

## TERV

Tétel: legyen  $f$  a  $g$  öregrési függvénye

(1)  $f$  multiplikatív  $\Rightarrow g$  multiplikatív

$g \dashv \vdash \Rightarrow f \dashv \vdash$

Tétel legyen  $f$  a  $g$  öregrési függvénye

$$f(n) = \sum_{d|n} f(d) \mu\left(\frac{n}{d}\right) \quad \text{Möbius féle visszaváltási formula}$$

$$= \sum_{d|n} f\left(\frac{n}{d}\right) \mu(d)$$

$$\sum_{d \in \mathcal{A}} f(d) \mu(d)$$

1. Lemma:  $f$  egy multiplikatív számelméleti függvény.

~~$\Rightarrow f(1) = 0$~~  Ha  $f$  azonosan nulla akkor  $f(1) = 0$  (az triviális)

Ha  $f$  nem azonosan nulla akkor  $f(1) = 1$  (az érdekes)

Biz: tegyük fel hogy  $f$  nem azonosan 0

akkor lesz  $f(1) = 1$

Vannak egyes  $a \in \mathbb{N}$  amire  $f(a) \neq 0$

Számoljuk ki  $f(1 \cdot a)$  egy relatív prím  $1$  és  $a$ -hoz minden  $a$ -ra.

$$f(1 \cdot a) = f(1) f(a)$$

$$\cancel{f(a)} = \cancel{f(1)} \cdot \cancel{f(a)}$$

$$f(a) = f(1) \cdot f(a) \Rightarrow f(1) = 1 \quad \text{mert } f(a) \neq 0$$

Multiplikatív-e  $f$ ?

$$f(n) = n^3 - 6n^2 + 2$$

Válasszunk: Nem

$$f \neq 0 \quad (f(0) = 2)$$

az azonosan nulla

$f(1) = 3$  sem lehet multiplikatív

☹

Egy  $f$  függvény adott a minden helyen adott

Ha  $f$  multilineáris akkor elég minimális helyen ismerni

$$f(n) = f(p_1^{d_1} \dots p_s^{d_s}) = \underbrace{f(p_1^{d_1})} \dots \underbrace{f(p_s^{d_s})}$$

Ha ezek ismeretével akkor  $f(n)$  is ismert

$$\begin{array}{ccccccc} p_1 & & A_{p_1,1} & A_{p_1,2} & A_{p_1,3} & & \\ & & A_{p_2,1} & A_{p_2,2} & A_{p_2,3} & & \\ & & & & & & A_{p_2,3} = f(p_2^3) \end{array}$$

Hogyan fűzhetjük a fennmaradtakat?

$$f(n) = \sum_{d|n} g(d) \quad \text{Ha } g \text{ ismeretében } f \text{ -t}$$

Ha  $f$  de  $g$ -t szeretnénk  $f$  ismeretében

$$f(1) = g(1)$$

$$f(2) = g(1) + g(2)$$

$$f(3) = g(1) + g(3)$$

$$f(4) = g(1) + g(4)$$

$$f(5) = g(1) + g(5)$$

$$f(6) = g(1) + g(2) + g(3) + g(6)$$

$$g(1) \quad g(2) \quad g(3) \quad \dots \quad \text{bél}$$

$$f(1) \quad f(2) \quad \dots \quad \text{rindmunka}$$

Fordítottan szeretnénk:

$$g(1) \quad g(2) \quad \dots \quad \text{rindmunka}$$

$$f(1) \quad f(2) \quad \dots \quad \text{bél}$$

$$g(1) = f(1) \quad \text{az első egyenletből}$$

$$g(2) = f(2) - f(1)$$

$$g(3) = f(3) - f(1)$$

$$g(4) = f(4) - f(1) - f(2)$$

$$g(5) = f(5) - f(1)$$

$$g(6) = f(6) - f(1) - g(2) - g(3) = f(6) - f(1) - f(2) - f(3) + f(1)$$

$$g(6) = f(6) - f(2) - f(3) - f(1)$$

$$g(4) = \underbrace{f(4)}_{f(1)} - \underbrace{g(2)}_{-f(1)+f(2)}$$





4, Föld tartomány van New York és az ABCD

7, karantén (hid) között van a b c d e f g

hid

a

b

c

d

e

f

g

tartomány

A, C

A, C

A, D

C, D

B, C

B, C

B, D

abszolút

abszolút

Van egy f fegy or élel balról és a pontok balról

Utolsó def

$(E, P, f)$

élel balról

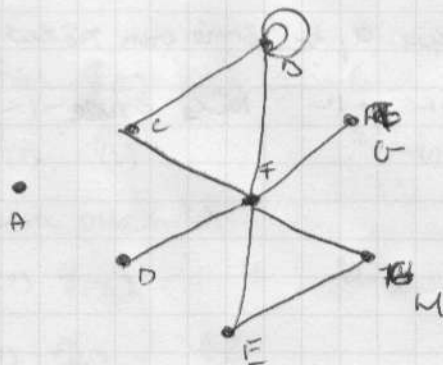
Pontok balról

$f: E \rightarrow$  rendezetlen páros, balról

Pont fegy:

Kellene a def

Örök gel fegyri or egy ponton ellentét élel és utolsó  
előfűti Mivel magánmagyar lágy, egy novelt.



C fegy = 2

G fegy = 1

A fegy = 0

F fegy = 6

B fegy = 6

1, minden ponton van fegy

2, minden ponton fegy 0

3, egy ponton 2-vel fegy a fegyri

4, minden ponton fegyri van fegyri és fegyri fegyri

Total:  $\frac{1}{2} a_1 + \dots + ds = 2e$  where  $e$  is a  $\mathbb{Z}$ -divisor on  $S$ .

