## Gyűrű homomorf képe gyűrű

Csoportnál már bebizonyítottuk. Új a disztributivitás, mert ez két műveletre vonatkozik.

R gyűrű (Ring szóból)

Bal oldali:

Jobb oldali ugyanígy.

## Egy R nullosztómentes gyűrűben a nem nulla elemek additív rendje megegyezik és vagy végtelen, vagy prímszám

### Példát láttunk MAPLE-ben.

Egészek mod 5, ekkor 5 maradékosztály (0..4), adogassuk össze modulo 5 az elemeket önmagukkal 3x, 4x, 5x, minden elemre, 2x összeadás ugyanazt adja vissza (más sorrendben, de mint halmaz ugyan az), 3x akkor is, 4x akkor is, 5x már 0 elem. Minden elemnek az additív rendje 5. Miért pont 5? Az pont prímszám. Összetett mod-ra nem lenne nullosztómentes. Később tanulunk más példákat.

### BIZ:

Legyen az gyűrűben nemnulla elem, valahányszor összeadva önmagával 0-t kapunk, ez röviden , ennél kevesebbszer összeadva nem kapok 0-t.

Ennek az elemnek additív rendje .

Vegyük egy másik elemet, -t és adjuk össze -t -szer:

Lehet kevesebbszer összeadva is n

 additív rendje additív rendje

Az összes többire is igaz.

Vegyük a legkisebb rendűt, annál is mindnek kisebb egyenlő, tehát mindnek az additív rendje.

Végtelen ebből kijön. Mi a helyzet a prímekkel:

TFH összetett. .

 prím.

## Nullosztómentes gyűrű karakterisztikája

Nemnulla elemek közös additív rendje (prím) vagy ha mind , akkor a karakterisztika .

### Érdekes számolási szabály karakterisztikás gyűrűben

A közbülső tagok mind 0, mert , és -szer összeadva 0 lesz, n többszöröse-szer összeadva is 0.

Ilyen gyűrűben az hozzárendelés endomorfizmus. Sőt, is az.

Egyetlen ilyen gyűrűt ismerünk jelenleg: Egész számok modulo egy prímszám.

## Részgyűrű, ideál

Megfelelő elnevezések csoportban: részcsoport, normálosztó.

 halmaz binér műveletekkel.

 egy részhalmazát … részgyűrű … résztest.

A résztestnek az eredeti gyűrű egy bővítése.

 részgyűrű

(, mert szorzás helyett összeadás van.)

Ha két tetszőleges S-beli elemet összeszorzok, a szorzat is része az S-nek.

### Ideál

 jobbideál, ha

 balideál, ha

Ideál, ha bal és jobb is.

(bal/jobb/bal∧jobb) Ideálok metszete is (bal/jobb/bal∧jobb) ideál.

### Gyűrűben találunk-e ideált

Igen, legalább -t: és maga az egész gyűrű.

Ezektől különbözőek a nemtriviálisak. Valódi ideálok.

Egyszerű gyűrű, ha nincs benne valódi ideál.

Kommutatív gyűrűben bal=jobb=ideál fogalma egybeesik.

 által generált ideál jele

Legszűkebb ideál, amely tartalmazza -t.

Ha véges halmaz

Nem írjuk ki a belső zárójelet.

Főideál Ha egy elem az ideál.

### Példák

Valós változós valós értékű függvények gyűrűjében a korlátos/folytonos/korlátos folytonos/polinom/stb. függvények részgyűrűket alkotnak. Ideált nem alkotnak.

Lineáris tér lineáris leképezései pontonkénti összeadással és függvényösszetétellel, mint szorzással az Ábel-csoportként tekintett endomorfizmusai gyűrűjének egy részgyűrűjét alkotják.

Ha a fenti dimenziós, akkor izomorf n×n-es mátrixoknak mátrixösszeadásával és szorzásával tekintett gyűrűjével.

Egész számok gyűrűjében egész szám többszörösei ideált alkotnak. Főideál, generálja.

Nemüres halmazon szimmetrikus differencia metszetképzés, részhalmazai gyűrűt alkotnak; adott elemet nem tartalmazó = főideál

stb…

## Mellékosztályok

 gyűrű ideálja, ami részcsoport az összeadásra nézve.

, ha

Ez az összeadással kompatibilis ekvrel, elem mellékosztálya az halmaz.

Ezeket az ekvivalenciaosztályokat mellékosztályoknak vagy maradékosztályoknak nevezzük.

## Tétel gyűrű ideál szerinti mellékosztályai mindkét művelettel kompatibilis osztályozást ad.

Mindkét művelettel kompatibilis osztályozás… 0 osztálya ideál…

### Következmény

 gyűrű ideál szerinti mellékosztályai az összeadásra is szorzásra nézve gyűrűt alkotnak.

 mellékosztályok szorzata: mellékosztály. Összeadásra hasonlóan.

BIZ: összeadástartó és szorzástartó. Homomorfizmus.

