

Discrete Mathematics III

ALGEBRA Group Theory

Gabor Farkas

farkasg@inf.elte.hu

gaborfarkasphd.wixsite.com/gaborfarkasphd

Spring 2017
ELTE

Ha A tetszőleges halmaz, akkor egy **A -n értelmezett n -ér műveleten (n -változós műveleten)** egy

$$f: (A^n =) A \times A \cdots \times A \rightarrow A$$

függvényt értünk ahol $A^n = A \times A \cdots \times A$ és $n \in \mathbb{N}_0$.

Ha $x_1, x_2, \dots, x_n \in A$, akkor

$f(x_1, x_2, \dots, x_n)$ a művelet **eredménye**,

míg $x_1, x_2, \dots, x_n$ a művelet **operandusai**.

Az (A, Ω) pár **algebrai struktúra**, ha az A nem üres halmaz, és

Ω az A -n értelmezett véges változós műveletek halmaza.

Szokásos jelölés, ha Ω 1 vagy 2 elemű: $(A, \otimes)$, ill. $(A, \oplus, \otimes)$,
ahol $\otimes, \oplus$ A -n értelmezett n -ér műveletek.

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

Def

Ha $\otimes$ egy A -n értelmezett n -ér művelet, akkor mondjuk, hogy
 $\otimes$ **zárt A -n** (**A zárt a $\otimes$ műveletre nézve**), azaz
 $\forall x_1, x_2, \dots, x_n \in A$ esetén $x_1 \otimes x_2 \otimes \dots \otimes x_n \in A$.

Def

Egy $(G, \cdot)$ algebrai struktúrát, amelyben $\cdot$ binér művelet,
grupoidnak nevezünk.

Def

Egy $(G, \cdot)$ grupoidban a műveletet

asszociatívnek 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 is következik, hogy $a = b$.

Def

Legyen $(G, \cdot)$ és $(G', \otimes)$ két grupoid. A $\varphi : G \rightarrow G'$ függvényt

homomorfizmusnak nevezzük, ha **művelettartó**, vagyis

$$\forall a_1, a_2 \in G : \varphi(a_1 a_2) = \varphi(a_1) \otimes \varphi(a_2).$$

Def

Epimorfizmus: szürjektív homomorfizmus.

Monomorfizmus: injektív homomorfizmus.

Izomorfizmus: bijektív homomorfizmus.

Endomorfizmus: ha $G = G'$.

Automorfizmus: ha $G = G'$ és bijektív.

Lemma

Homomorfizmusok összetétele is homomorfizmus.
Izomorfizmus inverze is izomorfizmus.

Biz

Legyen $\varphi : G_1 \rightarrow G_2$ és $\rho : G_2 \rightarrow G_3$ két homomorfizmus. Ekkor