Kémia: egy lútot a levele

tent.

A, C

ad egy fűtő "A" rútr és egy fűtő "C"

mivel a 2-vel rendelkező  $d_1 + \dots + d_5$  összeg

Tétel: Egy négyzet és a belvonalai fűző pontok négyzet

Bur Sequence d, yds a feet minor g-ben

Leeson  $d_1'', \dots, d_m''$  ger a pairesar  $d_1 \dots d_s$  rööst

desigen  $d_1', \dots, d_r'$  er a reaktör - 11 -

$d_1'' + d_4'' + d_1' + \dots + d_0 = 2e$   
 Folgerung:  $d_1 + d_0$  ist gerade  
 $\begin{matrix} \downarrow & \downarrow & \downarrow & \downarrow \\ \equiv 0 & \equiv 0 & \equiv 1 & \equiv 1 \end{matrix}$

$$V \equiv 0 \pmod{2}$$

~~{Total:  $\text{eşit farklar}$  or  $\text{eşit oranlar}$   $+1 = \text{silindirik}$ }~~



Def: egy öntefüggetlen zömök, grafit fehér színű  
fém, van lehetett kovács élel, és duplex élel,  
ardíveszár, rúti, és arányos.

Tétel: Egy felelőz az edzővel + 1 = Százalékos felelőz

So I buy bar well, keep from refer

Kendisi: fa-e o a qaf abirun seyyalatahn nige rat.

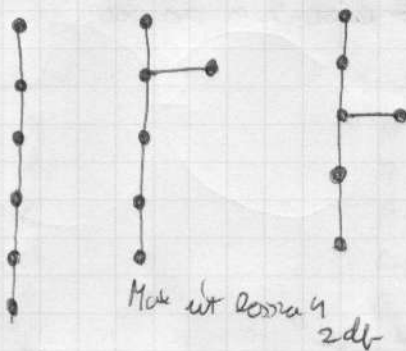
et debet fideri terrenti de me non ex a tunc.



 4 Partic fee

5 vertices

3 satir per

Maximális útak száma attól függ, hogy hány pontot fel



Max út hossza 5  
1 db

Max út hossza 4  
2 db

Max út hossza 3  
2 db

Indukcióval:

Bázis: vegyünk 1 pontot, ekkor a fára 1  
térközű út a pontot a mi  $\neq$  fánál  
egy 1 pontot és egy út tölti.

$F'$  epifaktus

$F'$  összefüggő  $F'$  maximális  $\Rightarrow F'$  fa

$F'$ -ben egy új pont és egy él hozzá  $+1 =$  csak másként lehet 1-et hozzá  
adhatunk. Helyesre az állítás.

Ha 1 pontot és a fát hozzá adunk a fát áll  $0+1=1$   
csak másként  
állás

Kérdés: miként lehet egy új pont egy fára?

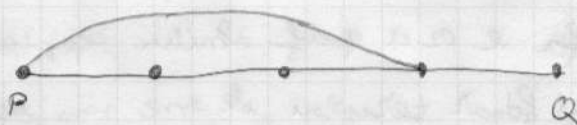
Lemma: egy <sup>új pont</sup> <sup>(amikor van)</sup> fára mindig van 1 fát hozzá.

0 pont, 1 pont fára nem lehet.

0 pont, 1 pont fára nem lehet.

Bizonyítás:

Nézzük egy maximális utat  $u$   $F'$ -ben / egy új pont  $F'$ -ben  
van el./



Ha  $P$ -ből nem fut ki több él akkor új pont

Feltételezhetjük hogy  $P$ -ből fut ki egy új él  $(e)$

$u$  és egy  $u$ -n áthaladó útfa fut át  $u$  nem maximális  $\Rightarrow$

$\Rightarrow e$  az új fa

Most látni fogjuk

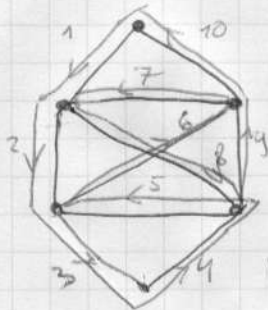
az állítást hogy 2 db 1 fát lehet használni



# Euler-féle Befejezés

Adott egy  $G$  gráf. Olyan bejárt gráfot keresünk mely minden ~~csomópont~~ csomópontunkon szomszoros és minden csomópontunkon a bejárt gráfba.

PL



Mi van ha van egy csomópontunk?  
Nem ábrát is...

Feltétel Euler-féle befejezés létezésére.

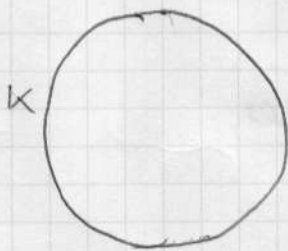
- 1, Ha  $G$  nem összefüggő akkor olyan befejezés nincs. (és van el a nem összefüggő - nem összefüggő)
- 2, Minden csomópontunkon szomszoros
- 3,  $G$  páros

Tétel egy gráfban van Euler-féle befejezés ha (1)(2)(3) teljesül

Bizonyítás: válasszunk egy pontot  $P$ -t  $P$ -ből induló útvonal

A gráfban nem  $O$ . Legyen  $2$ .  $P$ -ből induló útvonal

Most vizsgáljuk elhárul egy  $G$  gráfban a  $P$ -ből induló útvonal  $O$  szomszoros  $2$  egy csomópontunkon van egy  $2$  csomópontunkon. Ez végpontunk lehet az útvonal. Az útvonal végpontunk van egy csomópontunkon  $(K)$



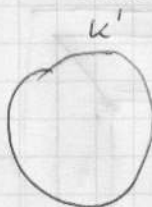
Ha  $K$  gráfban  $G$ -törés élét akkor megvan az Euler-féle befejezés.

