Farkas Gábor: Diszkrét matematika II.

(előadás diák)

Lektorálta: Láng Csabáné

Felhasznált irodalom:

Járai Antal & al:	**Bevezetés a matematikába** **ELTE Eötvös Kiadó 2005, 2006**
Láng Csabáné:	**Bevezető fejezetek a matematikába I.** **ELTE Budapest, 1997**
Láng Csabáné:	**Bevezető fejezetek a matematikába II.** **ELTE Budapest, 1998**
Gonda János:	**Bevezető fejezetek a matematikába III.** **ELTE TTK Budapest, 1998**
Láng Csabáné:	**Testbővítések, véges testek 2008** **Prezentációs anyag, ELTE IK, Digitális Könyvtár**

6. SZÁMELMÉLET

6.1. Oszthatóság

Oszthatóság a természetes számok körében

Def. Legyen n, $m \in$ **N**. m **osztója** n-nek, ha $\exists\, k \in$ **N**: $n = m \cdot k$.

jelben: $m \mid n$

n többszöröse m-nek

$m \neq 0$ esetén a regularitás miatt legfeljebb egy ilyen k létezik

$m \mid n \longleftrightarrow n/m \in \mathbb{N}$

6.1.2. Az oszthatóság tulajdonságai $\mathbb{N}$-ben. *A természetes számok körében*

(1) *ha* $m|n$ *és* $m'|n'$*, akkor* $mm'|nn'$*;*

(2) *a nullának minden természetes szám osztója;*

(3) *a nulla csak saját magának osztója;*

(4) *az* 1 *minden természetes számnak osztója;*

(5) *ha* $m|n$*, akkor* $mk|nk$ *minden* $k \in \mathbb{N}$*-re;*

(6) *ha* $k \in \mathbb{N}^+$ *és* $mk|nk$*, akkor* $m|n$*;*

(7) *ha* $m|n_i$ *és* $k_i \in \mathbb{N}$*,* $(i = 1, 2, \ldots, j)$*, akkor* $m| \sum_{i=1}^{j} k_i n_i$*;*

(8) *bármely nem nulla természetes szám bármely osztója kisebb vagy egyenlő, mint a szám;*

(9) *az* $|$ *reláció reflexív, tranzitív és antiszimmetrikus, azaz részben rendezés.*

Megjegyezzük, hogy bár a $|$ reláció $\mathbb{N}^+$-on a $\leq$ leszűkítése, $\mathbb{N}$-ben a 0 maximális elem az $|$ relációra nézve. $\square$

Oszthatóság egységelemes integritási tartományban

6.1.5. Az oszthatóság tulajdonságai egységelemes integritási tartományban. *Egy egységelemes integritási tartomány elemei körében*

(1) *ha* $b|a$ *és* $b'|a'$, *akkor* $bb'|aa'$;

(2) *a nullának minden elem osztója;*

(3) *a nulla csak saját magának osztója;*

(4) *az* 1 *egységelem minden elemnek osztója;*

(5) *ha* $b|a$, *akkor* $bc|ac$ *minden* $c \in R$*-re;*

(6) *ha* $bc|ac$ *és* $c \neq 0$, *akkor* $b|a$;

(7) *ha* $b|a_i$ *és* $c_i \in R$, $(i = 1, 2, \ldots, j)$, *akkor* $b| \sum_{i=1}^{j} c_i a_i$;

(8) *az* $|$ *reláció reflexív és tranzitív.* $\square$

A továbbiakban legyen *R* tetszőleges egységelemes integritási tartomány.

Def. Az az R -beli elem, amely minden más R -beli elemnek osztója R -beli **egység**. Az R -beli egységek halmaza $U(R)$.

Def. Ha a, $b \in R$ elemek egymás egységszeresei, akkor **asszociáltak**. Jelben $a \sim b$.

Észrevételek:

$\sim$ ekvivalencia reláció és kompatibilis az | relációval

az egységek Abel-csoportot alkotnak (R egységcsoportja)

0-nak önmaga az egyetlen asszociáltja

Def. Ha $a \in R^* \setminus U(R)$: a **triviális osztói** az egységek és önmaga egységszeresei.

Az $a \in R^* \setminus U(R)$ elem **felbonthatatlan (irreducibilis)** ***R*-ben,** ha

$$a = bc \Rightarrow b \text{ vagy } c \text{ egység } R\text{-ben.}$$

kizáró vagy

N esetén **törzsszám**

Def. Az $a \in R^* \setminus U(R)$ elem **prím** ***R*-ben**, ha

$$a \mid bc \Rightarrow a \mid b \vee a \mid c, \quad \text{ahol } b, c \in \mathrm{R}\ .$$

Az $a \in R^* \setminus U(R)$ elem **összetett**, ha nem csak triviális osztója van.

Tétel. Tetszőleges *R* egységelemes integritási tartományban minden *p* elemre:

$$p \text{ prím} \Rightarrow p \text{ felbonthatatlan} .$$

Biz. tfh p prím és $p = bc$

$\exists 1$

$p \mid b$

vagy $p \mid c$

$b = pq = b(cq) \qquad \Rightarrow cq = 1$

$\Rightarrow c, q$ egység p, b asszociáltak .

Def. Legyen $a_1, ..., a_n \in R$, $L \subseteq R$ és $\forall\, d \in L$ –re :

$$d \mid a_i \quad (i = 1, ..., n) \,,$$

$$d' \mid a_i \;\; (i = 1, ..., n) \;\Rightarrow d' \mid d \,.$$

Ekkor L elemei az $a_1, ..., a_n$ elemek **legnagyobb közös osztói.**

jelben: $\text{lnko}(a_1, ..., a_n) = (a_1, ..., a_n) = d$

d csak asszociáltság erejéig egyértelmű !

$\Rightarrow$ kijelölünk egyet.

$a_1, ..., a_n$ **relatív prímek**, ha d egység.

Erősebb : **páronként relatív prímek**

Pl.

$$(4, 8, 9) = 1$$

$$(4, 8) = 4,\ (4, 9) = 1, (8, 9) = 1$$

Def. Legyen $a_1, ..., a_n \in R$, $T \subseteq R$ és $\forall\, t \in T$ –re :

$$a_i \mid t \qquad (i = 1, ..., n) \,,$$

$$a_i \mid t' \ (i = 1, ..., n) \ \Rightarrow \ t \mid t' \ .$$

Ekkor T elemei az $a_1, ..., a_n$ elemek legkisebb közös többszörösei.

$$\text{lkkt}(a_1, ..., a_n) = [a_1, ..., a_n] = t \ .$$

t csak asszociáltság erejéig egyértelmű !

$\Rightarrow$ kijelölünk egyet.

Oszthatóság a egész számok körében

Észrevételek:

$k, m \in \mathbb{Z}$, akkor $|km| = |k| \cdot |m|$

± 1 egység, mert $\forall\, a \in \mathbf{Z} : a = a \cdot 1 = (-a)(-1)$

tfh e egység $\Rightarrow e \mid 1 \Rightarrow 1 = eq \Rightarrow |1| = |eq| = |e||q|$

$$\downarrow$$

$1 \le |e|,\ 1 \le |q| \Rightarrow |e| = 1 \Rightarrow e = \pm 1$

$$\downarrow$$

Z -ben az egységek pontosan a ± 1

Az **N**-beli állítások érvényben maradnak

Def. A 2-vel osztható egész számok a **páros számok**. **Páratlan** az az egész szám, amely nem páros.

Észrevételek:

$$\forall\, a, b \in \mathbf{Z} : a \mid b \wedge b \neq 0 \Rightarrow |a| \leq |b|\ .$$

érvényben van a maradékos osztás tétele:

Tetszőleges a , $b(\neq 0) \in \mathbf{Z}$ számhoz egyértelműen létezik olyan q , $r \in \mathbf{Z}$, hogy

$$a = qb + r \ \wedge\ 0 \leq r < |b|\ .$$

Elvégethető az euklidészi algoritmus!

6.1.11. Bővített euklideszi algoritmus. *A következő eljárás meghatározza az $a, b \in \mathbb{Z}$ egészek egy d legnagyobb közös osztóját, valamint az $x, y \in \mathbb{Z}$ egész számokat úgy, hogy $d = ax + by$ teljesüljön. (Az eljárás során végig $ax_n + by_n = r_n$, $n = 0, 1, \ldots$.)*

(1) *[Inicializálás.]* Legyen $x_0 \leftarrow 1$, $y_0 \leftarrow 0$, $r_0 \leftarrow a$, $x_1 \leftarrow 0$, $y_1 \leftarrow 1$, $r_1 \leftarrow b$, $n \leftarrow 0$.

(2) *[Vége?]* Ha $r_{n+1} = 0$, akkor $x \leftarrow x_n$, $y \leftarrow y_n$, $d \leftarrow r_n$, és az eljárás véget ért.

(3) *[Ciklus.]* Legyen $q_{n+1} \leftarrow \lfloor r_n / r_{n+1} \rfloor$, $r_{n+2} \leftarrow r_n \bmod r_{n+1} = r_n - r_{n+1} q_{n+1}$, $x_{n+2} \leftarrow x_n - x_{n+1} q_{n+1}$, $y_{n+2} \leftarrow y_n - y_{n+1} q_{n+1}$, $n \leftarrow n + 1$ és menjünk (2)-re.

Biz. szigorú monotonitás miatt biztosan véges számú lépés lesz

r_n közös osztó:

$$r_n \mid r_n \wedge r_n \mid r_{n\text{-}1} \Rightarrow r_n \mid r_{n\text{-}2}$$

$$\ldots \; r_n \mid a \wedge r_n \mid b$$

$$ax_0 + by_0 = a \cdot 1 + b \cdot 0 = a = r_0$$

tfh n – 1-ig igaz

$$ax_{\mathrm{n}} + by_{\mathrm{n}} = a(x_{n\text{-}2} - q_n x_{n\text{-}1}) + b(y_{n\text{-}2} - q_n y_{n\text{-}1}) =$$

$$ax_{n\text{-}2} + by_{n\text{-}2} - q_n(ax_{n\text{-}1} + by_{n\text{-}1}) = r_{n\text{-}2} - q_n r_{n\text{-}1}$$

$$= r_n$$

6.1.14. Következmény. *Bármely* $a_1, a_2, \dots, a_n \in \mathbb{Z}$ *számoknak létezik legnagyobb közös osztója és*

$$\operatorname{lnko}(a_1, a_2, \dots, a_n) = \operatorname{lnko}\bigl(\operatorname{lnko}(a_1, a_2), a_3, a_4, \dots, a_n\bigr).$$

Bizonyítás. Az a_1, a_2 számoknak létezik egy $d_{1,2}$ legnagyobb közös osztója. Az a_1, a_2 közös osztói pontosan $d_{1,2}$ osztói. Így $a_1, a_2, \dots, a_n$ közös osztói $d_{1,2}, a_3, a_4, \dots, a_n$ közös osztói. $\square$

Tétel. Az egész számok körében p akkor és csak akkor **prím**, ha felbonthatatlan.

Biz. Már láttuk, hogy prím felbonthatatlan !

Tfh p felbonthatatlan

Legyen $p \mid bc$ $\longrightarrow$ $p \mid b$ $\surd$

$\swarrow$

$p \nmid b \quad \Rightarrow \quad (p, b) = 1$

$$1 = px + by$$

$$c = pcx + bcy \;\Rightarrow\; 0 \bmod p \;\Rightarrow\; p \mid c$$

Észrevétel:

$$(a, b) = 1 \;\wedge\; a \mid bc \;\Rightarrow\; a \mid c$$

A számelmélet alaptétele. Minden ***n*** nemnulla, nem egység egész szám sorrendre és asszociáltságra való tekintet nélkül egyértelműen bontható fel felbonthatatlanok szorzatára.

Biz (pozitívakra)

(egzisztencia) tfh $n > 1$

Teljes indukció: $n = 2$ kész, tfh $n - 1$ -ig kész

Ha n felbonthatatlan $\longrightarrow$ kész

n ***nem*** felbonthatatlan $\longrightarrow$ $n = ab \wedge a, b$ nem egység!

$a, b < n \Rightarrow$ igaz rájuk az ind. feltétel

n felbontása = ***a*** felbontása szor ***b*** felbontása

(unicitás) tfh indirekte, hogy n a legkisebb olyan szám, amely felbontása nem egyértelmű**.**

$$n = p_1 \ldots p_k = q_1 \ldots q_r \quad \Rightarrow \qquad p_1 \mid n \;\Rightarrow\; p_1 \mid q_1 \ldots q_r$$

$$p_1 \mid q_1 \qquad\qquad p_1 \mid q_2 \ldots q_r$$

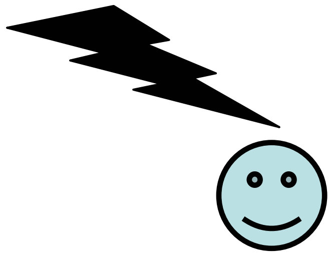
16

$$p_1 \mid q_2 \qquad\qquad p_1 \mid q_3 \ldots q_r$$

$$p_1 \mid q_i \qquad \Rightarrow\; p_1 = q_i \;\Rightarrow$$

$$n_1 = n / p_1 = p_2 \ldots p_k = q_1 \ldots q_{i-1} q_{i+1} \ldots q_r$$

$n_1 < n$ és van két lényegesen különböző felbontása !



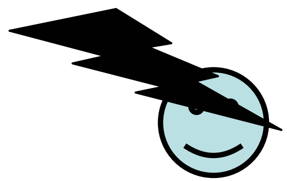
6.1.18. Eukleidész tétele. *Végtelen sok prímszám van.*

Biz. indirekt, tfh véges sok van $p_1, p_2, \cdots, p_k$

legyen $n = \prod_{j=1}^{k} p_j$

számelmélet alaptétele $\Rightarrow \exists \; p_j : \; p_j \mid n+1$

$\Rightarrow \; p_j \mid 1$



6.1.19. Megjegyzés. Ha, hasonlóan mint az előző bizonyításban, n az összes, a p_k prímnél nem nagyobb prímek szorzata, akkor $n+2, n+3, n+4, \ldots, n+p_k$ mind összetettek, azaz a természetes számok sorozatában találtunk $p_k - 1$ egymás utáni összetett számot. Mivel tetszőlegesen nagy prímszám létezik, akármilyen hosszú csupa összetett számot tartalmazó intervallum van.

$\circ$ **6.1.20. Megjegyzés.** Megmutatható, hogy „elég sok” prímszám van, például a prímszámok reciprokainak összege végtelen. A prímszámtétel szerint

$$\lim_{x\to\infty} \frac{\natural\{p : p \leq x,\, p \text{ prímszám}\}}{\frac{x}{\ln x}} = 1.$$

Def Egy $n > 1$ egész

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

alakú felírását, ahol p_i -k különböző (pozitív) prímek és $\alpha_i > 0$, n **kanonikus alakjának** nevezzük. **Módosított kanonikus alak,** ha $\alpha_i = 0$ is megengedett.

Észrevétel (*n* osztói)

$$n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$$

módosított kanonikus alakú osztói

$$d = p_1^{\beta_1} \ldots p_r^{\beta_r}$$

ahol $0 \leq \beta_i \leq \alpha_i$, $i = 1, 2, ..., r$.

Észrevétel (lnko és lkkt)

Legyen *a* és *b* módosított kan. alakja

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r} \qquad b = p_1^{\beta_1} \dots p_r^{\beta_r}$$

ekkor

$$(a, b) = p_1^{\min(\alpha_1, \beta_1)} \dots p_r^{\min(\alpha_r, \beta_r)}$$

$$[a, b] = p_1^{\max(\alpha_1, \beta_1)} \dots p_r^{\max(\alpha_r, \beta_r)}$$

6.1.22. Következmény. *Ha $a, b, c \in \mathbb{Z}$ és a is, b is relatív prím c-hez, akkor ab is.* $\square$

6.1.23. Következmény. *Tetszőleges $a, b \in \mathbb{Z}$ számoknak létezik legkisebb közös többszöröse, és* $\text{lnko}(a, b) \cdot \text{lkkt}(a, b) = |ab|$. $\square$

6.1.24. Következmény. *Ha $a, b, c \in \mathbb{Z}$, akkor*

$$\text{lkkt}(ac, bc) = c \cdot \text{lkkt}(a, b). \quad \square$$

6.1.25. Következmény. *Tetszőleges $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ számoknak létezik legkisebb közös többszöröse, és*

$$\text{lkkt}(a_1, a_2, \ldots, a_n) = \text{lkkt}\big(\text{lkkt}(a_1, a_2), a_3, a_4, \ldots, a_n\big). \quad \square$$

Erathosztenész szitája

1	2	3	4	5	6	7	8	9	10	11

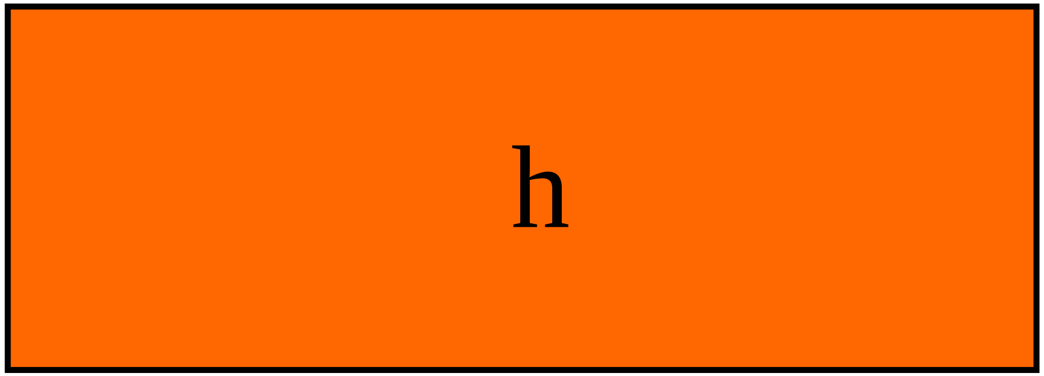
12	13	14	15	16	17	18	19
20	21	22	23	24	25	26	27

Általánosított szita

$$f_1(x),\ f_2(x),\ \ldots,\ f_n(x)$$

egész együtthatós, irreducibilis polinomok, pozitív főegyütthatóval.

$f_k(x)$



lineáris kongruencia *mod (p)*

h

***p*:szitáló prím**

innen kezdünk

$$1, \ldots, h+q\cdot p, \ldots, 2^r-1$$

$$f_k(1), \ldots, f_k(h+q\cdot p), \ldots, f_k(2^r-1)$$

Mennyit szitálhatunk p-vel ?

$$q = 0, 1, \ldots, (h+q\cdot p \leq 2^r-1)$$

6.2. Kongruenciák

Kongruenciák $\quad a \equiv b \pmod{m}$, ha $m \mid a - b$

Tétel(kongruencia tulajdonságai)

(1) ekvivalencia reláció,

(2) $a \equiv b$ (mod m) $\wedge$ $c \equiv d$ (mod m)

$$\Rightarrow a + c \equiv b + d \pmod{m}$$

(3) $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}$

$$\Rightarrow ac \equiv bd \pmod{m}$$

(4) $a \equiv b \pmod{m} \wedge f(x) \in \mathrm{Z}[x]$

$$\Rightarrow f(a) \equiv f(b) \pmod{m}$$

(5) Ha $(c, m) = d$

$$ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{m/d}$$

Biz. $\Rightarrow$ defből $m \mid (a-b)c$

$$\Rightarrow m/d \mid (a-b)\, c/d$$

másrészt

$$(m/d,\, c/d) = 1$$

$$\Rightarrow m/d \mid (a-b)$$

$$\Rightarrow a \equiv b \pmod{m/d}$$

$\Leftarrow$ **Tfh** $a \equiv b \ (\mathit{mod}\ m/d)$

$$\Rightarrow mq/d = (a-b)$$

$$\Rightarrow mqc/d = (a-b)c$$

c/d egész $\Rightarrow m \mid ac - bc$

Észrevétel

$$a' \equiv a \pmod{m} \longrightarrow \operatorname{lnko}(a,m) = \operatorname{lnko}(a',m)$$

Def. $[a]_m$ az a elem által reprezentált ***m* szerinti maradékosztály** az a -val kongruens elemek halmaza (mod m) .

Def. **Teljes maradékrendszer (TMR) modulo *m*** tartalmaz az összes m szerinti maradékosztályból pontosan egyet.

$[a]_m$ az ***a* elem által reprezentált *m* szerinti redukált maradékosztály**, ha $(a, m) = 1$.

Redukált maradékrendszer (RMR) modulo *m* tartalmaz az összes ***m*** szerinti redukált maradékosztályból pontosan egyet.

$[a]$ helyett szokásos jelölés még: $\overline{a}$.

Példák

1. Biztosan TMR-t alkotnak a következő számhalmazok mod *m* : $0, 1, \ldots, |m| - 1$

ha *m*

páratlan: $0, \pm 1, \ldots, \pm\big(|m| - 1\big)/2$

páros: $0, \pm 1, \ldots, \pm\big(|m|/2 - 1\big),$ $|m|/2$ vagy $-|m|/2$

2. Legyen $m \in \mathbf{N}$, és vegyünk egy TMR-t mod *m* . Definiáljunk műveleteket a következőképpen:

$$\overline{a} + \overline{b} = \overline{a + b},$$

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

Jelöljük Z_m-nel ezt a struktúrát. A (Z_m, +, ·) struktúra kommutatív, egységelemes gyűrű.

6.2.3. Tétel. *Legyen $m > 1$ egész. Ha*

$$1 < \text{lnko}(a, m) < m,$$

akkor a maradékosztálya nullosztó $\mathbb{Z}_m$-ben. Ha

$$\text{lnko}(a, m) = 1,$$

akkor a maradékosztályának van multiplikatív inverze $\mathbb{Z}_m$-ben. Speciálisan, ha m prímszám, akkor $\mathbb{Z}_m$ test.

Biz.

$$d = \text{lnko}(a, m)$$

$$1 < d < m \longrightarrow a \cdot (m/d) = (a/d) \cdot m \equiv 0 \pmod{m}$$

$$x = m/d \longrightarrow \overline{a} \cdot \overline{x} = \overline{0}, \text{ azaz } \overline{a} \text{ nullosztó } \mathbb{Z}_m\text{-ben}$$

Ha $d = 1$, akkor $\Rightarrow$

bővített euklidészi algoritmus $\Rightarrow$ $ax + my = 1$ $\quad x, y \in \mathbb{Z}$

$ax \equiv 1 \pmod{m} \longrightarrow \overline{a} \cdot \overline{x} = \overline{1}$

Ez azt jelenti, hogy $\mathbf{Z}_m$-ben $\overline{a}$ multiplikatív inverze $\overline{x}$

Ha m prím, és $a \not\equiv 0 \pmod{m}$

$\Rightarrow$ $d = 1$ mindig teljesül

$\Rightarrow$ $\mathbf{Z}_m$ test

6.2.4. Az Euler-féle φ függvény. Legyen $m > 0$ egész szám, és jelölje $\varphi(m)$ a modulo m redukált maradékosztályok számát; φ az *Euler-féle φ függvény*. Nyilván $\varphi(m)$ az m-hez relatív prím számok száma a $0, 1, 2, \ldots, m-1$ számok között. Például $\varphi(1) = 1$ (sic!), $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(8) = 4$.

Más megfogalmazásban:

Legyen $n \in$ $\mathbf{N}^+$, ekkor $\boldsymbol{\varphi(n)}$ jelenti az n – nél nem nagyobb, hozzá relatív pozitív prímek számát, azaz

$$\varphi(n) = \sum_{\substack{1 \le k \le n \\ (k, n) = 1}} 1$$

Tétel (*omnibusz*)

Legyen $m > 1$ egész,

$\{ a_1, ..., a_m \}$ TMR modulo m ,

$\{ b_1, ..., b_{\varphi(m)} \}$ RMR modulo m ,

$c, d \in \mathbf{Z}$ és $(c, m) = 1$.

Ekkor

$\{ ca_1 + d , ..., ca_m + d \}$ TMR modulo m ,

$\{ cb_1, ..., cb_{\varphi(m)} \}$ RMR modulo m .

Biz. tfh (indirekt) van két nem inkongruens elem

$$(c, m) = 1$$

$$ca_i + d = ca_j + d$$

$$ca_i = ca_j$$

$$a_i = a_j$$

és pontosan m db elem!

$(c, m) = 1$ és $(b_i, m) = 1$

$$\Rightarrow (cb_i, m) = 1$$

6.2.6. Euler–Fermat tétel. *Legyen $m > 1$ egész szám, a relatív prím m-hez. Ekkor* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Biz.

legyen $\{ r_1, \ldots, r_{\varphi(m)} \}$ RMR modulo m ,

$(a, m) = 1 \;\Rightarrow\; \{ ar_1 , \ldots, ar_{\varphi(m)} \}$ is RMR modulo m.

megfelelő párosítás $\Rightarrow\;\; r_i \equiv ar_j \pmod{m}$

összeszorozva:

$(r_i , m) = 1$

$$a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} r_i \equiv \prod_{i=1}^{\varphi(m)} {}_{r}\, r_i \pmod{m}$$

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

6.2.7. Következmény: Fermat-tétel. *Legyen* p *prímszám. Ha* $a \in \mathbb{Z}$ *és* $p \nmid a$, *akkor* $a^{p-1} \equiv 1 \pmod{p}$. *Ha* $a \in \mathbb{Z}$ *tetszőleges, akkor* $a^p \equiv a \pmod{p}$.

Biz.

$\varphi(p) = p - 1 \longrightarrow$ előző tétel miatt kész az első alak

$$\begin{tikzcd}
 & \text{második alak} \arrow[dl] \arrow[dr] & \\
p \mid a \arrow[d] & & p \nmid a \arrow[d] \\
0 \equiv 0 \arrow[dr] & & \text{első alak} \arrow[dl] \\
 & \text{kész} &
\end{tikzcd}$$

Lineáris kongruencia megoldása

$$ax \equiv b \pmod{m}$$

$m \mid ax - b \Rightarrow$ $\quad ax + my = b$

$d = \text{lnko}(a, m)$ $\quad d \mid ax + my \Rightarrow d \mid b$

$a = a'd,\ b = b'd,\ m = m'd$ $\quad a'x \equiv b' \pmod{m'}$

bővített euklidészi algoritmus $\Rightarrow$

$$ax_0 + my_0 = d$$

$$a'x_0 + m'y_0 = 1$$

$$a'x_1 + m'y_1 = b' \quad \text{ahol } x_1 = x_0 b' \text{ és } y_1 = y_0 b'$$

$$a'(x - x_1) = m'(y_1 - y)$$

$$m' | x - x_1 \qquad x = x_1 + km'$$

minden $k \in$ **Z**-re x megoldás, mert

$$\text{ha } y = y_1 - km' \qquad a'x + m'y = b'$$

Tehát minden megoldás ilyen alakú: $x \equiv x_1 \pmod{m'}$

az összes megoldás mod *m* : $x_1, x_1 + m', \ldots, x_1 + (d-1)m'$

Tétel (*diofantikus egyenlet megoldása*)

Rögzített a, b, c egész számok esetén az

$$ax + by = c$$

diofantikus egyenletnek akkor és csak akkor van megoldása, ha

$$(a, b) \mid c\ .$$

Biz. ($\Rightarrow$)

Tfh x_0, y_0 mego. $\Rightarrow$

$(a, b) \mid a \wedge (a, b) \mid b \;\Rightarrow\;$ lin. komb. tul. $\Rightarrow$

$$(a, b) \mid ax_0 + by_0 = c\ .$$

$(\Leftarrow)$ tfh $(a, b) \mid c$.

$$c = (a, b)q$$

$$c = (au + bv)q$$

$$c = a(uq) + b(vq)$$

$\Rightarrow$ egy mego: $x = uq$, $y = vq$.

Észrevétel ha $ax + by = c$

$\forall\, t \in \mathbf{Z}$:

$$x_1 = x + bt\,,\; y_1 = y - at \;\;\Rightarrow$$

$$ax_1 + by_1 = a(x + bt) + b(y - at) = ax + by$$

6.2.12. Kínai maradéktétel. *Legyenek* $m_1, m_2, \ldots, m_n$ *egynél nagyobb, páronként relatív prím természetes számok,* $c_1, c_2, \ldots, c_n \in \mathbb{Z}$. *Az* $x \equiv c_j \pmod{m_j}$, $j = 1, 2, \ldots, n$ *kongruenciarendszer megoldható, és bármely két megoldása kongruens modulo* $m_1 m_2 \cdots m_n$.

Biz.

$m = m_1 m_2$

bővített euklidészi algoritmus ⇒

$$m_1 x_1 + m_2 x_2 = 1$$

Legyen $c_{1,2} = m_1 x_1 c_2 + m_2 x_2 c_1 \longrightarrow c_{1,2} \equiv c_j \pmod{m_j}$

ha $x \equiv c_{1,2} \pmod{m} \Rightarrow x$ megoldása az első két kongruenciának

x megoldása az első két kongruenciának $\Rightarrow m_1, m_2 \mid x - c_{1,2}$

$$\Rightarrow m_1 m_2 \mid x - c_{1,2}$$

Kaptuk, hogy az eredeti kongr. rendszer ekvivalens a következővel:

$$\begin{gathered} x \equiv c_{1,2} \pmod{m} \\ x \equiv c_3 \pmod{m_3} \\ \dots \\ x \equiv c_n \pmod{m_n} \end{gathered}$$

indukcióval kész

RSA kódolás

Legyen $p \neq q$ két nagy prímszám és $pq = n$.

$$1 < e < (p-1)(q-1)$$

véletlen exponens $\longrightarrow$ nem jó, ha $\mathrm{lnko}\big(e, (p-1)(q-1)\big) > 1$

oldjuk meg: $ed \equiv 1 \pmod{(p-1)(q-1)}$

üzenet: $1 < m < n$

üzenet kódja: $c = m^e \bmod n$

Az üzenet visszafejtése (dekódolás):

$$(m^e)^d = m^{k(p-1)(q-1)+1} = \left(m^{(p-1)}\right)^{k(q-1)} \cdot m \equiv m \pmod{p}$$

mert

$p \mid a$ $\qquad$ $p \nmid a$

$0 \equiv 0$ $\qquad$ $m^{p-1} \equiv 1 \pmod{p}$

hasonlóan $(m^e)^d \equiv m \pmod{q}$ kínai mar. tétel $\Rightarrow$ $m = c^d \bmod n$

Megjegyzés: (n, e) nyílvános kulcs, (n, d) titkos

ezt kaptuk Aliztól: $m, m^{d_A} \bmod n_A$

Digitális aláírás

6.3. Számelméleti függvények

***Def*(*számelméleti függvény*)**

$$f : \mathbb{N}^+ \to \mathbb{C}$$

Továbbá, ha $m, n \in \mathbf{N}^+$ és $(m, n) = 1$, akkor f

additív, ha

$$f(mn) = f(m) + f(n)$$

multiplikatív, ha

$$f(mn) = f(m)f(n)$$

f **totálisan (teljesen) additív,** illetve **totálisan (teljesen) multiplikatív**, ha az előbbi összefüggések $(m, n) \neq 1$ esetén is fennállnak.

Észrevételek:

ha *f* additív, akkor

$$f(1) = 0$$

ha *f* multiplikatív, akkor

$$f(1) = 1$$

ha nem azonosan 0

6.3.2. Tétel. *Legyen* $n \in \mathbb{N}^+$ *kanonikus alakja* $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$
Ekkor

(1) *ha* f *additív számelméleti függvény, akkor*

$$f(n) = f(p_1^{\alpha_1}) + \cdots + f(p_k^{\alpha_k});$$

(2) *ha* f *multiplikatív számelméleti függvény, akkor*

$$f(n) = f(p_1^{\alpha_1}) \cdots f(p_k^{\alpha_k});$$

(3) *ha* f *teljesen additív számelméleti függvény, akkor*

$$f(n) = \alpha_1 f(p_1) + \cdots + \alpha_k f(p_k);$$

(4) *ha* f *teljesen multiplikatív számelméleti függvény, akkor*

$$f(n) = f(p_1)^{\alpha_1} \cdots f(p_k)^{\alpha_k}.$$

Példák

1. Möbius függvény (multiplikatív)

$$\mu(n) = \begin{cases} 0, \text{ ha } n\text{-nek van prímnégyzet osztója} \\ (-1)^k, \text{ ha } n\ k \text{ db különböző prím szorzata} \end{cases}$$

2. *n* prímosztóinak száma: **ν(*n*)** additív.

1. 2. nem totális, mert

$$0 = \mu(4) \neq \mu(2)^2 = 1 \qquad\qquad 1 = \nu(4) \neq 2\nu(2) = 2$$

3. Totálisan additív és multiplikatív is az azonosan 0 függvény.

4. Totálisan multiplikatív $n \mapsto n^a$, bármely valós *a*-ra.

5. Totálisan additív $n \mapsto \log_a n$, bármely $a > 0$ valós számra.

Tétel (φ multiplikatív)

φ multiplikatív.

Biz.