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

Továbbá

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

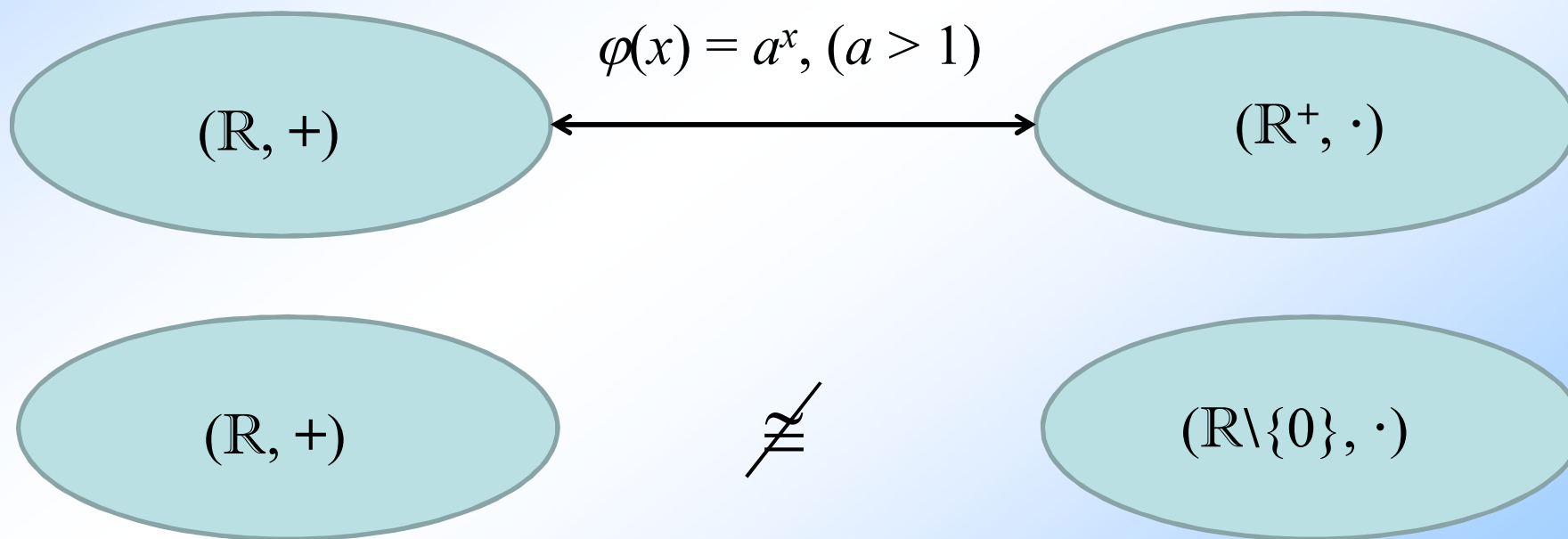


Def

$\varphi : G \rightarrow G'$ homomorfizmus esetén $\varphi(G)$ a **G homomorf képe**.

Def

Ha $(G, \cdot)$ és $(G', \otimes)$ grupoidokra $\exists \varphi : G \rightarrow G'$ izomorfizmus, akkor G és G' **izomorf**, jelben $G \cong G'$.



Def

A $(G, \cdot)$ grupoid **félcsoporth**, ha $\cdot$ asszociatív.

Egy félcsoporth **monoid**, ha egységelemes.

Def

A $(G, \cdot)$ félcsoporthban

$e_b \in G$ **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 $a e_j = a$.

$e \in G$ **egységelem**, ha egyszerre bal és jobb oldali egységelem.

$$G = \left\{ \begin{pmatrix} a & b \\ a & b \end{pmatrix}, \text{ ahol } a, b \text{ valós} \right\}$$

G félcsoporth a mátrixszorzással.

$$\begin{pmatrix} x & y \\ x & y \end{pmatrix} \text{ Baloldali egységelem,} \\ \text{ha } x + y = 1.$$

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

Def

Legyen a $(G, \cdot)$ félcsoporthban e egységelem. Ekkor az $a \in G$ elemnek

$a_b \in G$ **balinverze**, ha $a_b a = e$,

$a_j \in G$ **jobbinverze**, ha $aa_j = e$,

$a' \in G$ **inverze**, ha $aa' = a'a = e$.

Legyen $(G, \cdot)$ félcsoporthban e_b baloldali egységelem. Az $a \in G$ elemnek

$a_b \in G$ az e_b -re vonatkoztatott **balinverze**, ha $a_b a = e_b$,

illetve az e_b -re vonatkoztatott **jobbinverze**, ha $aa_b = e_b$.

A bal- és jobbinverz fogalma jobboldali egységelemre hasonlóan.

Tétel (egységelem és inverz félcsoporthban)

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

Biz

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

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

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 $a_b = a_j$:

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



Tétel (félcsoport homomorf képe)

Legyen G félcsoport φ homomorfizmussal.

(i) $\varphi(G)$ is félcsoport.

(ii) Ha $e \in G$ egységelem*, akkor $\varphi(e)$ egységelem* $\varphi(G)$ -ben.

(iii) Ha $e \in G$ egységelem és g inverze* g' , akkor $\varphi(G)$ -ben $\varphi(g)$ inverze* $\varphi(g')$.

(iv) Ha $a, b \in G$ felcserélhető, akkor $\varphi(G)$ -ben $\varphi(a)$ és $\varphi(b)$ felcserélhető.

* a jelzett fogalmak jobb-, ill. baloldali verziójukkal helyettesíthetők.