Dalok is  $K$  élét.

$G'$  gráfban  $G$  élét  $(1)(2)(3)$

Struktúra egy  $K'$  gráfban  $G'$ -ben

Struktúra struktúrában nem tovább vizsgáljuk

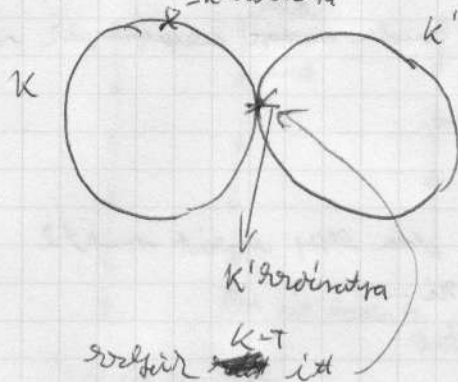


Lehet-e egy  $K$  és  $K'$  csomópontunk. (Ez lehet, lehet)

$K$  egy struktúrában kell vizsgálni  $K'$  struktúrában  
Lehet-e a gráf és nincs élét nem vizsgáljuk?



$k$  és  $k'$  összeegyeztethető a helyes névvel  
-  $k$  valószínű

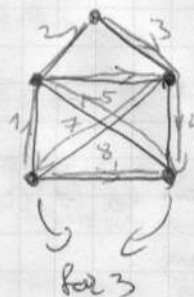


Most ismerjük az egész a nyelvről is  
az eljárás előbb-utóbb szeretn.

Eulen Seile von Er halt rest

Guln. Lede ut. alal oregon leqirant gresur egey munden elt 1000 emtaw.  
 is non feltexaul faktor nime a gresurten.

PL



Tétel: Euler-féle út létezik-e a "örösfüzeg" néps és mennyet  
főzők város hálójában?

Bu: İşletme P, Q a taitatları için taitat ziraatları P-T ve Q-T  
ağırlıkta maddeler taitatları için taitatlar.

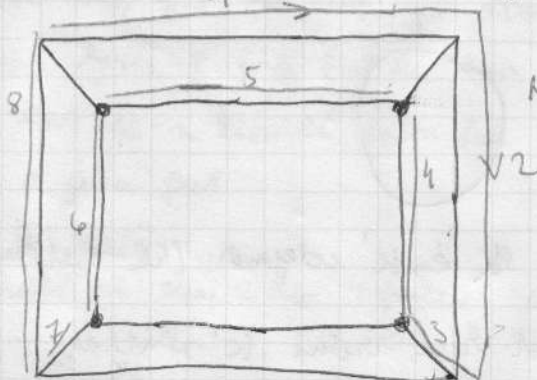
Akhirnya or di "n" tetak

Lez egy Euler féle kör dolgot mi a PQ él.

Hamilton gele beğendi

Adatt egy 6 fős olyan beérkezett kérésre amire most nem volt  
1. az ember és a másik a jövőre a reaktív.

Pelée



Membran feile nur



## GROUPOIDOK

Def: adott a  $G$  halmaz és legyen  $\circ$  egy binary művelet a  $G$ -n  
 az az a művelet nem vektor  $a \in G$ -ból

$A(G, \circ)$  egy csoport ha

$\rightarrow$  a művelet asszociatív  $(a \circ b) \circ c = a \circ (b \circ c)$

$\rightarrow$  egységelem létezése  $\exists e \in G \quad a \circ e = e \circ a = a$

$\rightarrow$  inverzum létezése  $\forall a \in G \exists a^{-1} \in G$  úgy, hogy  $a \circ a^{-1} = a^{-1} \circ a = e$

Pé 1. Milyenek lehetnek a csoportok? - e az alábbiak közül  
 / a megadott művelettel?

a,  $(\mathbb{R}, +)$

b,  $(\mathbb{Z}, +)$

c,  $(\mathbb{Z}, \cdot)$

d,  $(\mathbb{R}, \cdot)$

e,  $(\mathbb{N} \setminus \{0\}, \cdot)$

f,  $G = \{\pm 1, \pm i\}$

$(G, \cdot)$

Tétel:  $G$  egy csoport  $a \in G$  ellen  $a^{-1}$  egyértelmű  
( $a$ -nak más inverze)

Bizonyítás: tegyünk  $b$  és  $c$  az  $a$  inverze  $G$ -ben

$$a \cdot b = e \quad (1)$$

$$b \cdot a = e \quad (2)$$

$$a \cdot c = e \quad (3)$$

$$c \cdot a = e \quad (4)$$

Nézzük a  $b \cdot a \cdot c$ -t

$$c = e \cdot c = \underset{\substack{\uparrow \\ (2) \\ \text{mialt}}}{(a \cdot b)} \cdot c = \underset{\substack{\uparrow \\ \text{asszociativitás}}}{b(a \cdot c)} = \underset{\substack{\uparrow \\ (3) \\ \text{mialt}}}{b \cdot e} = b$$

Tétel:  $G$  egy csoport  $a \in G$  ellen  $(a^{-1})^{-1} = a$ .

