# 6. előadás – Polinomok

## DEF: Polinom irreducibilis (felbonthatatlan), ha felírásban vagy az -ben egység, vagyis invertálható.

(Ez nem az egységelemet jelenti, hanem hogy van reciproka.)

Csak nem nulla és nem egység polinomok lehetnek irreducibilisek.

egységelemes integritási tartomány feletti polinom:

### Példa

felírásai:

Például

Összes:

## Irreducibilis polinomok , , , és felett

(Ez olyan kérdés, mint "Mik a prímszámok?)

Algebra alaptétele: Minden legalább elsőfokú komplex polinomnak van gyöke.

Ebből ⇒, hogy: irreducibilis ⇔ (?) (nem látszik a jel, szerintem "" lesz)

Bizonyítást nem írom.

Bontsuk elsőfokú tényezők szorzatára.

### Lemma: Ha gyöke -nek, akkor konjugáltja, is gyöke -nek.

(Konjugált: Tükrözzük az x tengelyre, pl.: )

felírás jelentése: komplex, nem valós

Példát nem írom.

Tehát -nek van egy másodfokú osztója. Ha pedig gyök, akkor Emiatt:

* Ha nem irreducibilis.
* Ha irreducibilis.
* Ha : irreducibilis -nek nincs valós gyöke.

irreducibilis. Bizonyítás később.

Megjegyzés: Hallgatólagosan kihasználtuk, hogy -ben illetve -ben egyértelmű a prímfelbontás. Ezt később bizonyítani is fogjuk.

# Kitérő: Gyűrűk

Gyűrű, integritási tartomány már tudjuk.

## DEF: Gauss gyűrű

egységelemes integritási tartomány Gauss gyűrű, ha minden nem nulla eleme, egységektől és sorrendtől eltekintve, egyértelműen felírható irreducibilis elemek szorzataként.

Az egész számok (ℤ) például egy Gauss gyűrűt alkotnak.

"egységektől eltekintve" asszociáltság nem számít.

és irreducibilis, szorzatuk nem. Szorzat eredményét és négyféle példa felbontást nem írtam le.

## DEF: Euklideszi gyűrű

Euklideszi gyűrű, ha:

* Egységelemes integritási tartomány (Kommutatív, nullosztómentes, van egysége)
* vagy (Maradékos osztás)

## TÉTEL: Minden Euklideszi gyűrű Gauss gyűrű is

Bizonyítás nélkül.

Megj.: Ha van maradékos osztás, akkor van egyértelmű prímfelbontás. Bizonyítás ugyan úgy menne, mint -ben.

## Euklideszi gyűrű példák

, ahol (Itt, ami csökken, az az abszolút érték.)

, test , ahol ("-nek a -je")

Tudunk úgy maradékosan osztani, hogy közben van valami csökkenés.

Minden test euklideszi gyűrű. Minden osztható mindennel.

# Visszatérés: Polinomok

## DEF: Primitív polinom

Gauss gyűrű.

E feletti polinom primitív, ha együtthatóinak LNKO-ja az egységelem. Vagyis nem tudunk kiemelni konstanst.

### Példák

nem primitív, mert 3 közös osztója ezeknek az együtthatóknak.

primitív, mert nem lehet leegyszerűsíteni az együtthatókat.

## Gauss lemma: Primitív polinomok szorzata is primitív.

Bizonyítás hál' istennek nincs benne a tematikában.

## Hányadostest: Mint -nek a , azaz az alakú törtek.

## Gauss tétele

Gauss gyűrű, a hányadosteste

Ha felbomlik alakba -ben, akkor

is Gauss gyűrű.

Bizonyítás nélkül.

## Következmény: a -ben felbontható-ben felbontható. Konstansok erejéig.

Ezt a példát nem értem.

## Táblázat: alapgyűrű és polinomgyűrű viszonya egymáshoz

|  |  |
| --- | --- |
| Ha | akkor |
| gyűrű | gyűrű |
| kommutatív gyűrű | kommutatív gyűrű |
| integritási tartomány | integritási tartomány |
| egységelemes integritási tartomány | egységelemes integritási tartomány |
| Gauss gyűrű | Gauss gyűrű |
| Euklideszi gyűrű | Na, itt romlik el…  Csak Gauss gyűrű |
| Test | Euklideszi gyűrű |

(Vegyük észre, hogy a sorok a felette levőket tartalmazzák. Egyre erősödő feltétel.)

## Modulo egy polinom számolások (mese)

-ben volt ilyen, hogy " kongruens -vel modulo ": esetén

Ez polinomokra is működik:

-ben

Lemaradtam. Lehetséges maradékok halmaza.

## Testbővítések polinommal

Modulo egy polinom számolások (konkrétan)

És pont ez, a fontosabb rész, kerül a tábla jobb szélére, ami innen nem látszik…

Az így kapott struktúra test. Végezzünk bővített euklideszi algoritmust.

