

Diszkrét Matematika III

ALGEBRA

Gyűrűk

Gabor Farkas

farkasg@inf.elte.hu

gaborfarkasphd.wixsite.com/gaborfarkasphd

2017 Tavasz

ELTE

Az $(R, +, \cdot)$ algebrai struktúra **gyűrű**, ha $+$ és $\cdot$ R -en binér műveletek, valamint

I. $(R, +)$ Abel-csoport,

II. $(R, \cdot)$ félcsoport, és

III. teljesül mindkét oldalról a disztributivitás, vagyis

$$a(b + c) = ab + ac,$$

$$(b + c)a = ba + ca$$

minden $a, b, c \in R$ esetén.

Kommutatív a gyűrű, ha a szorzás kommutatív.

Az additív csoport egységeleme a gyűrű **nulleleme**, jelben 0.

Egységelemes a gyűrű, ha a szorzásra vonatkozóan van egységelem (amit e -vel, vagy 1-gyel jelölünk).

Nullgyűrű: egyetlen elemből áll (nullelem).

Zérógyűrű: ha tetszőleges két elem szorzata a nullelem.

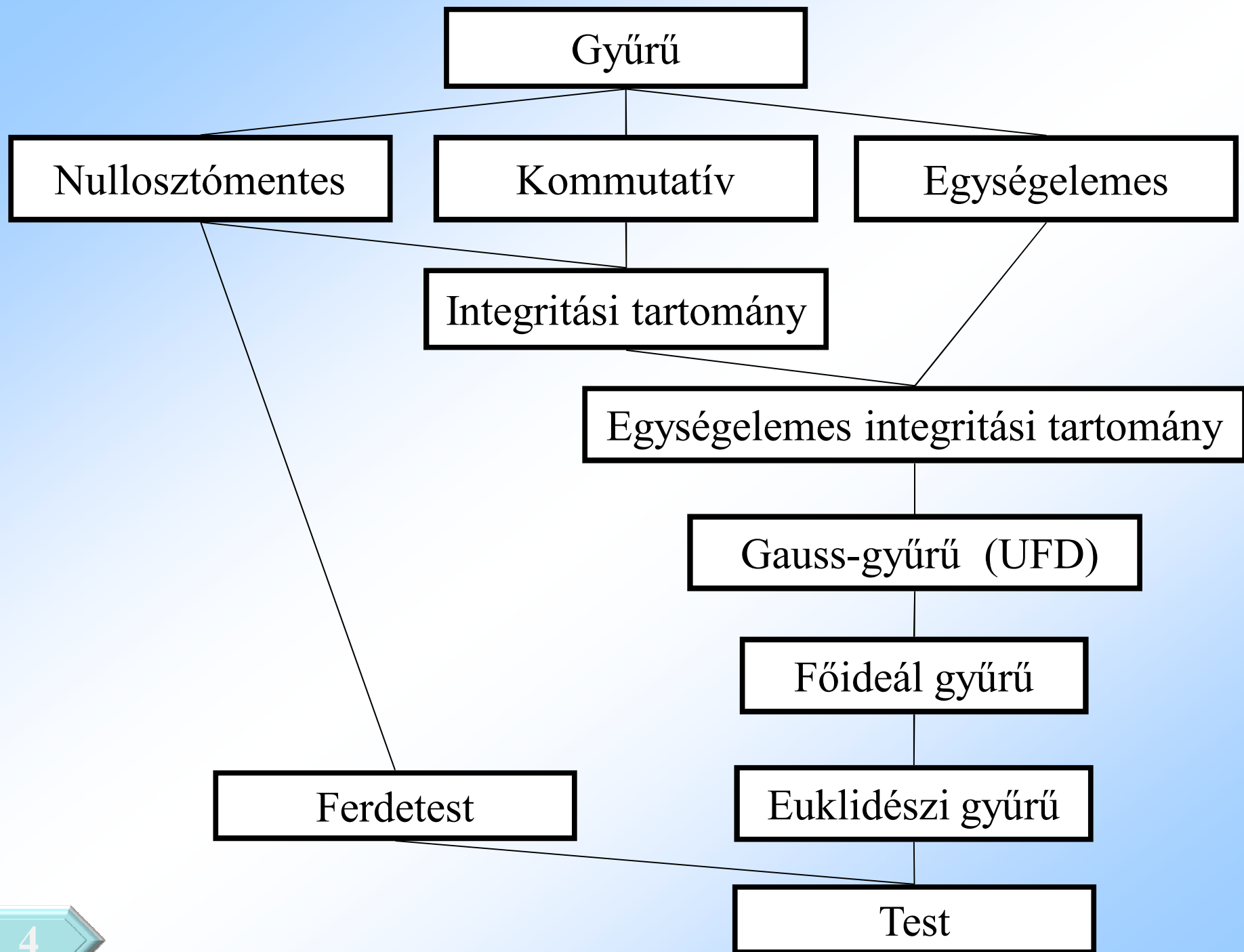
Az R gyűrűben a **bal oldali**, b **jobb oldali nullosztó**, ha $a \neq 0$, $b \neq 0$ és

$$ab = 0.$$

A (legalább két elemű), kommutatív, nullosztómentes gyűrűt **integritási tartománynak** nevezzük.

Az R gyűrű **test**, ha

$$(R^*, \cdot) \text{ Abel csoport.}$$



Lemma(észrevételek gyűrűkben)

(1) (szorzás nullelemmel): Legyen 0 az R gyűrű nulleleme. Ekkor

$$a0 = 0a = 0$$

minden $a \in R$ esetén.

(2) (előjelszabály): Legyen R gyűrű, és $a, b \in R$. Az a elem additív inverzét jelöljük $-a$ -val. Ekkor

$$-(ab) = (-a)b = a(-b), \text{ továbbá } (-a)(-b) = ab.$$

(3) Véges integritási tartomány test.

(4) Testben nincs nullosztó.



