - Kiválasztjuk A-nak néhány oszlopát, legyen ez A’. Ekkor A’ oszlopai csak akkor függetlenek ha az (A’|0) kibővített együtthatómátrixú egyenletrendszernek csupa 0 az egyetlen megoldása
    - Ekkor ha A-ra sorekvivalens lépést alkalmazunk, majd azt elvégezzük A’-n akkor a megoláshalmaz az A’|0 egyenletrendszer megoldáshalmaza nem változott.
  + II.
    - Legyen egy lépcsős alakú mátrix sorainak száma k. Ekkor kiválasztjuk azokat az oszlopakat amikben van vezéregyes, a kapott k x k-s mátrix determinánsa 1.
    - Ennél nagyobb értelemszerűen nem választható, így az állítást beláttuk

# 13. Lineáris leképezések

## Definíciók

* Lineáris leképezés
  + Egy Rn 🡪Rk hozzárendelés lináris leképezés ha létezik olyan [f] mátrix mellyel minden x-re f(x) = Ax
  + [f] k x n-es
* Lineáris transzformáció
  + Egy Rn 🡪Rn lineáris leképezés

## Tételek

* **Lineáris leképezés feltétele**
  + Egy függvény akkor és csak akkor lineáris leképezés ha
    - f(x + y) = f(x) + f(y)
    - a\*f(x) = f(a \* x)
  + Ekkor [f] egyértelmű és [f] i-edik oszlopa f(ei) (Rn beli sztandard bázis i-edik sora)
  + BIZONYÍTÁS
    - Ha f egy lineáris leképezés
      * f(x + y) = A(x + y) = Ax + Ay, ugyanez skalárral szorzásra
    - Ha a tulajdonságok teljesülnek
      * Válasszuk A-nak azt a mátrixot amit a tétel mond
      * Ekkor az értelmezési tartomány bármely vektora felírható az egységvektorok lineáris kombinációjaként, amelyre meg teljesülnek a tulajdonságok, úgyh megvagyunk
* Origó körüli forgatás lineáris transzformáció
  + f(u + v) = f(u) + f(v)
    - Legyen u = OP v = PQ, ekkor u + v = OQ
    - Ezt a háromszöget elforgatva valóban u és v elforgatott változatait kapjuk, és f(u) = OP’ f(v) = P’Q’ ebből egyértelmű, hogy f(u) + f(v) = OQ’ = f(u + v)
  + skalárral szorzás triviális
  + Egyégvektorokra alkalmazzuk a (cosa - sina)(sina cosa) oszlopú mátrixot
    - szögfüggvények definíciójából értelemszerű
* Leképezések szorzata
  + Ha f egy Rn 🡪 Rk és g: Rk 🡪Rm akkor f(g(x)) = [f][g]
  + BIZONYÍTÁS
    - [f] = A [g] = B, ekkor f(g(x)) = f(Bx) = A(Bx) = (AB)x
* Addíciós tételek
  + f: alfa szöggel forgatás, g: béta szöggel forgatás
  + ekkor az alfa + béta szöggel forgatás = f(g(x)), vagyis [f][g]
    - cos(alfa + beta) értéke az alfa + beta szöggel való forgatás mátrixának első eleme, mely az [f] és [g] szorzatának első eleme, mely a cos(alfa + beta) addíciós tételt bizonyítja
    - sin(a + b)-re ugyanez
* Inverz függvény
  + Lineáris transzformáció akkor és csak akkor invertálható, ha det[f] != 0. Ekkor [f-1] = [f]-1
    - f invertálható
      * Indirekt: detA = 0, ekkor az oszlopai összefüggőek
      * Ekkora 0 kifejezhető a triviális lineáriskombináción kívül máshogy is, vagyis ellentmondásra jutottunk az invertálhatóságról
    - detA != 0
      * Ekkor tudjuk, hogy A inverze létezik, és legyen B
      * Ekkor y = Ax szorozva jobbról B-vel, By = ABx = Ex = x, amivel az állítást beláttuk

# 14. Magtér, képtér

## Definíciók

* Magtér
  + f lineáris leképezés magetere vektorok azon halmaza melyeknek képe a nullvektor
  + Jele: Kerf
* Képtér
  + f lineáris leképezés képtere vektorok azon halmaza melyek előállnak egy bármely vektor képekén
  + Jele Imf
  + Ez a függvény értékkészlete