Bizonyítás  $G$ -ben minden elemnek van inverze így  $a^{-1}$ -nek legyen  $x$  és  $b$

$$(a^{-1}) \cdot b = e \quad (1)$$

$$b \cdot (a^{-1}) = e \quad (2)$$

Legyünk erre így  $(a^{-1}) \cdot a = e \quad (3)$

$$a \cdot (a^{-1}) = e \quad (4)$$

ebből  $b = a$  adódik

Tétel:  $G$  egy csoport,  $a, b \in G$  ellen  $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$  (inverz tétel)

Bizonyítás:  $G$ -ben minden elemnek van inverze így  $a \cdot b$ -nek is legyen  $c$ .

$$(a \cdot b) \cdot c = e \quad (1)$$

$$c \cdot (a \cdot b) = e \quad (2)$$

Legyünk erre:

$$(a \cdot b)(b^{-1} \cdot a^{-1}) = e \quad (3)$$

$$(b^{-1} \cdot a^{-1})(a \cdot b) = e \quad (4)$$

$$(a \cdot b)(a^{-1} \cdot b^{-1}) = [a(b \cdot b^{-1})]a^{-1} = [ae]a^{-1} = aa^{-1} = e$$

Ebből az asszociativitás így  $c = b^{-1} \cdot a^{-1}$

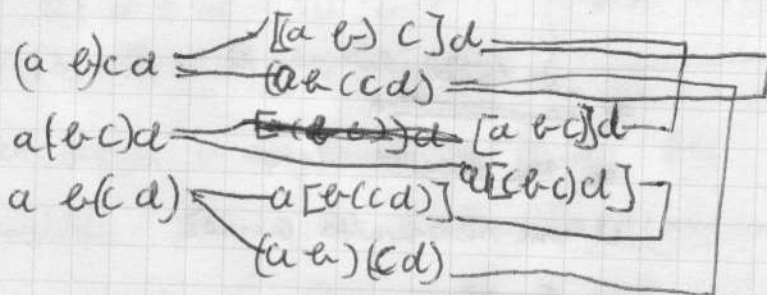
$c$  is és  $b^{-1} \cdot a^{-1}$  is inverze az  $ab$ -nek

De az inverz egyértelmű

Milyen mutatjuk meg hogy egy  $G$  is teljesíti ezeket a feltételeket?  
azaz egy zártfeladat (semidistributív):

~~abcde~~  
(a b) d

a b c d e



$$(a b)(c d) = (a b) \times = a(b \times) = a[b(c d)]$$

"Tétel:

Hosszú sorokat nem érintve a zárójelrendre "

## RÉSZCSOPORTOK

$(G, \cdot)$  egy csoport

azt jelenti

$G$  egy halmaz

$\cdot$  függvény  $(\cdot : G \times G \rightarrow G)$  két művelet

vagyis egy  $M \subseteq G$

$\cdot$ -t megmutatjuk  $M \times M$ -ra

$\cdot|_{M \times M} : M \times M \rightarrow G$  de ha  $M$ -ben lenne akkor  $\cdot$  magánítva  $M \times M$ -ra akkor művelet lenne  $M$ -n

Egy műveletet tessék fel egy  $\cdot|_{M \times M}$ -ra művelet  $M$ -n

van egy halmaz  $M$

van egy művelet  $\cdot|_{M \times M}$

megmutatjuk  $(M, \cdot|_{M \times M})$

Csoport-e?

Ha van akkor azt mondjuk egy  $M$  részcsoportha  $G$ -nek

Példa

1,  $G = \{0, 1, 2, 3\}$

$\cdot$  művelet  $G$ -n

$\cdot$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

00	→ 0
01	1
02	2
03	3
10	1
11	2
12	3
13	0
↓	↓



$$H = \{0, 3\}$$

$$\text{Hogy n\u00e9z} \quad \cdot \mid M \times M = *$$

$$\text{azaz } M \times M \rightarrow G \text{ f\u00fcggv\u00e9ly}$$

•	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- \u00e9nt\u00e9rt\u00e9slete nem  $M$   
\* nem ~~id\u00e9~~  $G$ -a

az nem n\u00edvelet  $M$ -n

is nem n\u00e9zessz\u00e1rta  $G$ -n\u00e9z

~~$$H = \{0, 2, 3\}$$~~

*	0	3
0	0	3
3	3	2

$$K = \{0, 2\}$$

$$\text{Hogy n\u00e9z} \quad \cdot \mid K \times K = \otimes$$

•	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

⊗	0	2
0	0	2
2	2	0

⊗ n\u00edvelet  $K$ -n

H\u00e1r sz\u00e9l a sz\u00e1r \u00e1ll\u00e1nd\u00edthat  
v\u00e9ll \u00e1ll\u00e1nd\u00edthat.

⊗ n\u00edvelet  $K$ -n ✓

⊗ asszociat\u00edv ✓

$$(x \otimes y) \otimes z = x \otimes (y \otimes z) \text{ minden } x, y, z \in K$$

$(0 \otimes 0) \otimes 0$	$0$	$0(0 \otimes 0)$	$0$
$(0 \otimes 0) \otimes 2$	$2$	$0(0 \otimes 2)$	$2$
$(0 \otimes 2) \otimes 0$	$2$	$0(2 \otimes 0)$	$2$
$(0 \otimes 2) \otimes 2$	$0$	$0(2 \otimes 2)$	$0$
$(2 \otimes 0) \otimes 0$	$2$	$2(0 \otimes 0)$	$2$
$(2 \otimes 0) \otimes 2$	$0$	$2(0 \otimes 2)$	$0$
$(2 \otimes 2) \otimes 0$	$0$	$2(2 \otimes 0)$	$0$
$(2 \otimes 2) \otimes 2$	$2$	$2(2 \otimes 2)$	$2$

negat\u00edv asszociat\u00edv \u00e1ll

Egys\u00e9gism

0 egys\u00e9gism

1-es (minden elemre kell ennie)

n\u00edvelet \u00e1ll\u00e1nd\u00edthat

$$0^{-1} = 0 \quad 2^{-1} = 2$$

$K$ -n\u00e9zessz\u00e1rta  $G$ -n\u00e9z

Részesen értelmezve tovább alsó

- (1)  $M \neq \emptyset$
  - (2)  $a \in M \Rightarrow a^{-1} \in M$
  - (3)  $a, b \in M \Rightarrow ab \in M$
- } ita 3 dolgot kell vizsgálni