$\mathbf{1}$	$\mathbf{2}$	......	$\boldsymbol{a}$
$\boldsymbol{a} + \mathbf{1}$	$\boldsymbol{a} + \mathbf{2}$	......	$\mathbf{2}\boldsymbol{a}$
		......	
$\mathbf{(}\boldsymbol{b} - \boldsymbol{1}\mathbf{)}\boldsymbol{a} + \mathbf{1}$	$\mathbf{(}\boldsymbol{b} - \boldsymbol{1}\mathbf{)}\boldsymbol{a} + \mathbf{2}$	......	$\boldsymbol{ba}$

számoljuk meg, hogy a táblázatban hány relatív prím van ab -hez : ennyi lesz $\varphi(ab)$ értéke.

6.1.22. következmény $\Rightarrow$ azokat kell számolni, amelyek a-hoz és b-hez is rel. prímek omnibusz tétel $\Rightarrow$ minden oszlop TMR mod b, ha $(a, b) = 1$

$\Rightarrow$ minden oszlopban $\varphi(b)$ relatív prím b -hez

minden oszlop kongruens elemeket tartalmaz mod a

minden sor egy TMR mod $a \Rightarrow$ minden sorban $\varphi(a)$ db elem relatív prím a-hoz

$\Rightarrow \varphi(a)$ db oszlopnak rel prímek az elemei a-hoz

$\Rightarrow$ összesen $\varphi(a)\varphi(b)$ rel. prím van ab -hez

☺

Tétel(*φ kiszámolása*)

Ha $n \in \mathbb{N}^+$ *kanonikus alakja* $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, *akkor*

$$\varphi(n) = \prod_{j=1}^{k} \left(p_j^{\alpha_j} - p_j^{\alpha_j - 1}\right) = n \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right).$$

Biz.

φ multiplikatív $\Rightarrow$

prímhatvány helyek, aztán összeszorzás

$\varphi(p^{\alpha}) = ?$

$$1,\ 2,\ \ldots,\ p,\ \ldots,\ 2p,\ \ldots,\ 3p,\ \ldots,\ (p-1)p,\ \ldots,\ p^2,\ \ldots,\ (p+1)p\ldots,\ (p-1)p^{\alpha-1},\ldots,\ p^{\alpha}$$

melyek nem relatív prímek p -hez ?

p^2 -ig $p - 1$ db van + maga p^2, azaz $\varphi(p^2) = p^2 - p^1$

tovább számolva

$$\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$$

7. GRÁFELMÉLET

7.1. Irányítatlan gráfok

Def. A $G = (V, E, \varphi)$ hármast **(irányítatlan) gráfnak** nevezzük, ha V, E halmazok, $V \neq \emptyset$, $V \cap E = \emptyset$ és $\varphi : E \to V\Delta V$.

$V\Delta V = \{ [a, b] \mid a, b \in V \}$, ahol $[a, b] = [b, a]$

V: pont-, csúcshalmaz, V(G) G pontjai, $v(G) = |V(G)| = \#V$

E: élhalmaz, $E(G)$ G élei, $e(G) = |E(G)| = \#E$

véges gráf: $V(G)$, $E(G)$ véges

$\boldsymbol{e \in E}$ **él végpontjai (e illeszkedik a-ra és b-re)**:

ha $a, b \in V$ esetén $\varphi(e) = [a, b]$

hurokél: $a = b$

párhuzamos (többszörös) él $\boldsymbol{e, f \in E}$: ha $\varphi(e) = \varphi(f)$

szomszédos él $\boldsymbol{e, f \in E}$ **:** ha $\varphi(e) = [a_1, a_2]$, $\varphi(f) = [b_1, b_2]$ esetén

$\{a_1, a_2\} \cap \{b_1, b_2\} \neq \emptyset$

szomszédos csúcsok $\boldsymbol{a_1, a_2} \in V$: ha $a_1 \neq a_2$ és $\exists\, e \in E$:

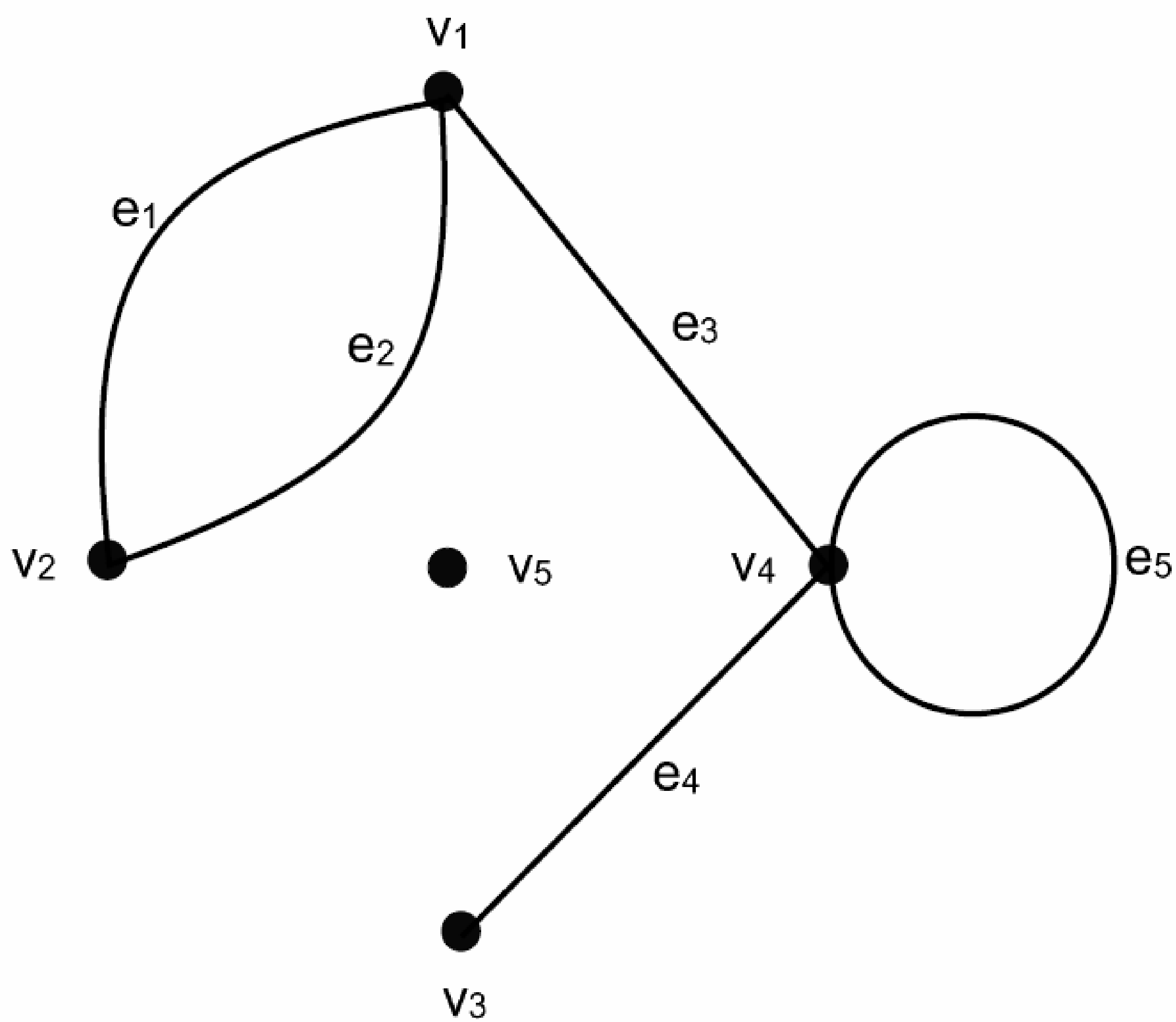
$$\varphi(e) = [a_1, a_2]$$

a **csúcs foka**: a rá illeszkedő élek száma (huroknál 2), jelölés: $\boldsymbol{d(a)}$

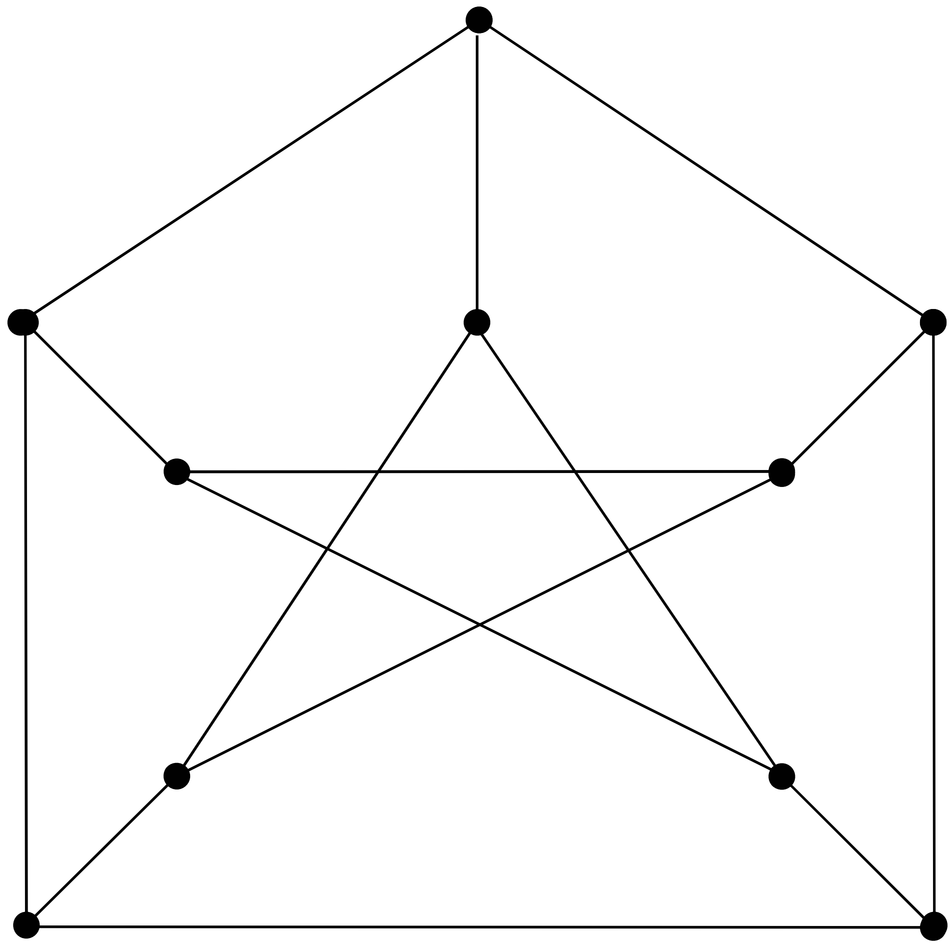
izolált csúcs ***a*** **:** $d(a) = 0$

egyszerű gráf: hurok és többszörös él nélküli gráf

A $G = (V, E)$ gráf **reguláris**, ha $d(a)$ értéke azonos minden $a \in V$-re, ***n*****-reguláris**, ha ekkor $d(a) = n$ valamely a természetes számra.



Jegyzetben 7.1. ábra!



Petersen – gráf (3-reguláris)

Tétel(fokszám-élszám).

Legyen $G = (V, E)$. Ekkor

$$\sum_{a \in V} d(a) = 2e(G).$$

Következmény: G-ben a páratlan fokú csúcsok száma páros.

Biz.

$$\sum_{a \in V} \mathrm{d}(a) = \sum_{\mathrm{d}(a) \equiv 0 \pmod 2} \mathrm{d}(a) + \sum_{\mathrm{d}(a) \equiv 1 \pmod 2} \mathrm{d}(a) \equiv 0 \pmod 2,$$

amiből kapjuk, hogy

$$\sum_{\mathrm{d}(a) \equiv 1 \pmod 2} \mathrm{d}(a) \equiv 0 \pmod 2.$$

☺

Def. A $G = (V, E)$ és $G' = (V', E')$ gráf **izomorf** , ha létezik $\pi : V \to V'$ és $\rho : E \to E'$ bijekció úgy, hogy $a \in V$ és $e \in E$ illeszkedik G-ben $\Leftrightarrow$ $\pi(a)$ és $\rho(e)$ illeszkedik G'-ben.

Def. A $G = (V, E)$ és $G' = (V', E')$ **egyszerű** gráf **izomorf** , ha létezik $\pi : V \to V'$ bijekció úgy, hogy $a, b \in V$ szomszédos G-ben $\Leftrightarrow$ $\pi(a)$ és $\pi(b)$ szomszédos G'-ben.

Def. A $G = (V, E)$ egyszerű gráf **teljes gráf**, ha bármely két pontja szomszédos. $\mathbf{K}_n$ jelöli az ***n*** pontú teljes gráfot.

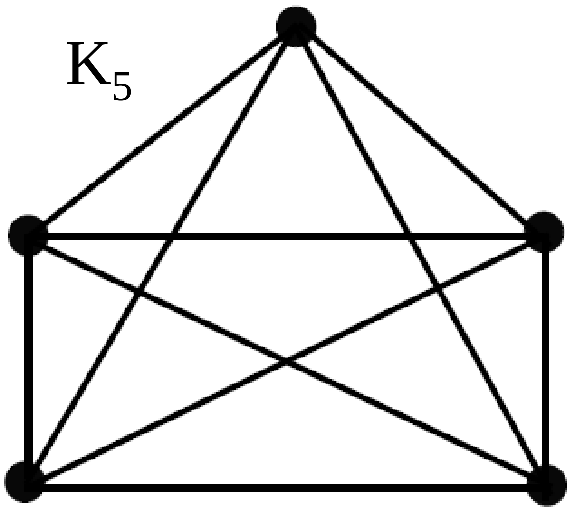
Észrevételek:

ugyanannyi csúcsszámú teljes gráfok izomorfak

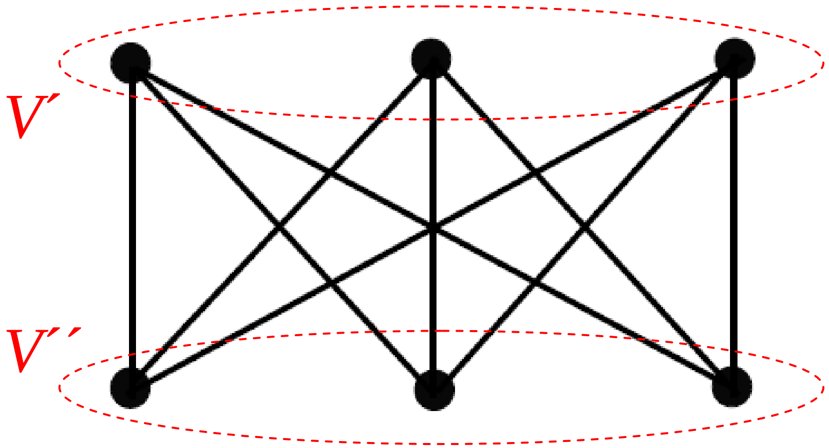
K_n-nek $n(n-1)/2$ éle van

Def. A $G = (V, E, \varphi)$ hármast **páros gráfnak** nevezzük, ha $V = V' \cup V''$, $V' \cap V'' = \emptyset$ és G minden élének egyik végpontja V'-ben, másik végpontja V''-ben van.

K_5

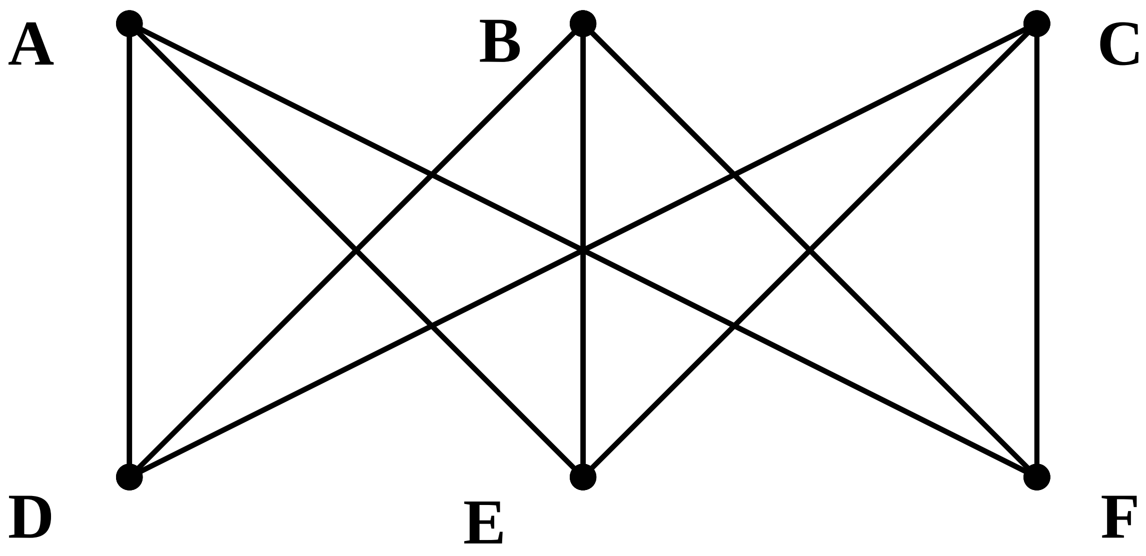


$K_{3,3}$ „3 ház 3 kút”

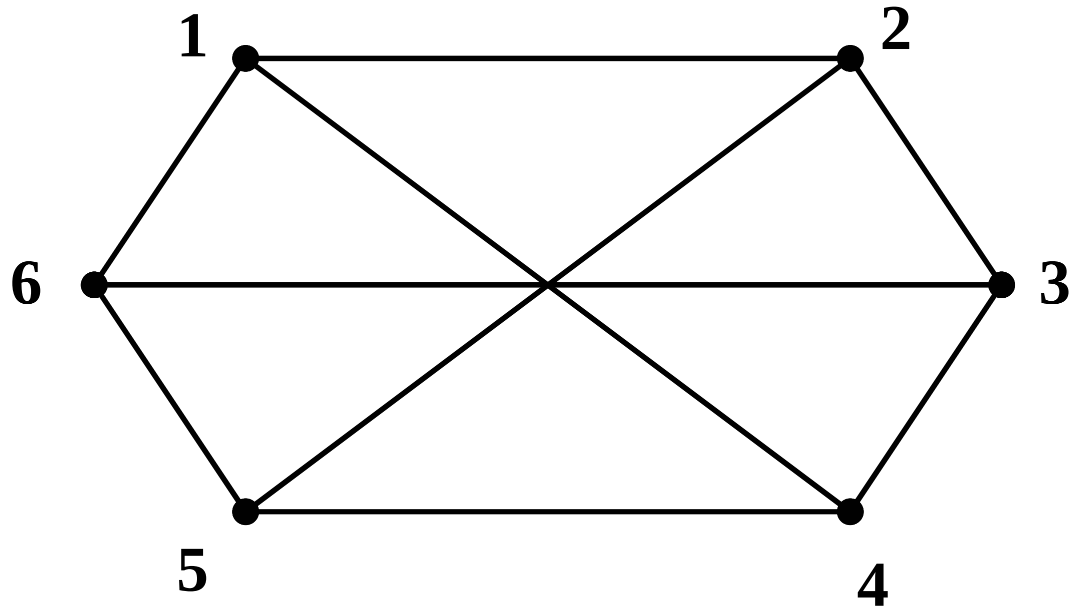


Kuratowski – gráfok

Jegyzetben 7.2. ábra



Izomorfak?



A→1, B →3, C →5, D →2, E →4, F →6

Def. A $G' = (V', E', \varphi')$ gráfot a $G = (V, E, \varphi)$ gráf **részgráfjának** nevezzük, ha

1. $V' \subseteq V$ és $E' \subseteq E$, valamint
2. $\varphi'(e) = \varphi(e)$ minden $e \in E'$-re.

Def. Ha a $G' = (V', E', \varphi')$ gráf a $G = (V, E, \varphi)$ gráf részgráfja, és E' mindazon E-beli éleket tartalmazza, melyek végpontjai V'-ben vannak, akkor G' -t **telített részgráfnak** nevezzük, vagy pontosabban ***V'* által meghatározott telített részgráfnak.**

Def. Ha H részgráfja G-nek, akkor a $(V(G), E(G) \setminus E(H), \varphi|_{E \setminus E'})$ gráf ***H G*-re vonatkozó komplementere**.

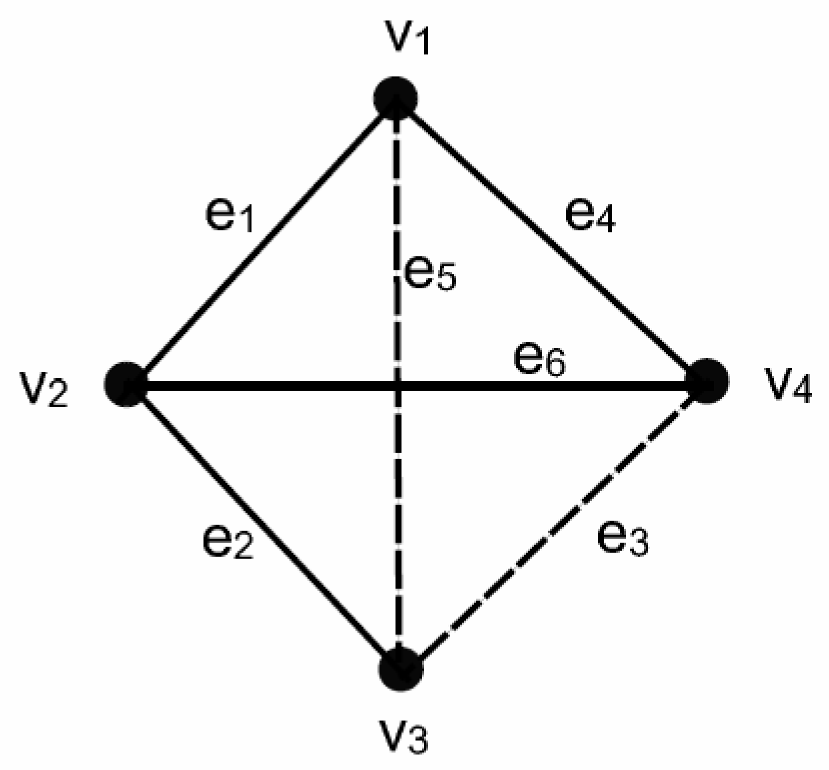
Def. Az egyszerű ***H* gráf komplementere** az ugyanezen ponthalmazon lévő teljes gráfra vonatkozó komplementerét jelenti.

Ha csúcsokat törlünk egy gráfból, akkor az illeszkedő éleket is törölni kell!

Def. Tehát, ha $G = (V, E, \varphi)$ egy gráf és $V' \subseteq V$, akkor legyen $E' \subseteq E$ azon élek halmaza, amelyek illeszkednek valamelyik V' –beli csúcsra. A G gráfból kapott V' csúcshalmaz törlésével kapott gráf:

$$G' = (V \setminus V', E \setminus E', \varphi|_{E \setminus E'})$$

12



Jegyzetben 7.3. ábra

Def. Legyen k természetes szám. **k hosszú élsorozat (séta) $\boldsymbol{a_0}$-ból $\boldsymbol{a_k}$-be** az $[a_0, e_1, a_1, e_2, a_2, ..., e_k, a_k]$ sorozat, ha $a_0, a_1, ..., a_k \in V(G)$, $e_1, e_2, ..., e_k \in E(G)$ és $\varphi(e_i)=[a_{i-1}, a_i]$ minden $i=1, 2, ..., k$-ra.

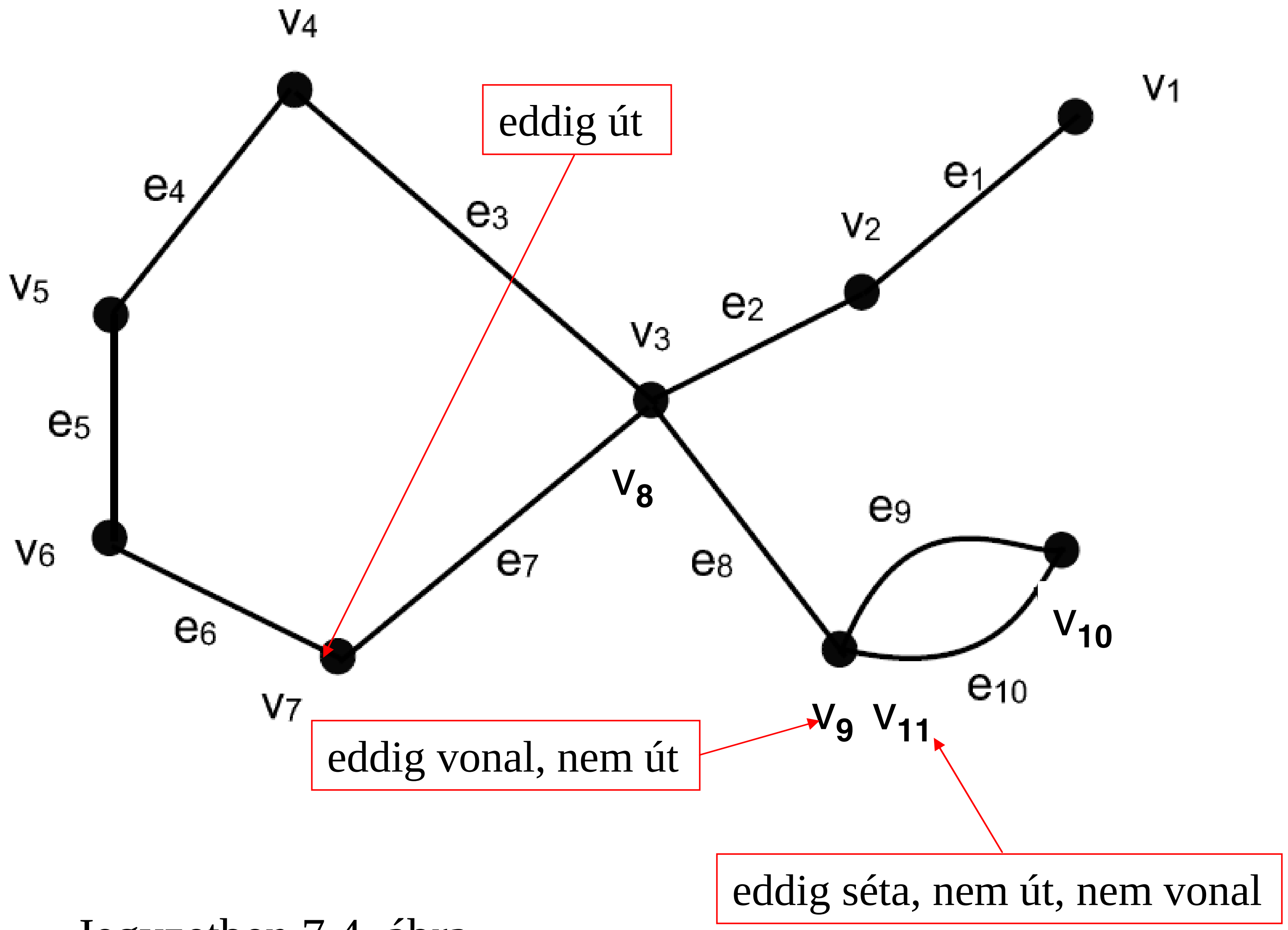
Def. Egy élsorozat **út** , ha benne minden csúcs különböző és **vonal**, ha minden éle különböző.

Def. Egy élsorozat **zárt**, ha $a_0 = a_k$, különben **nyílt**. **Kör** az a zárt élsorozat, melyben a többi csúcs egymástól és a_0-tól különbözik, és élei is mind különbözőek.

Észrevételek: út és kör hossza az éleinek száma

0 hosszúságú séta út

út mindig vonal



Jegyzetben 7.4. ábra

Tétel(út létezése)

Minden olyan nyílt élsorozat, amely az a_0 és a_n ($a_0 \neq a_n$) csúcsokat köti össze, tartalmaz részsorozatként ugyanezen csúcsokat összekötő utat.

Biz.

Ha minden i, j esetén $a_i \neq a_j$, akkor kész, különben legyen $a_i = a_j$ valamely indexekre.

$$\Rightarrow$$

$$[a_0, e_1, a_1, e_2, a_2, ..., e_{\mathrm{i}}, a_{\mathrm{i}}, e_{i+1}, ..., a_j, e_{j+1}, ..., e_n, a_n]$$

élsorozatból elhagyható az a_i, e_{i+1}, ..., rész, ...

Véges lépésben különböző csúcsokat kapunk

$\Rightarrow$ **út** ☺

7.1.8. Állítás. *Bármely G gráfban egy legalább egy hosszúságú zárt vonal véges sok páronként éldiszjunkt kör egyesítése.*

Biz.

Ha a vonalon csak az első és utolsó csúcs egyezik, akkor kész, mert 1 db körünk van.

Ha nem, „vágjuk le” azt a részt amely az első csúcs-ismétlődésig tart.

Tehát levágtunk egy kört és maradt egy zárt vonalunk.

Ha ez a zárt vonal kör, akkor készen vagyunk, ha nem ...

Def. Egy gráf **összefüggő**, ha benne bármely két csúcs összeköthető sétával (következésképpen úttal is).

Def. Legyen ~ a következő ekvivalenciareláció : $a_1, a_2 \in V(G)$ esetén $a_1 \sim a_2$, ha $a_1 = a_2$ vagy a_1 és a_2 között van út.

Az azonos osztályokba eső csúcsok által meghatározott telített részgráfok a G gráf **(összefüggő) komponensei**, számuk $\boldsymbol{c(G)}$.

Észrevételek: kül. osztályba eső csúcsok nem szomszédosak

$\forall$ él hozzárendelhető egy komponenshez

egy **gráf összefüggő**, ha egy komponense van

Def. A **fa** összefüggő és körmentes gráf.

7.1.11. Tétel. *Egy G egyszerű gráfra a következő feltételek ekvivalensek:*

(1) *G fa;*

(2) *G összefüggő, de bármely él törlésével a kapott részgráf már nem összefüggő;*

(3) *ha v és v' a G különböző csúcsai, akkor pontosan egy út van v-ből v'-be;*

(4) *G-nek nincs köre, de bármilyen új él hozzávételével kapott gráf már tartalmaz kört.*

Biz. **(1) ⇒ (2):**

Tfh indirekte v, v' közti él törlésével összefüggő marad a fa

⇒ marad egy másik út v, v' közt

ez az út + törölt él kört alkot az eredeti fában **(1)**

(2) ⇒ (3):

Tfh indirekte v, v' közt van két különböző út és induljunk el, v-ből v'-be

töröljük az első olyan élet, amely különbözik a két útban

ha van ilyen, akkor a másik úton eljutunk v'-be **(2)**

ha nincs ilyen, akkor kör van **(1)**

(3) ⇒ (1):

Tfh indirekte van kör a fában

⇒ a kör v, v' pontjai közt van két különböző út **(3)**

(1) ⇒ (4): fa körmentes összefüggő: húzzunk be egy élt v, v' közé

$v = v'$ hurokél kész

$v \neq v'$ „régi” út + új él: kör

(4) ⇒ (1): tetszőleges $v \neq v'$ csúcsokra a körmentes G gráfban

ha szomszédosak, akkor pontosan ez az egy út van, különben kör lenne ⇒ fa

ha nem, húzzunk be egy élt v, v' közé

(4) ⇒ kör „keletkezik”

ennek a körnek a „maradék” része az út ⇒ összefüggő ⇒ fa

7.1.12. Tétel. *Ha egy G véges gráfban nincs kör, de van él, akkor van legalább két elsőfokú csúcs.*

Biz.

válasszunk egy maximális hosszúságú *u* utat *v*, *v´* végpontokkal

Tfh (indirekte) *v*, *v´* nem elsőfokú

illeszkedik rájuk él

hol van ezen élek másik végpontja?

nincs rajta *u*-n

u-nál hosszabb utat találtunk

***u* max**

u-n van

kört találtunk

feltétel

7.1.13. Tétel. *Egy G egyszerű véges gráfra n csúccsal a következő feltételek ekvivalensek:*

(1) *G fa;*

(2) *G-ben nincs kör és $n-1$ éle van;*

(3) *G összefüggő és $n-1$ éle van.*

Biz.