Legyen $a, b, c \in G$.

$$(i) (\varphi(a)\varphi(b))\varphi(c) = \varphi(ab)\varphi(c) = \varphi(abc) = \\ = \varphi(a)\varphi(bc) = \varphi(a)(\varphi(b)\varphi(c))$$

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

$$\varphi(g)\varphi(e) = \varphi(ge) = \varphi(g)$$

(iii) Ha g -nek g' a jobb oldali inverze, akkor

$$\varphi(g)\varphi(g') = \varphi(gg') = \varphi(e)$$

(iv) Ha g és h felcserélhető, akkor

$$\varphi(g)\varphi(h) = \varphi(gh) = \varphi(hg) = \varphi(h)\varphi(g)$$



Def(csoport I. definíciója)

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:

$$a_b a = e_b.$$

Def(csoport III. definíciója)

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 :

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

Def(csoport III. definíciója)

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.

Def(csoport IV. definíciója)

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)

A csoport négy adott definíciója ekvivalens.

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. $\Rightarrow$ 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

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

Az $ya = b$ esetben hasonlóan bizonyítunk.

III. $\Rightarrow$ IV. Az állítás nyilvánvaló.

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.



Lemma(csoport regularitása)

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.



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

Tekintsük a $(H, \cdot)$ algebrai struktúrát, ahol $H = \{a, b, c\}$.

Műveleti tábla

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

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

Invertálható, egyértelmű.

Nincs egységelem! Nincs inverz!

Hogy fordulhat ez elő?

Válasz: nem asszociatív a művelet:

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

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

Példák

csoportokra

(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 $n = 1, 2, \dots$, 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.

Csoport hierarchia



Def

Legyen $(G, \cdot)$ grupoid, továbbá $H \subseteq G$.

H -t a G **részgrupoidjának** nevezzük, ha a G -beli művelettel maga is grupoidot alkot.

Hasonlóan, definiáljuk a többi tanult struktúra részstruktúráját is.

Jelölés: $H \leq G$, ha H **részstruktúrája** G -nek.

Ha $H \neq G$, akkor **valódi részstruktúráról** beszélünk.

Ha $H = G$ vagy $H = \{e\}$ akkor H **triviális részstruktúra**.

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

Komplexus szorzás:

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

Lemma(komplexusok félcsoportja)

H csoport komplexusai a komplexusszorzásra monoidot alkotnak.

Biz

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

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

$$\begin{aligned} K(LM) &= \{k \cdot (l \cdot m) \mid k \in K, l \in L, m \in M\} = \\ &= (KL)M = \{(k \cdot l) \cdot m \mid k \in K, l \in L, m \in M\} \end{aligned}$$

3. Egységelem: $E = \{e\}$, ahol e a H -beli egységelem, mivel tetszőleges $K \in \mathbf{P}$ 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 (4 ekvivalens állítás részcsoporthokra)

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

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

(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

$$e_G k = k.$$

$$\text{regularitás} \Rightarrow e_G = e_H$$

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

$$k_H^{-1},$$

G -ben pedig

$$k_G^{-1}.$$

A következő összefüggéseknek teljesülnie kell:

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

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

(2) $\Rightarrow$ (3):

Triviális

(3) $\Rightarrow$ (4):

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

(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. $k, l \in H \Rightarrow kl \in H$?

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

$\Rightarrow$

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



Ész

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

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

Lemma(részcsoporthat metszete)

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

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

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

$$\text{Tétel} \Rightarrow D \leq G.$$



Részcsoporthok 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 $L = \{e, b\}$
részcsoporthai H -nak, de

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

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

G -nek a K halmazt tartalmazó
legsűkebb részcsoportha

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

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

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

ahol az üres szorzat G egységeleme.

Biz

Legyen

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

1. Nyilvánvaló, 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

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



Ész

(1) Egy G csoport tetszőleges g eleme generál egy ciklikus csoportot:

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

(2) Ciklikus csoport homomorf képe is ciklikus csoport, ahol a generálóelem 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.

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

Példa: $(R^*, \cdot)$ csoportban $|+1| = 1$, $|-1| = 2$, a többi elem végtelenrendű.

Ész

$g \in G$ elem rendje megegyezik a $\langle g \rangle$ részcsoporthal.

Tétel (ciklikus csoportok izomorfája)

Végtelen ciklikus csoport izomorf az egész számok additív csoportjával, míg egy n elemű ciklikus csoport a modulo n maradékosztályok $\mathbb{Z}_n$ additív csoportjával izomorf.

Biz

1. Végtelen eset

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

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

Izomorf leképezés hozható létre köztük:

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

$n, m \in \mathbb{Z}$ 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

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

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

Miért ?

