## Bővített Euklideszi Algoritmus az Euklideszi gyűrűkben

Megadja és -ját és , -t, hogy ( nem derül ki, hogy mi.)

## Euklideszi gyűrű egy eleme pontosan akkor felbonthatatlan, ha prímelem

Mindkét oldalt osztja , mert a bal oldalt osztja, ami ugyan az, mint a jobb oldal.

## Euklideszi gyűrű minden nem nulla és nem egység eleme felírható felbonthatatlan elemek szorzataként. (Sorrendtől és asszociáltságtól eltekintve.) Azaz az euklideszi gyűrű Gauss-gyűrű is.

Felbontogatjuk a nem irreducibilis elemeket, csökken. Ez valamikor megáll. Ekkor csak irreducibilis tényezők vannak. Ez a felbontás.

Ha többet is találunk, azok lényegében megegyeznek. Tekintsük azt, ahol minimális.

és asszociáltak.

Ekkor kapunk -t aminek -je kisebb: Ez ellentmondás. Azt tettük fel, hogy minimális.

## Hányadostest

integritási tartomány, nem nullgyűrű

tört rendezett pár.

Mikor egyenlő két tört:

Ekvrel: , ha

Összeadás:

Szorzás:

A műveletek kompatibilisek az ekvivalenciarelációval, és az ekvivalenciaosztályok testet alkotnak, amelyet az hányadostestének nevezünk.

Bizonyítást nem csináljuk meg.

### Következmény: R integritási tartomány beágyazható hányadostestébe

Rögzített -re: ekvivalenciaosztálya:

Művelettartó, kölcsönösen egyértelmű, monomorfizmus.

# Polinomok

## Polinom

gyűrű

Együtthatók sorozata.

a határozatlan

Valahonnan kezdve csupa 0.

Összeg:

Szorzat:

Egységelem:

Konstans polinom:

0 együtthatójú tagok elhagyhatóak. További 0 együtthatójú tagokat felvehetünk. Ez viszont nem egyértelmű. Egyértelműsítés:

a főegyüttható, a polinom foka:

Nulla polinom, üres összeg, foka , nincs főegyütthatója.

Konstans polinom foka legfeljebb 0 (-∞ is benne van)

Lineáris polinom: legfeljebb elsőfokú.

Monom: alakú

esetén a monom

Főpolinom / normált polinom: főegyüttható egységelem.

Nullosztómentes gyűrű esetén két nem nulla polinom szorzatának főegyütthatója a főegyütthatók szorzata, foka pedig a fokok összege.

és karakterisztikája ugyan az.

## Polinomfüggvények

polinomhoz tartozó polinomfüggvény.

-vel is jelölhető.

Előfordulhat, hogy két különböző polinomhoz ugyanaz a polinomfüggvény tartozik.

Végtelen gyűrűknél nincs ilyen probléma.

## Maradékos osztás tétele polinomokra

R egységelemes integritási tartomány

és két polinom R[x] felett

főegyütthatója egység.

, ahol

Főpolinommal lehet maradékosan osztani.

Biz: fokszám szerinti indukció.

foka legalább ; TFH f foka kisebb, mint g foka

Indukcióval, ha foka , főegyütthatója

"Eggyel csökkentjük a fokszámot."

### Gyök

gyöke a polinomnak, ha azon a helyen -t vesz fel.

### Következmény: gyöktényező leválasztása

BIZ: Maradékos osztás tétele …

### Következmény: Ha , akkor -nek legfeljebb gyöke van

R kommutativitása és nullosztómentessége is szükséges.

BIZ: fokszám szerinti indukció.

deg(f)=0 nincs gyöke

…

### Következmény: Két legfeljebb n-ed fokú polinom n+1 különböző helyen ugyanazt az értéket veszi fel, akkor megegyezik.

BIZ: Egyébként a különbségpolinom olyan legfeljebb n-ed fokú nem nulla polinom lenne, amelynek gyöke van. Ez ellentmondás.

### Következmény: Ha végtelen, akkor két különböző polinomhoz nem tartozik ugyanaz a polinomfüggvény.

BIZ: …

### Következmény: Ha test, akkor a függvénnyel euklideszi gyűrű.

Prímelem=irreducibilis elem

Minden polinom egyértelműen felírható irreducibilis polinomok szorzataként.

BIZ: …

### Megjegyzés: Maradékos osztás tétele algoritmust is ad a maradékos osztás elvégzésére: polinom osztója-e polinomnak.

…

### Megjegyzés: Horner-elrendezés

(?)

Egyik leggyorsabb eljárás arra, hogy…

### Megjegyzés: Polinomnak hány gyöke van

Függ attól, hogy milyen gyűrű felett tekintjük.

Például :

felett nincs gyöke, Q felett sincs, felett sincs.

ℂ felett

felett p=2 esetén egy gyöke van; p=3 esetén nincs gyöke; p=5 esetén két gyöke van.

Kvaterniók ferdetestében végtelen sok gyök van.

felett 8, 18, 47, 57 mind gyök. Mert összetett nem nullosztómentes.

## Polinom algebrai deriváltja

deriváltja:

### tulajdonságai egységelemes integritási tartomány felett:

1. Konstans polinom deriváltja a nulla polinom
2. Az x polinom deriváltja az egységelem
3. Additivitás:
4. Szorzat differenciálási szabálya:

### BIZ

(Könyvben el van írva.)

### Következmény: Ha test, , az és LNKO-ja, akkor négyzetmentes, azaz egyetlen legalább elsőfokú polinomnak a négyzetével sem osztható.

BIZ: Adott -re legyen a legnagyobb szám, amelyre Mivel esetén így g^(n-1)|d Ha teljesülne, akkor ebből következne.

Hibajegyzékből:

## Többszörös gyökök

Egységelemes integritási tartományban polinomnak -szeres gyöke, ha -nel még osztható a polinom, de magasabbal már nem.

g-nek c nem gyöke

### Többszörös gyökök keresése

…

BIZ:

legalább -szeres gyöke -nek.

Zárójelben levő kifejezés helyen , ami miatt nem nulla, ha

### Megjegyzés: Derivált gyöke nem feltétlenül gyöke a polinomnak. Polinom -szeres gyöke lehet a deriváltnak több mint -szeres gyöke is.

-nek nem gyöke, de deriváltja , aminek gyöke.

## Irreducibilis polinomok és testbővítések

(Következő jegyzetbe átraktam, mert újra vettük.)