Tétel: Legyen  $G$  egy csoport  $M \subseteq G$  f.e. (1)(2)(3) áll  $\Rightarrow M$  részcsoport  $G$ -ben

Bizonyítás: Kétféle lenne egy  $|M \times M|$ -ra művelet  $M$ -n

- 1)  $*$  asszociatív  $\checkmark$  ~~asszociatív~~  $*$
- 2, van egységelem  $(M, *)$
- 3, van inverz  $(M, *)$ -ben

1, Ha lenne  $x, y, z \in M$

$$x * y * z = x * (y * z)$$

ebből egy lenne  $G$ -ben

2, Legyen  $e$  a  $G$  egységeleme

$$M \neq \emptyset \Rightarrow \text{van } a \in M \Rightarrow a^{-1} \in M$$

$\downarrow$   
2a b-heli inverz

$$a, a^{-1} \in M \Rightarrow a a^{-1} \in M$$

$$e \in M$$

$$e \cdot b = b$$

$$b \cdot e = b$$

mivel  $b \in M$

## MELLÉKOSZTÁLYOK

$(G, \cdot)$  csoport

$M \subseteq (M \times M)$  részcsoport

Értelmezve egy relációt az  $a \equiv b$  szorron

$$a \equiv b \pmod{M} \Leftrightarrow a b^{-1} \in M$$

$$1 \equiv 3 \pmod{4}$$

$$1 \cdot 3^{-1} = 1 \cdot 1 = 2 \in 4$$

Állítás:  $\equiv$  ekvivalencia reláció

Bizonyítás:

1) reflexív

$$a \equiv a \pmod{M} \text{ mivel } a \in M$$

$a$

$$\underbrace{a a^{-1}}_e \in M$$

$$2, \equiv \text{szimmetrikus} \quad a \equiv b \pmod{M} \Rightarrow b \equiv a \pmod{M}$$

$$a \cdot b^{-1} \in M$$

$$a \cdot b^{-1} \in M$$

$$b \cdot a^{-1} \in M$$

$$(a \cdot b^{-1})^{-1} = (b^{-1})^{-1} (a^{-1}) = b \cdot a^{-1} \in M$$

3,  $\equiv$  Transzitiv

$$a \equiv b \pmod{M}, b \equiv c \pmod{M} \Rightarrow a \equiv c \pmod{M}$$

$$a \cdot b^{-1} \in M$$

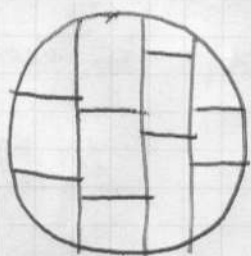
$$b \cdot c^{-1} \in M$$

$$(a \cdot b^{-1}) (b \cdot c^{-1}) \in M$$

$$[a(b^{-1}b)]c^{-1} \in M$$

$$a \cdot c^{-1} \in M$$

A  $\mathbb{G}$ -Halmaz fel van bontva ekvivalencia osztályokra



$$[a] = \{x : a \equiv x \pmod{M}\}$$



az  $a$  elem ekvivalencia osztálya

Hogyan néz ki  $[a]$ ?

$$x \in [a] \Leftrightarrow a \equiv x \pmod{M}$$

$$a \cdot x^{-1} \in M \Rightarrow a \cdot x^{-1} = h$$

$$(a \cdot x^{-1}) \cdot x = h \cdot x$$

$$a(x^{-1}x) = h \cdot x$$

$$a = h \cdot x$$

$$h^{-1}a = h^{-1}(h \cdot x)$$

$$h^{-1}a = (h^{-1}h) \cdot x$$

$$h^{-1}a = x$$

$$\text{Szállás } [a] = M_a$$

$$M_a = \{ha : h \in M\}$$

Bizonyítás  $[a] \subset M_a$  és  $[a] \supset M_a$

valamint  $x \in [a]$  és látjuk, hogy  $x \in M_a$

$$a \equiv x \pmod{M} \Rightarrow a \cdot x^{-1} \in M \Rightarrow a \cdot x^{-1} = h \Rightarrow a = h \cdot x$$

EH

$\sim$

$\sim$

$\sim$



~~h~~

$$h \Rightarrow a = hx \Rightarrow h^{-1}a = x \Rightarrow x \in H_a$$

$G$ -egy sorát  $M$  részesít

$A$   $M$  részi felbontási mellékrendű  $G$ -egy partíciója



$G_S$  derék mellékrendű uniója

$$G = Ma_1 \cup \dots \cup Ma_s$$

$a_1, a_2, \dots, a_s$  elemek teljes reprezentációt nyújt az  $M$  modulo  $M$

Transzformáció is bijektív.