(1) ⇒ (2) pontszámra vonatkozó teljes indukció

n = 1 esetén nyilvánvaló az állítás

Legyen *n* > 1, és tegyük fel, hogy minden *n*-nél kevesebb pontú fára igaz az állítás tekintsünk egy n pontú fát

próbáljunk kitörölni egy élt és egy pontot, úgy hogy fa maradjon

7.1.12. tétel $\Rightarrow$ létezik elsőfokú pont: egyet hagyjunk el éllel együtt

$\Rightarrow$ marad egy körmentes összefüggő gráf $\Rightarrow$ fa

továbbá ennek $n - 1$ pontja van

érvényes rá az indukciós feltevés: $n - 2$ éle van

(2) $\Rightarrow$ (3) pontszámra vonatkozó teljes indukció

n = 1 esetén nyilvánvaló az állítás

Legyen n > 1, és tfh $\forall$ n-nél kevesebb pontú ilyen gráfra igaz az állítás

tekintsünk egy n pontú körmentes gráfot, amelynek n – 1 éle van

próbáljunk kitörölni egy élt és egy pontot,
úgy hogy körmentes maradjon

7.1.12. tétel $\Rightarrow$ létezik elsőfokú pont: hagyjuk el az éllel együtt

marad egy n – 1 pontú körmentes gráf n – 2 éllel

Indukciós feltevés miatt ez összefüggő is

(3) $\Rightarrow$ (1)

tekintsünk egy n pontú összefüggő gráfot, amelynek $n - 1$ éle van

tfh van benne kör

körből elhagyunk egy élt, ettől még összefüggő marad

•••

végül, ha elfogytak a körök k db törlés után n pontú fát kapunk

az élek száma $n - 1 - k$

de (1) $\Rightarrow$ (2) miatt az élek száma $n - 1$

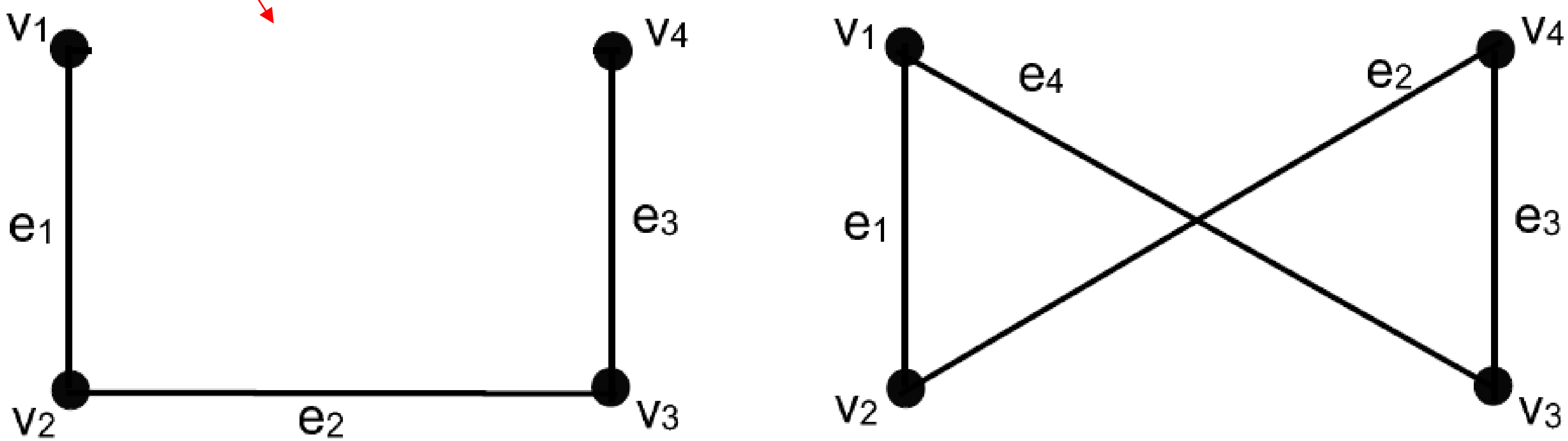
$\Rightarrow k = 0$

0 db kör volt az eredeti gráfban $\Rightarrow$ fa

Def. Az *F* gráf a *G* gráf **feszítőfája**, ha

1. pontjaik halmaza megegyezik,
2. *F* a *G* részgráfja, és
3. *F* fa.

feszítőfa ?

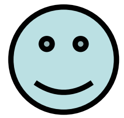


Jegyzetben 7.5. ábra

Tétel. Minden véges összefüggő G gráfnak létezik feszítőfája.

Biz.

Ha van kör, akkor elhagyjuk az egyik élt, ...



7.1.16. Állítás. *Egy $G = (\varphi, E, V)$ véges összefüggő gráfban létezik legalább $\natural(E) - \natural(V) + 1$ kör, amelyek élhalmaza különböző.*

Biz.

előző tétel $\Rightarrow$ létezik T feszítőfa, aminek $v(G) - 1$ éle van

Legyen K_f az a kör ami $T \cup \{ f \}$-ben van, ahol $f \in E(G) \setminus E(T)$

T_G komplementerben legalább $e(G) - v(G) + 1$ ilyen f él van

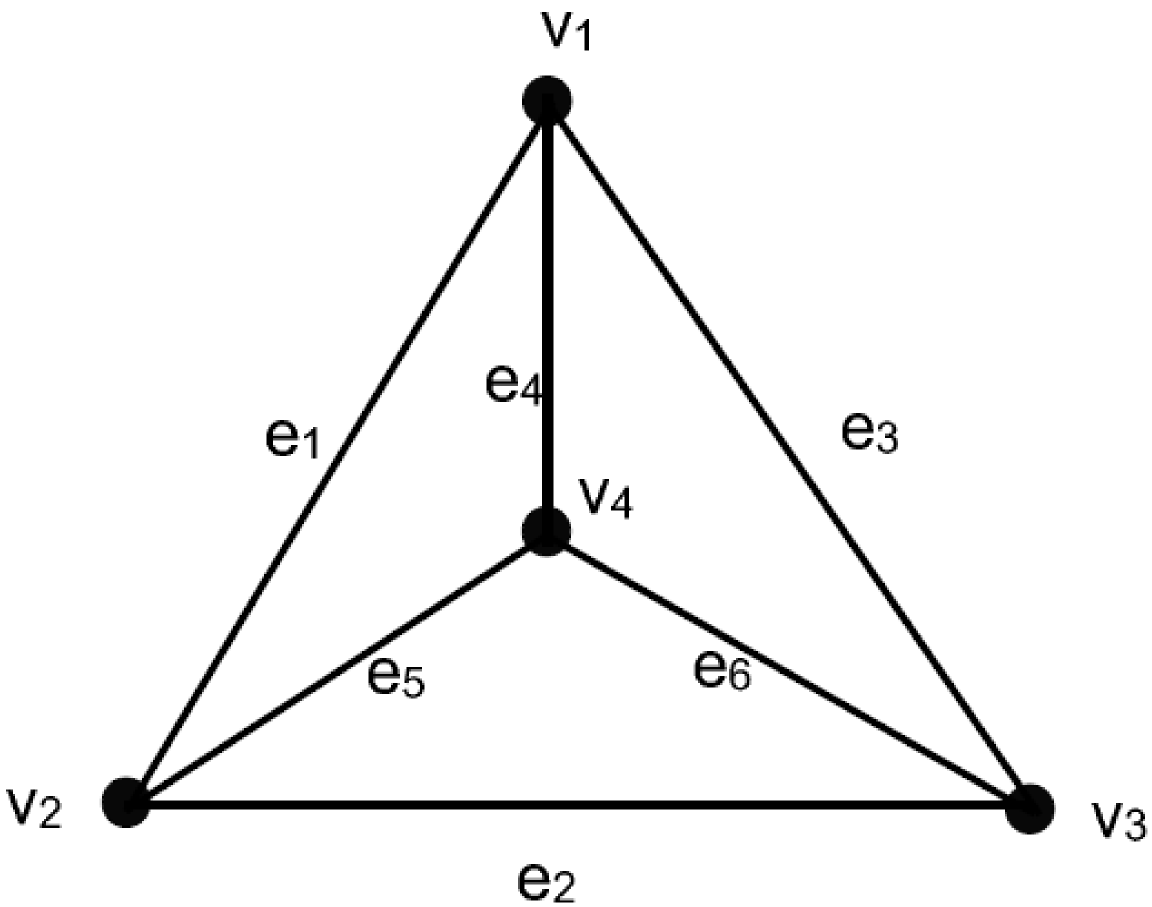
$\Rightarrow$ legalább $e(G) - v(G) + 1$ különböző kör

Észrevétel

A $T \cup \{ f \}$ alakú részgráfok pontosan egy kört tartalmaznak, tehát ez a rendszer egyértelműen definiált.

Def. Ha vesszük az összes K_f alakú kört, akkor ***G T*-re vonatkozó alapkörrendszeréről** beszélünk.

Előfordulhat azonban, hogy több kör is van G-ben!



Jegyzetben 7.6. ábra

***Def*.** Legyen $G = (V, E, \varphi)$ egy gráf , v, w csúcsok V-ben és $V' \subseteq V$. Ha minden v-ből w-be vezető út tartalmaz V'-beli csúcsot, akkor ***V´* elvágja *v*-t és *w*-t**.

Ha $E' \subseteq E$ és minden v-ből w-be vezető út tartalmaz E'-beli élet, akkor ***E´* elvágja *v*-t és *w*-t**.

Ha V', illetve E' egy elemű, akkor **elvágó (szeparáló) pontról**, illetve **elvágó (szeparáló) élről** beszélünk.

***Def*.** A $G = (V, E)$ gráfban $E' \subseteq E$ **elvágó (szeparáló)** élhalmaz, ha a $G' = (V, E \setminus E')$ több komponensből áll, mint G. (Azaz vannak olyan csúcsok G-ben, amelyeket E' elvág.)

Def. E' **vágás**, ha elvágó élhalmaz, de semelyik valódi részhalmaza nem az.

7.1.19. Állítás. *Egy $G = (\varphi, E, V)$ véges összefüggő gráfban létezik legalább $\natural(V) - 1$ különböző vágás.*

Biz.

T feszítőfa összefüggő

$\Rightarrow T_G$ komplementer nem vágás

Ha T_G komplementerhez hozzáveszünk egy élt *T*-ből, akkor vágás lesz

T-nek $v(G) - 1$ éle van

$\Rightarrow$ legalább ennyi különböző vágást kapunk

Def.

A körmentes gráfot **erdőnek** nevezzük.

G olyan részgráfját, mely összes pontját tartalmazza, és maximálisan sok élt G-ből úgy, hogy körmentes maradjon, G **feszítő erdőjének** nevezzük.

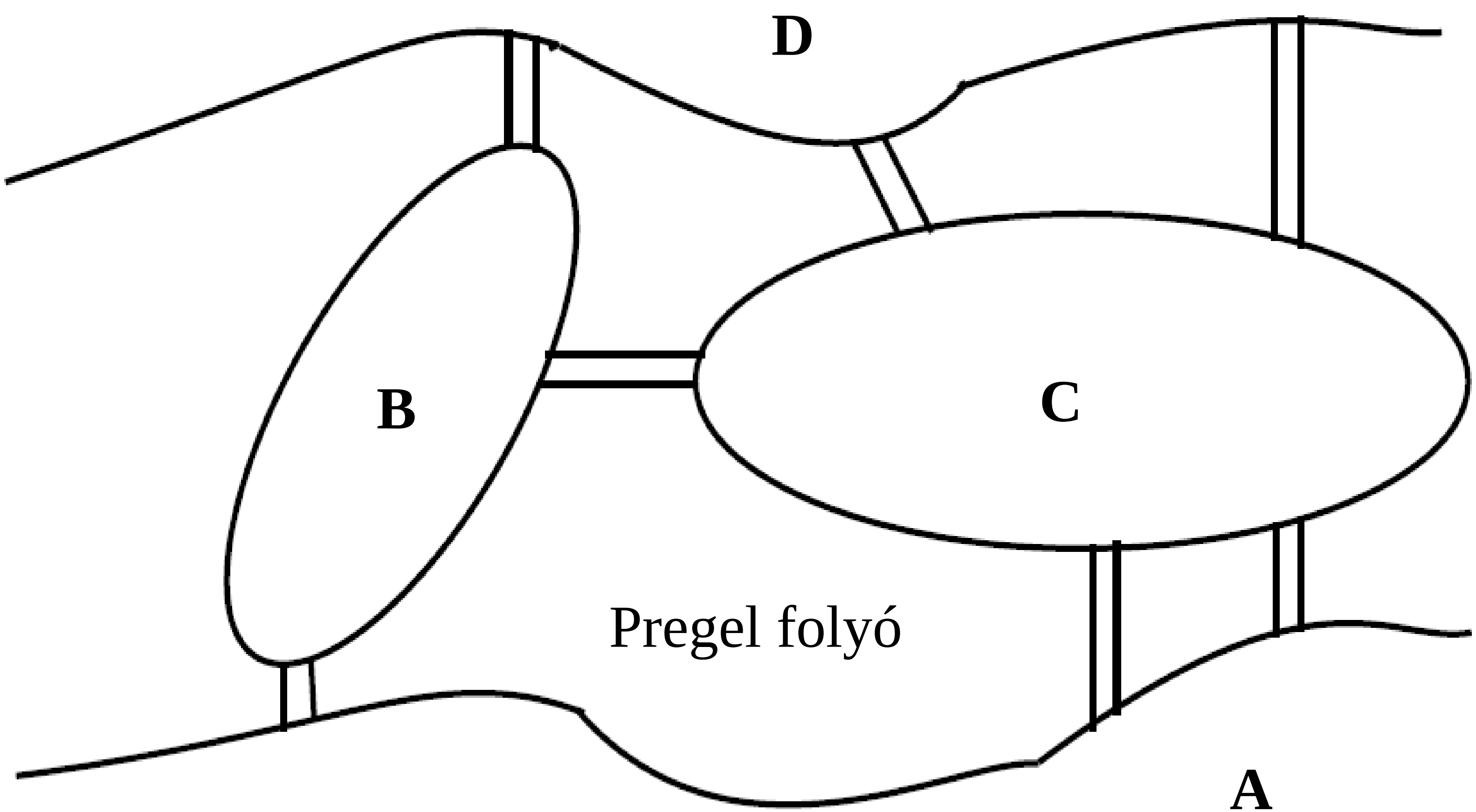
A feszítő erdő minden összefüggő komponense G megfelelő komponensének feszítőfája.

G **rangja** $r(G) = v(G) – c(G)$

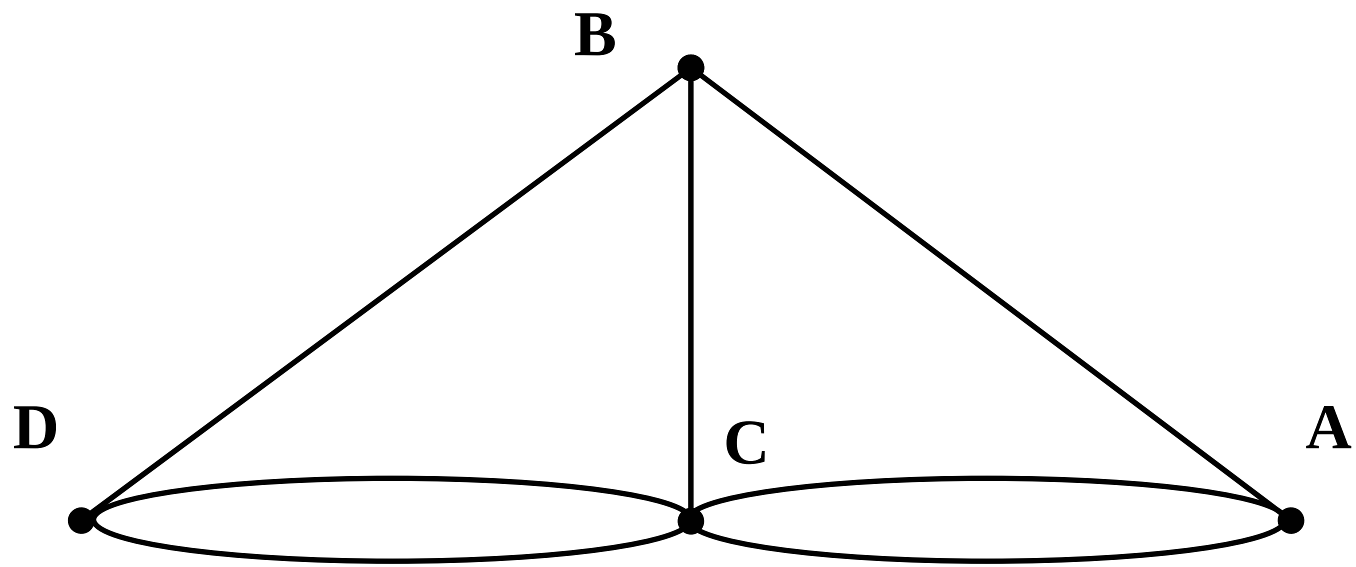
G **nullitása** $n(G) = e(G) – v(G) + c(G)$

33

Königsberg polgárainak problémája.



Jegyzetben 7.7. ábra



Def. Ha egy *G* gráfban van olyan *Z* zárt élsorozat, amelyik *G* minden élét pontosan egyszer tartalmazza, akkor *G*-t **Euler-gráfnak**, *Z*-t pedig **Euler-vonal**-nak **(Euler-körnek)** nevezzük.

Megjegyzés.

Többszörös éleket is megengedünk!

7.1.22. Állítás. *Egy véges összefüggő gráfban pontosan akkor létezik zárt Euler-vonal, ha minden csúcs páros fokú. Ha egy véges összefüggő gráf $2s$ páratlan fokú csúcsot tartalmaz, ahol $s \in \mathbb{N}^+$, akkor a gráf s darab páronként éldiszjunkt nyílt vonal egyesítése.*

Biz.

1. lépés: Legyen Z zárt Euler-vonal G gráfban. Végighaladva Z-n, minden olyan élhez, mely egy x ponthoz vezet, van egy másik, amelyiken x-et elhagyjuk. Ezért $d(x)$ kétszer annyi, mint ahányszor x előfordul Z-ben, tehát páros szám.

2. lépés: Tfh minden csúcs foka páros

$\Rightarrow$ létezik K_1 kör G-ben (biz. gyakorlaton)

Tekintsük most a $G \setminus K_1$ gráfot: minden csúcs foka páros, vagy izolált.

Hasonló módon kiválasztható K_2 kör, ami éldiszjunkt K_1 -gyel.

. . .

Végül csak izolált csúcsok maradnak $\Rightarrow$ G éldiszjunkt körök egyesítése

3. lépés: Ha $G = K_1$, akkor készen vagyunk. Egyébként az összefüggőség miatt kell léteznie egy K_i körnek, melynek K_1-gyel van x közös pontja.

x-en keresztül be tudjuk járni $K_1 \cup K_i$ -t úgy, hogy inden élet pontosan egyszer érintünk.

$\Rightarrow$ Euler - vonal.

Addig bővítjük, míg minden kört fel nem használtunk.

Tehát eddig beláttuk G összefüggő véges gráfra:

G Euler-gráf $\Leftrightarrow$

minden pontja páros fokú

$\Leftrightarrow$

G éldiszjunkt körök egyesítése

Tfh $s = 1$

legyen v, v' a két páratlan fokú pont

ha u egy v, v' -t összekötő max hosszú vonal, akkor

ha u minden élt tartalmaz: kész

ha nem : $\exists$ w csúcs az u vonalon amelyre illeszkedik „nem felhasznált” él iduljunk el w csúcsból egy ilyen élen

folytassuk az utat mindig „nem felhasznált” élen

a pontokra csak páros sok „nem felhasznált” él illeszkedik

$\Rightarrow$ előbb – utóbb visszaérünk w-be

$\Rightarrow$ kaptunk egy 0-nál hosszabb k kört

Tehát u w-ig + k + u w-től hosszabb vonal v-ből v'-be, mint u

***u* max**

$\Rightarrow$ u minden élt tartalmaz

Tfh $s > 1$

választunk két különböző elsőfokú pontot és egy őket összekötő utat

töröljük ezen út éleit a gráfból

a végpontoktnak eggyel, az út többi pontjának 2-vel csökken a fokszáma

$\Rightarrow$ a páratlan fokszámú pontok száma pontosan 2-vel csökkent

ezt a „műveletet” megismételhetjük (pontosan még s – 1-szer), mert a komponensekben párosával fordulnak elő a páratlan fokszámú pontok végül csupa páros fokszámú csúcs marad

ekkor már nem biztos, hogy összefüggő!

s = 0 eset $\Rightarrow$ izolált pontok, illetve éldiszjunkt körök maradhatnak

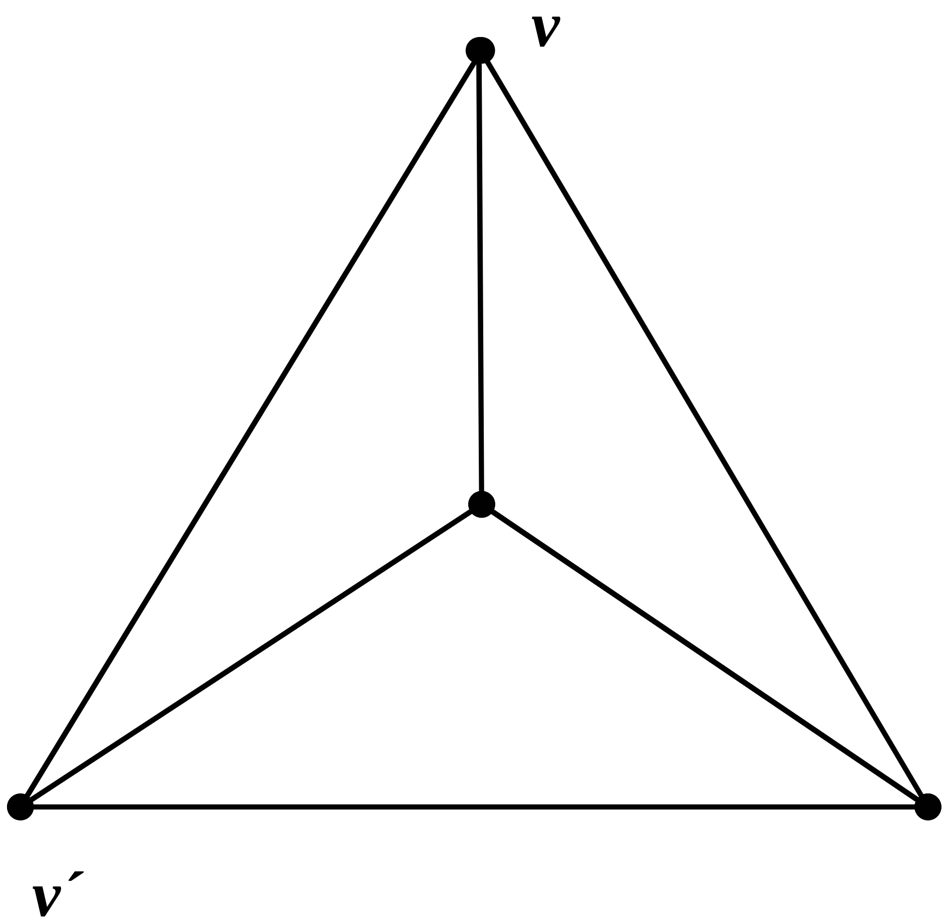
hogy jönnek ki az éldiszjunkt vonalak?

egy vonalhoz több kör is csatlakozhat, attól éldiszjunktak maradnak

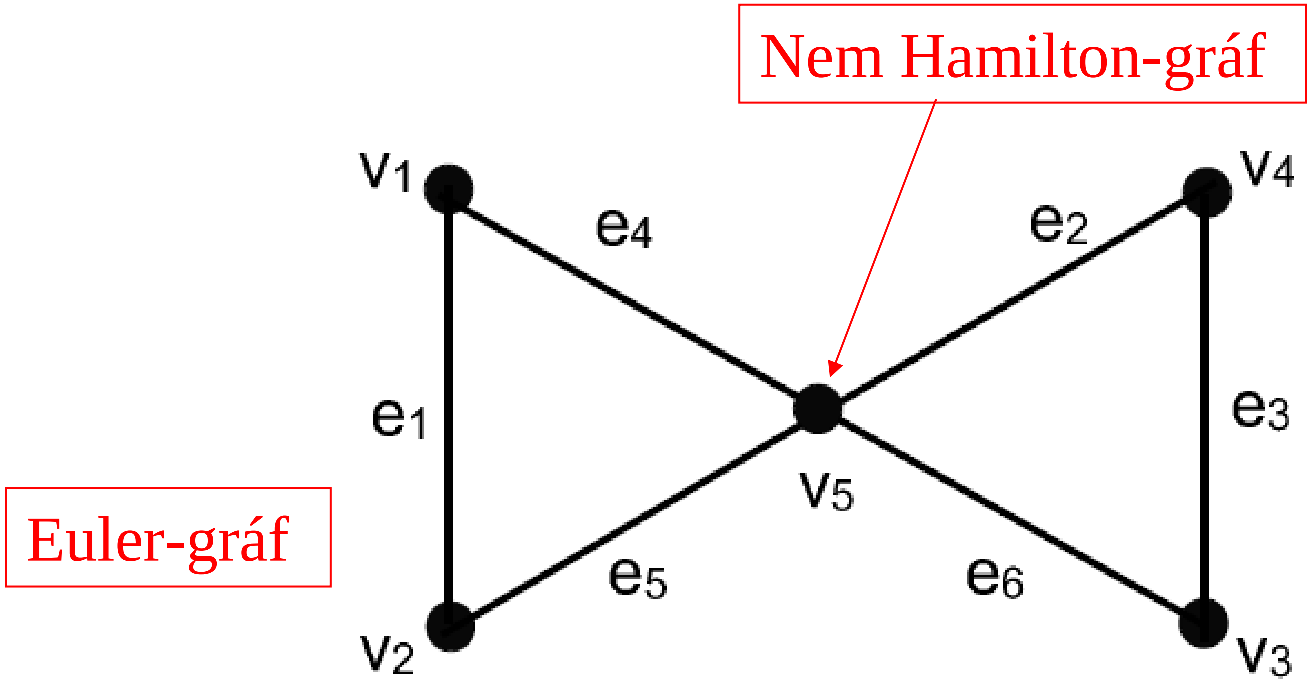
egy kört „egyesítünk" azzal a kivágott vonallal, amivel van közös pontja

s db éldiszjunkt „kivágást" csináltunk

$\Rightarrow$ s db éldiszjunkt vonalat kapunk

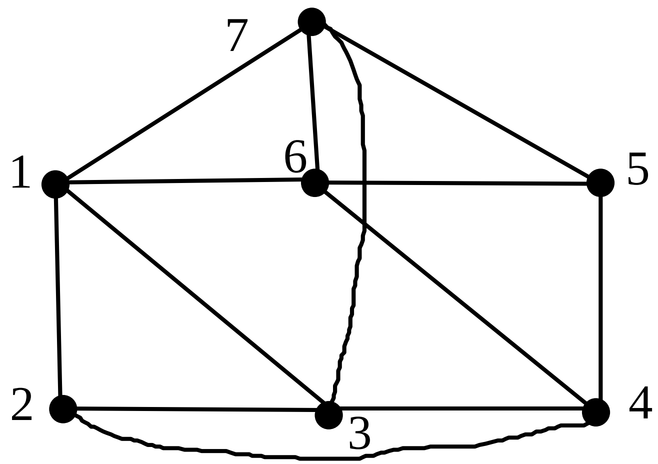

v
v´

Def. Ha van egy *G* gráfban olyan *K* kör, melyben minden *V*(*G*)-beli csúcs pontosan egyszer szerepel, akkor *K*-t **Hamilton-vonalnak** (**Hamilton-körnek**) nevezzük, *G*-t pedig **Hamilton-gráfnak**. Egy út **Hamilton-út**, ha *G* minden pontját pontosan egyszer tartalmazza.

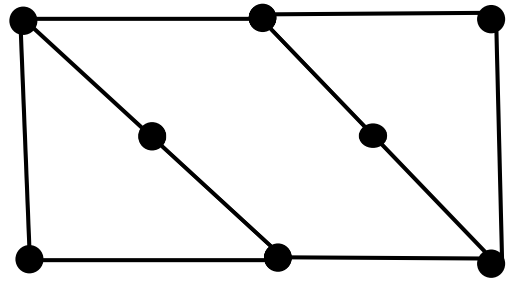


Jegyzetben 7.8. ábra

Példa



X



Y

Az *X* gráfban Hamilton-kört képeznek az

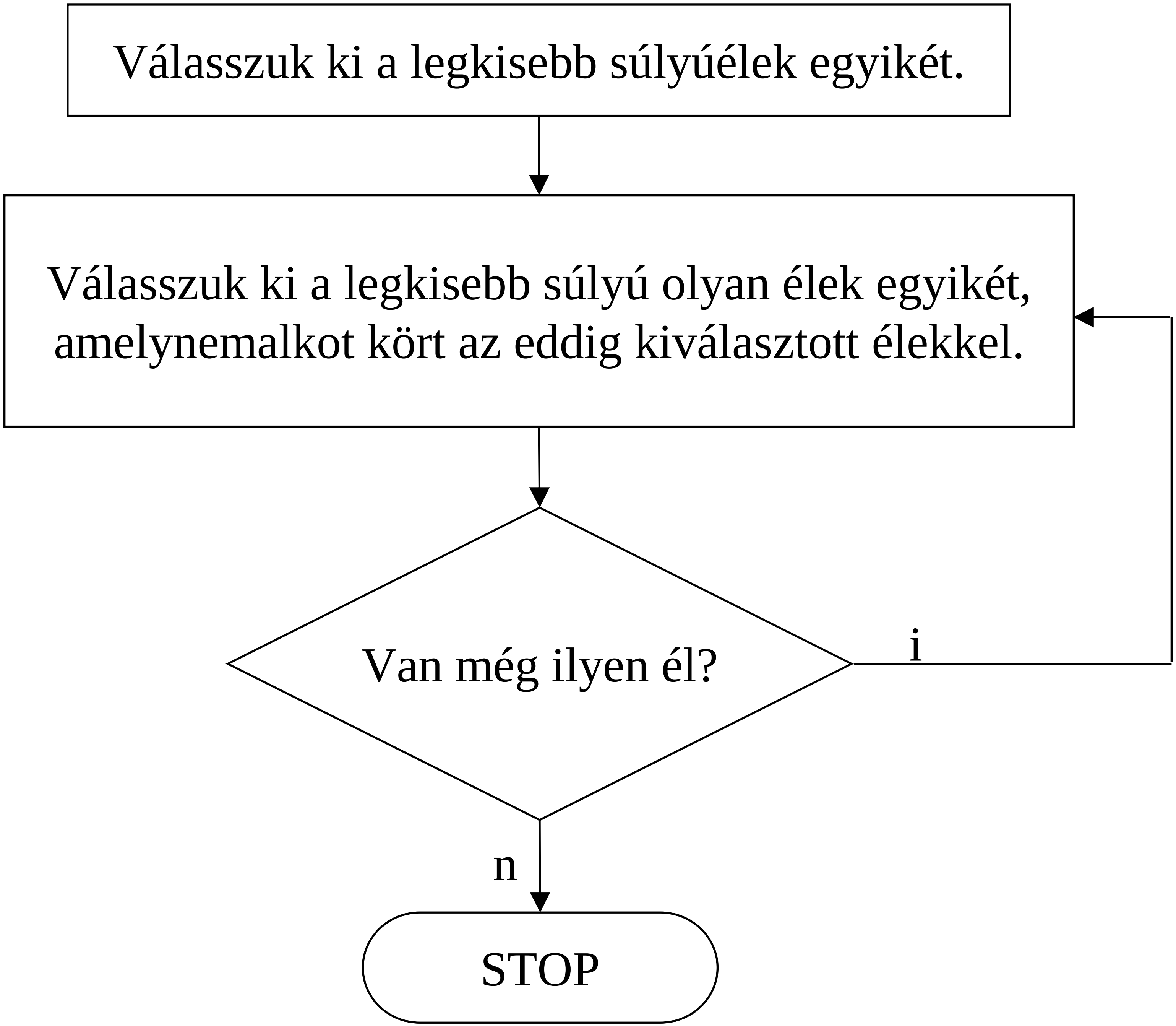
(1, 2, 3, 4, 5, 6, 7, 1) illetve az **(1, 2, 3, 7, 5, 4, 6, 1)** csúcsok.

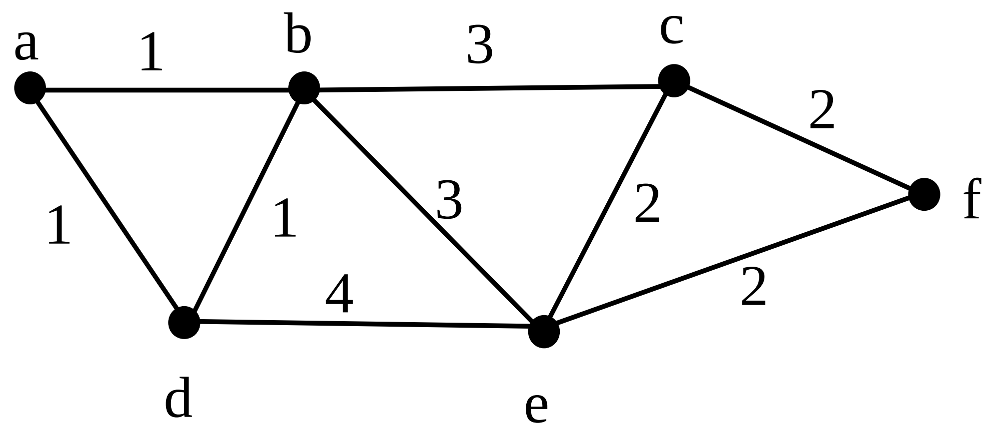
Y-ban nincs Hamilton-kör.