## Tételek

* Kerf egy altér
  + Azt kell megmutatni h Kerf zárt az összeadásra és a kivonásra, ez a lineáris leképezések tulajdonságából értelemszerű
* Imf egy altér
  + Imf definíció szerint [f] oszlopai által generált altér
* Dimenziótétel
  + f Rn 🡪 Rk lineáris leképezés akkor dimImf + dimKerf = n
    - Legyen dimKerf = m, és b1, b2, …bm egy bázis Kerf-ben
    - Mivel ez egy független rendszer, így kiegészíthető egy Rn beli bázissá c1, c2, … ,c(n-m) vektorokkal
    - Ekkor f(c1), f(c2), … f(cn-m) generátorrendszer Imf-ben
      * Veszünk egy tetszőleg y elemet Imf-ből, ekkor y = f(x) valmilyen x-re
      * x pedig kifejezhető b1, b2, …bm, c1, ck, …cn-m vektorok lineáris kombinációjaként, vagyis y = f(x) felbontható külön összegekre
      * Ekkor viszont f(bi) = 0 minden i-re, így az állítást beláttuk
    - Ekkor f(c1), f(c2), … f(cn-m) függetlenek
      * Lássuk be, hogy 0-t adó lineáris kombinációjuk csak a triviális
      * Vegyük egy 0-t adó lineáris kombinációjukat majd az f(x) + f(y) = f(x + y) azonosságot használva vonjuk össze az összeget.
      * Ekkor ami f(…..)-ben van Kerf definíciója szerint a Kerf része, vagyis egyenlővé tehető b1, b2, … bm vektorok egy lineáris kombinációjával
      * Rendezzük az egyenlőséget 0-ra, ekkor mivel b1, b2, …bm, c1, ck, …cn-m vektorok függetlenek így c1, c2, … vektorok együtthatója (mint az egyenletben minden vektor együtthatója) csak 0 lehet.

# 15. Bázistanszformációk

## Definíciók

* Transzformáció bázis szerinti mátrixa
  + Jele: [f]B
  + Ha adott egy f lineáris transzformáció és egy B bázis, akkor [f]B az [x]B 🡪[f(x)]B függvény mátrixa

## Tételek

* Legyen h az a függvény mely [x]B-hez x-et rendeli. Ekkor [h] = B
  + Írjuk fel egy általános x vektor B szerinti lineáris kombinációját
  + Ekkor a lineáris kombináció változói B oszlopai, együtthatói az [x]B koordinátavektorai
* [f]B értéke
  + Legyen f egy lineáris transzformáció és B egy mátrix melynek oszlopai bázisok Rn-ben
  + Legyen g az a függvény mely [x]B 🡪[f(x)]B-t rendeli
  + [g] = B-1[f]B
    - Az előző tételből tudjuk, hogy [x]B-hez x-et rendelve a függvény mátrixa B, amiből, hogy x-hez [x]B-t rendelve a fv mátrixa B-1
    - Ha [x]B-re alkalmazzuk h-t azzal x-et kapunk, amelyre alkalmazva f-et f(x)-et kapunk, melyre alkalmazva h-1-et kapunk [f(x)]B-t
    - Így a használatos mátrix valóban a B-1[f]B
* Bázistranszofmáció tételei
  + [f(x)]B = [f]B [x]B
    - [f(x)]B = B-1 [f]x
    - [f]B = B-1 [f]B
    - [x]B = B-1x
    - (B-1 [f]B)(B-1x) = B-1[f](BB-1)x = B-1 [f]Ex = B-1 [f]x
  + [f]B = B-1 [f]B
    - Már beláttuk
  + [f]B i-edik oszlopa egyenlő [f(bi)]B
    - [f]B = B-1 [f]B
    - [f(bi)]B = [f\*B]B i-edik oszlopával
    - B-1 [f]B = B-1 [f]B

# 16. Sajátérték, sajátvektor

## Definíciók

* Sajátérték
  + A négyzetes mátrix sajátértékei olyan lambda skalárok melyekhez létezik olyan x melyre Ax = lambdax
  + x != 0
* Sajátvektor
  + A négyzetes mátrix sajátvektorai azon x vektorok melyekhez létezik olyan lambda skalár, hogy Ax = lambdax
  + x != 0
* Karakterisztikus polinom
  + Egy A négyzetes mátrix karakterisztikus polinomja det(A - lambdaE) értéke, ahol lambda a változó

## Tételek

* Egy négyzetes mátrixnak lambda akkor és csak akkor sajátértéke, ha det(A - lambdaE) = 0
  + Mivel Ax = lambdax = lambdaEx így ezt 0-ra rendezve
  + Ax – lambdaEx = 0 lineáris egyenletrendszernek az x != 0 megoldásait keressük.
  + Ez akkor létezik ha az A – lambdaE mátrix oszlopai függetlenek vagyis determinánsa nem 0
* f egy lineáris transzformáció, B egy bázis. Ekkor [f]B akkor és csak akkor diagonális mátrix, ha [f]-nek B minden eleme a sajátvektora
  + [f]B akkor diagonális ha i-edik oszlopa ei \* lambdai
  + Mivel ez az oszlop = [f(bi)]B, amely = ei \* lambda. Ekkor felírható a koordinátavektor definíciója szerint, hogy f(bi) = 0b1 + 0b2 + … + lambdabi + … + 0bn 🡪 [f]bi (= f(bi))= lambdabi