$S$ : mellékrendű része  $H$   $G$ -ben valóban is bijektív

$$\text{Teljes } |G:M| \text{ v. } (G/M)$$

Lemma:  $A$  számítható mellékrendűben azonos méretű elem van

$$(|Ma_1| = |Ma_2| \text{ minden } a_1, a_2 \in G)$$

speciálisan  $|M \cdot a| = |M|$

Bizonyítás

Definíció egy  $f: M \rightarrow Ma$

$$f(h) = ha \text{ megmutatjuk hogy } f \text{ egy bijektív}$$

$$\text{In } f = Ma$$

Sőt az kell már hogy  $f$  1-1

$$f(h_1) = f(h_2) \Rightarrow h_1 = h_2$$

$$h_1 a = h_2 a \Rightarrow h_1 = h_2$$

(Bízzunk benne  $a^{-1}$ -vel felbontás)

III. Lagrange tétele:

Méretű  $G$ -ben

Legyen  $G$  egy véges csoport, akkor  $|G| = |M| |G:M|$

speciálisan  $|M| \mid |G|$

Bizonyítás: Bontsuk fel  $G$ -t  $M$  méretű felbontási mellékrendűre

$$G = Ma_1 \cup \dots \cup Ma_s$$

$$|G| = |Ma_1| + \dots + |Ma_s| \text{ mert } Ma_i \text{ k disjointok}$$

$$|G| = \underbrace{|M| + \dots + |M|}_s \text{ mert } |Ma_i| = |M|$$

$$De s = |G:M|$$

$$|G| = |M|s$$

$$|G| = |M| |G:M|$$

# ELEM RENDJE

$G$  csoport

$a \in G$ .

$a$  rendje egy nem negatív egész  $n$ .

~~úgyis teljesül  $a^0 = e$  és  $a^n \neq e$~~

úgyis teljesül  $a^n = e$  és  $a^m \neq e$  ha  $1 \leq m \leq n-1$

Ha  $a^n$  csak nem  $e$  akkor a rendje  $\infty$

jelölés  $|a|$  v.  $o(a)$

Tétel: Ha  $a^m = e$  akkor  $|a| \mid m$

Bizonyítás: Legyen  $|a| = n$ .

Lehetne legyen  $n \nmid m$

Összead el  $m$ -t  $n$ -el maradékosan

az  $q, r \in \mathbb{Z}$  amire  $m = nq + r$   $0 \leq r \leq n-1$

Számoljuk ki  $a^m$ -t

$$a^m = a^{nq+r} = a^{nq} \cdot a^r = \underbrace{(a^n)^q} \cdot a^r = a^r$$

$$\text{De } a^m = e \quad a^r = e$$

$a$  rendje  $n$

$$a^n = e \quad \text{és} \quad a^r \neq e \quad \text{ha} \quad 1 \leq r \leq n-1 \Rightarrow r = 0$$

$$\text{Így } m = nq \Rightarrow n \mid m$$

Tétel: Ha  $a$  rendje  $n$ , akkor  $a^{\frac{n}{d}}$  rendje

$$\frac{n}{d} \text{ ahol } d = \text{lko}(2, n)$$

Bizonyítás:

$$\text{Legyen } d = \text{lko}(2, n)$$

Legyen  $a^{\frac{n}{d}}$  rendje  $m$

$$\text{Lehetne } m = \frac{n}{d}$$

Standard trükk  $m \mid \frac{n}{d}$  és  $\frac{n}{d} \mid m$

$$\text{Számoljuk ki } (a^{\frac{n}{d}})^{\frac{n}{d}} = a^{\frac{n}{d} \cdot \frac{n}{d}} = a^{\frac{n^2}{d^2}} = \underbrace{(a^n)^{\frac{n}{d^2}}} = e$$

$$\text{Ebből következik } m \mid \frac{n}{d}$$

vésszer  $(a^2)^m = e$  ~~azaz  $a^{2m} = e$~~

$\Rightarrow a^{2m} = e$

$n/2 \cdot m \Rightarrow \left(\frac{n}{d}\right) \left\| \left(\frac{2}{d}\right) m\right.$

hellyen  $\frac{n}{d} \mid m$

Emelkedés:  $a \mid b \cdot c$   $b$  relatív prím  $a$ -val  
 akkor  $a \mid c$

$1 = u \cdot a + v \cdot b \Rightarrow c = \underbrace{u \cdot a \cdot c}_{a \mid} + \underbrace{v \cdot b \cdot c}_{a \mid} \Rightarrow a \mid c$

Tudjuk hogy  $\text{sz}(n/2) = d$

$\text{sz}\left(\frac{n}{d}, \frac{2}{d}\right) = 1$

$\frac{n}{d}$  és  $\frac{2}{d}$  relatív prímek

$\left(\frac{n}{d}\right) \left\| \left(\frac{2}{d}\right) m \Rightarrow \frac{n}{d} \mid m$  ✓

Tétel  $G$  egy véges csoport  $a \in G$   
 akkor  $|a| \mid |G|$

Bizonyítás: Lagrange tételét egyszerűen bebizonyítani

ahogy kell egy  $M$  részre az egyszerűen tagozható  $n$   
 legyen  $M = \{e, a, a^2, \dots, a^{n-1}\}$

Állítom  $M$  részre az  $a$ -ról

(1)  $M \neq \emptyset$  ✓

(2)  $u, v \in M \Rightarrow u \cdot v \in M$  ✓

(3)  $u \in M \Rightarrow u^{-1} \in M$  ✓

$\underbrace{u}_{a^i} \underbrace{v}_{a^j} \in M$   
 $a^i \cdot a^j$

Számoljuk ki  $uv = a^i a^j = a^{i+j}$

$a^{-1} = a^{n-i}$



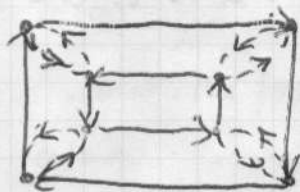
Hány eleme van  $M$ -nek?