A különbözőség n minimális voltából következik.

Vizsgáljuk az előbbi φ függvényt.

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

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

$\Rightarrow$

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

Mindezek alapján a $(*)$ elemek alkotják a csoportot.

Vizsgáljuk továbbá a következő függvényt: $\varphi'(x \pmod n) = \varphi(x) = g^r$.

φ' izomorfizmus a $(\text{mod } n)$ maradékosztályok additív csoportja és $(*)$ halmaz között.

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



Ész

A ciklikus csoportok kommutatívak, hiszen

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

Tétel (ciklikus csoport részcsoportha)

Ciklikus csoport minden részcsoportha 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:

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

$\Rightarrow$

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

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

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

inverzek

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



Tétel (Ciklikus részcsoporthok generálása)

Legyen G egy n -edrendű véges ciklikus csoport, g generátorral.

(1) Ha $a \in \mathbb{Z}$ és $d = \text{lko}(a, n)$ akkor g^a az egyetlen
$$\langle g^a \rangle = H = \{g^d, g^{2d}, \dots, g^{md} = e\}$$
 m -rendű részcsoporthot generálja, ahol $n = md$.

(2) A G minden részcsoporthja előáll így valamely $d|n$ -re.

Biz

Tétel (Ciklikus csoport részcsoporthja) $\Rightarrow$

$\exists$ ilyen d , méghozzá a legkisebb pozitív egész, amelyre $g^d \in H$, ekkor
 $\langle g^d \rangle = H = \{g^d, g^{2d}, \dots, g^{md} = e\}.$

$$\Rightarrow g^a = (g^d)^q \Rightarrow \langle g^a \rangle \subseteq H.$$

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

$$g^d = g^{ax + ny} = g^{ax} g^{ny} = g^{ax} e^y = (g^a)^x \Rightarrow H \subseteq \langle g^a \rangle$$



Lemma (generáló elemek száma)

Egy G n -edrendű véges ciklikus csoportnak $\varphi(n)$ generátor eleme van.

Biz

Legyen $\langle g \rangle = G$.

Minden generátor elem felírható g^a alakban valamely $a \in \mathbb{Z}$ -re:

Tétel (ciklikus részcsoporthok generálása) $\Rightarrow$

$$\langle g^a \rangle = \{g^d, g^{2d}, \dots, g^{md} = e\},$$

ahol $d = \text{lko}(a, n)$ és $n = md$.

A g^a pontosan akkor lesz generátor elem, ha $d = 1$, mivel ekkor $n = m$,

azaz G minden eleme benne van $\langle g^a \rangle$ -ban.

φ definíciója szerint $\varphi(n)$ ilyen a szám van.



Def

Legyen $(G, \cdot)$ csoport, $H \leq G$, és $a \in G$. Ekkor az

$aH = \{ak \mid k \in H\}$ komplexus egy a

G csoport H részcsoportha szerinti bal,

$Ha = \{ka \mid k \in H\}$ komplexus pedig a jobb oldali mellékosztálya.

Tétel (Mellékosztályok)

Adott részcsoportha szerinti mellékosztályok osztályozzák a csoport elemeit.

Biz

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

$\sim$ ekvivalencia reláció

1. Reflexív ?

✓

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

2. Szimmetrikus ?

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

✓

3. Tranzitív ?

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

✓

Tetszőleges $a \in G$ -re $a \sim b \Leftrightarrow b \in Ha$.

Tfh $b \in Ha$

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

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

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

Tfh $a \sim b$

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

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

Baloldali esetben hasonlóan bizonyíthatunk.



Def

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

Lemma(mellékosztályok száma)

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

Biz

A következő leképezés bijeció a jobb, illetve bal oldali mellékosztályok halmaza között:

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



Def

Legyen G csoport és $H \leq G$. A H szerinti mellékosztályok halmazának számossága **H indexe** (lehet ∞ is) G -ben. Jelölése: $|G : H|$, $[G : H]$.

Tétel (Lagrange)

Legyen G véges csoport és $H \leq G$, ekkor $|G| = |H| \cdot |G : H|$.

Biz

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

ahol R egy bal oldali reprezentánsrendszere H -nak.

Legyen $\varphi(h) = ah \Rightarrow \varphi$ 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 $\Rightarrow h_1 = h_2 \Rightarrow |H| = |rH|$

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



Lemma(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.