## Irreducibilis polinomok és testbővítések (tavalyelőttről)

(Tavalyelőtti jegyzetből átemeltem ide. De más tanártól.)

Legyen test és egy -ed fokú főpolinom.

Az gyűrűben minden mellékosztályban a legalacsonyabb fokú polinom fokszáma kisebb, mint és csak egy -nél alacsonyabb fokú polinom van (mivel a mellékosztály bármely két polinomjának különbsége többszöröse -nek)

Ez meghatározható úgy, hogy a mellékosztály tetszőleges elemére vesszük az -fel való osztásnál adódó maradékot: mivel

A műveleteket végezhetjük ezekkel a reprezentánsokkal: ha a szorzat foka nem kisebb, mint , akkor osztunk -fel, és vesszük a maradékot. Jelölje az polinom osztályát -ben. Az gyűrű elemei egyértelműen felírhatók alakban, ahol

Így részteste -nak.

Ha irreducibilis főpolinom, akkor testet kapunk. Hogy lehet reciprokot számolni? reciproka bővített euklideszi algoritmussal:

konstans. 0 fokú. Csak az egységek és asszociáltak (…)

Legyen prím. valamelyik osztálya test. (?) Minden osztályban csak 1 (…) alacsonyabb fokú polinom van.

elemű lesz.

### Példa

-nak eleme lesz.

### Példa 2

felett irreducibilis az polinom. Ez által generált főideál (többszörösei), faktorgyűrű (?)

Legfeljebb elsőfokú, lineáris (…)

Összeadás: (?)

Szorzás: (…) maradékosan elosztjuk x+1-gyel (?)

Ez nem más, mint a számok teste.

### Példa 3

(mod 2 egész számok fölötti polinomok)

irreducibilis.

4 reprezentáns:

Négyelemű test

Összeadás: mod 2 összeadás.

Szorzás: mod2 szorzunk, majd maradékosan osztjuk -gyel.

== Átmásolt jegyzet vége. ==

## Nekünk kell ebből

-ed fokú irreducibilis polinom -ben.

-t -fel bővítve kapunk egy elemű véges testet.

Például kilencelemű testet úgy kapunk, hogy -mat bővítjük -gyel. Tovább nem írom.

## Mire jók a testek?

Hibajavító kódolás

Titkosítás (Kriptográfia)

## Véges testek alaptétele

Minden véges test elemszámú valamilyen prímszámra, valamilyen egészre (mi?)

Nincs tízelemű test, mert (…), de van kilenc, mert (…).

Mindenre létezik, és ez lényegében egyértelmű, izomorfizmustól eltekintve. Tehát csak egy van. Tudunk beszélni "A" kilencelemű testről.

## TÉTEL: (cím?)

véges test. A testből ki kell venni a nullát, hogy a szorzással csoportot alkosson. Ekkor ciklikus csoportú.

Ez kriptográfiában hasznos (…)-ra.

## TÉTEL: Schönemann-Eisenstein kritérium

Gauss gyűrű.

polinom ilyen együtthatókkal, legalább elsőfokú

"szám" a gauss gyűrűből

TFH: nem osztója főegyütthatójának, a többinek igen.

nem osztója -nak

Ekkor irreducibilis.

Például megfelel a fenti feltételeknek.

Megj.: és szerepet cserélhet

## Lagrange interpoláció

Bemenet:

számok

függvényértékek

Kimenet:

polinom, amire:

…

Megköthető, hogy és ekkor egyértelmű is.

### Részfeladat

Annak a speciális esetnek a megoldása, hogy az összes nulla, kivéve az -ediket, ami ráadásul 1.

Lagrange alap polinom:

### Eredeti feladat megoldása

egyértelműségét bizonyítja: TFH és is megoldás, ekkor legalább (…) helyen nulla, de legfeljebb -edfokú. Tehát , ennek a feladatnak mindig csak egy megoldása van. Két ponton át pontosan egy vonal húzható át. Három ponton át pontosan egy másodfokú vonal húzható át. És így tovább.

Alkalmazása:

## Titokmegosztás

Van egy titok, amit résztvevő között akarunk megosztani. Külön-külön egyikük se tudják kinyitni a széfet. De résztvevő együtt már ki tudja találni, viszont már nem.

a titok egy ℕ szám lesz (általában nagyon nagy szám, vagy egy jelszó).

ennél is nagyobb prímszám.

véletlen számok

Kulcs: Kiszámoljuk ezt a polinomot az helyen, és az -edik résztvevő kapja meg az értéket.

Ha legalább db emberre ismerjük értékét, akkor a polinom helyreállítható.

Kevesebb esetén viszont nem.

Jövő hétre hagyjuk: Többváltozós polinomokkal dolgozni Hogyan lehet racionális törtfüggvényeket integrálni.

Előadás vége