## Faktorgyűrű

### Példa

## Homomorfizmus magja

R gyűrű R' gyűrűbe való f homomorfizmusánál a homomorfizmus magján az R' nullelemének teljes inverz képét értjük. magját most -vel jelöljük.

## Homomorfizmus tétel

R gyűrű f homomorfizmusánál a mag az egy ideál. R' izomorf a faktorgyűrűvel.

 izomorfizmus.

…

### Példa



…

K a kanonikus leképezés.

### Másik példa

…

Ha elég kicsire veszem csak a {0} a mag, akkor R/{0} izomorf R-rel.

## Direkt szorzat

Legyen két binér művelettel ellátott halmazok egy indexelt családja.

 a család direkt szorzata. Hatvány általánosítása.

Nullelem:

Egységelem:

Ha minden gyűrű/kommutatív/egységelemes, akkor a G is az lesz.

Az nem igaz, hogy ha mindegyik nullosztómentes/test, akkor a szorzat is nullosztómentes/test lenne.

Részgyűrű, ha néhányból 0-t veszünk.

## Kommutatív egységelemes gyűrűben generált főideálok (egy elem által)

 Vagyis többszöröseinek halmaza.

### BIZ:

A halmaz tartalmazza -t, nem vezet ki a különbségképzés, gyűrűelemmel való szorzás, másrészt a benne van I-ben is.

### Következmény

 egységelemes integritási tartomány (kommutatív nullosztómentes) elemeire:

### Következmény BIZ: minden triviális

 által generált főideál része által generált főideálnak. a többszörösei kevesebben vannak, mint b többszörösei.

 többszörösei azok többszörösei -nek is.

## Gauss-gyűrűk

Oszthatóság vizsgálata gyűrűkben. Miért? Mert polinomokkal akarunk majd műveleteket végezni, pl.: maradékos osztást.

Számelmélet alaptétele volt a legfontosabb főtétel: Minden egész szám lényegében egyértelműen előáll prímtényezők szorzataként. (prím=törzs=irreducibilis volt)

R egységelemes integritási tartomány UFD unique factorization domain, ha minden a≠0 és a≠e elem egyértelműen felírható irreducibilis elemek véges szorzataként.

Lényegében egyértelmű: és egyik felbontás a másik permutációja. ( és asszociáltak) ( a szigma)

 Lényegében ugyan az a felbontás. Sorrend változik, és asszociáltak.

osztó…

 akkor és irreducibilis tényezőkre való felbontásának szorzata irreducibilis tényezőkre való felbontása kell, hogy legyen.

Gauss gyűrűben minden irreducibilis elem prím is, mert ha akkor vagy vagy … ott van felbontásában, ezért vagy vagy felbontásában szerepel.

Tehát fent irreducibilis helyett mondhattunk volna prímet is.

## Euklideszi gyűrűk

Elegendő nem szükséges kritérium gauss gyűrűre.

Egységelemes integritási tartomány , amiben megy a maradékos osztás.

 leképezés, ami

 lehet maradékosan osztani a-t nemnulla b-vel, úgy hogy q hányados r maradék

 vagy másképp felírva:

Egész számok körében a lényeg, hogy a maradék abszolút értéke kisebb legyen, mint az osztó.

 nem egyértelmű. pl.: maradék lehet vagy

Polinomnál hozzárendeljük a polinomhoz a fokszámát

## Állítások Euklideszi gyűrűben

Pontosan azok az elemek egységek, amelyekre minimális.

Ha , akkor és Ennek bizonyítása:

### BIZ:

 minimális

-t osszuk el -nal maradékosan: vagy mivel minimális, csak lehet igaz.

 osztja -t egység

Egységek -je minimális: egység. Letörölte.

Egyenlőség akkor teljesül, ha és asszociáltak.

TFH egyenlőség teljesül: -t felírva alakban

 Ellentmondás, ezért

 asszociáltak.

TFH egység minimális. , mert: , minimális.

## Példa Euklideszi gyűrűre Gauss egészek

 Olyan ℂ számok, melyek a komplex síkban egész koordinátákkal rendelkeznek.

Egységek, melyeknek -je minimális. Origótól vett távolságának négyzete minimális:

Minden elemnek négy asszociáltja van, egységekkel szorzom.

Nulla csak saját magával asszociált.

### Bővített Euklideszi algoritmus erre a gyűrűre

Nem a maradék abszolút értékét figyeljük, hanem a -jét.

 Euklideszi gyűrű, az algoritmus meghatározza:

Bebizonyítva, hogy létezik ilyen.

Invariáns:

Inicializálás:

Ciklusfeltétel (vége?):

Ciklusmag:

, ahol

(…)

Ez az algoritmus véget ér, mikor kilép, d az lnko(a,b)

### BIZ:

Megáll, mert : állandóan csökken 0 alá nem mehet; és r=0-nál is kilép.

Jó, mert: a a-nak és b-nek minden közös osztója osztja d-t.

d közös osztó, mert az -ek osztják az előzőeket végig.

Tehát Euklideszi gyűrűben van közös osztó.