$$|M| = n$$

Lagrange tétele miatt  $|M| \mid |G|$

$$n \mid 6 \Rightarrow |G| \mid 6$$

## CAYLEY GRÁFOK



2 egy gráf

8 csomópont van

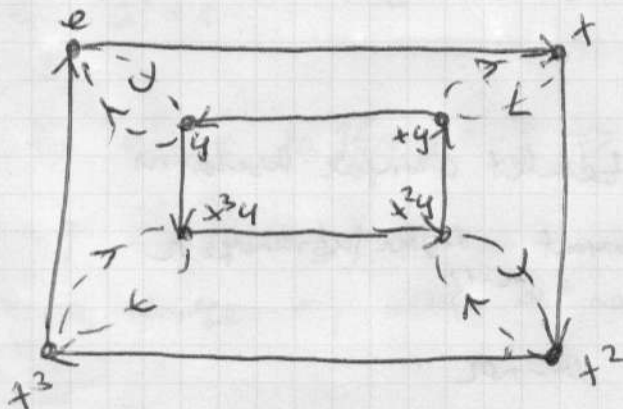
először: 8 rel és 8 megfigyelhető irányított

2 egy 8 elemű csoport része

$$a \xrightarrow{b} b = ax$$

$$c \xrightarrow{d} d = cy$$

A gráf 1 mentéssel is leírható:  $e \rightarrow a$



diéder csoport

A csoport elemei:

$$e, x, x^2, x^3, y, xy, x^2y, x^3y$$

6 szorzótábla:

rel  
major egy feladat  
de nem

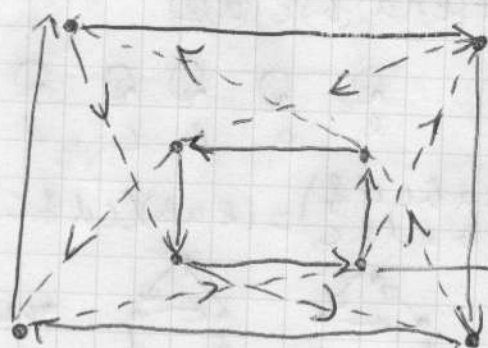
$$(xy)(x^2y) = (xy)x \cdot y = x^3$$

ide tart az egyen

$$(x^3y)x^3$$

	$e$	$x$	$x^2$	$x^3$	$y$	$xy$	$x^2y$	$x^3y$
$e$								
$x$								
$x^2$								
$x^3$								
$xy$								
$x^2y$								
$x^3y$								

A graféket meg lehet vizsgálni a normalitásra.



Geometrical Space

if vanulhat az en az a rendjét

## NORMALIS RÉSZESPORT

G-csoport

$M$  a  $G$  részcsoportja

Azt mondjuk legrs  $M$  normális részcsoportja  $G$ -nek ha

$Hg = gH$  minden  $g \in G$ -re

↓

mondjuk  $M = \{h_1, \dots, h_s\}$

$Hg = \{h_1g, h_2g, \dots, h_sg\}$

$gH = \{g \cdot h_1, g \cdot h_2, \dots, g \cdot h_s\}$

$Hg = gH$

de az nem feltétlenül áll legrs  
 $h_1g = gh_1$

Ször mindig rendezhetjük legrs az első lista a második lista  
egy permutációval

I. Példa  $G$ -t a Cayley gráfjával adhat meg



Mit  $G$  elemei?

$G = \{e, u, u^2, uv, uv^2, u^2v\}$

legrs van az  $G$  normalitására

	e	u	u <sup>2</sup>	uv	uv <sup>2</sup>	u <sup>2</sup> v
e	e	u	u <sup>2</sup>	v	uv	u <sup>2</sup> v
u	u	u <sup>2</sup>	e	uv	u <sup>2</sup> v	v
u <sup>2</sup>	u <sup>2</sup>	e	u	u <sup>2</sup> v	v	uv
uv	v	u <sup>2</sup> v	uv	e	u <sup>2</sup>	u
u <sup>2</sup> v	uv	v	u <sup>2</sup> v	u	e	u <sup>2</sup>
u <sup>2</sup> v	u <sup>2</sup> v	uv	v	u <sup>2</sup>	u	e

	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	f	d	e	b	a
d	d	c	f	a	e	b
f	f	d	c	b	a	e

$$(e a b c d f) = (e a b c d f) = (e)(a)(b)(c)(d)(f)$$

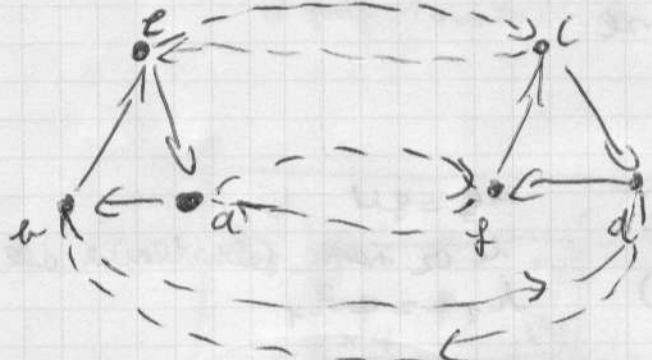
$$(e a b c d f) = (e a b c d f)$$

$$(e a b c d f) = (e a b c d f)$$



2. egy szimmetrikus reláció

$$(e a b c d f) = (e c)(a f)(b d)$$



Legyen  $M = \{e, v\}$

allítás  $M$  a  $G$  részreláció

1.  $H \neq \emptyset$
2.  $a, b \in M \Rightarrow ab \in M$

a	b	ab
e	e	e
e	v	v
v	e	v
v	v	e

3.  $a \in M \Rightarrow a^{-1} \in M$

a	$a^{-1}$
e	e
v	v



Normális-e  $M$ ?