Def. Legyen G = (V, E, φ, w) olyan gráf, ahol w függvény egy $e \in E(G)$ élhez rendel valós számhalmazbeli értéket, amelyet e **súlyának** nevezzük. $X \subseteq E(G)$ esetén az X részhalmaz súlya:

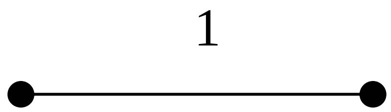
$$\boxed{\sum_{e \in X} w(e)}$$

7.1.25. Kruskal algoritmusa. *Egy* (φ, E, V, w) *élsúlyozott összefüggő véges gráfban az összes csúcsot tartalmazó üres részgráfból indulva, és a már kiválasztott részgráfhoz addig adva hozzá a minimális súlyú olyan élt, amellyel a kiválasztott részgráf még nem tartalmaz kört, egy minimális súlyú feszítőfát kapunk.*

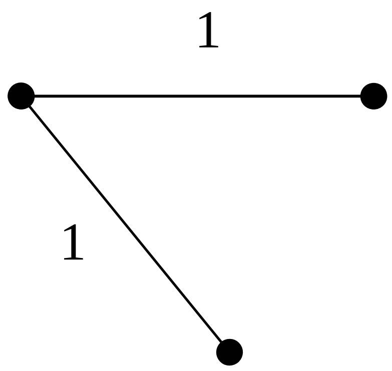

Válasszuk ki a legkisebb súlyúélek egyikét.
Válasszuk ki a legkisebb súlyú olyan élek egyikét, amelynemalkot kört az eddig kiválasztott élekkel.
Van még ilyen él?
i
n
STOP



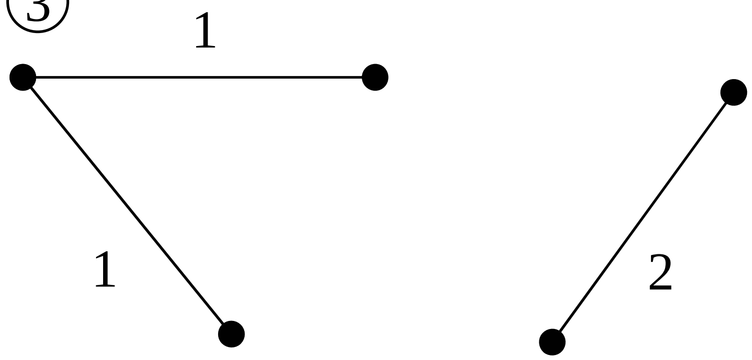
①



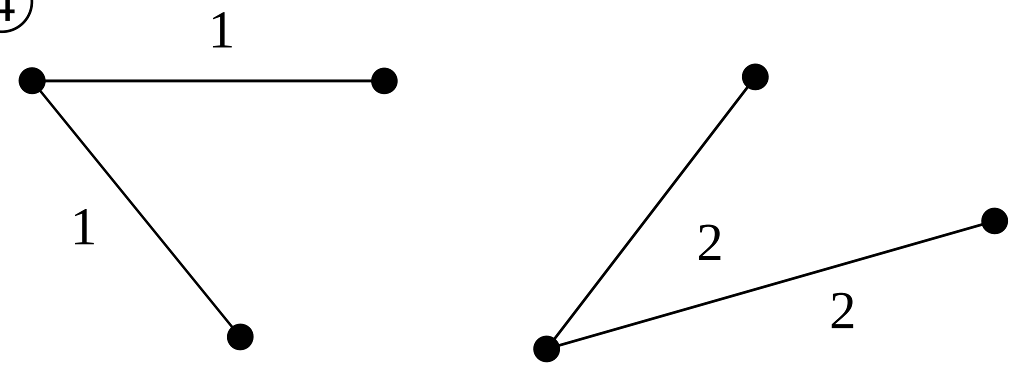
②



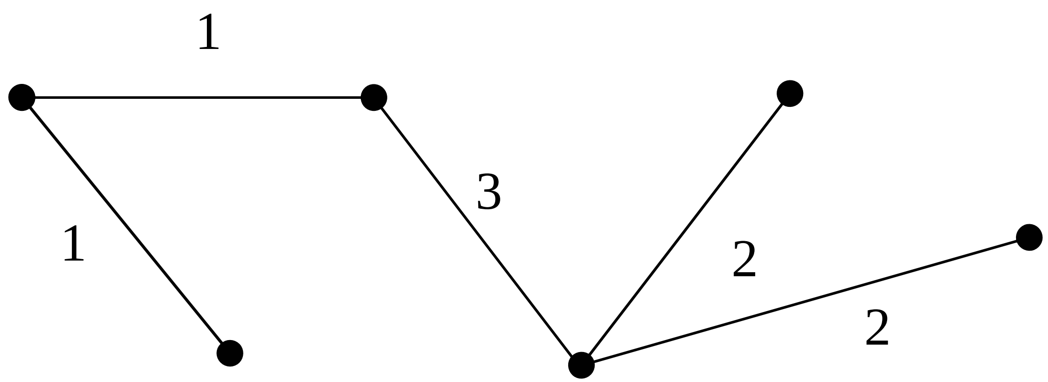
③



④



⑤



Bizonyítás (indirekt)

Nyilvánvaló, hogy a kiválasztott élek feszítőfát adnak. Ezt jelölje F.

Feltétel:

Tegyük fel az állítással ellentétben, hogy F_0 minimális súlyú feszítőfa, és $w(F_0) < w(F)$.

Ha több ilyen ellenpélda is van, akkor ezek közül válasszuk F_0-nak azt, melynek a lehető legtöbb közös éle van F-fel.

Tekintsük az $\boldsymbol{e_0} \in E(F_0) \setminus E(F)$ élt.

F fa $\Rightarrow$

$F \cup e_0$ tartalmaz K kört (*)

Algoritmus

$\Rightarrow$

K kör minden $e \in E(K) \backslash \{e_0\}$ élére $w(e) \leq w(e_0)$ (**)

F_0 fa

$\Rightarrow$

F_0 - e_0 két komponensre esik szét

(*) $\Rightarrow$

K körnek e_0 -on kívül tartalmaznia kell e_1 élt, ami összeköti F_0 - e_0 két komponensét, mivel e_0 mindkét végpontja K-ban van, illetve az egyik F_0 - e_0 egyik, a másik F_0 - e_0 másik komponensében van.

$\Rightarrow$

$F_1 = F_0 - e_0 \cup \{e_1\}$ feszítőfa lesz, és

(**) $\Rightarrow$

$w(e_1) \leq w(e_0)$.

Két esetet kell vizsgálnunk:

1. eset: $w(e_1) < w(e_0)$

$\Rightarrow$

$w(F_1) < w(F_0)$ ***F*₀ minimális**

2. eset:

$$w(e_1) = w(e_0).$$

$$\Rightarrow$$

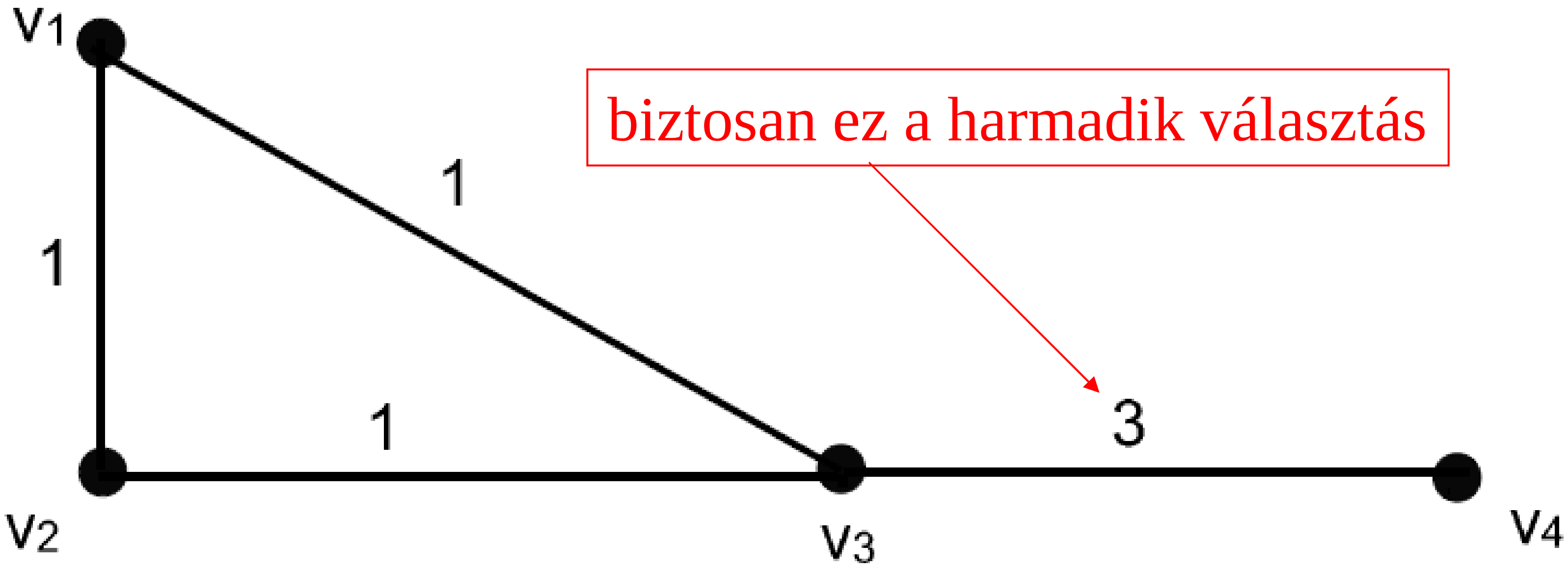
F_1 -nek eggyel több közös éle van F-fel, mint F_0 nak.

F_0 tartalmazza a legtöbb közös élt F-fel a minimális súlyú feszítőfák közül

☺

Megjegyzés

nem tudunk mindig minimális súlyú élt választani

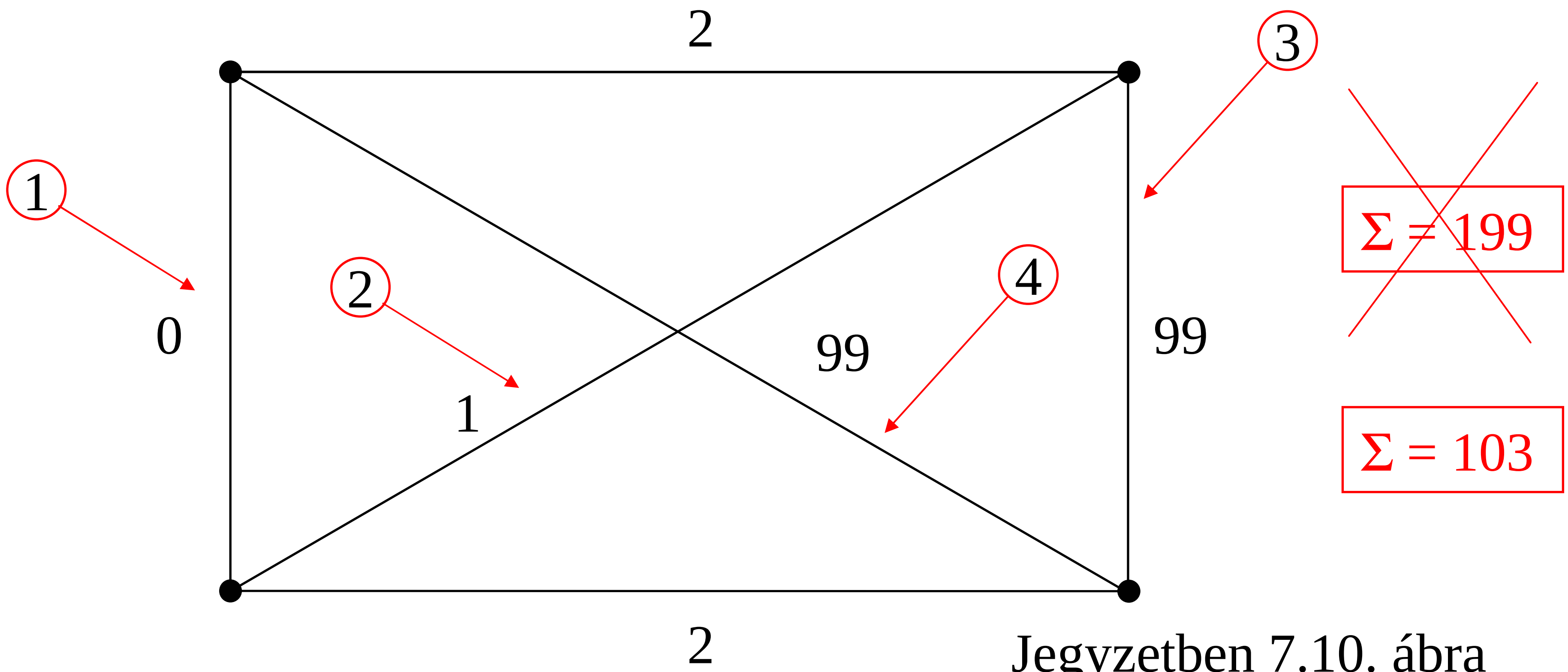


Jegyzetben 7.9. ábra

∀ lépésben a lehetséges lehetőségek közül az adott lépésben, a végcél szempontjából lehető legkedvezőbb választással élünk.

Nem biztos, hogy bejön !!!

Példa: minimális súlyú Hamilton-kört keresünk.



Jegyzetben 7.10. ábra

7.2. Irányított gráfok, síkbarajzolhatóság

Def. A $G = (V, E, \varphi)$ hármast **irányított gráfnak** nevezzük, ha V, E halmazok, $V \neq \emptyset$, $V \cap E = \emptyset$ és $\varphi : E \to V \times V$.

Def. Legyen $e \in E$. Ha $\varphi(e) = (u, v)$, akkor az e irányított él **kezdőpontja *u*, végpontja *v*.**

Def. Ha $(h) = (u, u)$, akkor h **hurokél.**

Def. e és f **(szigorúan) párhuzamos élek**, ha $\varphi(e) = (u, v)$ és $\varphi(f) = (u, v)$.

$\varphi(g) = (v, u)$ esetén e és g nem azok !

Def. Pont **kifoka**, $\boldsymbol{d^+(a)}$ a kimenő élek száma,

Def**.** Pont **befoka**, $\boldsymbol{d^-(a)}$ pedig a bemenő élek száma.

A hurokél a ki- és befok értékét is 1-gyel növeli.

Def**. Forrásnak** nevezzük a 0 befokú pontot, **nyelőnek** azt, amelyiknek kifoka 0.

Észrevétel: ha G véges irányított gráf, akkor

$$\sum_{a \in V(G)} d^+(a) = \sum_{a \in V(G)} d^-(a) = e(G).$$

Megjegyzés.

A $G = (V, E, \varphi)$ *irányított* gráfhoz **egyértelműen** hozzárendelhetjük a $G' = (V, E', \varphi')$ *irányítatlant*, oly módon, hogy minden $e \in E$, $\varphi(e) = (u, v)$ élhez felveszünk az E' halmazba egy e' élt, melyre $\varphi'(e') = [u, v]$.

A $G' = (V, E', \varphi')$ *irányítatlan* gráfhoz is hozzárendelhetünk egy $G = (V, E, \varphi)$ *irányítottat* úgy, hogy ha $e' \in E'$ és $\varphi'(e') = [u, v]$, akkor beveszünk az E halmazba egy e élt, amelyre $\varphi(e) = (u, v)$ vagy $\varphi(e) = (v, u)$. Ez az utóbbi hozzárendelés már nem lesz egyértelmű.

7.2.3. Irányított gráfok izomorfiája. A $G = (\psi, E, V)$ és $G' = (\psi', E', V')$ irányított gráfok *izomorf*ak, ha van olyan az E-t E'-re képező kölcsönösen egyértelmű f és a V-t V'-re képező kölcsönösen egyértelmű g leképezés, hogy minden $e \in E$-re egy $v \in V$ pontosan akkor kezdőpontja e-nek, ha $g(v)$ kezdőpontja $f(e)$-nek és pontosan akkor végpontja e-nek, ha $g(v)$ végpontja $f(e)$-nek.

Def. Legyen k természetes szám. **Irányított élsorozat** a $[v_0, e_1, v_1, \ldots, e_k, v_k]$ sorozat, ha $v_0, v_1, \ldots, v_k \in V(G)$ és $e_1, e_2, \ldots, e_k \in E(G)$, valamint $\varphi(e_i) = (v_{i-1}, v_i)$ minden $i = 1, 2, \ldots, k$-ra .

kapcsolódó fogalmak hasonlóan, mint irányítatlannál...

Def. A *G irányított* gráf **összefüggő**, ha a megfelelő $G' = (V, E')$ irányítatlan gráf összefüggő. A *G irányított* gráf **komponensei** a megfelelő G' irányítatlan gráf komponenseit jelentik. A komponensek száma $c(G) = c(G')$.

Def. A $G = (V, E)$ gráf **erősen összefüggő**, ha minden $v_1, v_2 \in V(G)$ esetén $v_1 = v_2$, vagy v_1-ből vezet v_2-be irányított út, és v_2-ből v_1-be is.

Tétel (irányított gráf erős összefüggősége)

A $G' = (V, E')$ összefüggő gráf akkor és csak akkor irányítható úgy, hogy a nyert $G = (V, E)$ erősen összefüggő legyen, ha G minden **éléhez** tartozik rajta áthaladó kör.

Hasonló nem mondható el olyan gráfról, melyben minden **csúcson** halad át kör.

Def.

Legyen $G = (V, E)$. Tekintsük a következő ekvivalenciarelációt:

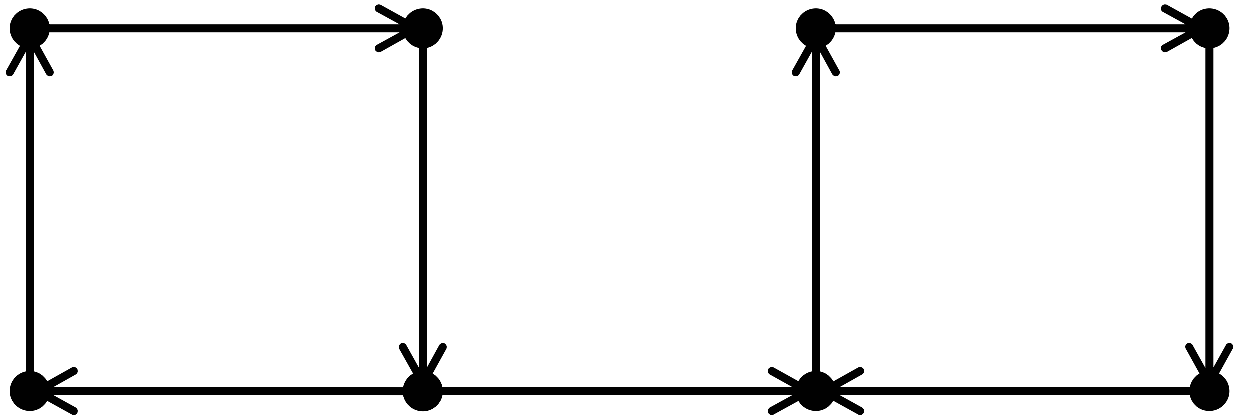
$v_1, v_2 \in V(G)$ esetén legyen $v_1 \sim v_2$, ha $v_1 = v_2$, vagy v_1 csúcsból v_2-be és v_2-ből v_1-be is vezet irányított út.

Osztályok: a csúcsok diszjunkt részhalmazai.

Általuk meghatározott telített részgráfok a G **erősen összefüggő komponensei** (**erős komponensek**).

Példa

1. Minden csúcson halad át kör, mégsem irányítható úgy, hogy erősen összefüggő legyen.



2. Az erős komponensek diszjunktak, és tartalmazzák a gráf minden pontját, de nem feltétlenül minden élét

7.2.7. Irányított fák. Egy irányított gráfot *irányított fának* nevezünk, ha fa, és van olyan csúcsa, amelyből minden csúcshoz vezet irányított út. Ez a csúcs nyilván egyértelműen meghatározott, ez az irányított fa *gyökere*.

A gyökértől minden csúcshoz pontosan 1 út vezet

$\Rightarrow$ gyökéren kívüli csúcsok befoka 1

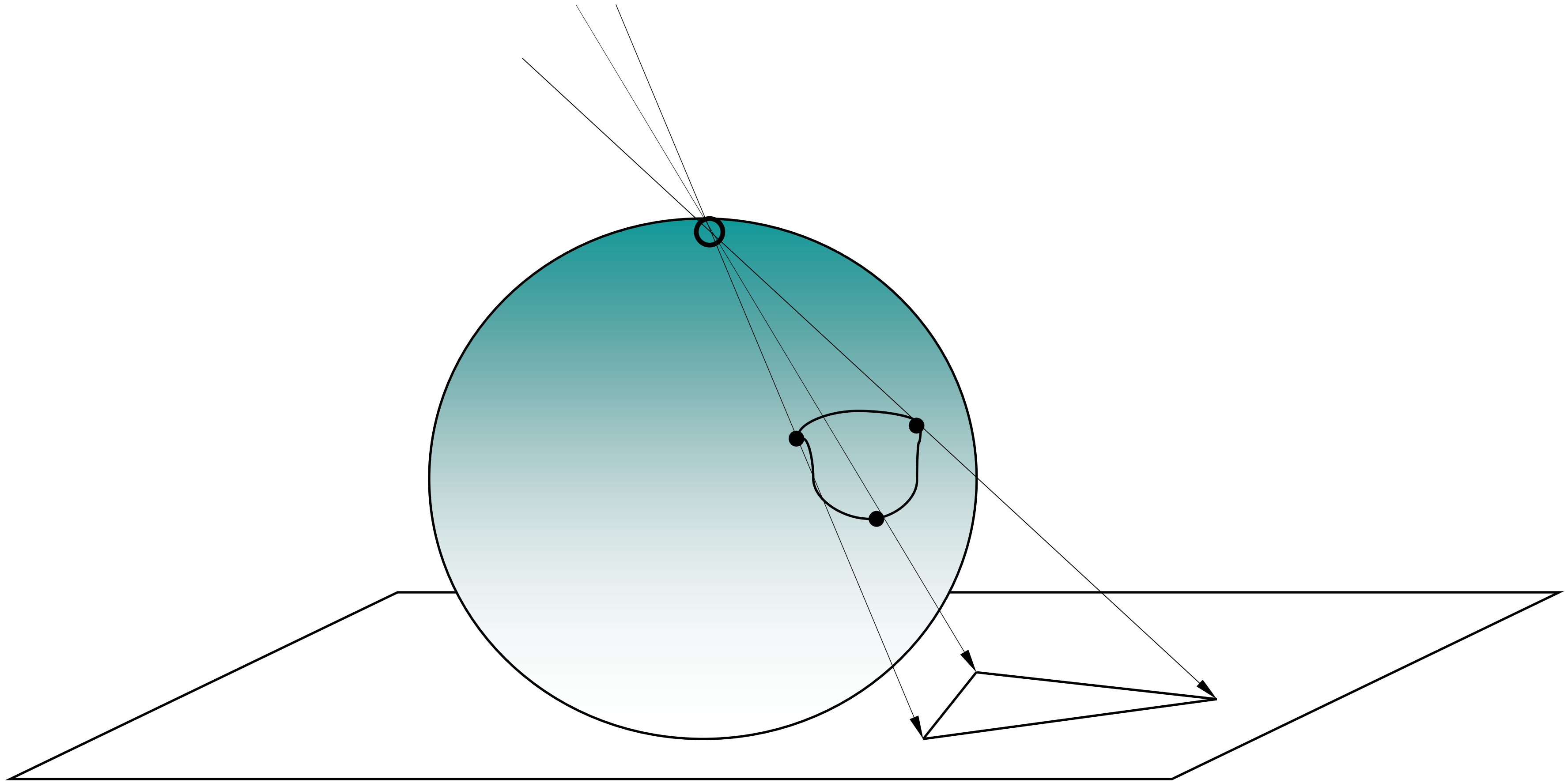
***n*-edik szint**: azon csúcsok halmaza, amelyekhez *n* hosszúságú út vezet a gyökérből, a szintek maximuma a fa **magassága.**

Ha *v* kezdő, *v´* és *v´´* végpontja egy élnek, akkor *v* a **szülő**, *v´* és *v´´* a **gyerekek (testvérek).**

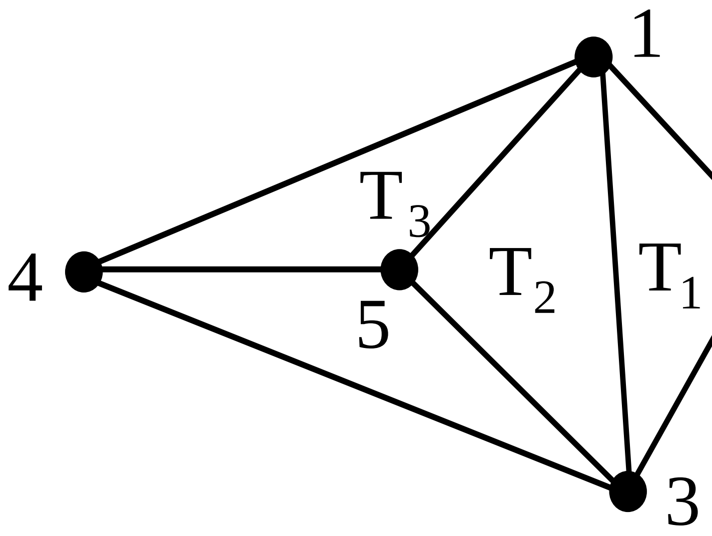
Irányított fa 0 kifokú csúcsa a **levél.**

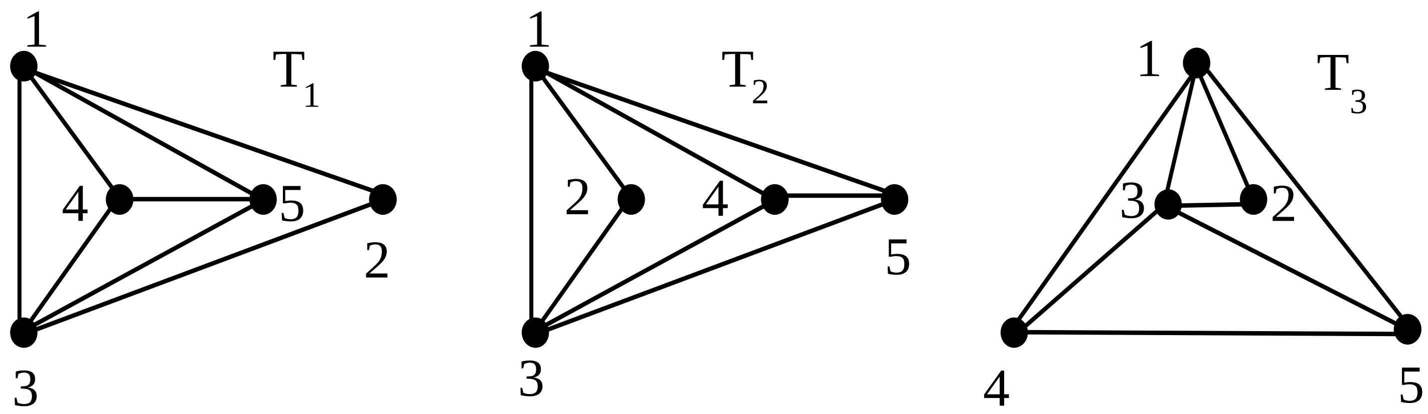
Síkba rajzolható gráfok

Egy gráf akkor és csak akkor rajzolható gömbre, ha síkba rajzolható.



Egy **tartomány** a síknak azon legnagyobb része, amelynek bármely két pontja összeköthető síkbeli vonallal, amely nem tartalmazza a gráf csúcsait, illetve éleinek egyetlen pontját sem. Síkba rajzolható gráf tetszőleges belső tartománya egy másik lerajzolásban lehet külső tartomány.





Tétel (Euler-formula)

Egy összefüggő síkbeli gráf, amelynek t tartománya van (a külső tartományt is beleértve), eleget tesz az **Euler-formulának**:

$$v(G) – e(G) + t = 2.$$

Bizonyítás (vázlatos)

Tekintsük a gráf egy K körét (ha van) és ennek egy a élét. A K kör a síkot két részre osztja. Mindkét részben van egy-egy tartomány, amelynek a határa.

a-t elhagyjuk $\Rightarrow$

A két tartomány egyesül, a tartományok és az élek száma eggyel csökken, és így $v(G) – e(G) + t$ értéke nem változik.

. . .

Ekkor a maradék gráf feszítőfa, melyre az állítás nyilvánvaló, hiszen $t = 1$ és $e(G) = v(G) - 1$.

$$\Rightarrow$$

$$v(G) - e(G) + t = v(G) - (v(G) - 1) + 1 = 2.$$ ☺

Tétel(síkgráf éleinek száma)

Ha G egyszerű, síkba rajzolható gráf, és $v(G) \geq 3$, akkor

$$e(G) \leq 3v(G) - 6.$$

Biz. **1. eset:** Tegyük fel, hogy G **összefüggő**.

$v(G) = 3$ -ra igaz $\Rightarrow$ tfh $v(G) > 3$

Mivel G egyszerű $\Rightarrow$ minden tartományát legalább 3 él határolja.

$\Rightarrow$ legalább $3t$ élet számoltunk

az elvágó éleket egyszer számoltuk, a többit kétszer $\Rightarrow$

$$3t \leq 2e(G).$$

Euler - formula $\Rightarrow$ $3(e(G) - v(G) + 2) \leq 2e(G)$

$$\Rightarrow \quad e(G) \leq 3v(G) - 6.$$

2. eset: Ha G **nem összefüggő,** + élek $\Rightarrow$ 1. eset. ☺

Tétel (síkgráf fokszámai)

Ha G egyszerű, síkba rajzolható gráf, akkor

$$\delta = \min_{a \in V(G)} d(a) \leq 5.$$

Bizonyítás (indirekt)

Az általánosság megsértése nélkül feltehetjük, hogy $v(G) \geq 3$.

Feltétel: tfh $\delta \geq 6$.

$$\sum_{a \in V(G)} d(a) = 2e(G) \qquad \delta \geq 6 \Rightarrow \qquad 6v(G) \leq 2e(G)$$

előző tétel $\Rightarrow$ $\quad 2e(G) \leq 6v(G) - 12$

$$6v(G) \leq 6v(G) - 12$$

☺

Tétel(Kuratowski gráfok)

K_5 és $K_{3,3}$ nem rajzolható síkba.

Bizonyítás (indirekt) **Feltétel:** K_5 és $K_{3,3}$ síkba rajzolható.

$K_{3,3}$ esetén, mivel $v(G) = 6$ és $e(G) = 9$,

Euler - formula $\Rightarrow t = 5$

Viszont $K_{3,3}$ nem tartalmaz háromszöget és nincs szeparáló éle.

$\Rightarrow \quad 4t \leq 2e(G) \quad \Rightarrow \quad 20 \leq 18$

K_5 esetén, mivel $v(G) = 5$ és $e(G) = 10$,

élszám tétel $\Rightarrow e(G) \leq 3v(G) - 6$

$10 \leq 9$

Def.

Egy gráf síkba rajzolhatóságát nem befolyásolja, hogyha egy élét helyettesítjük kettő hosszúságú úttal, illetve, ha valamelyik kétfokú csúcsra illeszkedő éleit egybeolvasztjuk, és a csúcsot elhagyjuk.

Két gráf **topologikusan izomorf**, ha az előbb említett transzformációk véges sokszori alkalmazásával izomorf gráfokba transzformálhatóak.

Tétel (Kuratowski)

Egy egyszerű véges gráf **akkor és csak akkor** rajzolható síkba, ha nem tartalmaz a Kuratowski gráfok valamelyikével topologikusan izomorf részgráfot.

Legyen a G gráfban: $V = \{v_1, ..., v_n\}$ és $E = \{e_1, ..., e_m\}$

Csúcsmátrix (szomszédsági mátrix) $\boldsymbol{B_{n\times n}}$

ha irányított $b_{ij} =$ ahány él van v_i kezdő és v_j végponttal

ha irányítatlan $b_{ij} = \begin{cases} i = j \text{ esetén ahány hurokél illeszkedik } v_i\text{-re} \\ i \neq j \text{ esetén ahány él van } v_i \text{ és } v_j \text{ közt} \end{cases}$

Illeszkedési mátrix (élmátrix) $\boldsymbol{B_{n\times m}}$

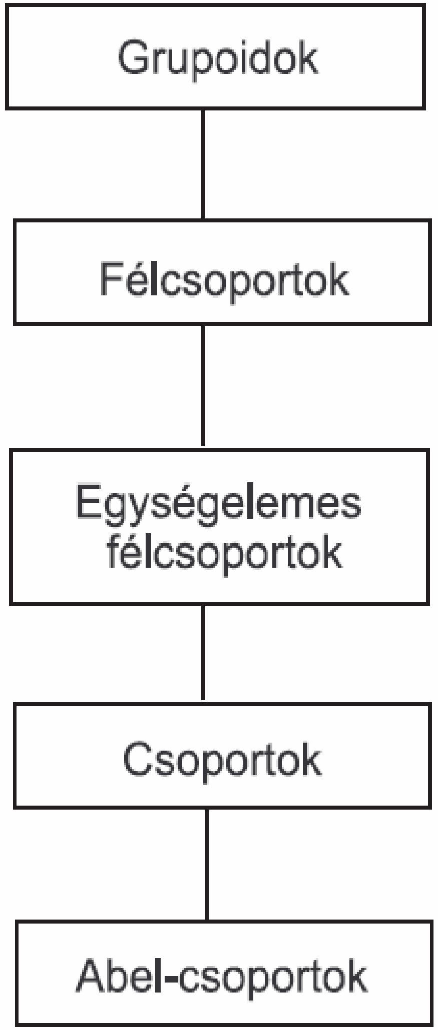
ha irányított $b_{ij} = \begin{cases} 1 \text{ ha } e_j\text{-nek } v_i \text{ kezdőpontja} \\ -1 \text{ ha } e_j \text{ nem hurokél és } v_i \text{ a végpontja} \\ 0 \text{ egyébként} \end{cases}$

ha irányítatlan $b_{ij} = \begin{cases} 1 \text{ ha } e_j \text{ illeszkedik } v_i \text{ pontra} \\ 0 \text{ egyébként} \end{cases}$

Algebra: csoportelmélet

8. ALGEBRA

8.1. Csoportok



Jegyzetben 8.1. ábra

Algebrai struktúrák

Def. Legyen H tetszőleges halmaz. Egy H-beli **n-ér műveleten** egy $f : H \times H \cdots \times H \to H$ függvényt értünk. Ha $x_1, x_2, \ldots, x_n \in H$, akkor $f(x_1, x_2, \ldots, x_n)$ a művelet **eredménye**, míg $x_1, x_2, \ldots, x_n$ a művelet **operandusai**.