(1. 3. és 4. gyakorlaton)

(2) ab additív inverze létezik, mert $(R, +)$ csoport. $\Rightarrow$

$$ab + (-(ab)) = 0,$$

valamint

$$ab + (-a)b = (a + (-a))b = 0b = 0,$$

$\Rightarrow$

$$-(ab) = (-a)b.$$

Továbbá: $(-a)(-b) + (-a)b = (-a)((-b) + b) = 0 = ab + (-a)b,$

+ egyszerűsíthető $\Rightarrow (-a)(-b) = ab.$



Lemma(nullosztó és regularitás)

R gyűrűben a multiplikatív művelet **akkor és csak akkor** reguláris,
ha R zérusosztómentes.

Biz

1. Tfh $a \neq 0$, a nem bal oldali nullosztó és

$$ab = ac \quad / \quad -(ac) \text{ mindkét oldalhoz,}$$

$$ab + (-(ac)) = 0.$$

Előjel szabály + disztri. $\Rightarrow$

$$ab + (a(-c)) = a(b + (-c)) = 0.$$

feltétel $\Rightarrow$

$$b + (-c) = 0 \Rightarrow$$

$$b = c.$$

2. Tfh a bal oldali nullosztó, tehát $a \neq 0$ és létezik $b \neq 0$: $ab = 0$.

tetszőleges $c \in R$ -re

$$ac = ac.$$

Adjuk a jobb oldalhoz az $ab = 0$ -t.

$$ac = ac + ab,$$

disztributivitás $\Rightarrow$

$$ac = a(c+b).$$



mert

$$b \neq 0 \Rightarrow$$

$$c \neq c + b.$$



Tétel (gyűrű karakterisztikája)

Ha az R gyűrű legalább két elemű, nullosztómentes, akkor $(R, +)$ -ban a 0-tól különböző elemek rendje megegyezik. Ez a közös rend vagy végtelen, vagy egy p prímszám.

Jelölés: Előző esetben a gyűrű **nulla-karakterisztikájú**, azaz $\text{char}(R) = 0$, az utóbbiban **p-karakterisztikájú**, azaz $\text{char}(R) = p$.

Biz

$$1. \text{ Tfh } \exists a \in R^* : |a| = n_a \in \mathbb{N}$$

$\Rightarrow$

$$n_a a = 0$$

Továbbá tetszőleges $b \in R^*$ -re:

$$n_a(ab) = ab + \dots + ab = (a + \dots + a)b = (n_a a)b = 0b = 0$$

másrészt

$$n_a(ab) = a(b + \dots + b) = a(n_a b)$$

nullosztó mentesség $\Rightarrow$

$$n_a b = 0$$

$$\Rightarrow |b| \leq |a| = n_a$$

$|b| \geq |a|$ hasonlóan látható be $\Rightarrow$

$$|b| = |a| = n_a$$

2. Tfh nem létezik véges rendű elem.

$\Rightarrow$

Minden elem rendje végtelen.

3. Tfh a közös rend $n = 1$ véges szám.

$\Rightarrow$

$$0 = 1a = a \Rightarrow a = 0.$$



4. Tfh a közös rend n összetett véges szám:

$$n = kl \text{ és } 1 < k < n, 1 < l < n,$$

$$na = (kl)a = \underbrace{\underbrace{a + \dots + a}_{k \text{ db } a} + \dots + \underbrace{a + \dots + a}_{k \text{ db } a}}_{l\text{-szer}} = l(ka) = 0.$$

1. eset: $ka \neq 0. \Rightarrow |ka| = n$ és $|ka| \leq l < n.$



2. eset: $ka = 0. \Rightarrow |a| \leq k < n$ és $|a| = n.$



Példa

Legyen H egy tetszőleges halmaz, és R a H részhalmazainak halmaza. Tekintsük az $(R, \Delta, \cap)$ struktúrát, ahol Δ a szimmetrikus differenciát, $\cap$ pedig a metszetet jelöli.

Bizonyítható:

a, R gyűrű, $\emptyset$ nullelemmel,

b, $\forall A \subseteq H$ -ra $A \cap A = A^2 = A$ is teljesül (Boole-gyűrű),

c, $\forall A \subseteq H$ -ra $A \Delta A = \emptyset, \Rightarrow \text{char} R = 2$,

d, R kommutatív,

e, R nem nullosztómentes (diszjunkt halmazokra: $A \cap B = \emptyset$),

f, *c*, és *d*, pont $\forall$ Boole-gyűrűben igaz.

Def

Tegyük fel, hogy $(R, +, \cdot)$ gyűrű, és $(R_1, \oplus, \otimes)$ két binér műveletes algebrai struktúra. A $\varphi: R \rightarrow R_1$ leképezés **homomorfizmus**, ha minden $r, s \in R$ esetén fennáll, hogy

$$\varphi(r + s) = \varphi(r) \oplus \varphi(s),$$

$$\varphi(r \cdot s) = \varphi(r) \otimes \varphi(s).$$

Lemma(gyűrű homomorf képe)

Gyűrű homomorf képe gyűrű.

Biz

Csak a disztributivitást kell látni!

$$a'(b' + c') = a'(b + c)' = (a(b + c))' =$$

$$(ab + ac)' = (ab)' + (ac)' = a'b' + a'c'$$

képelemek

másik oldali hasonlóan



Def

R gyűrűben $S \subseteq R$ **részgyűrű**, ha az R -beli műveletek S -re történő leszűkítésére nézve S maga is gyűrűt alkot.

Ész

1. Mivel $S \subseteq R$ teljesül, műveleti zártság esetén az asszociativitás, kommutativitás és disztributivitás is teljesülni fog.

2. A csoportelméletben tanultak szerint csoport valamely S részhalmaz

$$\Leftrightarrow S \cdot S^{-1} \subseteq S$$

3. Tehát R -ben S komplexus részgyűrű $\Leftrightarrow$

$$S - S \subseteq S \text{ és}$$

$$S \cdot S \subseteq S.$$

Def

Legyen R gyűrű, $I \subseteq R$ és $I \neq \emptyset$. Ekkor I az R
balideálja, ha $I - I \subseteq I$ és $R \cdot I \subseteq I$,
jobbideálja, ha $I - I \subseteq I$ és $I \cdot R \subseteq I$,
ideálja, ha jobb és baloldali is egyszerre.