$Mg \stackrel{?}{=} gH$  minden  $g \in G$ -re

$g$	$\overset{2g,vg}{\overbrace{Mg}}$	$\overset{ge,gv}{\overbrace{gH}}$	
$e$	$eV$	$eV$	✓
$u$	$u, u^2V$	$u, uV$	szé nem egyenlő
$u^2$			
$\vdots$			

$M$  nem normális

definiáljuk  $K = \{e, u, u^2\}$

Nézzük meg  $K$ -t,

(1)  $K \neq \emptyset$  ✓

(2)  $a, b \in K \Rightarrow a \cdot b \in K$

$a$	$b$	$ab$
$e$	$e$	$e$
$e$	$u$	$u$
$e$	$u^2$	$u^2$
$u^2$	$e$	$u^2$
$u^2$	$u$	$u$
$u^2$	$u^2$	$e$

}  $\in K$

$K$  a  $G$  normális résnégyesével.

(3)  $a \in K \Rightarrow a^{-1} \in K$

$a$	$a^{-1}$
$e$	$e$
$u$	$u^2$
$u^2$	$u$

}  $\in K$

$K$  szint az  $G$  inverzártányos

$K$  résnégyes  $G$ -re

Normális-e  $K$ ?

$Kg = gK$  minden  $g \in G$ -re

$g$   ~~$Kg$~~   $Kg$   
 $\{eg, ug, u^2g\}$  }

	$Kg$			$gk$			
$g$	$e$	$u$	$u^2$	$e$	$u$	$u^2$	
$e$	$e$	$u$	$u^2$	$e$	$u$	$u^2$	✓
$u$	$u$	$u^2$	$e$	$u$	$u^2$	$e$	✓
$u^2$	$u^2$	$e$	$u$	$u^2$	$e$	$u$	✓
$v$	$v$	$uv$	$u^2v$	$v$	$u^2v$	$uv$	✓
$uv$	$uv$	$u^2v$	$v$	$uv$	$v$	$u^2v$	✓
$u^2v$	$u^2v$	$v$	$uv$	$u^2v$	$uv$	$v$	✓

$K$  Normális négyzetes  $G$ -ra

## Faktor csoportok

Egy csoport részhalmaza

$G$  csoport

$M$  normális részcsoport  $G$ -ben

Most egy új csoport részhalmaza

$M$  az új csoport

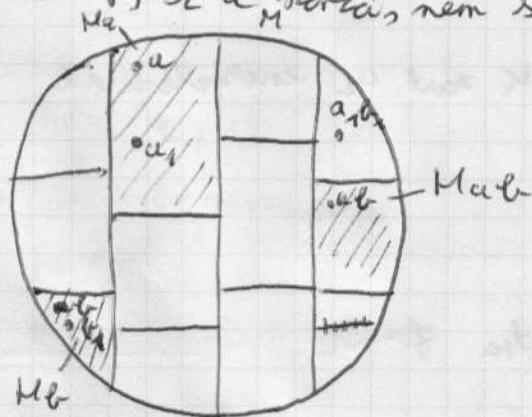
Melanci  $a \in G$   $M$  részcsoport mellékletét (transzfer felelőse)

$$M = \{Ma : a \in G\}$$

Művelet  $M$ -ben

$$(M \cdot a)(M \cdot b) = M \cdot ab$$

Lehet hogy az  $a$  része, nem is lehet?



$Ma = Ma_1$   $Mb = Mb_1$  mert  $a_1 b_1 = b$   
Lehet h.  $a_1 b_1 \in Ma b$

Kellene egy  $a_1 b_1 \in Ma b$

Tudjuk hogy  $a \in Ma$   $a_1 \in Ma \Rightarrow a_1 = h_1 a$

$b \in Mb$   $b_1 \in Mb$

$$\Rightarrow b_1 = h_2 b$$

Számok ri

$$(Ma)(Mb) = [M(z_1, a)] [M(z_2, b)] = [M(z_1, a)] [M(z_2, b)] = (Ma)(Mb) = \\ = Mab$$

Teljes a rendszer értelmezése:

Kellene hogy  $M$  értelmezés a rendszerre legyen.

(1) A rendszernek egy művelet

$M \times M \rightarrow M$  alakú függvény  
↑  
egyetlen  $M$ -ben  $M$ -ra alakú

$$(Ma)(Mb) = \underline{Mab} \text{ az alakú}$$

(2) A művelet asszociatív

$$\underline{[(Ma)(Mb)]} Mc = (Ma) \underline{[(Ma)(Mc)]} \\ (Mab) Mc = (Ma) (Mbc) \\ Mabc = Mabc$$

(3)  $M$ -ben van egységelem

$Me$  az egységelem

$$(Me)(Ma) = Ma \text{ és } (Ma)(Me) = Ma$$

$$Mea = Ma$$

$$Ma = Ma$$

(4)  $M$ -ben minden elemnek van inverze

A  $Ma$  elem inverze  $Ma^{-1}$

$$(Ma)(Ma^{-1}) = Me \text{ és } (Ma^{-1})(Ma) = Me$$

$$Ma a^{-1}$$

$$Me$$

Jelölés:  $M$ -t  $G/M$ -vel jelöljük

$G$  az  $M$  rendszer generátorja

Mivel  $M$  az  $M$ -vel osztott  $M$ -t nem kell osztani és így

VEGE