Az (A, Ω) pár **algebrai struktúra**, ha A nem üres halmaz, és Ω az A-n értelmezett véges változós műveletek halmaza. (Ha tehát $\omega \in \Omega$, akkor egyértelműen létezik olyan $n \in \mathbf{N}_0$, melyre $\omega : A^n \to A$ függvény.)

A-t **tartóhalmaznak (alaphalmaz)** hívjuk.

Emlékeztető

Legyen $\cdot$ a G, $\otimes$ a G' halmazon értelmezett binér művelet. A $\varphi : G \to G'$ függvényt **homomorfizmusnak** nevezzük, ha művelettartó, vagyis minden $a_1, a_2 \in G$ esetén

$$\varphi(a_1 a_2) = \varphi(a_1) \otimes \varphi(a_2).$$

Epimorfizmus: szürjektív homomorfizmus

Monomorfizmus: injektív homomorfizmus

Izomorfizmus: bijektív homomorfizmus

Endomorfizmus: ha $G = G'$

Automorfizmus: ha $G = G'$ és bijektív

Észrevételek

Homomorfizmusok összetétele is homomorfizmus, mert ha $\varphi' : G' \to G''$ is homomorfizmus, akkor

$$\begin{aligned}(\varphi' \circ \varphi)(xy) &= \varphi'\big(\varphi(xy)\big) = \varphi'\big(\varphi(x)\varphi(y)\big) \\ &= \varphi'\big(\varphi(x)\big)\varphi'\big(\varphi(y)\big) = (\varphi' \circ \varphi)(x)(\varphi' \circ \varphi)(y).\end{aligned}$$

Izomorfizmusok összetétele nyilván izomorfizmus. Izomorfizmus inverze is izomorfizmus, mert

$$\varphi^{-1}\big((\varphi(x)\varphi(y)\big) = \varphi^{-1}\big(\varphi(xy)\big) = xy = \varphi^{-1}\big(\varphi(x)\big)\varphi^{-1}\big(\varphi(y)\big).$$

Def. Legyenek $(H, \cdot)$ és $(G, \otimes)$ binér műveletes algebrai struktúrák. **Izomorfaknak** nevezzük őket, ha létezik $\varphi : G \to H$ izomorfizmus. Ezt a tényt $H \cong G$ -vel jelöljük. $\varphi(G)$-t **G homomorf képének** nevezzük.

Példák

(1) Ha $a > 1$, akkor az $x \mapsto a^x$ leképezés $(\mathbb{R}, +)$-nak a pozitív valós számok szorzással tekintett csoportjára izomorfizmus.

(2) $(\mathbb{R}, +)$ és $(\mathbb{R} \setminus \{0\}, \cdot)$ nem izomorfak, mert a másodikban két olyan elem is van, amelynek a négyzete az egységelem.

Def.

Legyen (A, Ω) algebrai struktúra, ha Ω az n_0 , n_1 , ..., n_i, ... nullér, unér, stb. véges változós műveletek halmaza, akkor

$(n_0 , n_1 , ..., n_i, ...)$ az (A, Ω) algebrai struktúra **típusa**.

A (0, 0, 1, 0, ...) típusú algebrai struktúrákat **grupoidnak** hívjuk.

(0, 0, 2, 0, ...) típusú algebrai struktúrák például a gyűrűk.

Emlékeztető

Az (G, $\cdot$) binér műveletes algebrai struktúrában a műveletet

asszociatívnak nevezzük, ha minden a, b, $c \in G$ esetén $a(bc) = (ab)c$

kommutatív a műveletet, ha minden a, $b \in G$ esetén $ab = ba$.

reguláris, ha minden a, b, $c \in G$ esetén $ac = bc$ -ből következik, hogy $a = b$, valamint $ca = cb$ -ből következik, hogy $a = b$.

A (G, $\cdot$) algebrai struktúra **félcsoport**, ha egyetlen kétváltozós műveletet tartalmaz, amely asszociatív.

Tétel (Általános asszociativitási törvény).

Ha $(G, \cdot)$ félcsoport, akkor minden szorzat tetszőlegesen bontható zárójelekkel két részre:

$$(a_1 a_2 \ldots a_k)(a_{k+1} \ldots a_n) = a_1 a_2 \ldots a_n$$

minden $1 \leq k < n$ esetén.

Def. A $(G, \cdot)$ félcsoportban az $e_b \in G$ **bal oldali egységelem**, ha minden $a \in G$ esetén $e_b a = a$. $e_j \in G$ **jobb oldali egységelem**, ha minden $a \in G$ esetén $a e_j = a$. Az e **egységelem**, ha egyszerre bal és jobb oldali egységelem.

Példa.

$$G = \left\{ \begin{pmatrix} a & b \\ a & b \end{pmatrix} \middle| \, a, b \in \mathbf{R} \right\}$$

G félcsoport a mátrixszorzással, továbbá baloldali egységelem:

$$\begin{pmatrix} x & \mathrm{y} \\ x & \mathrm{y} \end{pmatrix},$$

végtelen sok van!

ahol $x + y = 1$, hiszen

$$\begin{pmatrix} x & \mathrm{y} \\ x & \mathrm{y} \end{pmatrix} \cdot \begin{pmatrix} c & d \\ c & d \end{pmatrix} = \begin{pmatrix} (x+y)\cdot c & (x+y)\cdot d \\ (x+y)\cdot c & (x+y)\cdot d \end{pmatrix} = \begin{pmatrix} c & d \\ c & d \end{pmatrix}$$

Def.

Legyen a $(G, \cdot)$ félcsoportban e egységelem. Az $a \in G$ elemnek $a_b \in G$ **balinverze**, ha

$$a_b a = e,$$

$a_j \in G$ **jobbinverze**, ha

$$aa_j = e.$$

Inverze a-nak az a' elem, ha

$$aa' = a'a = e.$$

G a $(G, \cdot)$ félcsoportban e_b baloldali egységelem. Az $a \in G$ elemnek $a_b \in G$ az $\boldsymbol{e_b}$**-re vonatkoztatott balinverze**, ha $a_b a = e_b$, illetve az $\boldsymbol{e_b}$**-re vonatkoztatott jobbinverze,** ha $aa_b = e_b$. Hasonlóan definiáható a bal- és jobbinverz fogalma jobboldali egységelemre.

Tétel(egységelem és inverz unicitása)

Félcsoportban legfeljebb egy egységelem létezik, és minden elemnek legfeljebb egy, az egységelemre vonatkozó inverze létezik.

Biz.

Legyen $(G, \cdot)$ félcsoport, e_b bal oldali, e_j pedig jobb oldali egységelem G-ban. Ekkor $e_b = e_j$, hiszen

$$e_b e_j = e_j \quad \text{és} \quad e_b e_j = e_b,$$

mert e_b bal-, e_j jobb oldali egységelem.

Asszociatív tulajdonság

Függvény egyértelmű!

Ha az $a \in G$ elemnek a_b balinverze, a_j pedig jobbinverze, akkor $a_b = a_j$:

$$a_b a a_j = a_b(a a_j) = a_b e = a_b \quad \text{és} \quad a_b a a_j = (a_b a) a_j = e a_j = a_j.$$

☺

Tétel(homomorf invariánsok félcsoportban)

(1) *ha G félcsoport, akkor a homomorf képe is félcsoport;*

(2) *ha G-ben e jobb oldali egységelem, bal oldali egységelem, illetve egységelem, akkor a homomorf képében e képe jobb oldali egységelem, bal oldali egységelem, illetve egységelem;*

(3) *ha G-ben e egységelem, és g-nek g^* jobb oldali inverze, bal oldali inverze, illetve inverze, akkor a homomorf képében g^* képe a g képének jobb oldali inverze, bal oldali inverze, illetve inverze;*

(4) *ha G-ben g és h felcserélhetőek, akkor a homomorf képben g és h képei felcserélhetőek.*

Biz. Legyen *a*, *b*, *c* ∈ G, a képelemeket jelölje ´ .

(1) $(a'b')c' = (ab)'c' = (abc)' = a'(bc)' = a'(b'c')$

(2) Ha *G*-nek *e* egységeleme, *g* tetszőleges eleme, akkor

$$g'e' = (ge)' = g' \quad \ldots$$

(3) Ha *g*-nek g^* a jobb oldali inverze, akkor

$$g'g^{*\prime} = (gg^*)' = e' \quad \ldots$$

(4) Ha *g* és *h* felcserélhető, akkor

$$g'h' = (gh)' = (hg)' = h'g'$$

Definíció I.

A $(H, \cdot)$ félcsoport **csoport**, ha

1. létezik benne e_b bal oldali egységelem, és

2. minden $a \in H$ elemnek létezik erre a bal oldali egységelemre vonatkozó a_b balinverze:

$$a_b a = e_b\,.$$

Definíció II.

A $(H, \cdot)$ félcsoport **csoport**, ha

1. létezik benne e egységelem, és

2. minden $a \in H$ elemnek létezik erre az egységelemre vonatkozó a^{-1} inverze :

$$a^{-1}a = aa^{-1} = e.$$

Definíció III.

A (H, $\cdot$) félcsoport **csoport**, ha

minden a, $b \in H$ esetén ***egyértelműen*** létezik az

$$ax = b \text{ és az } ya = b$$

egyenletek megoldása H-ban.

Definíció IV.

A (H, $\cdot$) félcsoport **csoport**, ha a művelet **invertálható**, azaz

minden a, $b \in H$ esetén létezik az

$$ax = b \text{ és az } ya = b$$

egyenletek megoldása H-ban.

Tétel(csoport definíciói) 16

A csoport definíciói ekvivalensek egymással.

Biz.

I. $\Rightarrow$ II.

Legyen $a \in H$ bal oldali egységelemre vonatkozó balinverze a_b, az a_b bal oldali egységelemre vonatkozó balinverze pedig b, ekkor egyrészt

$$ba_baa_b = (ba_b)aa_b = e_baa_b = (e_ba)a_b = aa_b\,,$$

másrészt

$$ba_baa_b = b(a_ba)a_b = be_ba_b = ba_b = e_b\,.$$

Tehát $aa_b = e_b$.

$$\Rightarrow$$

a_b az a elem kétoldali inverze e_b-re vonatkozóan: a^{-1}.

Továbbá e_b jobb oldali egységelem is, mert

$$aa^{-1}a = (aa^{-1})\,a = e_b a = a \ ,$$

és

$$aa^{-1}a = a(a^{-1}\,a) = ae_b \ ,$$

$$\Rightarrow$$

$$ae_b = e_b a = a \ .$$

II. ⇒ III.

Belátható, hogy az $ax = b$ egyenletnek legfeljebb egy megoldása van, legyen ugyanis x_0 egy megoldás, azaz

$$ax_0=b.$$

Ekkor balról szorozva a^{-1}-nel kapjuk, hogy

$$a^{-1}ax_0 = a^{-1}b\ ,$$

$$ex_0 = a^{-1}b$$

$$x_0 = a^{-1}b$$

Függvény egyértelmű!!!

Tehát az egyenlet megoldása legfeljebb az $a^{-1}b$ elem lehet, és valóban az is, mert

$$a(a^{-1}b) = (a^{-1}a)b = eb = b.$$

Az $ya = b$ esetben hasonlóan bizonyítunk.

III. $\Rightarrow$ **IV.** Az állítás nyílvánvaló.

IV. $\Rightarrow$ **I.**

Első kérdés: létezik-e baloldali egységelem?

Tekintsünk egy tetszőleges $a \in H$ elemet és oldjuk meg az

$$ya = a$$

egyenletet. Legyen a megoldás e_b.

IV. $\Rightarrow$ tetszőleges $b \in H$ -ra megoldható az

$$ax = b$$

egyenlet is. Legyen x_0 egy megoldás. Ekkor

$$e_b b = e_b(ax_0) = (e_b a)x_0 = ax_0 = b.$$

Második kérdés: létezik-e a baloldali egységelemre vonatkozó balinverz is H-ban?

Válasz: Igen, mert

tetszőleges $a \in H$-re az $ya = e_b$ egyenlet megoldható

a megoldás lesz a bal oldali egységelemre vonatkozó balinverz.

☺

Def. **Abel-csoportnak** nevezzük a kommutatív csoportokat.

Következmény

Csoportban a művelet **reguláris** .

Biz.

Tegyük fel, hogy $ac = bc = d$.

az $yc = d$ egyenlet megoldása egyértelmű,

a és b megoldásai az egyenletnek,

$$\Rightarrow$$

$$a = b.$$

A másik oldali regularitás hasonlóan látható be. ☺

Észrevétel(szorzat inverze):

$$(ab)^{-1} = b^{-1}a^{-1} \ .$$

Hiszen:

$$(b^{-1}a^{-1})\, ab = b^{-1}(a^{-1}a)b = b^{-1}b = e.$$

Példa

Legyen $(H, \cdot)$ a következő algebrai struktúra:

$$H = \{a, b, c\},$$

a műveletet pedig definiálja a következő tábla:

$\forall\, a, b \in H$ -ra megoldható: $ax = b$ (sorok) és $ya = b$ (oszlopok) is

.	a	b	c
a	b	a	c
b	a	c	b
c	c	b	a

Invertálható, egyértelmű.

Nincs egységelem! Nincs inverz!

Hogy fordulhat ez elő?

Válasz: nem asszociatív a művelet:

$$(ab)c = ac = c,$$

$$\neq a(bc) = ab = a.$$

8.1.9. Példák. (1) Ha $n \in \mathbb{N}^+$, az n-edik komplex egységgyökök a szorzással Abel-csoportot alkotnak.

(2) Legyen p prímszám. Az összes p^n-edik egységgyökök halmaza, ahol $n = 1, 2, \ldots$, a szorzással szintén Abel-csoport, ez a $Z(p^\infty)$ *Prüfer-csoport.*

(3) Az összes egységgyökök halmaza a szorzással (tehát az első példában szereplő csoportok egyesítése) szintén Abel-csoport.

(4) Az egységnyi abszolút értékű komplex számok a szorzással Abel-csoport.

(5) A $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ kvaterniók a kvaterniószorzással nem kommutatív csoportot alkotnak.

(6) A *Klein-féle csoport*ot a szorzótáblájával definiáljuk:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Def. Legyen (A, Ω_1), (B, Ω_2) algebrai struktúra és $B \subseteq A$.

Ha létezik Ω_1 és Ω_2 között olyan kölcsönösen egyértelmû leképezés, hogy minden Ω_1-beli f_1-nek megfelelő Ω_2 -beli f_2 az f_1 B-re való megszorítása, akkor azt mondjuk, hogy

B **részstruktúrája** A-nak, jelben $B \leq$ A. Ha B valódi részhalmaza A-nak **valódi részstruktúráról** beszélünk.

Csoport tetszőleges, nem üres részhalmaza: **komplexus**.

Komplexus szorzás:
Legyen (H, $\cdot$) csoport, P ={ K | K komplexus H-ban }. K, $L \in P$ esetén $KL = \{ kl \mid k \in K \text{ és } l \in L \}$.

Lemma (komplexusok félcsoportja)

Adott H csoport komplexusai a komplexusszorzásra egységelemes félcsoportot alkotnak.

Biz.

1. A komplexusszorzás zárt P-re nézve, hiszen $P^2 \to P$ alakú függvény.

2. A művelet asszociatív, mivel $K, L, M \in$ P esetén

$$K(LM) = \{k \cdot (l \cdot m) \mid k \in K, l \in L, m \in M\} =$$

$$= (KL)M = \{(k \cdot l) \cdot m \mid k \in K, l \in L, m \in M\}$$

3. Egységelem: $E = \{e\}$, ahol e a H-beli egységelem, mivel tetszőleges $K \in$ **P** esetén

$$EK = \{ek \mid k \in K\} = \{k \mid k \in K\} = K,$$

$$KE = \{ke \mid k \in K\} = \{k \mid k \in K\} = K\,.$$

☺

Tétel (ekvivalens állítások részcsoportokra)

Legyen $(G, \cdot)$ csoport és H komplexus G-ben. Ekkor a következő állítások ekvivsalensek:

(1) H részcsoport G-ben,

(2) A $\cdot$ művelet H-ra való leszűkítése egy $H \times H$-t H-ba képező leképezés, H tartalmazza G egységelemét és $H^{-1} \subseteq H$,

(3) $HH \subseteq H$ és $H^{-1} \subseteq H$,

(4) $H^{-1}H \subseteq H$.

Biz.

(1) $\Rightarrow$ (2):

Feltesszük, hogy $H \leq G$

1. Ekkor a leszűkítésnek belső műveletnek kell lennie H-n, azaz bármely két H-beli elem szorzata H-beli, különben nem lenne csoport.

2. H-nak van egységeleme e_H, mert csoport, így $\forall$ H-beli k elemre

$$e_H k = k,$$

továbbá a G-ban levő e_G egységelemre is teljesül G-ben, hogy

$$e_G k = k.$$

regularitás $\Rightarrow$ $\quad e_G = e_H$

3. Legyen $k \in H$ elem inverze H-ban

$$k_H^{-1},$$

G-ben pedig

$$k_G^{-1}.$$

A következő összefüggéseknek teljesülnie kell:

$$k_G^{-1} \cdot k = e_H, \qquad k_H^{-1} \cdot k = e_H.$$

regularitás $\Rightarrow$ $k_G^{-1} = k_H^{-1}.$

(2) $\Rightarrow$ (3): Triviális

(3) $\Rightarrow$ (4):

$$H^{-1} \subset H \longrightarrow H^{-1}H \subset HH \longrightarrow H^{-1}H \subseteq H$$

(4) $\Rightarrow$ (1):

Most tegyük fel, hogy $H^{-1}H \subseteq H$.

1. $H \neq \emptyset \Rightarrow$

$$\exists\, k \in H \Rightarrow k^{-1} \in H^{-1} \Rightarrow k^{-1}k \in H^{-1}H \subseteq H.$$

$$\Rightarrow$$

$$e \in H.$$

2. $\forall\, k \in H \Rightarrow$

$$k^{-1}e \in H^{-1} H \subseteq H,$$

tehát H-beli elem inverze is H-ban van.

3. $k, l \in H \;\Rightarrow\; kl \in H$?

$$k, l \in H \Rightarrow k^{-1} \in H^{-1} \Rightarrow k^{-1} \in H$$

$$\Rightarrow$$

$$kl = (k^{-1})^{-1} l \in H^{-1}H \subseteq H.$$

☺

Megjegyzés

$H \leq G \Rightarrow H^{-1}H = H$ és $HH = H$, mert

$H = eH \subseteq H^{-1} H \subseteq H$, illetve $H = eH \subseteq HH \subseteq H$.

Következmény

Legyen G csoport, $\Gamma \neq \emptyset$ adott indexhalmaz, és minden $\gamma \in \Gamma$ esetén $H_\gamma \leq G$. Ekkor a részcsoportok metszete is részcsoport, vagyis

$$D = \bigcap_{\gamma \in \Gamma} H_\gamma \leq G.$$

Biz.

$$e \in D \Rightarrow D \neq \emptyset,$$

tehát D komplexus G-ben, továbbá tetszőleges $\gamma \in \Gamma$-ra:

$$D^{-1}D \subseteq H_\gamma^{-1} H_\gamma \subseteq H_\gamma, \qquad \text{mert } H_\gamma \leq G$$

$$\Rightarrow D^{-1}D \subseteq \bigcap_{\gamma \in \Gamma} H_\gamma = D$$

Tétel $\Rightarrow D \leq G$. ☺

Megjegyzés

Részcsoportok uniójára hasonló állítás nem mondható.

Példa (Klein-csoport)

Adott $(H, \cdot)$, ahol $H = \{e, a, b, c\}$, továbbá:

.	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Ekkor $K = \{e, a\}$ és $L = \{e, b\}$ részcssoportjai H-nak, de

$K \cup L = \{e, a, b\}$ nem részcsoport!

Def

Legyen G csoport és K komplexus G-ben. K **generátuma**

G-nek a K halmazt tartalmazó legszűkebb részcsoportja

$$\langle K \rangle = \bigcap_{\substack{L \le G \\ K \subseteq L}} L.$$

Ha $\langle K \rangle = G$, akkor K a G **generátorrendszere.**

Ha $K = \{g\}$ (egyelemű), akkor

generátor, vagy generáló elem

G az g elem által generált **ciklikus csoport**.

Tétel (generátum elemei)

Ha K komplexusa a G csoportnak akkor

$$\langle K \rangle = \{ k_1 \cdot \ldots \cdot k_s \mid s \in \mathbf{N},\, k_j \in K \cup K^{-1},\ 1 \le j \le s \}$$

üres szorzat az egységelem!

Biz. Legyen

$$H = \{ k_1 \cdot \ldots \cdot k_s \mid s \in \mathbf{N},\, k_j \in K \cup K^{-1},\ 1 \le j \le s \}$$

1. Nyílvánvaló, hogy $H \subseteq \langle K \rangle$, mivel $\langle K \rangle$ részcsoport G-ben.

2. H is részcsoport G-ben, mivel benne van G egységeleme, zárt a szorzásra és az inverzképzésre.

továbbá, minden K-beli elemet tartalmaz

$$\Rightarrow \langle K \rangle \subseteq H$$

☺

8.1.18. Következmény. *Ha $g \in G$, akkor $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Egy ciklikus csoport homomorf képe is ciklikus, egy generátor képe generálja a homomorf képet.*

Def. **Csoport rendje** a csoport elemeiből álló halmaz számossága. G csoport esetén ezt $|G|$ -vel vagy $O(G)$-vel jelöljük.

***g* ∈ *G* elem rendje** a legkisebb n pozitív egész, amelyre $g^n = e$, ha nincs ilyen n, akkor ∞.

Példák.

1. Az $(R^*, \cdot)$ csoportban +1 és –1 végesrendű elemek, a többi végtelenrendű.

2. Prüfer-csoport (az összes p^n-edik egységgyök, ahol p rögzített prímszám és a művelet a közönséges szorzás)

Minden elem végesrendű, maga a csoport végtelenrendű.

8.1.20. Tétel. *Végtelen ciklikus csoport izomorf az egész számok additív csoportjával, míg n elemű ciklikus csoport a modulo n maradékosztályok $\mathbb{Z}_n$ additív csoportjával izomorf. Speciálisan, a ciklikus csoportok kommutatívak.*

Biz. 1. Végtelen eset

($\mathbf{Z}$, +) csoport, továbbá tekintsünk egy g elem által generált végtelen ciklikus csoportot:

$$g^0 = e,\ g,\ g^{-1},\ g^2,\ g^{-2},\ \ldots$$

Izomorf leképezés hozható létre köztük:

$$\varphi(n) = g^n, \quad n \in \mathbf{Z}$$

$n, m \in \mathbf{Z}$ esetén:

$$\varphi(n+m) = g^{n+m} = g^n g^m = \varphi(n)\varphi(m),$$

tehát lényegében egyetlen végtelen ciklikus csoport van.

2. Véges eset

Biztosan léteznek $k > s$ egészek úgy, hogy

$$g^k = g^s \quad \Rightarrow \quad g^{k-s} = e\,.$$

Az ilyen tulajdonságú természetes számok közül a legkisebbet jelöljük n-nel.

Ekkor az

$$g^0 = e,\ g,\ g^2,\ \ldots,\ g^{n-1} \qquad (*)$$

elemek egyrészt mind különbözőek, másrészt g-nek minden hatványa előfordul a fenti halmazban.

Miért ?

A különbözőség n minimális voltából következik.

Legyen m tetszőleges egész, maradékos osztás n-nel egyértelmű:

$m = qn + r$, ahol $0 \leq r < n$

$$\Rightarrow$$

$$g^m = g^{qn+r} = g^{qn}g^r = (g^n)^q g^r = e^q g^r = g^r.$$

Mindezek alapján a (*) elemek alkotják a csoportot.

Vizsgáljuk továbbá a következő függvényt: $\varphi(x \text{ (mod } n)) = g^x.$

φ izomorfizmus a (*mod n*) maradékosztályok additív csoportja és (*) halmaz között.

Ezek szerint minden n természetes számhoz lényegében egyetlen n-edrendű ciklikus csoport van.

A ciklikus csoportok kommutatívak, hiszen

$$g^k g^s = g^{k+s} = g^s g^k \text{ minden } k, s \in \mathbf{Z}\text{-re.}$$

☺

Észrevétel: $g \in G$ elem rendje megegyezik az elem által generált részcsoport rendjével.

Tétel (ciklikus csoport részcsoportja)

Ciklikus csoport minden részcsoportja ciklikus.

Biz.

Legyen $\langle g \rangle = G$ és $H \leq G$.

1. eset: $H = \{e\}$, ekkor kész.

2. eset: $H \neq \{e\}$, ekkor biztosan létezik g-nek pozitív kitevős hatványa H-ban.

Legyen ***d*** az a legkisebb pozitív kitevő, melyre $g^d \in H$.

$$g^d \in H \Rightarrow$$

$$\langle g^d \rangle \subseteq H$$

Most már csak azt kell bizonyítanunk, hogy H-nak tetszőleges g^m eleme g^d-nek hatványa.

Maradékos osztás d-vel egyértelmű:

$m = qd + r$, ahol $0 \leq r < d$.

$$\Rightarrow$$

$$g^r = g^{m-qd} = g^m (g^d)^{-q} \in H.$$

$0 \leq r < d$ és d minimalitása $\Rightarrow$

$$r = 0 \Rightarrow \quad g^r = e = g^m (g^d)^{-q} \Rightarrow$$

inverzek

$$g^m = (g^d)^q \Rightarrow \quad \langle g^d \rangle \supseteq H.$$

☺

8.1.23. Tétel. *Legyen G egy n rendű véges ciklikus csoport, g pedig egy generátoreleme G-nek. Ha $a \in \mathbb{Z}$ és $d = \mathrm{lnko}(a, n)$, akkor g^a a $H = \{g^d, g^{2d}, \ldots, g^{md} = e\}$ ciklikus részcsoportot generálja, ahol $n = md$. A G minden részcsoportja előáll így valamely $d|n$-re. A G-nek $\varphi(n)$ generátora van.*

Biz.

előző tétel bizonyításánál láttuk, hogy $\exists$ ilyen d, méghozzá a legkisebb pozitív egész, amelyre $g^d \in H$

ez $\varphi(n)$ definíciójából következik

$$d \mid a \Rightarrow a = qd \Rightarrow g^a = (g^d)^q \qquad \Rightarrow \langle g^a \rangle \subseteq H$$

euklidészi alg. $\Rightarrow \exists\, x, y \in \mathbf{Z}$: $d = ax + ny$

$$g^d = g^{ax+ny} = g^{ax}g^{ny} = g^{ax}e^y = (g^a)^x$$

$$\Rightarrow \mathrm{H} \subseteq \langle g^a \rangle$$

☺

Mellékosztályok

Legyen G csoport, $H \leq G$ és $a \sim b$, ha $ab^{-1} \in H$, valamely $a, b \in G$-re.

Észrevétel: $\sim$ ekvivalencia reláció

1. Reflexív ? $\surd$

$aa^{-1} \in H$, mert H csoport.

2. Szimmetrikus ? $\surd$

$ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} = ba^{-1} \in H$

3. Tranzitív ? $\surd$

$ab^{-1} \in H$ és $bc^{-1} \in H \Rightarrow ab^{-1}bc^{-1} = ac^{-1} \in H$

Lemma (*a* elem ekvivalencia osztálya)

$a \in G$ elem ekvivalencia osztálya a Ha mellékosztály.

Biz.

Tfh $b \in Ha$

$\Rightarrow b = ha$, valamely $h \in H$ ra.

$$ba^{-1} = h \Rightarrow$$

$$(ba^{-1})^{-1} = ab^{-1} = h^{-1} \in H \text{ , azaz } a \sim b.$$

Tfh $a \sim b$

$$\Rightarrow ab^{-1} = h \in H \Rightarrow ba^{-1} = h^{-1} \in H^{-1}$$

$$\Rightarrow b = h^{-1}a \in H^{-1}a \subseteq Ha.$$

☺

Így is bevezethetjük:

Legyen G csoport, $H \leq G$ és $a \sim b$, ha $b^{-1}a \in H$, valamely $b \in G$-re.

Def. Legyen G csoport, $H \leq G$, és $a \in G$.

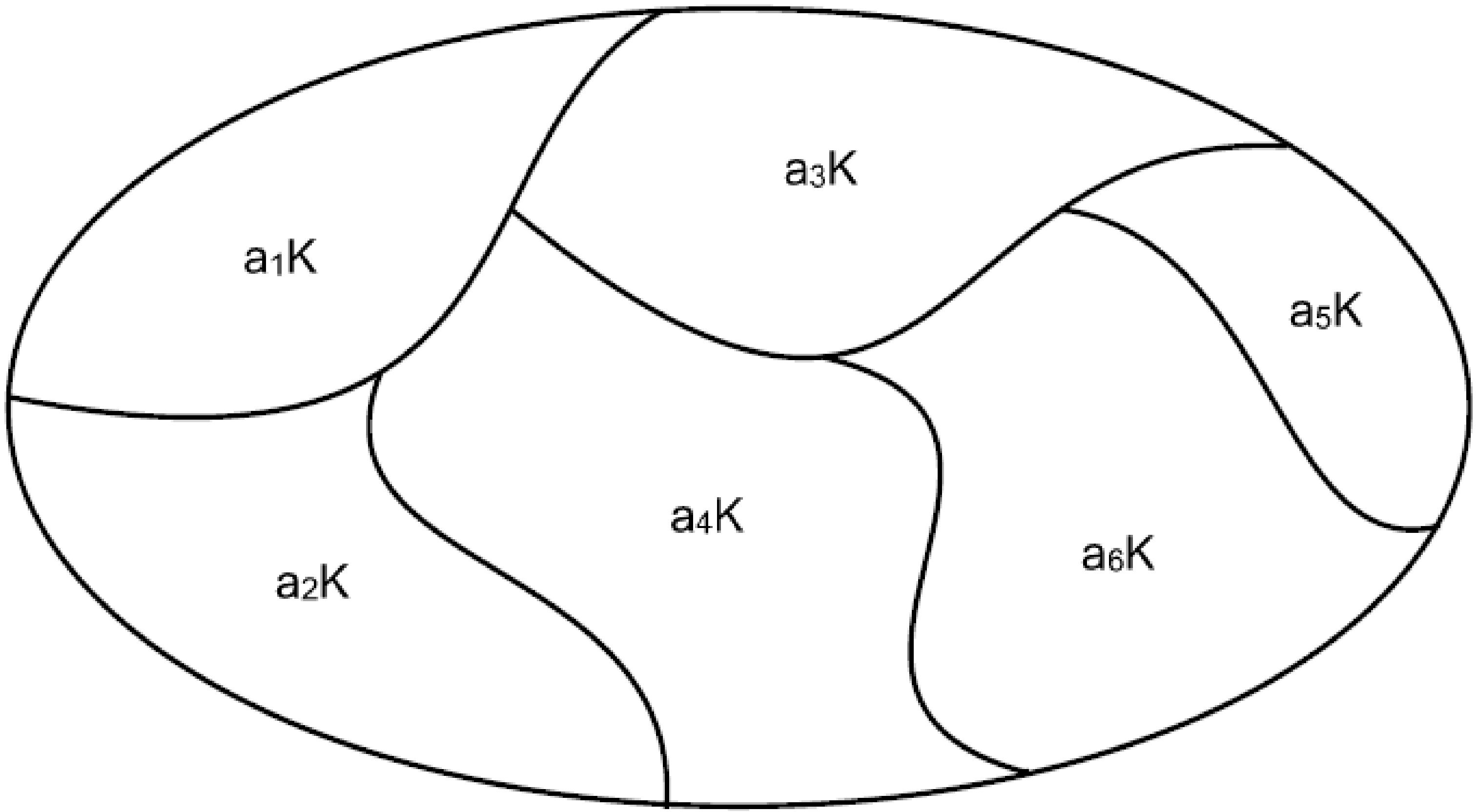
A G csoport H részcsoportja szerinti **bal oldali mellékosztálya** az

$$aH = \{ak \mid k \in H\} \text{ komplexus,}$$

Ha komplexus pedig **jobb oldali mellékosztálya**.