Triviális ideál: $\{0\}$, R

Valódi ideál: R -től különböző ideál.

Egyszerű gyűrű: csak triviális ideálja van.

Ész

- (1) Bal/jobb/ideálok metszete is bal/jobb/ideál.
- (2) Kommutatív gyűrűben bal/jobb/ideálok fogalma megegyezik.

Def

Legyen R gyűrű és $A \subseteq R$. Ekkor az

A által generált ideál R összes, A -t tartalmazó ideáljának metszete (A).

A az **a elem által generált főideál**, ha $A = \{a\}$ valamely $a \in R$ -re (a).

Főideálgyűrű: egy egységelemes integritási tartomány, ha benne minden ideál főideál.

Példa

Legyen R integritási tartomány, és $A = \{a_1, \dots, a_n\} \subseteq R$. Ekkor

$$\langle a_1, \dots, a_n \rangle = \left\{ \sum_{i=1}^n r_i a_i \mid r_1, \dots, r_n \in R \right\} \quad \text{ideál } R\text{-ben.}$$

A elemeinek összes véges R feletti lineáris kombinciója.

Ész

$$(a) = \langle a \rangle = \{ra \mid r \in R\}$$

Tehát (a) az $a \in R$ elem összes többszöröseiből áll.

Def

Legyen R gyűrű és I additív részcsoprtja R -nek, továbbá $\sim$ egy ekvivalenciareláció R -n, úgy hogy $\forall a, b \in R$ esetén $a \sim b$, ha $a - b \in I$. Ekkor $\forall a \in R$ elemre az $I + a$ ekvivalenciaosztály **R -nek egy I szerinti mellékosztálya (maradékosztálya).**

Tétel (ideál szerinti osztályozás)

Egy R gyűrű egy I ideál szerinti mellékosztályai a gyűrű elemeinek mindkét művelettel kompatibilis osztályozását alkotják. Minden, mindkét művelettel kompatibilis osztályozás esetén a nulla osztálya ideál, és az osztályokat ezen ideál szerinti mellékosztályok alkotják.

Biz

$(I; +)$ Abel csoport, tehát normálosztó R -ben

Tétel (normálosztó szerinti osztályozás) $\Rightarrow$

az osztályozás kompatibilis az összeadással

továbbá az osztályok összeadása a komplexusszorzás.

A multiplikatív művelet is kompatibilis az osztályozással:

$$(I + a)(I + b) = II + aI + Ib + ab \subset I + ab.$$

Most tfh $\exists$ egy, mindkét művelettel kompatibilis osztályozás és legyen I a 0 additív egységelem osztálya, ekkor

Tétel (művelettel kompatibilis osztályozás) $\Rightarrow$ I normálosztó R -ben

továbbá az osztályozás pont az I szerinti mellékosztályokból áll

I ideál?

$$\forall X \text{ osztályra : } 0 \in I \Rightarrow 0 \in X \cdot I \Rightarrow X \cdot I \subseteq I$$

$$\Rightarrow RI \subseteq I. IR \subseteq I \text{ hasonlóan.}$$



Ész

Egy R gyűrűnek egy I ideál szerinti mellékosztályi az additív és a multiplikatív műveletre nézve gyűrűt alkotnak.

Def

Legyen R gyűrű, I ideál R -ben. R -nek I szerinti **maradékosztálygyűrűje (faktorgyűrűje)** $R/I = \{I + r \mid r \in R\}$ a következő műveletekkel:

$$(1) \quad (I + r) + (I + s) = I + (r + s)$$

$$(2) \quad (I + r) \cdot (I + s) = I + r \cdot s.$$

Ész

(2) -ben nem a normál értelemben vett komplexus szorzásról van szó!

Példa

Legyen $R = \mathbb{Z}$, $I = 8\mathbb{Z}$, $a = b = 4$, ekkor

$$\begin{aligned}(I + a)(I + b) &= (8\mathbb{Z} + 4)(8\mathbb{Z} + 4) = 64\mathbb{Z}^2 + 32\mathbb{Z} + 32\mathbb{Z} + 16 \\ &= 64\mathbb{Z} + 32\mathbb{Z} + 16 \subset 16\mathbb{Z},\end{aligned}$$

$\forall$ elem osztható 16-tal

$8\mathbb{Z} + 16$ viszont 8-cal osztható elemeket tartalmaz, tehát

$$(8\mathbb{Z} + 4)(8\mathbb{Z} + 4) \subset 16\mathbb{Z} \subsetneq 8\mathbb{Z} + 16.$$

Def

Egy R gyűrű egy R' gyűrűbe való φ homomorfizmusánál a **homomorfizmus magján** az R' gyűrű nullelemének teljes inverz képét értjük, jelben $\ker(\varphi)$.

Tétel (homomorfizmustétel gyűrűben)

Egy R gyűrű egy φ homomorfizmusánál a homomorfizmus magja ideál. Az $R/\ker(\varphi)$ faktorgyűrű izomorf $R' = \varphi(R)$ -rel.

Az R bármely I ideálja magja valamely homomorfizmusnak, például R R/I -re való kanonikus leképezése homomorfizmus, amelynek magja I .

Def

Legyen R integritási tartomány és $a, b \in R$.

a **osztója** b -nek ha létezik $c \in R$, amelyre $b = ac$, jelben $a \mid b$. $x \in R$ **egység**, ha $x \mid r$ minden $r \in R$ -re.

Def

Legyen R egységelemes integritási tartomány, és $a, b \in R$.

Azt mondjuk, hogy a és b **asszociáltak**, ha létezik olyan c egység, amelyikkel $a = bc$. Ezt a tényt $a \sim b$ -vel jelöljük.

Ész

Egy R egységelemes integritási tartományban

- (1) az egységek halmaza (jel. $U(R)$) a szorzásra csoportot alkot.
- (2) Az asszociáltság R -ben ekvivalenciareláció.
- (3) két elem asszociált $\Leftrightarrow$ kölcsönösen oszthatóak egymással.

Tétel (főideálok)

Egy R kommutatív egységelemes gyűrűben az $a \in R$ elem által generált főideálra $(a) = aR$. A nullelem által generált főideál $\{0\}$, az egységelem által generált főideál R .

Lemma (állítások főideálokra)

Egy R egységelemes integritási tartomány a, b elemeire

- (1) $(a) \subseteq (b) \Leftrightarrow b|a$.
- (2) $(a) = (b) \Leftrightarrow b$ és a asszociáltak.
- (3) $(a) = R \Leftrightarrow a$ egység.

Def

Legyen R egységelemes integritási tartomány és $a, b \in R$. Azt mondjuk, hogy $d \in R$ az **a és b legnagyobb közös osztója**, ha

1. közös osztó, vagyis $d \mid a$ és $d \mid b$, valamint
2. $c \mid a$ és $c \mid b$ esetén $c \mid d$.

Def

Legyen R egységelemes integritási tartomány, ekkor

1. $a \in R^* \setminus U(R)$ **felbonthatatlan**, ha $a = b \cdot c$ ($b, c \in R$) esetén $b \in U(R)$ vagy $c \in U(R)$.
2. $a \in R^* \setminus U(R)$ **prím**, ha $a \mid b \cdot c$ ($b, c \in R$) $\Rightarrow a \mid b$ vagy $a \mid c$.

Később megválaszolandó kérdés: mely struktúrákban esnek egybe prímek és felbonthatatlanok?

Def

Legyen R egységelemes integritási tartomány és $U(R)$ az egységeinek halmaza.

R **Gauss-gyűrű ((Egyértelmű) faktorizációs tartomány, UFD)**, ha minden $r \in R^* \setminus U(R)$ felírható

$$r = p_1 p_2 \dots p_n$$

alakban, ahol n pozitív egész és a tényezők nem feltétlenül különböző felbonthatatlan elemek, és ha létezik egy $r = q_1 q_2 \dots q_k$ előállítás is k felbonthatatlannal, akkor $n = k$ és minden $1 \leq i, j \leq n$ esetén p_i asszociáltja egy q_j -nek.

Másképp: Gauss-gyűrűben fennáll a **számelmélet alaptétele**.

Van egységelemes integritási tartomány, ami nem Gauss-gyűrű ?

A válasz : IGEN

$R = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ egységelemes integritási tartomány.

Egységelem : 1

Mik az egységek?

Legyen $c = a + b\sqrt{-5} \in R$ tetszőleges, ekkor

$$|c|^2 = a^2 + 5b^2 \equiv 0, \pm 1 \pmod{5}$$

továbbá $d \mid c \Rightarrow |d|^2 \mid |c|^2$

azaz ha $|1|^2 = 1$ osztóit keressük, akkor $a = \pm 1$ és $b = 0$

$\Rightarrow$ egységek: ± 1

$9 = 9 + 0\sqrt{-5}$ felbontása egyértelmű ?

$$9 = (3 + 0\sqrt{-5})(3 + 0\sqrt{-5}) = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

különböző felbontások?

Van 3-nak d nemtriviális osztója?

$$|3|^2 = 9 \Rightarrow |d|^2 \mid 9 \text{ és } |d|^2 \equiv 0, \pm 1 \pmod{5}$$

NINCS $\Rightarrow 3$ irreducibilis

$(2 + \sqrt{-5})$ és $(2 - \sqrt{-5})$ is, mivel az ő hosszénegyzetük is 9

$\Rightarrow R$ nem Gauss-gyűrű !

Tehát a hierarchiában a Gauss-gyűrű az egységelemes integritási tartomány „alatt” lesz.

Tétel (felbonthatatlan és prím integritási tartományban)

Legyen R egységelemes integritási tartomány és $a \in R^* \setminus U(R)$. Ekkor

ha a prím R -ben $\Rightarrow a$ felbonthatatlan R -ben.

Biz

tfh a prím és $a = bc$

$$\Rightarrow 1 \cdot a = bc$$

$$\Rightarrow a \mid bc$$

a prím $\Rightarrow a \mid b$ vagy $a \mid c$

$$\text{így } 1 = \underset{\substack{\nearrow \\ \in R}}{b/a} \cdot c \text{ vagy } 1 = b \cdot \underset{\substack{\nwarrow \\ \in R}}{c/a} \quad \leftarrow \in R$$

$\Rightarrow b$ vagy c egység.



Ha a felbonthatatlan R -ben $\nRightarrow$ a prím R -ben.

Legyen $R = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$

$$2 = (a + b\sqrt{-5})(e + g\sqrt{-5})$$

konjugáltakkal szorozva

$$4 = (a^2 + 5b^2)(e^2 + 5g^2)$$

$$\Rightarrow a^2 + 5b^2 \mid 4$$

$$\Rightarrow a^2 + 5b^2 = 1, 2, 4$$

$$\Rightarrow b = 0, a = \pm 1, \pm 2$$

$$\Rightarrow a + b\sqrt{-5} = \pm 1 \text{ vagy } e + g\sqrt{-5} = \pm 1$$

$\Rightarrow 2$ irreducibilis, de

$$2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}) = 6$$

$$2 \nmid 1 \pm \sqrt{-5} \Rightarrow 2 \text{ nem prím.}$$

Tétel (felbonthatatlan és prím Gauss – gyűrűben)

Legyen R tetszőleges Gauss - gyűrű és $a \in R^* \setminus U(R)$.

a prím R -ben $\Leftrightarrow a$ felbonthatatlan R -ben.