Ha minden aH / Ha-ból kiveszünk egy reprezentáns elemet, akkor H-nak **bal / jobb oldali reprezentánsrendszerét** kapjuk.

Egy csoport valamely részcsoportja szerinti mellékosztályok a csoport elemeinek osztályozását adják, így két mellékosztály vagy megegyezik, vagy diszjunkt halmaz.



Jegyzetben 8.2. ábra

Észrevétel: a

$$Ha \mapsto (Ha)^{-1} = a^{-1}H$$

leképezés bijektív leképezés jobb, illetve bal oldali mellékosztályok halmaza között $\Rightarrow$

A G csoport tetszőleges részcsoportja szerinti különböző bal oldali és különböző jobb oldali mellékosztályainak a száma megegyezik.

Def. Legyen G csoport, $H \le G$. A H szerinti mellékosztályok halmazának számossága ***H* indexe** *G-ben*. Jelölése: $|G : H|$, $[G : H]$.

lehet végtelen is

Tétel (Lagrange)

Legyen G véges csoport és $H \le G$. H rendjének és G-beli indexének a szorzata egyenlő G rendjével.

Biz.

$$|G| = \sum_{r \in R} |rH|,$$

ahol R egy bal oldali reprezentánsrendszere H-nak.

Legyen $\varphi(h) = ah \Rightarrow$ φ egy bijekció H és aH között, mert

szürjektív: minden $ah \in aH$-nak az őse: $h \in H$,

injektív: tfh $ah_1 = ah_2$, valamely $h_1, h_2 \in H$-ra

regularitás $\Rightarrow$ $h_1 = h_2$. $\Rightarrow |H| = |rH|$

$$\Rightarrow |G| = |H| \cdot |R| = |H|\,|G:H|$$

☺

A Lagrange-tétel következményei:

1. Véges csoportban elem rendje osztója a csoport rendjének.

2. Prímszámrendű csoport ciklikus.

Biz. Tfh $|G| = p$, p prím.

$\Rightarrow \exists\, a\ (\neq e) \in G$

Lagrange-tétel $\Rightarrow$ $|a| \mid |G|$

Tehát $|a|$ csak p vagy 1 lehet, és így az a elem generálja az egész G csoportot, tehát G ciklikus.

Megjegyzés:Az egységelem kivételével bármelyik eleme generálja G-t.

Def. **Triviális csoportnak** nevezzük a pusztán az egységelemből álló csoportot. Minden más G csoport esetén különböző részcsoportot alkotnak az egységelem és a G maga. Ezeket **triviális részcsoportoknak** nevezzük.

Tétel (prímszámrendű csoport)

Egy nem egyelemű csoport akkor és csak akkor **prímszámrendű,** ha csak triviális részcsoportja van.

Biz.

$\Rightarrow$ **:** Előző megjegyzés $\Rightarrow$

ha G prímszámrendű, akkor ciklikus és a részcsoportok:

$\{e\}$ és maga a G.

$\Leftarrow$: Tfh G olyan csoport, amelynek pontosan két részcsoportja van, és legyen $a \in G$, $a \neq e$.

$$\Rightarrow \langle a \rangle = G$$

$$\Rightarrow G \text{ ciklikus.}$$

1. Kérdés: Lehet-e $|G| = \infty$?

Válasz: **nem**, mert akkor pl. a^n valódi részcsoportot generálna G-ben.

2. Kérdés: Lehet-e $|G|$ = nem prím ?

Válasz: **nem**, mert ha $|G| = n_1 n_2 \ldots n_k$, ahol $n_i > 1$, akkor

$$\left\langle a^{n_i} \right\rangle \leq G, \qquad \text{mert} \qquad \left(a^{n_i}\right)^{n_1 n_2 \ldots n_{i-1} n_{i+1} \ldots n_k} = e.$$

☺

Def. A G csoport N részcsoportját **invariáns** vagy **normális részcsoportnak** (**normálosztónak**) nevezzük, jelben $N \triangledown G$, ha $Na = aN$ minden $a \in G$-re teljesül.

8.1.30. Tétel. *Legyen N a G csoport részcsoportja. A következő feltételek ekvivalensek:*

(1) *N normálosztó;*

(2) *$a^{-1}Na = N$ minden $a \in G$-re;*

(3) *$a^{-1}Na \subset N$ minden $a \in G$-re;*

Biz.

(1) $\Rightarrow$ (2)

$$a^{-1}Na = a^{-1}aN = N \text{ minden } a \in G\text{-re.}$$

(2) $\Rightarrow$ (1)

$$Na = a(a^{-1}Na) = aN$$

(2) $\Rightarrow$ (3) trivi

(3) $\Rightarrow$ (2)

Tfh $a^{-1}Na \subseteq N$ minden $a \in G$-re, de

a^{-1} is eleme G-nek $\Rightarrow$

$$\underbrace{\left(a^{-1}\right)^{-1}}_{a} Na^{-1} \subseteq N$$

$$N = a^{-1}(aNa^{-1})a \subset a^{-1}Na \qquad \Rightarrow a^{-1}Na = N$$

☺

Következmények

(3)-ból következik:

normálosztók metszete is normálosztó

Def. Ha G csoport és $a \in G$ rögzített, akkor a G-n értelmezett

$$x \mapsto a^{-1}xa$$

leképezést **belső automorfizmusnak** nevezzük.

(2)-ből következik:

a normálosztók pontosan azok a részcsoportok, amelyeknek minden belső automorfizmus melletti képe saját maga.

Emlékeztető: tétel(homomorf invariánsok félcsoportban)

(1) *ha G félcsoport, akkor a homomorf képe is félcsoport;*

(2) *ha G-ben e jobb oldali egységelem, bal oldali egységelem, illetve egységelem, akkor a homomorf képében e képe jobb oldali egységelem, bal oldali egységelem, illetve egységelem;*

(3) *ha G-ben e egységelem, és g-nek g^* jobb oldali inverze, bal oldali inverze, illetve inverze, akkor a homomorf képében g^* képe a g képének jobb oldali inverze, bal oldali inverze, illetve inverze;*

(4) *ha G-ben g és h felcserélhetőek, akkor a homomorf képben g és h képei felcserélhetőek.*

csoport homomorf képe csoport

8.1.34. Tétel. *Legyen G csoport. Ekkor*

(1) *egy N normálosztó szerinti mellékosztályok a csoportnak a művelettel kompatibilis osztályozását alkotják;*

(2) *minden, a művelettel kompatibilis osztályozás esetén az egységelem osztálya normálosztó, és az osztályozás ezen normálosztó szerinti mellékosztályokból áll;*

(3) *a mellékosztályok közötti művelet megegyezik az osztályok mint halmazok komplexusszorzásával.*

Biz.

(1) Tfh $a' \in Na$, $b' \in Nb$. Ekkor

$$Na' = Na \text{ és } Nb' = Nb$$

$\Rightarrow$

$$a'b' \in (Na')(Nb') = (Na)(Nb) = N(aN)b$$

$$= N(Na)b = N^2ab = Nab$$

tehát *a'b'* ~ *ab* .

(3)

$$\{a'b' : a' \in Na, b' \in Nb\} = (Na)(Nb) = Nab$$

(2) Tfh ∃ a művelettel kompatibilis osztályozás és legyen *N* az *e* egységelem osztálya, ekkor

$$a \in N \text{ esetén } e = a^{-1}a \sim a^{-1}e = a^{-1}$$

$$\Rightarrow \quad N^{-1} \subset N$$

$b \in N \quad \Rightarrow \quad ab \sim ee = e$, így $NN \subset N$

$\Rightarrow N$ részcsoport

Ha $x \in N$ és g tetszőleges, akkor $g^{-1}xg \sim g^{-1}eg = e$

$\Rightarrow g^{-1}Ng \subset N$, tehát N normálosztó

Mik lesznek az ekvivalencia osztályok?

Ha $a \sim b \Rightarrow a^{-1}ab^{-1} \sim a^{-1}bb^{-1} \Rightarrow b^{-1} \sim a^{-1} \Rightarrow e = aa^{-1} \sim ab^{-1}$

$\Rightarrow ab^{-1} \in N$

és fordítva, ha $ab^{-1} \in N \Rightarrow ab^{-1} \sim e$

$\Rightarrow a = ab^{-1}b \sim eb = b$

azaz az osztályozás pontosan az N szerinti mellékosztályokból áll ☺

8.1.35. Következmény. *Egy G csoportnak egy N normálosztó szerinti mellékosztályai a (komplexus)szorzásra nézve csoportot alkotnak.*

Biz.

Az $a \mapsto Na$ keképezés homomorf

homomorf invariánsok félcsoportban tétel $\Rightarrow$

G homomorf képe csoport

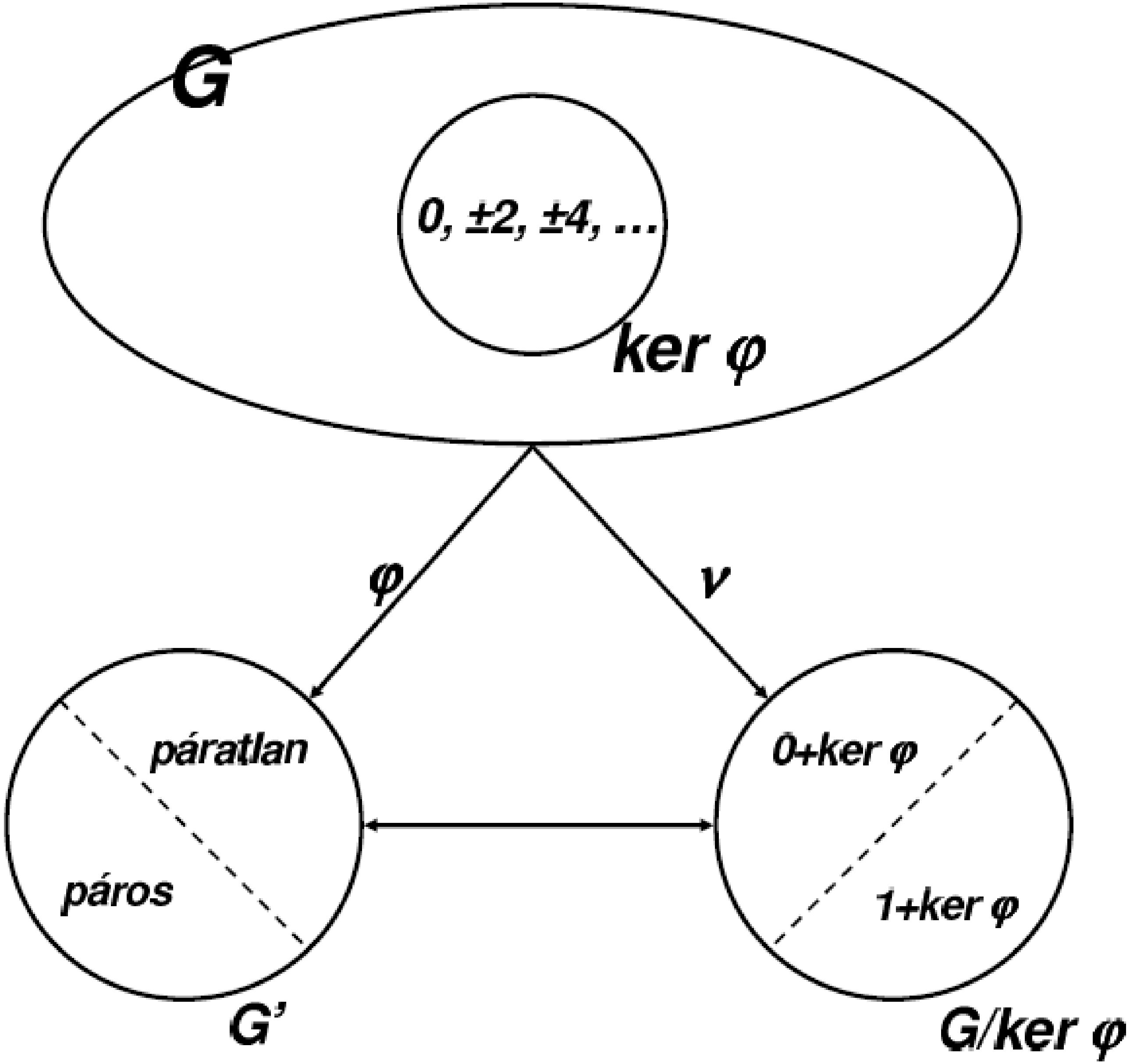
kanonikus leképezés

☺

Def. A G csoport N normálosztója szerinti mellékosztályok a komplexusszorzással ***G N* szerinti faktorcsoportját alkotják (*G*/*N*).**

8.1.38. Homomorfizmus magja. Egy G csoportnak egy G' csoportba való φ homomorfizmusánál a *homomorfizmus magján* a G' csoport e' egységelemének a teljes inverz képét értjük. A φ magját $\ker(\varphi)$-vel jelöljük.

8.1.39. Homomorfizmustétel. *Egy G csoport egy φ homomorfizmusánál a homomorfizmus magja normálosztó, és a $G/\ker(\varphi)$ faktorcsoport izomorf $G' = \varphi(G)$-vel. A G bármely N normálosztója magja valamely homomorfizmusnak: G-nek G/N-re való kanonikus leképezése homomorfizmus, amelynek magja N.*



Jegyzetben 8.3. ábra

Biz.

A $\varphi^{-1}(a')$, $a' \in G'$ halmazrendszer a G egy osztályozása

Kompatibilis a szorzással?

szerinti

Ha $a \in \varphi^{-1}(a')$ és $b \in \varphi^{-1}(b') \Rightarrow$

$$\varphi(ab) = \varphi(a)\varphi(b) = a'b'$$

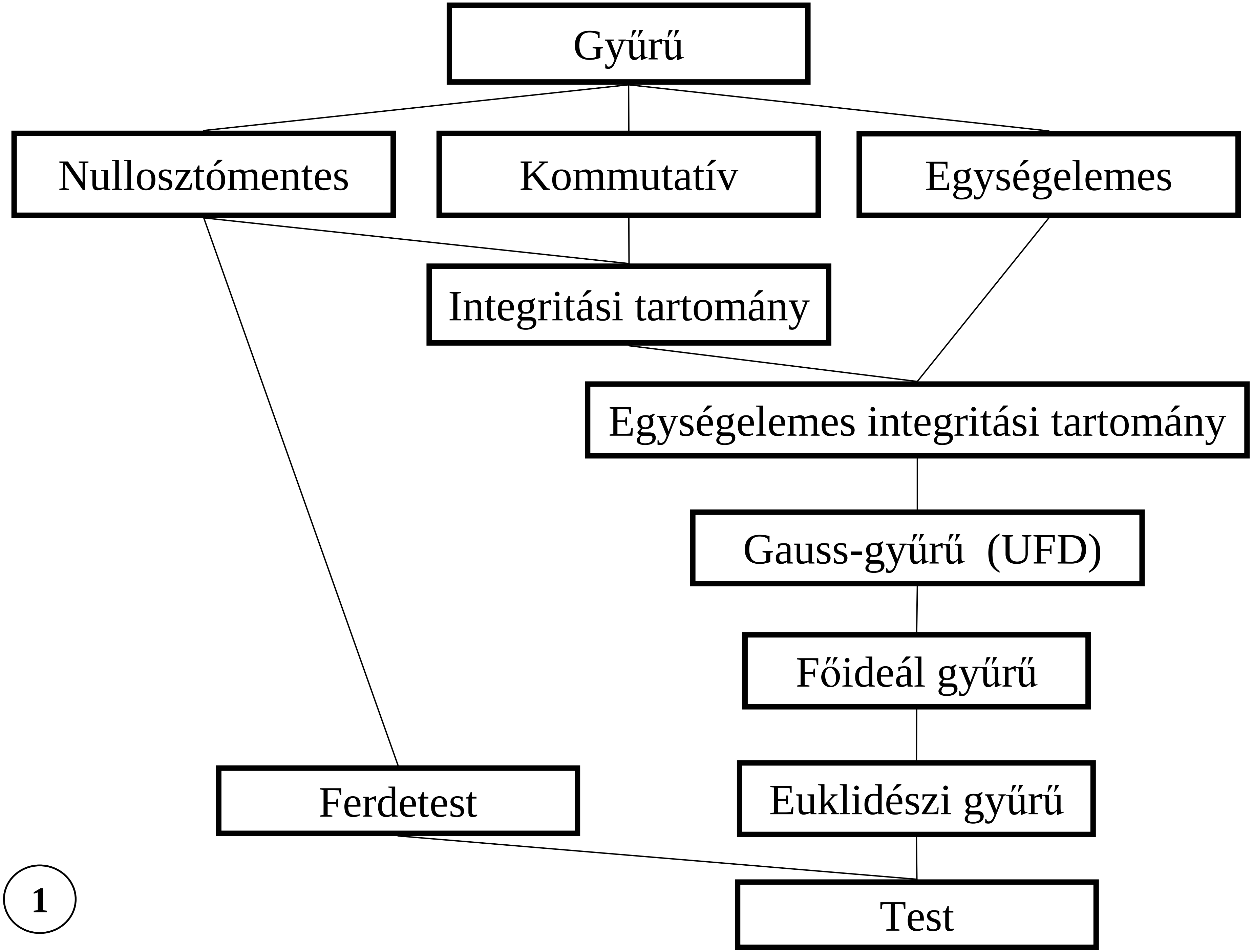
$$\Rightarrow ab \in \varphi^{-1}(a'b')$$

Előző tétel (2) pont $\Rightarrow$ e osztálya, azaz ker(φ), normálosztó $\Rightarrow$

Az $a' \mapsto \varphi^{-1}(a')$ leképezés G' izomorfizmusa $G/\ker(\varphi)$-re.

Tétel második fele 8.1.35. bizonyítása alapján trivi. ☺

Algebra: gyűrűk, testek elmélete


Gyűrű
Nullosztómentes
Kommutatív
Egységelemes
Integritási tartomány
Egységelemes integritási tartomány
Gauss-gyűrű (UFD)
Főideál gyűrű
Ferdetest
Euklidészi gyűrű
Test

1

Def. 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 egységelemét a gyűrű **nullelemének** nevezzük és 0-val jelöljük. **Egységelemes** a gyűrű, ha a szorzásra vonatkozóan van egységelem (amit e-vel 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

1. R kommutatív,
2. $(R^*, \cdot\ )$ csoport.

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

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

3. Véges integritási tartomány test.

4. Testben nincs nullosztó.

Biz. (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

$ab = ac$ / $-(ac)$ 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 char(R) = 0, az utóbbiban **p-karakterisztikájú,** azaz char(R) = p .

Biz. **1. Tfh** $\exists\, \boldsymbol{a} \in \boldsymbol{R}^* :\ |\boldsymbol{a}| = \boldsymbol{n_a} \in \mathbf{N}$

$$\Rightarrow$$

$$n_a a = 0$$

Továbbá tetszőleges $b \in R^*$ -re:

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

másrészt

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

nullosztó mentesség $\Rightarrow$

$$n_a b = 0$$

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

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

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

2. Tfh nem létezik véges rendű elem.

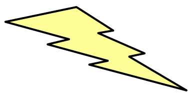
$\Rightarrow$

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:

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

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

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

2. eset: $ka = 0. \Rightarrow |a| \leq \mathrm{k} < n$ 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 $A \,\Delta\, A = \emptyset$, $\Rightarrow$ charR = 2,

d, R kommutatív,

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

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

Def. Tegyük fel, hogy $(R, +, \cdot)$ gyűrű, és $(R_1, \oplus, \otimes)$ két binér műveletes algebrai struktúra. A φ: $R \to R_1$ leképezés **homomorfizmus,** ha

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

és

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

minden $r, s \in R$ esetén fennáll.

8.2.8. Tétel. *Gyűrű homomorf képe gyűrű.*

Biz. Csak a disztributivitást kell látni!

$$a'(b'+c') = a'(b+c)' = \left(a(b+c)\right)' =$$

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

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.

Megjegyzések:

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 részcsoport

$$\Leftrightarrow$$

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

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

$$S - S \subseteq S \text{ és}$$

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

Def. Legyen R gyűrű, $I \subseteq R$, $I \neq \emptyset$. 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.

Észrevételek:

– Bal/jobb/ideálok metszete is bal/jobb/ideál.

– Kommutatív gyűrűben bal/jobb/ideálok fogalma megegyezik.

Triviális ideál: $\{0\}$, R

Valódi ideál: R-től különböző ideál.

Egyszerű gyűrű: csak triviális ideálja van.

Def. Legyen R gyűrű és $A \subseteq R$. Az ***A* által generált ideálon** R összes, A-t tartalmazó ideáljának metszetét értjük. Jelben (A). Ha $A = \{a\}$ valamely $a \in R$ elemre, akkor az ***a* által generált főideálról** beszélünk. Jelben (a). Bal és jobboldali def. hasonlóan.

Példa: legyen R integritási tartomány, és $A = \{ a_1, \ldots, a_n \} \subseteq R$. Ekkor

$$\langle a_1, \ldots, a_n \rangle = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_1, \ldots, r_n \in R \right\}$$

ideál R-ben.

A elemeinek összes véges R feletti lineáris kombinciója

Észrevétel:

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

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

Def. Egy egységelemes integritási tartomány **főideálgyűrű,** ha benne minden ideál főideál.

Def. Legyen R gyűrű és I additív részcsoprtja R-nek, továbbá ~ 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).**

8.2.15. Tétel. *Egy R gyűrű egy I ideál szerinti mellékosztályai a gyűrűnek mindkét művelettel kompatibilis osztályozását alkotják. Minden, mindkét művelettel kompatibilis osztályozás esetén a nulla osztálya ideál, és az osztályozás ezen ideál szerinti mellékosztályokból áll.*

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

8.1.34 Tétel (1) pont $\Rightarrow$

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

8.1.34 Tétel (2) pont $\Rightarrow$ I normálosztó R-ben

továbbá az osztályozás pont az I szerinti mellékosztályokból áll

I ideál?

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

$\Rightarrow RI \subseteq I$. $IR \subseteq I$ hasonlóan.

☺

8.2.16. Következmény. *Egy R gyűrűnek egy I ideál szerinti mellékosztályai a összeadásra és a szorzásra nézve gyűrűt alkotnak.*

Bizonyítás. Ha $\sim$ a megfelelő ekvivalenciareláció, akkor $x \mapsto \tilde{x}$ mindkét műveletre nézve művelettartó. $\square$

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

1. $$(I + r) + (I + s) = I + (r + s)$$

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

Megjegyzés

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

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

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

mert **Z**·**Z** = **Z**

mert **Z**+**Z** = **Z**

∀ elem osztható 16-tal

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

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

8.2.20. Homomorfizmus magja. Egy R gyűrűnek egy R' gyűrűbe való φ homomorfizmusánál a *homomorfizmus magján* az R' gyűrű nullelemének a teljes inverz képét értjük. A φ magját $\ker(\varphi)$-vel jelöljük.

8.2.21. Homomorfizmustétel. *Egy R gyűrű egy φ homomorfizmusánál a homomorfizmus magja ideál. Ha R képe R', akkor az $R/\ker(\varphi)$ maradékosztály-gyűrű izomorf R'-vel. Az R bármely I ideálja magja valamely homomorfizmusnak, például R kanonikus leképezése R/I-re 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 $x \mid r$ $\forall r \in R$-re.

Def. Legyen $\boldsymbol{R}$ egységelemes integritási tartomány, és $\boldsymbol{a, b} \in \boldsymbol{R}$. Azt mondjuk, hogy $\boldsymbol{a}$ és $\boldsymbol{b}$ **asszociáltak**, ha létezik olyan $\boldsymbol{c}$ egység, amelyikkel $\boldsymbol{a = bc}$. Ezt a tényt $\boldsymbol{a \sim b}$-vel jelöljük.

Észrevételek: $\boldsymbol{R}$ egységelemes integritási tartományban

1. az egységek halmaza — jelöljük $\boldsymbol{U(R)}$-rel —, a szorzásra csoportot alkot.

2. Az asszociáltság $\boldsymbol{R}$-ben ekvivalenciareláció.

3. két elem asszociáltságához a kölcsönös oszthatóságuk **szükséges és elégséges** feltétel.

8.2.25. Tétel. *Egy R kommutatív egységelemes gyűrűben az $a \in R$ elem által generált főideálra $(a) = aR$. Speciálisan a nulla által generált főideál $\{0\}$, az egységelem által generált főideál pedig R.*

8.2.26. Állítás. *Egy R egységelemes integritási tartomány a, b elemeire*

(1) *$(a) \subset (b)$ akkor és csak akkor, ha $b|a$;*

(2) *$(a) = (b)$ akkor és csak akkor, ha a és b asszociáltak;*

(3) *$(a) = R$ akkor és csak akkor, ha a egység.* $\square$

Emlékeztető:

Def. Legyen $\boldsymbol{R}$ egységelemes integritási tartomány és $\boldsymbol{a, b \in R}$. Azt mondjuk, hogy $\boldsymbol{d \in R}$ 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 $\boldsymbol{R}$ egységelemes integritási tartomány, ekkor

1. $a \in R^*\backslash U(R)$ **felbonthatatlan**, ha $a = b \cdot c$ $(b, c \in R)$ esetén $b \in U(R)$ vagy $c \in U(R)$.

2. $a \in R^*\backslash U(R)$ **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

$$\boldsymbol{r = p_1 p_2 \ldots p_n}$$

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

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

Van egységelemes integritási tartomány, ami nem Gauss-gyűrű ?

A válasz : IGEN

$R = Z + Z\sqrt{-5}$ 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 hossznégyzetük 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)

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

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 $a \mid c$

így $1 = \underbrace{b/a}_{\in R} \cdot c$ vagy $1 = b \cdot \underbrace{c/a}_{\in R}$

$\Rightarrow b$ vagy c egység.

☺

Ha a felbonthatatlan R –ben $\not\Rightarrow$ a prím R –ben.

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

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

konjugáltakkal szorozva

$$\mathbf{4} = (\boldsymbol{a}^2 + 5\boldsymbol{b}^2)(\boldsymbol{e}^2 + 5\boldsymbol{g}^2)$$

$\Rightarrow \boldsymbol{a}^2 + 5\boldsymbol{b}^2 \mid 4$

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

$\Rightarrow \boldsymbol{b} = 0,\ \boldsymbol{a} = \pm 1, \pm 2$

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

$\Rightarrow$ **2** irreducibilis, de

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

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

Tétel (felbonthatatlan és prím Gauss – gyűrűben)

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

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

Biz. $\Rightarrow$: Előző tétel

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

egyértelmű felbontás $\Rightarrow$

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

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

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

$\Rightarrow a \mid p$ vagy $a \mid q$.

☺

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

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

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

$\delta \neq 0$ 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 $G = \{\ a+bi \mid a, b \in \mathbf{Z}\ \}$

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

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

1. Kérdés: II. tulajdonság teljesül?

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

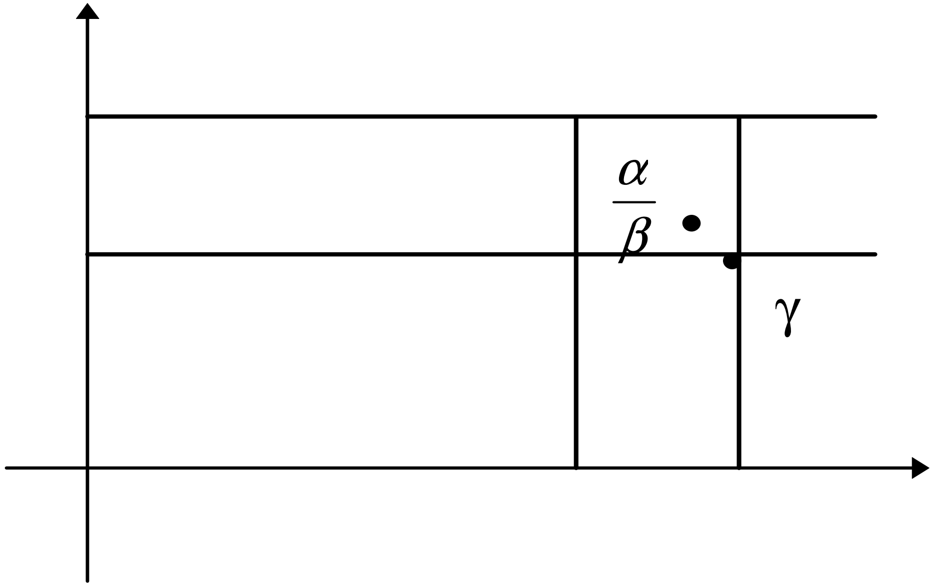
$\forall\ \alpha, \beta \in G^*$ -ra.

2. Kérdés: I. tulajdonság teljesül?

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

$\gamma = \alpha/\beta$ és $\delta = 0$.

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



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

| β |²-tel szorozva:

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

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

Lemma (egységelem és egység int. tartományban)

R integritási tartományban **akkor és csak akkor** létezik egységelem, ha létezik egység. Az R egységelemes integritási tartományban $a \in R$ **akkor és csak akkor** egység, ha $a \mid e$.

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

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

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

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 ☺

8.2.30. Állítás. *Euklideszi gyűrűben pontosan azok az elemek az egységek, amelyekre φ minimális értéket vesz fel. Az a, b nem nulla elemekre $a|b$ esetén $\varphi(a) \leq \varphi(b)$ és egyenlőség pontosan akkor teljesül, ha a és b asszociáltak.*

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 φ (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 $\Rightarrow$

$$\varphi(b) = \varphi\left(a \cdot c\right) \geq \max\left(\varphi(a), \varphi(c)\right),$$

$$\Rightarrow \varphi(b) \geq \varphi\,(a).$$

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

Euklidészi gyűrű II. tulajdonsága miatt φ(a)≤φ(b).

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

$a = b \cdot r + s$, ahol a. $s = 0$, vagy

b. $s \neq 0$ és φ(s)<φ(b)=φ(a). (*)

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

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

$$s = a \cdot \left(e + t \cdot (-r)\right) \Rightarrow \quad \left(e + t \cdot (-r)\right) \in R \Rightarrow a \mid s.$$

Ha s≠0 ⇒

$$\varphi(s) \geq \max\left(\varphi(a), \varphi(e + t(-r))\right) \geq \varphi(a)$$

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

$a \sim b$. ☺

8.2.32. Bővített euklideszi algoritmus. *A következő eljárás egy R euklideszi 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. (Az eljárás során végig $ax_n + by_n = r_n$, $n = 0, 1, \dots$.)*

(1) *[Inicializálás.]* Legyen $x_0 \leftarrow e$, a gyűrű egységeleme, $y_0 \leftarrow 0$, $r_0 \leftarrow a$, $x_1 \leftarrow 0$, $y_1 \leftarrow e$, $r_1 \leftarrow b$, $n \leftarrow 0$.

(2) *[Vége?]* Ha $r_{n+1} = 0$, akkor $x \leftarrow x_n$, $y \leftarrow y_n$, $d \leftarrow r_n$, és az eljárás véget ért.

(3) *[Ciklus.]* Legyen $r_n = q_{n+1}r_{n+1} + r_{n+2}$, ahol $r_{n+2} = 0$ vagy $\varphi(r_{n+2}) < \varphi(r_{n+1})$, legyen $x_{n+2} \leftarrow x_n - q_{n+1}x_{n+1}$, $y_{n+2} \leftarrow y_n - q_{n+1}y_{n+1}$, $n \leftarrow n + 1$, és menjünk (2)-re.

8.2.33. Tétel. *Egy euklideszi gyűrű egy eleme pontosan akkor felbonthatatlan, ha prímelem.*

Biz. Láttuk: ha p prím $\Rightarrow p$ felbonthatatlan

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

$p \nmid a \quad \Rightarrow \quad (p, a) = e$ egység

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

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

☺

8.2.34. Tétel. *Euklideszi 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 $a \in R^*\backslash U(R)$, és legyen

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

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

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

Indirekte tfh f nem felbonthatatlan $\Rightarrow$

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

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

8.2.30. Tétel $\Rightarrow \varphi(b) \neq \varphi(f) \Rightarrow \varphi(b) < \varphi(f)$,

mert ekkor b lenne D-ben f helyett.

tehát van a-nak felbonthatatlan osztója

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

8.2.30. Tétel $\Rightarrow$ a felbonthatatlan .

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

$\exists\, f$ felbonthatatlan : $f \mid a \;\Rightarrow\quad a = fh$.

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

Ekkor $h \mid a \Rightarrow$

$a \sim h$ 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:

$$h = f_1 \cdot f_2 \cdot \ldots \cdot f_r \Rightarrow$$

$$a = f \cdot f_1 \cdot f_2 \cdot \ldots \cdot f_r \, .$$

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

$$a = p_1 \ldots p_k = q_1 \ldots q_r \quad \Rightarrow \qquad p_1 \mid a \Rightarrow p_1 \mid q_1 \ldots q_r$$

$$p_1 \mid q_i \qquad \Rightarrow \text{asszociáltak, mert irreducibilisek}$$

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

☺

8.2.35. Tétel. *Euklideszi gyűrűben minden ideál főideál.*

Biz.