Biz

$\Rightarrow :$

Tétel (felbonthatatlan és prím integritási tartományban)

$\Leftarrow :$ tfh a irreducibilis és $a \mid p \cdot q \Rightarrow p \cdot q = a \cdot r$

egyértelmű felbontás $\Rightarrow$

$$p = p_1 \dots p_k, \quad q = q_1 \dots q_l, \quad r = r_1 \dots r_t \Rightarrow$$

$$p_1 \dots p_k \cdot q_1 \dots q_l = a \cdot r_1 \dots r_t$$

a asszociált p_i -vel, vagy q_j -vel, különben nem lenne egyértelmű a felbontás

$$\Rightarrow a \mid p \text{ vagy } a \mid q.$$



Def

Az R egységelemes integritási tartományt **euklidészi gyűrűnek** nevezzük, ha $\exists$ olyan φ függvény, amelyre $\varphi : R^* \rightarrow \mathbb{N}$, és

I. $\forall \alpha, \beta \in R, \beta \neq 0$ esetén létezik olyan $\gamma, \delta \in R$, hogy

$$\alpha = \beta\gamma + \delta, \text{ ahol } \delta = 0 \text{ vagy}$$

$$\delta \neq 0 \text{ és } \varphi(\delta) < \varphi(\beta),$$

II. valamint $\varphi(\alpha\beta) \geq \max(\varphi(\alpha), \varphi(\beta))$, $\forall \alpha, \beta \in R^*$ -ra.

Példa

Gauss-egészek $G = \{ a+bi \mid a, b \in \mathbb{Z} \}$

$\varphi: \forall a+bi \in G$ esetén legyen

$$\varphi(a+bi) = (a+bi)(a-bi) = |a+bi|^2 = a^2 + b^2.$$

1. Kérdés: II. tulajdonság teljesül?

$$\varphi(\alpha \cdot \beta) = |\alpha \cdot \beta|^2 = |\alpha|^2 \cdot |\beta|^2 \geq \max(|\alpha|^2, |\beta|^2),$$

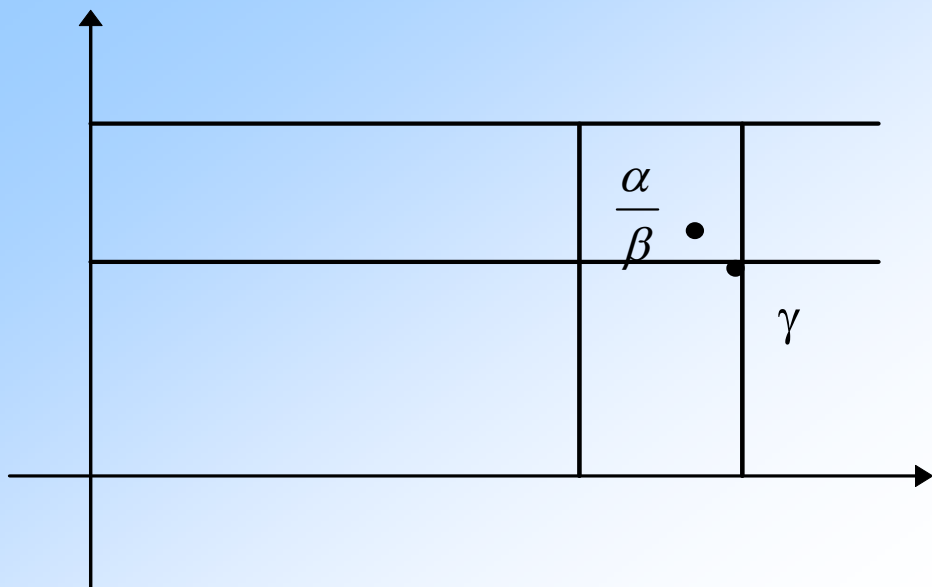
$\forall \alpha, \beta \in G^*$ -ra.

2. Kérdés: I. tulajdonság teljesül?

1. eset: Legyen $\alpha, \beta \in G$, $\beta \neq 0$ és tfh $\alpha/\beta \in G$. Ekkor

$$\gamma = \alpha/\beta \text{ és } \delta = 0.$$

2. eset: Ha $\alpha/\beta \notin G$, akkor válasszuk γ -nak a számsíkon az α/β -hoz legközelebbi (egyik) rácspontot.



$$d\left(\frac{\alpha}{\beta}, \gamma\right) \leq \frac{\sqrt{2}}{2} \Rightarrow \left|\frac{\alpha}{\beta} - \gamma\right|^2 < 1$$

$|\beta|^2$ -tel szorozva:

$$|\beta|^2 \left|\frac{\alpha}{\beta} - \gamma\right|^2 < |\beta|^2,$$

$$|\alpha - \beta\gamma|^2 < |\beta|^2,$$

tehát legyen $\delta = \alpha - \beta\gamma$.

Lemma(egységelem és egység int. tartományban)

Az R integritási tartományban létezik egységelem $\Leftrightarrow$ létezik egység.

Az R egységelemes integritási tartományban $a \in R$ egység $\Leftrightarrow a \mid e$.

Biz

Ha van e egységelem, akkor $er = r$ minden $r \in R$ esetén.

Ha $\exists a \in R$ egység, akkor tetszőleges $r \in R$ esetén

$$a \mid a \Rightarrow \exists e \in R : ae = a.$$

Ekkor e egységelem, mert $a \mid r \Rightarrow \exists s \in R : as = r$,

tehát

$$e \cdot r = e \cdot a \cdot s = (e \cdot a) \cdot s = (a \cdot e) \cdot s = a \cdot s = r.$$

a többi trivi



Tétel (egységek euklidészi gyűrűben)

Euklidészi gyűrűben pontosan azok az elemek egységek, amelyekre a φ függvény felveszi minimumát..

Biz

Legyen $E = \{ r \mid r \in R^*, \varphi(r) \text{ minimális} \}$

1. Kérdés: E elemei egységek?

Legyen $a \in E$, és $b \in R$ tetszőleges. b -t oszthatjuk a -val maradékosan $\Rightarrow \exists c, d \in R$:

$b = ac + d$, ahol

- a. $d = 0$, vagy
- b. $d \neq 0$ és $\varphi(d) < \varphi(a)$.

A b. eset nem fordulhat elő $\varphi(a)$ minimalitása miatt $\Rightarrow$

$$d = 0 \Rightarrow a \mid b.$$

2. Kérdés: Minden egység E -ben van?

Legyen $a \in R$ egység, $b \in E$ adott $\Rightarrow a \mid b \Rightarrow b = ac$.

$$b \in E, b \neq 0 \Rightarrow a, c \in R^*.$$

Az euklidészi gyűrűk II. tulajdonsága $\Rightarrow$

$$\begin{aligned} \varphi(b) = \varphi(a \cdot c) &\geq \max(\varphi(a), \varphi(c)), \\ &\Rightarrow \varphi(b) \geq \varphi(a). \end{aligned}$$

$\varphi(b)$ minimális $\Rightarrow \varphi(a)$ is minimális.



Tétel (asszociáltak euklidészi gyűrűben)

Euklidészi gyűrűben az a, b nemnulla elemekre $a|b$ esetén $\varphi(a) \leq \varphi(b)$, és az egyenlőség pontosan akkor teljesül, ha a és b asszociáltak.

Biz

Euklidészi gyűrű II. tulajdonsága miatt $\varphi(a) \leq \varphi(b)$.

Tfh $a | b$ és $\varphi(a) = \varphi(b)$. Az I. tulajdonság miatt létezik $r, s \in R$:

$$a = b \cdot r + s, \quad \text{ahol} \quad \begin{array}{l} \text{a. } s = 0, \text{ vagy} \\ \text{b. } s \neq 0 \text{ és } \varphi(s) < \varphi(b) = \varphi(a). \end{array} \quad (*)$$

$$s = a + (- (b \cdot r)) = a + b \cdot (-r)$$

$$a | b \Rightarrow \exists t \in R : b = a \cdot t \quad \text{továbbá} \quad a = a \cdot e$$

$$s = a \cdot (e + t \cdot (-r)) \Rightarrow (e + t \cdot (-r)) \in R \Rightarrow a | s.$$

$$\text{Ha } s \neq 0 \Rightarrow \varphi(s) \geq \max(\varphi(a), \varphi(e + t(-r))) \geq \varphi(a)$$

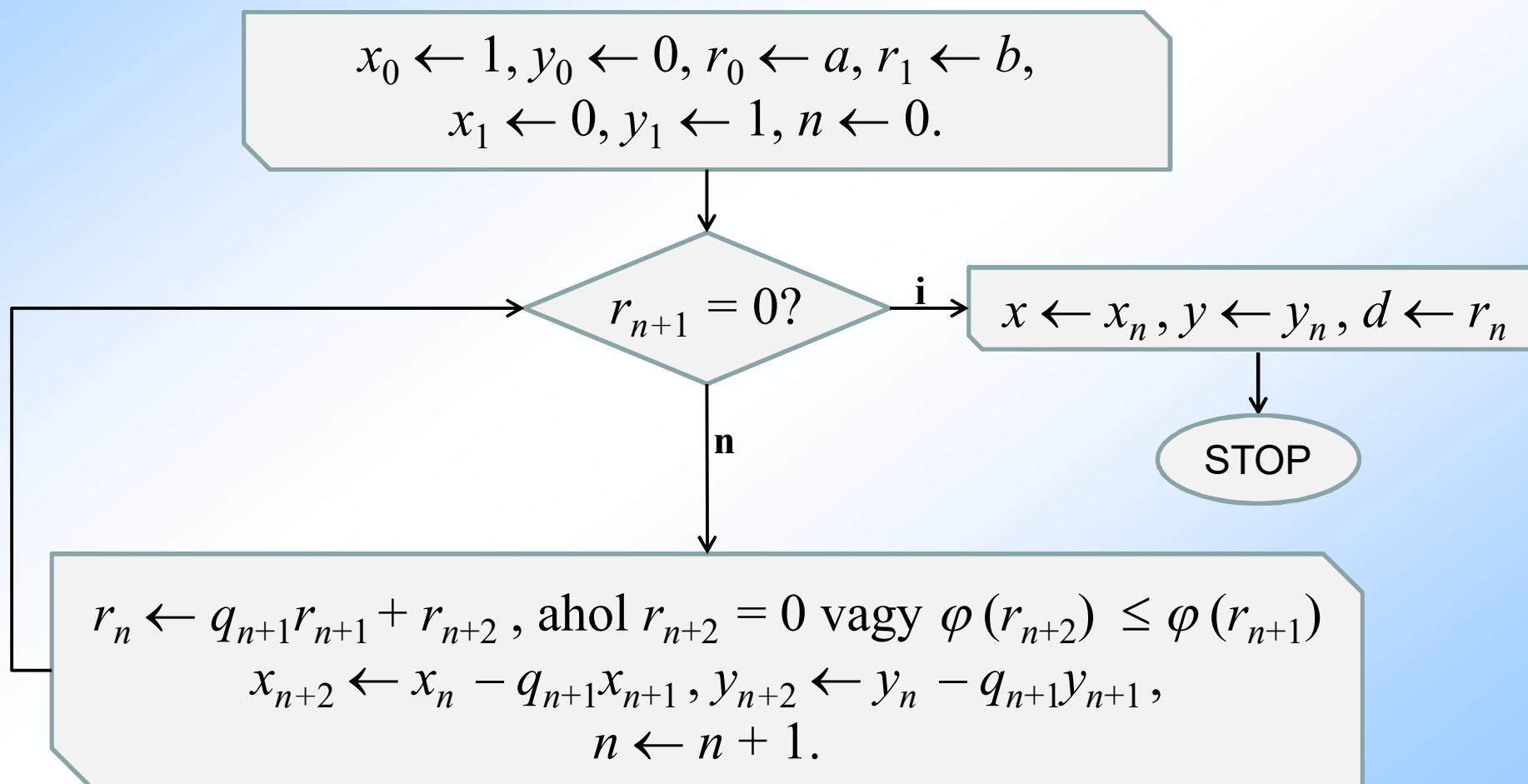
(*) miatt ez nem fordulhat elő $\Rightarrow s = 0$, $b | a$ azaz

$$a \sim b.$$



Def

A **bővített euklidészi algoritmus** egy euklidészi R gyűrűben meghatározza az $a, b \in R$ elemek egy d legnagyobb közös osztóját, valamint az $x, y \in R$ elemeket úgy, hogy $d = ax + by$ teljesüljön.