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:

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

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

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

$$b = aq \Rightarrow \qquad \mathrm{I} = \langle a \rangle$$ ☺

Megjegyzés

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

bizonyítható, hogy főideálgyűrű, de nem euklidészi

$\Rightarrow$ az előző tétel megfordítása nem igaz.

8.2.36. Definíció. Egy R gyűrű egy I valódi ideálját *maximális ideál*nak nevezzük, ha nincs nála bővebb valódi ideál, amely tartalmazza, azaz ha a valódi ideálok között a tartalmazásra nézve maximális.

Lemma (irreducibilitás és főideál kapcsolata euklidészi gyűrűben)

Legyen $\boldsymbol{R}$ tetszőleges euklidészi gyűrű és $a \in R^* \setminus U(R)$.

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

$$\Leftrightarrow$$

a felbonthatatlan R –ben.

Biz. $\Rightarrow$

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

Feltétel : a felbotható

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

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

valódi

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

$\Leftarrow$: Indirekt feltétel :

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

$\exists\ \boldsymbol{I}\ \ \boldsymbol{R}$ –beli ideál :

$$\langle \boldsymbol{a} \rangle \subset \boldsymbol{I} \subset \boldsymbol{R}$$

$\boldsymbol{R}$ főideálgyűrű $\Rightarrow$

$\exists\ 0 \neq \boldsymbol{b}$ nemegység :

$$\boldsymbol{I} = \langle \boldsymbol{b} \rangle \subset \boldsymbol{R}$$

$$\langle \boldsymbol{a} \rangle \subset \langle \boldsymbol{b} \rangle \subset \boldsymbol{R}$$

azaz $\boldsymbol{a}$ minden többszöröse $\boldsymbol{b}$ többszöröse

$$\Rightarrow \boldsymbol{a} = \boldsymbol{bc}$$

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

$\Rightarrow \boldsymbol{a}$ 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.** $\mathbf{2Z}$ prímideál $\mathbf{Z}$-ben :

$ab \in \mathbf{2Z} \Rightarrow ab$ páros a vagy b páros $\Rightarrow$

$a \in \mathbf{2Z}$ vagy $b \in \mathbf{2Z}$.

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

Tfh $\mathbf{2Z} \subseteq \boldsymbol{I} \subseteq \mathbf{Z}$ **.**

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

különben $I = \mathbf{2Z}$.

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

$\mathbf{49Z \subset 7Z \subset Z}$ **,** $\mathbf{7 \cdot 7 = 49 \in 49Z}$ **, de** $\mathbf{7 \notin 49Z}$ **.**

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

I. R/I **akkor és csak akkor** integritási tartomány, ha $I \neq R$ és I prímideál.

II. R/I **akkor és csak akkor** test, ha I maximális ideál.

Biz. I.

R/I int. tart.

$\Leftrightarrow$

nincs nullosztó.

$\Leftrightarrow$

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

II/1. Tfh hogy *I* maximális ideál *R*-ben, és (*I* ≠) *I*+*a* ∈ *R*/*I* .

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

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

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

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 invertálható ⇒ test.

II/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* $a \in M \Rightarrow$

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

$$b \in M \Rightarrow$$

$$M = R.$$

☺

Következmény.

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

Biz.

Legyen R kommutatív, egységelemes gyűrű.

Ha I maximális ideál R-ben $\Rightarrow$

R/I test $\Rightarrow$

R/I integritási tartomány $\Rightarrow$

tétel $\Rightarrow$ I prímideál

☺

Lemma. 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 $I \neq \{0\} \Rightarrow$

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

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. (Hányadostest) Legalább 2 elemű R integritási tartomány T testbe ágyazható. Legyen $T = \{ (a, b) \mid a, b \in R,\ b \neq 0 \}$ és

~ ekvivalenciareláció $R \times R^*$ halmazon: $(a, b) \sim (c, d) \iff a \cdot d = b \cdot c$

A ~ által meghatározott osztályok testet alkotnak a köv. műveletekre:

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

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

Algebra: polinomok

Def. Legyen R gyűrű. R **feletti egyváltozós (egy határozatlanú) polinomoknak** nevezzük az

$$(a_0, a_1, \ldots, a_n, \ldots)$$

végtelen sorozatokat, amelyekben $a_i \in R$ ($i = 0, 1, \ldots$), és csak véges sok a_i különbözik 0-tól. Az a_i elemek a polinom **együtthatói.**

Az R feletti egyváltozós polinomok halmazát ***R*[x]**-szel jelöljük.

Def. Ha n a legnagyobb olyan index, amire $a_n \neq 0$ de bármely $i > n$ -re $a_i = 0$: a_n **főegyüttható**.

A továbbiakban legyen:
$\boldsymbol{f = (a_0, a_1, \ldots, a_n, \ldots)}$ **és** $\boldsymbol{g = (b_0, b_1, \ldots, b_m, \ldots)}$ ***R*** **feletti polinom.**

$$f = g \quad \Leftrightarrow \; \forall\, i: \; a_i = b_i$$

Műveletek $R[x]$-en:

1. $u = f + g = (c_0, \ldots, c_q, \ldots)$, $\quad c_i = a_i + b_i \quad (i \in \mathbf{N}_0)$

2. $v = f \cdot g = (d_0, \ldots, d_s, \ldots)$, ahol

$$d_k = \sum_{i=0}^{k} a_i \cdot b_{k-i} = a_0 \cdot b_k + a_1 \cdot b_{k-1} + \ldots + a_k \cdot b_0$$

3. $a \in R$ esetén $\quad a \cdot f = (a \cdot a_0, \ldots, a \cdot a_n)$.

Tétel. Ha R **(**egységelemes/ kommutatív/ nullosztómentes**)** gyűrű, akkor R**[**x**]** is **(**egységelemes/ kommutatív/ nullosztómentes**)** gyűrű.

Észrevételek:

1. Egységelem az $(e, 0, \ldots, 0, \ldots)$ polinom, ahol e az R egységeleme.

2. Az $a \to f_a = (a, 0, \ldots, 0, \ldots)$ megfeleltetés injektív és művelettartó.

Ekkor $\forall$ f R feletti polinomra

$$a \cdot f = f_a \cdot f$$

$\Rightarrow$ R elemei R feletti polinomoknak tekinthetők (**konstans polinomok**)

A *változó* fogalma :

Legyen $\mathbf{x = (0, e, 0, \ldots, 0, \ldots)}$

Lehet, hogy e $\not\subseteq$ R !!!

2. művelet definíciója $\Rightarrow$

$$x^2 = x \cdot x = (0 \cdot 0 = 0, e \cdot 0 + 0 \cdot e = 0, 0 \cdot 0 + e \cdot e + 0 \cdot 0 = e, \\ 0 \cdot 0 + e \cdot 0 + 0 \cdot e + 0 \cdot 0 = 0, \ldots).$$

$$\Rightarrow \quad x^n = (0, \ldots, e, 0, \ldots), \quad n \in \mathbf{N}.$$

n edik pozíció

Legyen továbbá $x^0 = (e, 0, \ldots, 0, \ldots)$, ekkor

$$f = (a_0, a_1, \ldots, a_n, \ldots) =$$

$$= (a_0, 0, \ldots, 0, \ldots) + \ldots + (0, 0, \ldots, a_n, \ldots) =$$

$$= a_0 + a_1 x + \ldots + a_n x^n + \ldots ,$$

ahol az $a_i \in R$ az $= (a_i, 0, \ldots, 0, \ldots)$ polinomnak felel meg.

Def. Legyen $f = a_0 + a_1x + \ldots + a_nx^n \in R[x]$, ekkor

a_i az ***i*-edfokú tag együtthatója**.

A 0-adfokú tag együtthatója a polinom **konstanstagja**.

Ha $a_n \neq 0$, akkor a_n a polinom **főegyütthatója,** és n a polinom **foka (jel: deg(*f*))**.

Nullpolinom : $(0, 0, \ldots) \in R[x]$.

Nullpolinom foka –1 (–∞)

Monom : $f(x) = a_ix^i$ alakú polinom

Lineáris polinom: legfeljebb elsőfokú polinom

Főpolinom (normált polinom): a főegyütthatója R egységeleme

Ha R nullosztómentes és $f, g \in R[x]^* \Rightarrow$

$$\deg(f + g) \leq \max(\deg(f), \deg(g)).$$

Ha $h = fg$, akkor h főegyütthatója $h_k = a_n b_m$, ahol $k = n+m$

tehát $\deg(f \cdot g) = \deg(f) + \deg(g) \geq \max(\deg(f), \deg(g))$.

Tétel (polinomok maradékos osztása)

Legyen R egységelemes integritási tartomány, $f, g \in R[x]$ és $\boldsymbol{g}$ **főegyütthatója,** $\boldsymbol{b_k}$ **legyen** $\boldsymbol{R}$**-ben egység.**

Ekkor **egyértelműen léteznek** olyan $q, r \in R[x]$ polinomok, melyekkel

$$f(x) = g(x) \cdot q(x) + r(x), \text{ ahol}$$

$$\deg(r) < \deg(g).$$

Biz. 1. Egzisztencia.

1.1. Ha $f = 0$, vagy $n < k \Rightarrow$

$$q(x) \equiv 0, \quad r(x) = f(x)\ .$$

1.2. Legyen most $n \geq k$. n szerinti teljes indukció:

1.2.1. Ha $n = k = 0 \Rightarrow$ akkor

$$r = 0, q = a_n \cdot b_k^{-1},$$

mivel b_k egység R-ben.

1.2.2. Legyen $n > 0$ és tfh az n-nél kisebb fokszámok esetén igaz az állítás.

$$f_1(x) = f(x) - g(x) \cdot a_n \cdot b_k^{-1} \cdot x^{n-k}. \qquad (*)$$

1.2.2.1. Ha $f_1 = 0 \Rightarrow$

$$q(x) = a_n \cdot b_k^{-1} \cdot x^{n-k}, \qquad r(x) = 0.$$

1.2.2.2. Ha deg (f_1) < deg (f), ind. feltétel $\Rightarrow$

$\exists\, q_1(x),\ r_1(x) \in R[x]$:

$$f_1(x) = g(x) \cdot q_1(x) + r_1(x),$$

ahol

$$\deg(r_1) < \deg(g).$$

(*) $\Rightarrow$

$$f(x) = g(x) \cdot a_n \cdot b_k^{-1} \cdot x^{n-k} + g(x) \cdot q_1(x) + r_1(x),$$

$$f(x) = g(x) \cdot (\underbrace{a_n \cdot b_k^{-1} \cdot x^{n-k} + q_1(x)}_{q(x)}) + \underbrace{r_1(x)}_{r(x)} .$$

2. Unicitás.

Tfh $f = g{\cdot}q_1 + r_1 = g{\cdot}q_2 + r_2 \Rightarrow$

$$g{\cdot}(q_1 - q_2) = r_2 - r_1.$$

Tegyük fel indirekte, hogy $q_1 - q_2 \neq 0 \Rightarrow$

$$\deg(r_2 - r_1) = \deg(\,g{\cdot}(q_1 - q_2)\,) \geq \deg(\,g\,)$$

Kaptuk, hogy $q_1 - q_2 = 0 \Rightarrow$

$$r_2 - r_1 = 0$$

Következmény:

Legyen R test, és $f \in R[x]^*$ esetén $\varphi : R[x]^* \to \mathbf{N}_0$, $\varphi(f) = \deg(\,f\,)$.

Ekkor $R[x]$ φ-vel euklidészi gyűrűt alkot.

Def. Legyen S egységelemes integritási tartomány, R részgyűrűje S-nek, és R tartalmazza S egységelemét (e). Egy $f \in R[x]$ polinom $c \in S$ -beli **helyettesítési értéke**

$$f(c) = a_0 + a_1 c + \ldots + a_n c^n.$$

c az f **gyöke**, ha a helyettesítési érték 0.

Polinomfüggvény :

$f : R \to R$, ahol $f(c) = a_0 + a_1 \cdot c + \ldots + a_n \cdot c^n \in R$, és $c \in R$.

f és g polinomfüggvény egyenlő, ha minden $c \in R$ esetén $f(c) = g(c)$

Két különböző polinom polinomfüggvénye megegyezhet! Legyen például $R = \boldsymbol{Z}_3$:

$$f = x^4 + x + 2 \neq g = x^3 + x^2 + 2 \text{ ,}$$

$$f(0) = 2 = g(0) \text{ ,} \quad f(1) = 1 = g(1) \text{ ,} \quad f(2) = 2 = g(2) \text{ .}$$

Tétel (gyöktényező leválasztása)

Legyen R egységelemes integritási tartomány, $f \in R[x]^*$, és $c \in R$ az ***f* gyöke**. Ekkor $\exists\, q \in R[x]^*$:

$$f(x) = (x - c) \cdot q(x).$$

Biz.

$x - c$ polinom főegyütthatója egység $\Rightarrow$

maradékos osztás : $$f(x) = (x - c) \cdot q(x) + r(x),$$

a. $r = 0 \Rightarrow$ kész.

b. $\deg(r) < \deg(x - c) = 1 \Rightarrow$

$$f(c) = (c - c) \cdot q(x) + r(c) = r(c) = 0. \quad ☺$$

Tétel. Legyen $f \in R[x]^*$, ahol R egységelemes integritási tartomány, és $\deg(f) = n \geq 0$. Ekkor f-nek legfeljebb n különböző gyöke van R-ben.

Biz. (*n* szerinti teljes indukció)

12

$n = 0$ esetén $f \in$ R : kész

Tegyük fel, hogy $n > 1$, és az n-nél kisebb fokúakra igaz az állítás.
Legyen $c \in R$ gyöke f-nek :

$f(x)=(x-c)\cdot g(x)$, ahol $\deg(g) = \deg(f) - 1 = n - 1$

Ha d is gyöke f-nek, akkor $f(d) = 0 = (d - c)\cdot g(d) = 0$,

R nullosztómentessége $\Rightarrow$ $d = c$ vagy $g(d) = 0$.

Ind. feltétel $\Rightarrow$ g különböző gyökeinek száma $\leq n - 1$.

$\Rightarrow$ ha c nem gyöke g-nek, akkor is f -nek max. n különböző gyöke van

☺

8.3.7. Következmény. *Ha két, legfeljebb n-ed fokú polinom (a nulla polinomot is ideértve) $n+1$ különböző helyen ugyanazt az értéket veszi fel, akkor megegyezik.*

Biz.

Tfh f és g ilyen polinom, de különbözőek $\Rightarrow$

$f - g$ polinom foka $\leq n$ és legalább $n + 1$ gyöke van

☺

8.3.8. Következmény. *Ha R végtelen, akkor két különböző polinomhoz nem tartozik ugyanaz a polinomfüggvény.*

Biz.

Ha így lenne $f - g$ polinomnak végtelen sok gyöke lenne

☺

Horner-elrendezés

$$f(\mathrm{c}) = ?$$

n szorzással és n összeadással megkapjuk !

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

$$f(c) = a_0 + a_1 c + \ldots + a_n c^n = a_n c^n + \ldots + a_1 c + a_0 =$$

$$= (a_n c^{n-1} + \ldots + a_1)c + a_0 = ((a_n c^{n-2} + \ldots + a_2)c + a_1)c + a_0 =$$

$$= ((\ldots(a_n c + a_{n-1})c + a_{n-2})c + \ldots + a_1)c + a_0 \,.$$

Példa.

$$f(x) = 5x^3 - 7x^2 + x - 8 = ((5x - 7)x + 1)\, x - 8 \,.$$

c	5	-7	1	-8	$f(c)$
3		5	8	25	67

Gyökök száma ?

Függ ***R*** –től !

Keressük az $f(x) = x^2 + 1$ polinom gyökeit

1. $\mathbf{Z}[x]$, $\mathbf{Q}[x]$, $\mathbf{R}[x]$ –ben nincs gyöke

2. $\mathbf{C}[x]$ –ben a gyökök száma kettő: i és $-i$

3. $\mathbf{Z_2}[x]$ –ben egy gyöke van: 1

4. $\mathbf{Z_3}[x]$ –ben nincs gyöke .

5. $\mathbf{Z_5}[x]$ –ben két gyöke van: 2 és 3 .

Def. Legyen R egységelemes integritási tartomány, és

$$f \to f' = a_1 + 2a_2x + \ldots + n\,a_nx^{n-1}$$

$R[x]$-nek önmagába való leképezése a következő feltételekkel:

1. $c' = 0$, ha c konstans polinom,

2. $(f + g)' = f' + g'$,

3. $(f \cdot g)' = f'g + f g'$,

4. $(e \cdot x)' = e$.

Az f' polinom a f **(algebrai) deriváltpolinomja** .

Def. Legyen R egységelemes integritási tartomány, és $f \in R[x]^*$. Azt mondjuk, hogy $c \in R$ az $f(x)$ ***n*-szeres gyöke** ($n \in \mathbf{N}$), ha

$$(x - c)^n \mid f(x) \text{ és } (x - c)^{n+1} \nmid f(x)$$

Jel:

$$(x - c)^n \parallel f(x)$$

Tétel.

Legyen R egységelemes integritási tartomány, $f \in R[x]$, $c \in R$, $n \in \mathbf{N}^+$

Ha c az $f(x)$-nek n-szeres gyöke, akkor c az $f'(x)$-nek legalább (n–1) -szeres gyöke, és pontosan (n–1)-szeres gyök abban az esetben, ha $\mathrm{char}(R) \nmid n$.

Biz.

$$=(x-c)^{n-1}\cdot\big((x-c)\cdot g'(x)+ng(x)\big)=(x-c)^{n-1}\cdot h(x).$$

Tehát c legalább $(n–1)$-szeres gyöke $f\,'(x)$-nek és

$$h(c)=(c-c)\cdot g'(x)+ng(c)=ng(c)=\underbrace{g(c)+\ldots+g(c)}_{n\text{ db}}.$$

$$(x-c)^n \mid f(x) \Rightarrow g(c)\neq 0\,.$$

Ha $\mathrm{char}(R) \nmid n \Rightarrow$ az összeg sosem 0. ☺

Megjegyzés.

Fordítva nem igaz pl :

$f(x) = x^n + 1$, $f'(x) = nx^{n-1} \Rightarrow$

$f'(x)$ –nek a 0 $(n-1)$ –szeres gyöke, $f(x)$ –nek nem .

Irreducibilis polinomok

Észrevételek:

test fölötti polinomok euklidészi gyűrűt alkotnak

$$\Rightarrow$$

felbonthatatlanok és a prímek egybeesnek.

$\forall$ nemnulla konstans polinom egység.

$\forall$ elsőfokú polinomok felbonthatatlan.

Komplex eset.

Algebra alaptétele $\Rightarrow$

$f \in \mathbf{C}[x]$:

$$f(x) = a_n (x - c_1)^{\alpha_1} \cdot (x - c_2)^{\alpha_2} \cdot \ldots \cdot (x - c_k)^{\alpha_k}$$

ahol $c_j \in$ **C,** $c_i \neq c_j$, ha $i \neq j$ és

$$\alpha_1 + \alpha_2 + \ldots + \alpha_k = n = \deg f.$$

$\Rightarrow$

C fölött az irreducibilis polinomok pontosan az elsőfokúak.

Valós eset.

Észrevétel.

Ha $f \in \mathbf{R}[x]$, $c \in \mathbf{C}$ és $f(c) = 0$. Akkor

$$f\left(\overline{c}\right) = 0$$ is teljesül.

Következmény.

Legyen $c \in \mathbf{C} \setminus \mathbf{R}$ gyöke $f \in \mathbf{R}[x]$-nek $\Rightarrow$

$$x - c \,\big|\, f(x) \qquad \text{és} \qquad x - \overline{c} \,\big|\, f(x),$$

felbonthatatlanok és nem asszociáltak $\Rightarrow$

$$g(x) = (x - c)\cdot(x - \overline{c}) \,\big|\, f(x)\,.$$

$$g(x) = x^2 - 2Re(c)x + |c|^2 \in \mathbf{R}[x] \,.$$

$$\Rightarrow \quad \exists\, h(x) \in \mathbf{R}[x] :$$

$$f(x) = g(x)\, h(x),$$

ahol $deg(h) = deg(f) - 2$.

$$\Rightarrow$$

$\forall\, f \in \mathbf{R}[x]$ legfeljebb másodfokú polinomok szorzatára bontható **R** felett.

$$\Rightarrow$$

Azok a másodfokú polinomok felbonthatatlanok, amelyeknek nincs valós gyökük.

Racionális eset

Def. Legyen R Gauss-gyűrű. R[x] egy elemét **primitív polinomnak** nevezzük, ha együtthatóinak legnagy közös osztója az egységelem.

8.3.28. Schönemann–Eisenstein-tétel. *Ha az R Gauss-gyűrű feletti legalább elsőfokú f primitív polinomhoz van olyan $p \in R$ prímelem, amely nem osztója a főegyüttható-nak, de osztója minden más együtthatónak, p^2 viszont nem osztója a konstans tagnak, akkor f irreducibilis. Hasonlóan, ha az R Gauss-gyűrű feletti legalább elsőfokú f polinomhoz van olyan $p \in R$ prímelem, amely nem osztója a konstans tagnak, de osztója minden más együtthatónak, p^2 viszont nem osztója a főgyütthatónak, akkor f irreducibilis.*

Legyen tehát $f = x^n + p$, ahol p prím, n pozitív egész. Ekkor

f R és hányadosteste felett is irreducibilis.

Def. Valamely K test esetén a $K[x]$ integritási tartomány hányadostestét **racionális függvénytestnek** nevezzük és $K(x)$-szel jelöljük.

Gauss-tétel.

Legyen R tetszőleges Gauss – gyűrű és K a hányadosteste.

1. Ha egy $f \in R[\mathrm{x}]$ polinom előállítható két nem konstans g, h polinom szorzataként $K[x]$-ben, akkor $R[x]$-ben is előállítható két g^*, h^* polinom szorzataként, úgy hogy

g és g^*, illetve h és h^* asszociáltak $K[x]$-ben.

2. $R[x]$ is Gauss-gyűrű.

Észrevételek

$$f(x) = 6x^2 + 12x + 12 = 2\cdot 3\cdot (x^2 + 2x + 2)$$

Q[x]-ben irreducibilis

Z[x]-ben nem irreducibilis

$$f(x) = \frac{1}{3}x^2 + \frac{1}{2}x + 3$$

$$g(x) = 6\cdot f = 2x^2 + 3x + 18$$

Q[x]-beliek és $f \sim g$, $f \notin$ **Z**[x]

Z euklidészi gyűrű $\Rightarrow$

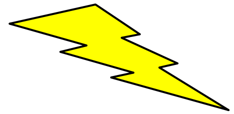
Z Gauss - gyűrű $\Rightarrow$

Z[x] Gauss - gyűrű

Z[x] **nem alkot euklidészi gyűrűt**, különben

$$(x, 2) = 1 \Rightarrow$$

$$1 = u2 + vx$$



Z[x] **nem alkot főideálgyűrűt**:

$$J = \left\{ f(x) \middle| f(x) \in Z[x] \text{ és } f(0) \equiv 0 \bmod(2) \right\} =$$

$$= \left\langle 2, x \right\rangle \subset Z[x]$$

Testbővítések, véges testek

Def. Legyen F tetszőleges test. ***K* az *F* részteste**, ha $K \subseteq F$ és K maga is testet alkot az F műveleteivel.

Jelölés F : K

Ekkor ***F* a *K* test bővítése**. Ha $K \neq F$, akkor ***K* valódi részteste *F*** -nek, illetve ***F* valódi bővítése *K*** -nak .

Észrevétel

Legyen F test és K részteste F –nek, ekkor F és K karakterisztikája megegyezik. Véges test karakterisztikája prímszám.

Def. Egy test **prímtest**, ha nincs valódi részteste.

Észrevétel

Résztestek metszete résztest $\Rightarrow$

F test összes résztestének metszete résztest F –ben

$\Rightarrow$ a legszűkebb résztest F –ben

$\Rightarrow$ nincs valódi résztete

$\Rightarrow$ prímtest

Def. Ha K az F –nek a legszűkebb részteste, akkor K az F **prím részteste (prímteste). (jelölés *K* = *Fp*)**

Észrevételek.

– Test prím részteste prímtest.

– Ha F a K test bővítése, akkor prím résztesteik megegyeznek.

Tétel (prím résztestek)

Tetszőleges F test prím résztestesté izomorf

$\mathbf{Z}\boldsymbol{p}$ –vel, ha char(F) = p,

$\mathbf{Q}$ –val, ha char(F) = 0 .

Biz.

p prímszám $\Rightarrow$ $\mathbf{Z}\boldsymbol{p}$ prímtest, továbbá $0, e \in Fp$.

char(*F*) = *p* : **(*Fp*, +)** elemei : e^n alakúak, azaz

$$
\begin{array}{ccccccc}
Fp & = & \{\ 0 = e^0, & e^1, & \ldots, & e^{p-1} & \} \\
 & & \updownarrow & \updownarrow & & \updownarrow & \\
\mathbf{Z}\boldsymbol{p} & = & \{\ 0 = 1^0, & 1^1, & \ldots, & 1^{p-1} & \}
\end{array}
$$

izomorfizmus

Ha char(*F*) = 0, legyen

$$R = \left\{ \frac{ke}{le} \,\middle|\, k, l(\neq 0) \in \mathrm{Z} \right\}$$

ahol $ke = e + e + \ldots + e$.

Tudjuk:

$$\mathrm{Q} = \left\{ \frac{k}{l} \,\middle|\, k, l(\neq 0) \in \mathrm{Z} \right\}$$

$\frac{k}{l} \mapsto \frac{ke}{le}$ Izomorfizmus **Q** és R között.

Tehát R is test $\Rightarrow R$ résztest F -ben.

Továbbá : $e \in Fp \Rightarrow R$ elemei Fp -ben vannak $\Rightarrow R \subseteq Fp$.

Fp a legszűkebb résztest F -ben $\Rightarrow Fp = R$

$\Rightarrow Fp$ is izomorf $\boldsymbol{Q}$ -val ☺

Észrevételek

Az előző tétel $\Rightarrow$ minden p karakterisztikájú test **Z*p*** bővítése, és

minden nullkarakterisztikájú test **Q** bővítése.

Ha K részteste F -nek, akkor F K feletti vektortér, azaz teljesül:

(1) $a\cdot(v+w) = a\cdot v+a\cdot w$, $a \in K$ *és* $v,w \in F$,

(2) $(a+b)\cdot v = a\cdot v+b\cdot v$, $a,b \in K$ *és* $v \in F$,

(3) $(ab)\cdot v = a\cdot(b\cdot v)$, $a,b \in K$ *és* $v \in F$,

(4) $1\cdot v = v$, minden $v \in F$,

ahol $\cdot$: $K \times F \rightarrow F$ egy külső művelet művelet , és

(a, v) $\cdot$ melletti képe $a\cdot v$.

Def. Legyen egy K részteste, M egy részhalmaza F -nek .

***K*(*M*) a *K* test *M* halmazzal való bővítése,**

ha F –nek a legszűkebb részteste, mely tartalmazza K –t és M –et is.

Ha $M = \{ \alpha \}$ alakú, valamely $\alpha \in F$ –re , akkor

$K(\alpha)$ **egyszerű bővítés az $\boldsymbol{\alpha}$ bővítő elemmel.**

Legyen egy K részteste F –nek, és $\alpha \in F$,

ha α gyöke egy nem nulla K feletti polinomnak, akkor $\boldsymbol{\alpha}$ **algebrai elem *K* felett .**

F **algebrai bővítése** K –nak, ha F minden eleme algebrai K felett.

Tétel (minimálpolinom egyértelmű létezése)

Tetszőleges $F[x]$ test feletti polinomgyűrűben minden $J \neq \langle 0 \rangle$ ideálhoz egyértelműen létezik olyan $g \in F[x]$ főpolinom, amire

$$J = \langle g \rangle .$$

Biz. 1. Egzisztencia

Legyen h minimális fokszámú polinom J –ben,

h főegyütthatója b, ekkor belátható, hogy a

$$g = b^{-1}h$$

főpolinom jó választás lesz.

Maradékos osztás tetszőleges $f \in J$ –re :

$$f = gq + r \text{ és } deg(r) < deg(g) = deg(h)$$

J ideál $\Rightarrow$ $r = f - gq \in J$

$deg(h)$ minimális $\Rightarrow r = 0$.

Kaptuk: tetszőleges $f \in J$ g –nek többszöröse $\Rightarrow$ $J = \langle g \rangle$.

2. Unicitás

Tfh $\exists$ $g' \in F[x]$: $J = \langle g' \rangle$

$\Rightarrow \exists$ $c, c' \in F[x]$: $g = c'g'$ és $g' = cg$

$\Rightarrow$ $g = c'cg$ $\Rightarrow$ $c'c$ az egységelem

c, c' konstans és g, g' főpolinom $\Rightarrow$

$g = g'$ ☺

Def. Legyen F tetszőleges test és K egy részteste F –nek. Ha $\alpha \in F$ algebrai elem K felett, akkor

az az egyértelműen meghatározott $g \in K[x]$ főpolinom, amelyre

$$J = \{ f(x) \in K[x] \mid f(\alpha) = 0 \} = \langle g \rangle ,$$

azaz, g generálja a J $K[x]$ –beli ideált,

az ***α K* feletti minimálpolinomja.**

***α K* feletti fokszámán** $deg(g)$ –t értjük.

Tétel (minimálpolinom tulajdonságai)

Legyen F tetszőleges test és K egy résszteste F –nek, továbbá $\alpha \in F$ K felett algebrai elem.

Ha α K feletti minimálpolinomja g , akkor

(1) g irreducibilis $K[x]$-ben.

(2) $\forall f \in K[x]$ –re $f(\alpha) = 0$

$$\Leftrightarrow$$

g osztója f –nek.

(3) g a legalacsonyabb fokszámú főpolinom $K[x]$-ben, amelynek α gyöke.

Biz. (1) indirekte tfh *g* nem irreducibilis.

$\Rightarrow \exists\ h_1, h_2 \in K[x]$:

$deg(g) > 0$, hiszen van gyöke $\Rightarrow$

$g = h_1 h_2$ és $1 \leq deg(h_i) < deg(g) \quad i = 1, 2$

$0 = g(\alpha) = h_1(\alpha) h_2(\alpha)$

$\Rightarrow$ h_1 vagy h_2 J –beli és

$g \mid h_1$ vagy $g \mid h_2$

(2) a definícióból következik.

(3) Legyen $f \in K[x]$ –re $f(\alpha) = 0$

$\Rightarrow f \in J$, azaz f a g többszöröse.

g főpolinom $\Rightarrow$

$f = g$ vagy $deg(f) > deg(g)$.

☺

***Def*.** $F : K$ esetén, ha F mint K feletti vektortér nem véges dimenziós akkor a **bővítés végtelen,** egyébként **véges bővítésről** beszélünk.

***Def*.** Az $F : K$ **testbővítés foka** az F K feletti vektortér dimenziója, jelben **$[F : K]$** **.**

Tétel (testbővítések fokszámtétele)

Ha $M : L$ és $L :$ K véges testbővítés, akkor $M : K$ véges bővítés és

$$[M : K] = [M : L][L : K] .$$

Tétel (véges bővítés algebrai)

Tetszőleges K test véges bővítése algebrai K felett.

Tétel (egyszerű bővítés izomorfiája faktorgyűrűvel)

$F : K$ esetén legyen $\alpha \in F$ K felett n –edfokú algebrai elem g K feletti minimálpolinommal. Ekkor

$$K(\alpha) \text{ izomorf } K[x] / \langle g \rangle \text{ –vel} .$$

Tétel (egyszerű bővítés bázisa)

$F : K$ esetén legyen $\alpha \in F$ K felett n –edfokú algebrai elem g K feletti minimálpolinommal. Ekkor

$$[K(\alpha) : K] = n \quad \text{és}$$

hatványbázis

$$K(\alpha) \;\; K \text{ feletti bázisa } \langle 1, \alpha, \ldots, \alpha^{n\text{-}1} \rangle .$$

Következmény

Ha $K(\alpha)$ tetszőleges egyszerű testbővítése K -nak , akkor $\forall\, c \in K(\alpha)$

$$c = b_0 + b_1\alpha + \ldots + b_{n\text{-}1}\alpha^{n\text{-}1}$$

alakban írható fel, valamely $b_i \in K$ együtthatókkal, azaz

c előáll egy legfeljebb $n - 1$ -edfokú K feletti polinom α helyen vett helyettesítési értékeként.

Tétel (egyszerű bővítés létezése)

Legyen $f \in K[x]$ irreducibilis polinom K test felett. Ekkor létezik K –nak olyan egyszerű algebrai bővítése, ahol a bővítő elem f –nek gyöke.

Biz.