Tétel (prímek és felbonthatatlanok euklidészi gyűrűben)

Euklidészi gyűrűben egy elem felbonthatatlan $\Leftrightarrow$ prím.

Biz

Láttuk: ha p prím $\Rightarrow p$ felbonthatatlan

$\Leftarrow$: tfh p irreducibilis és $p \mid ab \longrightarrow p \mid a \quad \checkmark$

$\swarrow$
 $p \nmid a \quad \Rightarrow \quad (p, a) = e \text{ egység}$

Eukl. alg $\Rightarrow \quad e = px + ay$

$$b = bee^{-1} = pbxe^{-1} + abye^{-1} \Rightarrow p \mid b$$



Tétel (euklidészi gyűrű UFD)

Euklidészi gyűrűben minden nem nulla és nem egység elem sorrendtől és asszociáltságtól eltekintve egyértelműen felírható prímelemek szorzataként.

Biz

Először megmutatjuk, hogy R euklidészi gyűrűben minden nullától és az egységektől különböző elemnek van felbonthatatlan osztója.

Tfh $a \in R^* \setminus U(R)$, és legyen

$$D = \{r \mid r \in R^* \setminus U(R), r \mid a \text{ és, ha } s \in R^* \setminus U(R) \text{ és } s \mid a \Rightarrow \varphi(r) \leq \varphi(s)\}.$$

Tehát D az a elem azon nem nulla, nem egység osztóit tartalmazza, amikre a φ érték minimális.

$$D \neq \emptyset \Rightarrow \exists f \in D$$

Indirekte tfh f nem felbonthatatlan $\Rightarrow$

$$f = b \cdot c \text{ és } b, c \notin U(R) \Rightarrow b \mid a .$$

$b \mid f$ és nem asszociáltak $\Rightarrow$

Tétel (asszociáltak euklidészi gyűrűben) $\Rightarrow$

$$\varphi(b) \neq \varphi(f) \Rightarrow \varphi(b) < \varphi(f) ,$$



mert ekkor b lenne D -ben f helyett.

tehát van a -nak felbonthatatlan osztója

Tfh $\varphi(a)$ minimális az $R^* \setminus U(R)$ -beli elemekre nézve

Tétel (egységek euklidészi gyűrűben) $\Rightarrow$ a felbonthatatlan.

Most legyen $a \in R^* \setminus U(R)$, $\varphi(a) = n$, és tegyük fel, hogy n -nél kisebb φ értékkel rendelkező elemek esetén az állítás igaz.

$$\exists f \text{ felbonthatatlan} : f \mid a \Rightarrow a = fh .$$

Kérdés: lehet-e $\varphi(h) = \varphi(a)$?

$$\text{Ekkor } h \mid a \Rightarrow a \sim h \text{ lenne,}$$

de f nem egység, tehát $\varphi(h) \neq \varphi(a)$.

$$h \mid a \Rightarrow \varphi(h) < \varphi(a).$$

1. eset: Tfh h egység $\Rightarrow$ a felbonthatatlan.

2. eset: Tfh h nem egység $\Rightarrow$

indukciós feltétel $\Rightarrow h$ -nak $\exists$ megfelelő felbontása:

$$h = f_1 \cdot f_2 \cdot \dots \cdot f_r \Rightarrow a = f \cdot f_1 \cdot f_2 \cdot \dots \cdot f_r.$$

Unicitás: tfh indirekte, hogy van olyan *elem*, amelynek két különböző felbontása létezik. Legyen ezek közül a olyan, hogy $\varphi(a)$ minimális.

$$a = p_1 \dots p_k = q_1 \dots q_r \Rightarrow p_1 \mid a \Rightarrow p_1 \mid q_1 \dots q_r$$

$p_1 \mid q_i \Rightarrow$ asszociáltak, mert irreducibilisek

egyszerűsítve kapjuk a' -t, amelyre $\varphi(a') < \varphi(a)$.



Tétel (euklidészi gyűrű főideálgyűrű)

Euklidészi gyűrűben minden ideál főideál.

Biz

$$\text{Ha } I = \{ 0 \} \Rightarrow I = \langle 0 \rangle .$$

Tfh $I \neq \{ 0 \}$, ekkor legyen

$$S = \{ \varphi(x) \mid x \in I \text{ és } x \neq 0 \}$$

S legkisebb eleme $\varphi(a) : a \neq 0 \in I$.

Maradékosan osztjuk $b \in I$ -t a -val:

$$b = aq + r \text{ és } r = 0, \text{ vagy } r \neq 0 \text{ és } \varphi(r) < \varphi(a)$$

$$I \text{ ideál} \Rightarrow r = b - aq \in I$$

$$\varphi(a) \text{ minimális} \Rightarrow r = 0.$$

$$b = aq \Rightarrow I = \langle a \rangle.$$



Megjegyzés

$$R_{\sqrt{-19}} = \left\{ a + b \left(\frac{1 + \sqrt{-19}}{2} \right) \mid a, b \in \mathbb{Z} \right\}$$

bizonyítható, hogy főideálgyűrű, de nem euklidészi

$\Rightarrow$ az előző tétel megfordítása nem igaz.

Def

Egy R gyűrű egy I valódi ideálját **maximális ideálnak** nevezzük, ha nincs nála bővebb valódi ideál.

Tétel (irreducibilitás és főideál kapcsolata)

Legyen R tetszőleges főideálgyűrű és $a \in R^* \setminus U(R)$.

$\langle a \rangle$ valódi ideál maximális R -ben

$\Leftrightarrow$

a felbonthatatlan R -ben.



$\Rightarrow :$

Legyen R tetszőleges egységelemes integritási tartomány, $a \in R^* \setminus U(R)$

Feltétel : a felbontható

$$\exists \ b, c \in R^* \setminus U(R) : a = bc .$$

$$\langle a \rangle \subset \langle b \rangle \subset R$$

valódi

Tehát $\langle a \rangle$ nem maximális ideál.

$\Leftarrow :$ Indirekt feltétel :

a felbonthatatlan, de $\langle a \rangle$ nem maximális.

$\exists I$ R -beli ideál :

$$\langle a \rangle \subset I \subset R$$

R főideálgyűrű $\Rightarrow$

$\exists 0 \neq b$ nemegység :

$$I = \langle b \rangle \subset R$$

$$\langle a \rangle \subset \langle b \rangle \subset R$$

azaz a minden többszöröse b többszöröse

$$\Rightarrow a = bc$$

c nem egység, mert akkor $\langle a \rangle = \langle b \rangle$ lenne

$\Rightarrow a$ nem felbonthatatlan.



Def

Legyen R egységelemes, kommutatív gyűrű. Egy R -beli I ideált **prímideálnak** nevezünk, ha $a \cdot b \in I$ -ből $a \in I$ vagy $b \in I$ következik.

Példa

1. $2\mathbb{Z}$ prímideál $\mathbb{Z}$ -ben :

$$ab \in 2\mathbb{Z} \Rightarrow ab \text{ páros, } a \text{ vagy } b \text{ páros} \Rightarrow \\ a \in 2\mathbb{Z} \text{ vagy } b \in 2\mathbb{Z} .$$

2. $2\mathbb{Z}$ maximális ideál is $\mathbb{Z}$ -ben :

$$\text{Tfh } 2\mathbb{Z} \subseteq I \subseteq \mathbb{Z} .$$

$$\text{Ha } \exists a \in I \text{ páratlan} \Rightarrow 1 \in I \Rightarrow \langle a \rangle = I = \mathbb{Z} ,$$

$$\text{különben } I = 2\mathbb{Z} .$$

3. $49\mathbb{Z}$ nem maximális és nem prímideál is $\mathbb{Z}$ -ben :

$$49\mathbb{Z} \subset 7\mathbb{Z} \subset \mathbb{Z} ,$$

$$7 \cdot 7 = 49 \in 49\mathbb{Z} , \text{ de } 7 \notin 49\mathbb{Z} .$$

Tétel (faktorgyűrű és prímiideál)

Legyen R kommutatív, egységelemes gyűrű és I az R -nek ideálja.

R/I integritási tartomány $\Leftrightarrow I \neq R$ és I prímiideál.

Biz

R/I int. tart.

$\Leftrightarrow$

nincs nullosztó.

$\Leftrightarrow$

$$(I+a) \cdot (I+b) = I \Rightarrow I+a = I \text{ vagy } I+b = I.$$



Tétel (faktorgyűrű és maximális ideál)

Legyen R kommutatív, egységelemes gyűrű és I az R -nek ideálja.

R/I test $\Leftrightarrow I$ maximális ideál.

Biz

1. Tfh hogy I maximális ideál R -ben, és $(I \neq) I+a \in R/I$.

$\Rightarrow S = \{i+a \cdot x \mid i \in I, x \in R\}$ ideál, hiszen:

$$S-S \subseteq S : i_1 + ax_1 - i_2 - ax_2 = \underbrace{(i_1 - i_2)}_{\in I} + a \underbrace{(x_1 - x_2)}_{\in R} \in S.$$

$$RS \subseteq S : \underbrace{ri}_{\in I} + \underbrace{rax}_{\in R} = ri + arx \in S.$$

Valamint $I \subset S$, mert $a \notin I$.

I maximális $\Rightarrow S = R \Rightarrow$

alkalmas $i \in I, x \in R$ -rel $e = i+a \cdot x \Rightarrow$

$$I + e = I + i + a \cdot x = I + a \cdot x = (I + a) \cdot (I + x)$$

R/I kommutatív egységelemes gyűrű és invertálható $\Rightarrow$ test.

2. Tfh R/I test, és legyen M egy olyan ideál, amely valódi módon tartalmazza I -t, azaz $\exists a \in R$ elem, amelyre $a \in M$ és $a \notin I$.

R/I test $\Rightarrow$

$$(I + a) \cdot (I + x) = (I + b)$$

egyenlet bármely $b \in R$ -re megoldható $\Rightarrow$

$$I + a \cdot x = I + b.$$

$I \subset M$ és $a \in M \Rightarrow$

$$I + a \cdot x \subseteq M \Rightarrow$$

$$b \in M \Rightarrow$$

$$M = R.$$



Lemma (maximális és prímeál kapcsolata)

Kommutatív, egységelemes gyűrűben $\forall$ maximális ideál prímeál.

Biz

Legyen R kommutatív, egységelemes gyűrű.

Ha I maximális ideál R -ben $\Rightarrow$

R/I test $\Rightarrow$

R/I integritási tartomány $\Rightarrow$

Tétel (faktorgyűrű és prímeál) $\Rightarrow$

I prímeál.



Lemma (triviális ideálok)

Legalább 2 elemű kommutatív egységelemes R gyűrűnek, **akkor és csak akkor** vannak csupán triviális ideáljai, ha test.

Biz

1. Tfh R nem test $\Rightarrow$

$\exists a \neq 0$ elem, amelyik nem invertálható $\Rightarrow$

a többszörösei között nem fordul elő $e \Rightarrow$

(a) az R -nek nem triviális ideálja.

2. Tfh R test, I ideálja, és $I \neq \{0\} \Rightarrow$

$\exists a \in I: a \neq 0.$

R test $\Rightarrow$ a -nak létezik a^{-1} inverze

továbbá az ideál 2. tulajdonsága $\Rightarrow$

$$e = a^{-1}a \in I \Rightarrow \quad \forall b \in R : be \in I \Rightarrow$$

tehát $I = R$, triviális ideál.



Def

Legyen R integritási tartomány és $T = \{ (a, b) \mid a, b \in R, b \neq 0 \}$ és $\sim$ ekvivalenciareláció $R \times R^*$ halmazon:

$$(a, b) \sim (c, d) \Leftrightarrow a \cdot d = b \cdot c.$$

A $\sim$ által meghatározott osztályok testet alkotnak a köv. műveletekre:

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(a \cdot d + b \cdot c, b \cdot d)},$$

$$\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(a \cdot c, b \cdot d)},$$

amelyet **R hányadostestének** nevezünk.