$L = K[x] / \langle f \rangle$ test

L elemei $[h] = h + \langle f \rangle$ maradékosztályok

$a \in K \Rightarrow a \to [a]$ izomorfizmus $\Rightarrow$

beágyazzuk K –t L –be $\Rightarrow L : K$

Maradékosztályok műveleti szabályai szerint:

$$h(x) = a_0 + a_1x + \ldots + a_mx^m \in \ \boldsymbol{K[x]} \ \Rightarrow$$

$$[h] = [a_0 + a_1x + \ldots + a_mx^m] =$$

$$[a_0] + [a_1][x] + \ldots + [a_m][x]^m =$$

$$a_0 + a_1[x] + \ldots + a_m[x]^m \ \Rightarrow$$

L minden eleme ***K*** feletti **[*x*]** határozatlanú polinom kifejezés $\Rightarrow$

L egyszerű algebrai bővítése ***K*** –nak az **[*x*]** bővítőelemmel.

Egy kérdés maradt:

[*x*] gyöke *f* –nek ?

Ha $f(x) = a_0 + a_1 x + \ldots + a_n x^n \quad \Rightarrow$

$$f([x]) \;=\; [a_0] + [a_1][x] + \ldots + [a_\mathrm{n}][x]^n \;=$$

$$[a_0 + a_1 x + \ldots + a_n x^n\,] \;=\; [\,f\,] = [\,0\,] \;\Rightarrow$$

[*x*] gyöke *f* –nek !

☺

Példa

$$\boldsymbol{f(x) = x^2 + x + 2 \in \mathbf{Z_3}}$$

$$f(0) = -1 \quad \& \quad f(1) = 1 \quad \& \quad f(-1) = -1$$

$f(x)$ irreducibilis Z_3 felett.

Legyen $u^2 + u + 2 = 0$ azaz

u gyöke f –nek $\Rightarrow$

u egy maradékosztály $Z_3/\langle f \rangle$ -ben

legyen a tétel szerint $u = [x] = x + \langle f \rangle$.

Mivel $Z_3/\langle f \rangle = Z_3(u)$

tétel $\Rightarrow$ $Z_3/\langle f \rangle$ bázisa : $\{ 1, u \}$

$Z_3/\langle f\rangle$ elemei : $0, 1, 2, u, u+1, u+2, 2u, 2u+1, 2u+2$

Észrevétel:

f –nek $2u+2$ is gyöke !

$$f(2u+2) = (2u+2)^2 + (2u+2) + 2 =$$

$$4u^2 + 8u + 4 + 2u + 2 + 2 =$$

$$\underbrace{4(u^2 + u + 2)}_{0} + 4u - 4 + 2u + 2 + 2 =$$

$$6u = 0$$

Ha $2u+2$ -vel végezzük a bővítést, algebrai szempontból ugyanazt a testet kapjuk!

Tétel (egyszerű bővítések izomorfiája)

Legyen $\boldsymbol{\alpha}$ és $\boldsymbol{\beta}$ gyöke a $\boldsymbol{K}$ test felett irreducibilis $\boldsymbol{f} \in \boldsymbol{K[x]}$ polinomnak. Ekkor $\boldsymbol{K(\alpha)}$ és $\boldsymbol{K(\beta)}$ izomorf.

Az izomorfizmus $\boldsymbol{\alpha}$ –t $\boldsymbol{\beta}$ –ba viszi át, $\boldsymbol{K}$ elemeit pedig fixen hagyja.

Kérdés: van olyan bővítés, ami $\boldsymbol{f}$ minden gyökét tartalmazza ?

Def. Legyen $\boldsymbol{K}$ test és $\boldsymbol{f} \in \boldsymbol{K[x]}$, úgy, hogy $\boldsymbol{deg(f) = n > 0}$. Ekkor $\boldsymbol{K}$ -nak az a legszűkebb bővítése, amelyben $\boldsymbol{f}$ -nek multiplicitással számolva pontosan $\boldsymbol{n}$ gyöke van, $\boldsymbol{f}$ **polinom *K* feletti felbontási teste.**

Az előző két tétel következménye :

Tétel (felbontási test egzisztenciája és unicitása)

Legyen K test és $f \in K[x]$, úgy, hogy $deg(f) = n > 0$.

Ekkor létezik f polinom K feletti felbontási teste és bármely két ilyen izomorf, azon a leképezés mellett, amely K elemeit önmagukba, f gyökeit egymásba képezi le.

Tétel (véges test elemszáma)

Legyen F tetszőleges véges test. Ekkor $|F| = p^n$, ahol F_p az F prímteste és $[F : F_p] = n$.

Biz. Ha $\boldsymbol{F = Fp}$ valamely $\boldsymbol{p}$ prímszámra $\Rightarrow$ $\boldsymbol{|F| = p^1}$.

Ha nem $\Rightarrow$ $\exists\, K:\ [F : K] = n$.

F n –dimenziós vektortér K felett $\{a_1, ..., a_n\}$ bázissal.

$\Rightarrow$ $\boldsymbol{F}$ minden eleme felírható $a_1 k_1$, ..., $a_n k_n$ alakban $\boldsymbol{K}$ felett.

$\forall$ $\boldsymbol{k_i}$ együttható helyébe $|\boldsymbol{K}|$ különböző értéket helyettesíthetünk.

$\Rightarrow$ $\boldsymbol{F}$ –nek $|\boldsymbol{K}|^{\boldsymbol{n}}$ különböző eleme van.

Speciálisan $\boldsymbol{F_p}$ az $\boldsymbol{F}$ prímteste

$\Rightarrow$ legszűkebb résztest

$\Rightarrow \boldsymbol{|F| = |F_p|^n = p^n}$. ☺

Kérdés: mindig található megfelelő $\boldsymbol{n}$ –edfokú irreducibilis polinom tetszőleges $\boldsymbol{F_p}$ felett?

Ha igen $\Rightarrow$ minden prímhatványhoz konstruálható véges test, amelynek pont annyi az elemszáma.

Tétel(véges testben $\boldsymbol{a^q = a}$)

Tetszőleges $\boldsymbol{q}$ elemszámú $\boldsymbol{F}$ véges testben minden $\boldsymbol{a} \in \boldsymbol{F}$ -re $\boldsymbol{a^q = a}$ **.**

Biz.

Ha $\boldsymbol{a = 0}$ vagy $\boldsymbol{a = 1}$ triviális.

Nem nulla elemek:

q – 1 elemű csoport (test definíciója miatt) .

Ha $n = |a| > 1$: $a^{|F^*|} = ?$

Lagrange tétel $\Rightarrow |a| \mid |F^*|$

$|F^*| = ns \Rightarrow$

$a^{q-1} = a^{|F^*|} = a^{ns} = (a^n)^s = 1^s = 1$. ☺

Tétel ($x^q - x$ felbontási teste)

Legyen tetszőleges $\boldsymbol{q}$ elemszámú $\boldsymbol{F}$ véges testben $\boldsymbol{K}$ résztest. Ekkor az $\boldsymbol{f = x^q - x \in K[x]}$ polinomnak $\boldsymbol{F}$ a $\boldsymbol{K}$ feletti felbontási teste és

$$f = x^q - x = \prod_{a \in F} (x - a).$$

Biz.

Előző tétel $\Rightarrow$

F minden eleme gyöke ***f*** –nek,

deg(f) = q $\Rightarrow$ ***f*** –nek legfeljebb *q* gyöke van.

$\Rightarrow$ ***pontosan F*** elemei a gyökök.

$\Rightarrow$ nincs szűkebb test, ami ***f*** összes gyökét tartalmazná.

☺

Tétel (véges testben $(a + b)^q = a^q + b^q$)

Tetszőleges q elemszámú F véges testben minden $a, b \in F$ –re $(a \pm b)^q = a^q \pm b^q$.

Megjegyzés : az állítás testszőleges prímkarakterisztikájú kommutatív gyűrűre érvényes.

Biz.

Legyen F karakterisztikája p

$\Rightarrow \quad q = p^n$.

Binomiális együtthatók:

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{i(i-1)\ldots1} \equiv 0 \bmod (p)$$

mivel nem egyszerűsíthető p –vel .

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \ldots + \binom{p}{p-1} a b^{p-1} + b^p = a^p + b^p$$

n szerinti teljes indukció $\Rightarrow$

$$(a+b)^{p^n} = a^p + b^p,$$

$$a^{p^n} = \left((a-b)+b\right)^{p^n} = (a-b)^{p^n} + b^{p^n},$$

$$(a-b)^{p^n} = a^{p^n} - b^{p^n}.$$

☺

Tétel(véges testek egzisztenciája)

Tetszőleges véges test elemszáma p^n, ahol p prím és n pozitív egész, továbbá tetszőleges p prím és n pozitív egész számhoz található p^n elemszámú véges test.

Biz.

1. rész: már láttuk.

2. rész: legyen $q = p^n$ és az

$f = x^q - x \in F_p[x]$ polinomnak F az F_p feletti felbontási teste.

Tudjuk az előző tételből :

F tartalmazza f gyökeit és

f gyökei pontosan F elemei , ha F –nek q eleme van.

Van-e többszörös gyöke *f* –nek vagy mind különböző ?

$$f' = qx^{q-1} - 1$$

$F_p[x]$ –ben $q \equiv 0 \mod(p)$

$$f' = -1$$

$$\Rightarrow (f, f') = 1$$

$\Rightarrow$ f –nek nincs többszörös gyöke.

Legyen $S = \{ a \in F : a^q - a = 0 \}$

Mit mondhatunk *S* –ről ?

1. S –nek q eleme van: f gyökei .

2. $0, 1 \in S$.

3. $\forall a, b \in S$ –re :

   előző tétel + S konstrukciója $\Rightarrow$

$$(a - b)^q = a^q - b^q = a - b \,.$$

$$\Rightarrow a - b \in S \,.$$

4. $\forall a, b(\neq 0) \in S$ –re :

$$(a^{b-1})q = a^q b^{-q} = ab^{-1}$$

$$\Rightarrow ab^{-1} \in S \,.$$

$\Rightarrow$ S test, ami tartalmazza f összes gyökét

F a legszűkebb ilyen $\Rightarrow$ $F = S$. ☺

Tétel(véges testek unicitása)

Tetszőleges $\boldsymbol{q = p^n}$ elemszámú véges test izomorf az $\boldsymbol{f = x^q - x}$ polinom $\boldsymbol{F_p}$ feletti felbontási testével.

Biz. Legyen $\boldsymbol{F}$ $\boldsymbol{q = p^n}$ elemszámú véges test

véges test elemszáma tétel $\Rightarrow$

F karakterisztikája p és $F : Fp$.

$x^q - x$ felbontási teste tétel $\Rightarrow$

F az f polinom F_p feletti felbontási teste.

felbontási test egzisztenciája és unicitása tétel $\Rightarrow$

Test feletti polinom felbontási teste izomorfizmustól eltekintve egyértelműen létezik.

☺

Tétel (véges testek résztest kritériuma)

Legyen $\boldsymbol{F_q}$ tetszőleges $\boldsymbol{q = p^n}$ elemszámú véges test.

$\boldsymbol{F_q}$ minden résztestе $\boldsymbol{p^m}$ –edrendű, ahol $\boldsymbol{m \mid n}$, és

minden $\boldsymbol{m \mid n}$ -hez egyértelműen létezik $\boldsymbol{F_q}$ -nak $\boldsymbol{p^m}$ –edrendű résztestе.

Példa:

$$
\begin{tikzcd}
 & F_{2^{30}} \arrow[dl] \arrow[d] \arrow[dr] & \\
F_{2^6} \arrow[d] \arrow[dr] & F_{2^{10}} \arrow[dl] \arrow[dr] & F_{2^{15}} \arrow[dl] \arrow[d] \\
F_{2^2} \arrow[dr] & F_{2^3} \arrow[d] & F_{2^5} \arrow[dl] \\
 & F_2 &
\end{tikzcd}
$$

Tétel (véges test multiplikatív csoportja)

Tetszőleges $\boldsymbol{F_q}$ véges test $\boldsymbol{F_q^*}$ multiplikatív csoportja ciklikus.

Def. Tetszőleges $\boldsymbol{F_q}$ véges test $\boldsymbol{F_q^*}$ multiplikatív csoportjának generáló eleme $\boldsymbol{F_q}$ **primitív eleme**.

Tétel (bővítőelem létezése)

Legyen $\boldsymbol{F_q}$ tetszőleges véges test és $\boldsymbol{F_r}$ véges bővítése. Ekkor $\boldsymbol{F_r}$ egyszerű bővítése $\boldsymbol{F_q}$ –nak és $\boldsymbol{F_r}$ minden primitív eleme megfelelő bővítőelem $\boldsymbol{F_q}$ –ról $\boldsymbol{F_r}$ –re való bővítésnél.

Következmény

$\forall$ F_q véges testhez és n pozitív egészhez létezik egy n –edfokú irreducibilis polinom $F_q[x]$ –ben . Nevezetesen: $F_r = F_q(\alpha)$ esetén α $F_q[x]$ feletti minimálpolinomja .

10. ALGORITMUSELMÉLET

Def. **Számítási eljárás** alatt a (Q, Q_b, Q_k, f) négyest értjük, ahol Q állapotok halmaza, Q_b (**bemeneti állapotok**), Q_k (**kimeneti állapotok**) részhalmazai Q-nak, $f : Q \to Q$ **átmeneti függvény,** amelyre $f(q) = q$ minden $q \in Q_k$-ra.

$\forall\, x \in Q_b$ állapot definiál egy $q_0, q_1, q_2, \ldots$ **számítási sorozatot,** ahol

$$q_0 = x \quad \text{és} \quad q_{n+1} = f(q_n), \quad \text{ha} \quad n \geq 0$$

x bemenetre a számítási sorozat ***n*** **lépésben véget ér**, ha n a legkisebb pozitív egész, amelyre $q_n \in Q_k$. Ekkor az **eredmény**:

$$q_n = q_{n+1} = q_{n+2} = \ldots$$

Lehet, hogy nem ér véget!

Példa: az euklidészi algoritmus formalizálása.

Legyen $Q_{\mathrm{k}} = \mathbf{Z}$, $Q_b = \mathbf{Z}^2$, $Q = (\mathbf{Z}^2 \times \{2, 3\}) \cup Q_b \cup Q_k$, továbbá

$$f(a) = a,$$

$$f(a, b) = (a, b, 2)$$

$$f(a, b, 2) = \begin{cases} a, & \text{ha } b = 0 \\ (a, b, 3) & \text{különben} \end{cases}$$

$$f(a, b, 3) = (b, a \bmod b, 2)$$

Szimulálás

$$C' = (Q', Q'_b, Q'_k, f')$$

számítási eljárás szimulálja a

$$C = (Q, Q_b, Q_k, f)$$

k megadja, hogy a szimulált „gép” 1 lépését a szimuláló hány lépésben hajtja végre

ha $\exists$ olyan g: $Q_b \rightarrow Q_b$’ (**bemeneti kódolás**), $h : Q' \rightarrow Q$ (**állapot dekódolás**) és $k : Q' \rightarrow \mathbf{N}^+$ függvény, amelyekre

(1) ha $x \in Q$, akkor a C számítási eljárás pontosan akkor adja az y eredményt, ha van olyan $y' \in Q_k'$, hogy g(x) bemenettel a C' számítás az y' eredményt adja, és $h(y') = y$

(2) ha $q' \in Q'$, akkor $f(h(q')) = h(f'^{k(q')}(q'))$, ahol $f'^{k(q')}$ az f' leképezés $k(q')$-edik iteráltját jelenti.

Példa: a bővített euklidészi algoritmus formalizálása.

Legyen $Q_{\mathrm{k}} = \mathbf{Z}^3$, $Q_b = \mathbf{Z}^2$, $Q = (\mathbf{Z}^7 \times \{2, 3.1, 3.2\}) \cup Q_b \cup Q_k$, továbbá

$$f(a, b) = (a, 1, 0, b, 0, 1, 0, 2)$$

szimulálja az előző eljárást, de fordítva nem igaz!

$$f(a, x, y) = (a, x, \mathrm{y})$$

$$f(a, x, y, b, u, v, q, 2) = \begin{cases} (a, x, y), & \text{ha } b = 0 \\ (a, x, y, b, u, v, q, 3.1) & \text{különben} \end{cases}$$

$$f(a, x, y, b, u, v, q, 3.1) = (a, x, y, b, u, v, \lfloor a/b \rfloor, 3.2)$$

$$f(a, x, y, b, u, v, q, 3.2) = (b, u, v, a - qb, x - qu, y - qv, q, 2)$$

Ordó

Legyen $f : \mathbf{R} \to \mathbf{N}$ egy számsorozat.

Jelölje **O(*f*),** vagy **O(*f*(*n*))** mindazon $g : \mathbf{R} \to \mathbf{N}$ számsorozatok halmazát, amelyekre van olyan *g*-től függő $C \in \mathbf{R}$ konstans és $N \in \mathbf{N}$ index, hogy

$$|g(n)| \leq C \cdot |f(n)|, \text{ ha } n \geq \mathrm{N}.$$

Ha f és f^*, illetve g és g^* csak véges sok tagban különböznek, akkor

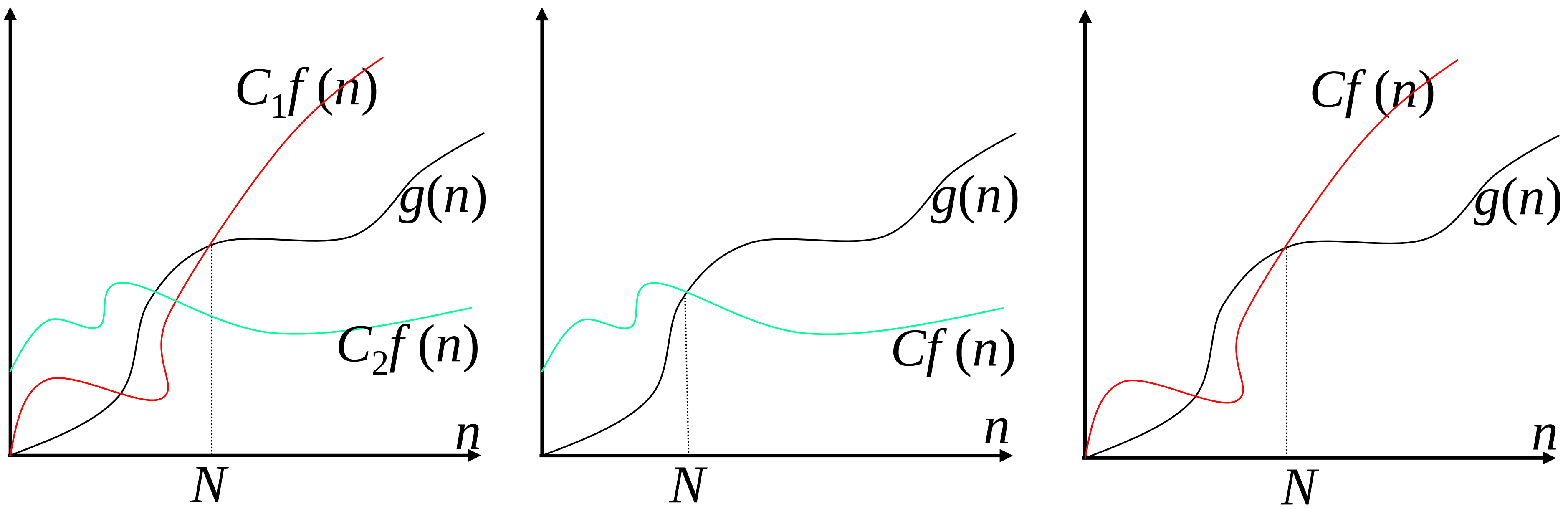
$$\mathrm{g} \in \mathrm{O}(f) \Leftrightarrow \mathrm{g}^* \in \mathrm{O}(f^*),$$

így a jelölés értelmes, akkor is ha *f* vagy *g* véges sok indexre nem értelmezett.

Ha pl. *g* egy legfeljebb *k*-adfokú polinom, akkor $\mathrm{g} \in \mathrm{O}(n^k)$.

Fordítva, ha $f \in O(g)$, akkor ez így jelöljük: $\boldsymbol{g \in \Omega(f)}$.

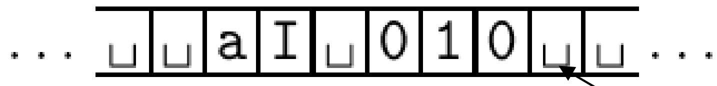
Az $O(f)$ és $\Omega(f)$ halmazok metszetét $\boldsymbol{\Theta(f)}$ jelöli.



$g(n) \in \Theta(f(n))$ $\quad$ $g(n) \in \Omega(f(n))$ $\quad$ $g(n) \in O(f(n))$

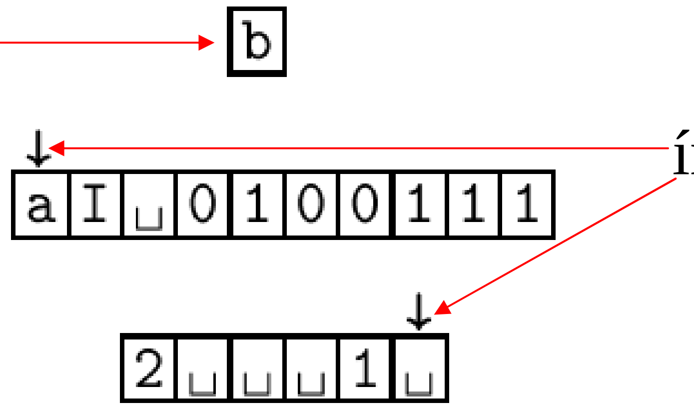
Turing - gépek

Egy Turing - gép $k \geq 1$ db **szalagból** és egy **vezérlőegységből** áll.



∀ mezőn az **ábécé** egy **betűje** áll, véges sok nem az **üres** jel (**szóköz**)

a vezérlőegység véges sok **belső állapotot** vehet fel



író - olvasó fejek

mindig van *s* és *h* állapot!

Def. *T* Turing - gép egy *T* = (*B*, *A*, *φ*) hármas, ahol *A* a szalagábécé, *B* a belső állapotok halmaza, *A*, *B* véges, továbbá

$$\sqcup \in A,\ s, h \in B$$

és

$$\varphi : B \times A^k \to B \times A^k \times \{<, =, >\}^k$$

k a szalagok száma!

tetszőleges leképezés.

Így is szokás megadni (precízebb): $T = (k, B, A, \sqcup, s, h, \varphi)$

egy lépés $\varphi : (b, a_1, \ldots, a_k) \mapsto (b', a'_1, \ldots, a'_k, c_1, \ldots, c_k),$

ahol $b, b' \in B$, és ha $1 \leq i \leq k$, akkor $a_i, a'_i \in A$, $c_i \in \{<, =, >\}$

illetve $\varphi : (h, a_1, \ldots, a_k) \mapsto (h, a_1, \ldots, a_k, =, \ldots, =).$

Turing - gép mint számítási eljárás

egy aktuális állapot:

β_i-k: fejtől jobbra eső szavak

$$q = (b, \alpha_1, \beta_1, \alpha_2, \beta_2, \ldots, \alpha_k, \beta_k) \in B \times A^{*2k}$$

α_i-k: fejtől balra eső szavak

Bemeneti állapotok: ahol $b = s$, kimeneti állapotok: ahol $b = h$

Induláskor $\forall \beta_i$ üres szó, azaz a fejek a bemenet jobb szélén állnak.

Bementnél feltesszük, hogy α_i-k nem tartalmaznak üres jelet.

Kimenetnél β_i-ket „**szemétnek**” tekintjük.

Kimenet: α_i-k leghosszabb üres jel mentes suffixei.
α_i-k többi része szemét.

$m < k$ bemeneti szó esetén azokat az első m szalagra írjuk, a többi üres.

$m = 1$ esetén **standard inputról** beszélünk.

Benenet **hossza** az α_i-k hosszának összege.

$n < k$ kimeneti szó esetén azok az utolsó n szalagra kerülnek, a többi szalag tartalma szemét.

$n = 1$ esetén **standard outputról** beszélünk.

Kinenet **hossza** a kimeneti szavak hosszának összege.

Elnevezés A_0 elemszáma szerint: **unáris**, **bináris**, stb Turing-gép

10.1.11. Példák. (1) Az a Turing-gép, amelynek csak az $s = h$ belső állapota van, nem csinál semmit, kimenete a bemenet.

(2) Az a Turing-gép, amelynek csak az $s \neq h$ belső állapotai vannak, mindig üres jelet ír és balra lép minden szalagon, és mindig az s állapotban marad, törli a szalagokat, de soha nem áll meg.

(3) Az az egyszalagos Turing-gép, amelynek csak az $s \neq h$ belső állapotai vannak, ha nem üres jelet olvas, akkor balra lép, ha pedig üres jelet olvas, akkor jobbra lép és megáll, továbbá mindig azt írja vissza, amit olvasott, megkeresi a bemenet balszélső betűjét. Hasonlóan kereshetünk egy adott betűt.

(4) Egy egyszalagos gépen azt, hogy `abrakadabra` kiírathatjuk a szalagra 12 állapottal.

(5) Könnyű megadni olyan kétszalagos gépet, amely

$$a_1a_2\dots a_n$$

bemenetre kimenetként az $a_na_{n-1}\dots a_1$ szót adja: elmegyünk a bemenet bal széléig, majd visszafelé haladva a betűket egyenként a második szalagra másoljuk. Hasonlóan könnyű megadni olyan kétszalagos gépet, amely $a_1a_2\dots a_n$ bemenetre $a_1a_2\dots a_na_na_{n-1}\dots a_1$, illetve $a_1a_1a_2a_2\dots a_na_n$ kimenetet ad.

(6) Bináris gépen $\{\sqcup, \mathtt{0}, \mathtt{1}\}$ jelkészlettel, 3 szalaggal könnyen megadható olyan gép, amely kettes számrendszerben felírt számokat összead. Jelentse az s start állapot azt, hogy nincs átvitel, a c állapot pedig, hogy van átvitel. Leolvasva a két utolsó számjegyet, az összeg megfelelő számjegyét kiírjuk a harmadik szalagra, balra lépünk, és az átvitelnek megfelelő állapotba megyünk át. Ha valamelyik szalagon elfogyott a szám, akkor úgy viselkedünk, mintha onnan nullát olvasnánk. Ha mindkét szalagon elfogyott a szám, akkor átvitel esetén 1-et írunk, egyébként üres jelet, és az eredmény jobb szélére megyünk. Hasonlóan adható meg 3 vagy 4 szalaggal olyan gép, amely kettes számrendszerben felírt számokat összehasonlít, kivon (ha az eredmény negatív lenne, nullát ad vissza), szoroz, maradékosan oszt.

10.1.12. Turing-gép szimulálása csökkentett jelkészlettel. *Legyen $T = (B, A, \varphi)$ egy Turing-gép, és A' egy tetszőleges véges ábécé, amelynek legalább két eleme van. Ekkor T szimulálható olyan T' Turing-géppel, amelynek ábécéje A'. Ha egy számítás során a T gép t lépést tesz, akkor a T' gép $O(t)$ lépést tesz.*

Biz.

Alkalmas *n*-re *A* üres jelének kódja *A'* üres jeléből álló *n*-es

Legyen $A = \{0, 1, 2, 3\}$ és $A' = \{u, I\}$, üres jel a 0, illetve az u, továbbá

$0 \to$ uu, $1 \to$uI, $2 \to$Iu, $3 \to$II.

$\forall\, h \neq b \in B$ belső állapotához *T*-nek a T'-nek a

b, b_u, b_I, b_i ($i \in A$), $b_{i,c}$ ($i \in A$ és $c \in \{<, >\}$) belső állapotok tartoznak

***T’* működése**: ha T’ valamely b állapotban van és a bemenet jobbszélső betűjét olvassa, akkor attól függően, hogy mit olvasott, b_{u}, vagy b_{I} állapotba megy át és balra lép.

Itt attól függően, hogy mit olvasott, a b_i állapot valamelyikébe megy át, jobbra lép és *i*’ kódjának bal oldali betűjét írja ki, azaz

$i = 0$, ha a b_{u} állapotban voltunk és u betűt olvastunk, $i = 1$, ha b_{I} állapotban voltunk és u betűt olvastunk, $i = 2$, ha a b_{u} állapotban voltunk és I betűt olvastunk, $i = 3$, ha b_{I} állapotban voltunk és I betűt olvastunk és $\varphi(b, i) = (b', i', c)$.

A b_i állapotban, ha *c* az = jel, akkor a szalagra *i*’ jobbszélső betűjét írjuk, átváltunk a *b*’ állapotra és a fej marad. Ha nem =, akkor a szalagra *i*’ jobbszélső betűjét írjuk, átváltunk a $b_{i,\,c}$ állapotra és a fej mozdul *c* szerinti irányba.

$b_{i,\,c}$ állapotban azt írjuk aszalagra, ami ott van, az állapot *b’* lesz és a fej mozdul *c* szerint.

Így *T’* a *T* gép bármely lépését legfeljebb 4 lépésben szimulálja.

Például, ha $\varphi(b, 3) = (b', 1, <)$ a *T*-ben, akkor *T’*-ben:

u	u	I	I

^$\mathbf{b}$

u	u	I	I

^$\mathbf{b}_{\mathbf{I}}$

u	u	u	I

^$\mathbf{b}_{\mathbf{3}}$

u	u	u	I

^$\mathbf{b}_{\mathbf{3,\,<}}$

u	u	u	I

^$\mathbf{b'}$

Szavak kódolása számmá

Tfh A = {0, 1, ..., r – 1} számjegyek, üres jel a 0. Egy A*-beli $\alpha = a_n a_{n-1} \ldots a_0$ bemeneti szó vagy üres, vagy nem 0-val kezdődik és r alapú számrendszerben:

$$|\alpha|_r = \sum_{i=0}^{n} a_i r^i$$

r nincs a jegyek közt!

Az $\alpha \mapsto |\alpha|_r$

leképezés kölcsönösen egyértelműen képezi le A* nem 0-val kezdődő szavait **N**-re.

Ha csak A_0*-beli $\alpha = a_n a_{n-1} \ldots a_0$ bemeneti szavakat akarunk kódolni, akkor :

$$|\alpha|_{r-1} = \sum_{i=0}^{n} a_i (r-1)^i$$

r – 1 a jegyek közt van!

Az $\alpha \mapsto |\alpha|_{r-1}$

leképezés kölcsönösen egyértelműen képezi le A*-ot **N**-re.

10.1.15. Turing-gép szimulálása egy szalaggal. *Legyen* $T = (B, A, \varphi)$ *egy Turing-gép* k *szalaggal. Ekkor* T *szimulálható olyan egyszalagos* S *Turing-géppel, amelynek ábécéje* A. *Ha egy számítás során a* T *gép* t *lépést tesz, akkor az* S *gép* $2kt(2t+3) = O(t^2)$ *lépést tesz.*

Biz.

S minden mezőjét 2k db mezőből álló csoportokra bontjuk bontjuk:

a_i-k mutatják, hogy *T*-ben 1., 2., ...*k*., fej hol állt induláskor

egy mezőcsoport tartalma: $a_1 a_2 \ldots a_k f_1 f_2 \ldots f_k$

f_i-k mutatják, hogy a szimuláció során hol állnak *T*-ben 1., 2., ...*k*., a fejek: ha a *T* gép *i*-edik szalagján a mezőcsoportban szereplő a_i betűn áll a fej, akkor f_i a nem üres, különben az üres jel.

Kezdetben a fej egy mezőcsoport jobbszélén áll.

A tekintett mezőcsoporttól balra lévő mezőcsoportban a_i-k mutatják, hogy *T*-ben 1., 2., ...*k*., fejtől eggyel balra milyen betű volt induláskor, és így tovább...

A *T* egy lépésének szimulálása annak a 2*k* hosszú mezőcsoportnak a jobbszéléről indul, amelyben a „leginkább jobbra” lévő fej van.

S „emlékszik” arra, hogy *T* milyen állapotban van és arra is hogy egy mezőcsoport melyik mezőjén áll.

S balra lépkedve megkeresi minden T-beli szalagra a fej állását és megjegyzi a ott lévő betűvel együtt. (f_i-k alapján meg tudja tenni)

Ekkor S már tudja, hogy mit kell tennie.

Ha kell, akkor balra lép egy mezőcsoportot, aztán jobbra indul és a megfelelő helyeken ír a szalagra és mozgatja a fejet.

Ha eddig szimuláltunk *n* lépést, minden fej legfeljebb *n* mezőcsoporttal mozdult el balra, vagy jobbra. Tehát leghosszabb eset, ha egyik fej mindig balra, egy másik mindig jobbra mozdult T-ben (ezek 2*n* „mezőcsoportnyira” lesznek egymástól).

A következő lépés során legfeljebb 2*n*+1 mezőcsoportot kell balra haladva végigolvasni, hogy minden információt megtaláljunk, ami leírja a jelenlegi helyzetet.

Ezután legfeljebb 1 mezőcsoportot kell balra menni, így max 2*n*+3-at visszafelé

tehát az *n*+1-dik lépés szimulálása közben legfeljebb 2n+1+1+2n+3 = 4n+5 mezőcsoportot érintünk, amelyek 2*k* jel hosszúak, így összesen 2k(4n+5) lépést tesz *S*

Tehát a *t* lépés szimulálása:

$$\sum_{n=0}^{t-1} 2k(4n+5) = 2kt(2t+3)$$

☺