Tétel (prímszámrendű csoport)

Egy nem egyelemű csoport prímszámrendű

$\Leftrightarrow$ ha csak triviális részcsoportha van.

Biz

$\Rightarrow :$

Lemma(A Lagrange tétel következményei) $\Rightarrow$

ha G prímszámrendű, akkor ciklikus és a részcsoporthok:

$\{e\}$ és maga a G .

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

$\Rightarrow \langle a \rangle = G$

$\Rightarrow G$ ciklikus.

1. Kérdés: Lehet-e $|G| = \infty$?

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

2. Kérdés: Lehet-e $|G| = \text{nem prím}$?

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

$$\langle a^{n_i} \rangle \leq G,$$

mert

$$(a^{n_i})^{n_1 n_2 \dots n_{i-1} n_{i+1} \dots n_k} = e.$$



Def

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

Tétel (normálosztók ekvivalens definíciói)

Legyen G csoport és $N \leq G$. Ekkor a következő feltételek ekvivalensek:

- (1) N normálosztó.
- (2) $\forall a \in G: a^{-1}Na = N$.
- (3) $\forall a \in G: a^{-1}Na \subseteq N$.

Biz

(1) $\Rightarrow$ (2)

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

(2) $\Rightarrow$ (1)

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

(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 $\Rightarrow$

$$a \rightarrow (a^{-1})^{-1}Na^{-1} \subseteq N$$

$$N = a^{-1}(aNa^{-1})a \subseteq a^{-1}Na.$$

$$\Rightarrow a^{-1}Na = N$$



Ész

Hasonló módon bizonyítható, mint részcsoporthok esetében, hogy normálosztók metszete is normálosztó.

Tétel (normálosztó szerinti osztályozás)

Csoportban egy N normálosztó szerinti mellékosztályok a csoport elemeinek a művelettel kompatibilis osztályozását alkotják.

Biz

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

$$Na' = Na \text{ és } Nb' = Nb$$

$\Rightarrow$

$$\begin{aligned} a'b' &\in (Na')(Nb') = (Na)(Nb) = N(aN)b = \\ &= N(Na)b = N^2ab = Nab \end{aligned}$$

tehát $a'b' \sim ab$.



Tétel (művelettel kompatibilis osztályozás)

Csoportban minden, a művelettel kompatibilis osztályozás esetén az egységelem osztálya normálosztó, és az osztályokat ezen normálosztó szerinti mellékosztályok alkotják.

Biz

Tfh $\exists$ a művelettel kompatibilis osztályozás és legyen N az e egységelem osztálya, ekkor

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

$$b \in N \Rightarrow ab \sim ee = e \Rightarrow NN \subseteq N \Rightarrow N \text{ részcsoport}$$

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

$$\Rightarrow g^{-1}Ng \subseteq N \Rightarrow N \text{ normálosztó.}$$

Mik az ekvivalencia osztályok?

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

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

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



Lemma(művelet mellékosztályok között)

Csoport normálosztó szerinti osztályozása esetén az osztályok közötti művelet megegyezik az osztályok mint halmazok komplexusszorzásával.

Biz

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



Lemma(faktorcsoporth)

Csoportban egy normálosztó szerinti mellékosztályok a komplexusszorzással csoportot alkotnak.

Biz

Az $a \mapsto Na$ kanonikus leképezés homomorf

Tétel (félcsoport homomorf képe) $\Rightarrow$ a homomorf kép is csoport.



Def

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

Def

Egy G csoportnak egy G' csoportba való φ homomorfizmusánál a **homomorfizmus magján** a G' csoport e' egységelemének teljes inverz képét értjük, jelben $\ker(\varphi)$.

Tétel (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 .

$$G = (\mathbb{Z}, +)$$

..., -3, -2, -1, 0, 1, 2, 3, ...

..., -2, 0, 2, ...

$\ker(\varphi)$

φ

φ^{-1}

v

páros

páratlan

$0 + \ker(\varphi)$

$1 + \ker(\varphi)$

$$a' \mapsto \varphi^{-1}(a')$$

$$G' = \varphi(G)$$

$$G / \ker(\varphi)$$

Biz

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

Kompatibilis a szorzással?

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

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

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

szerinti

Tétel (művelettel kompatibilis osztályozás) $\Rightarrow$

e osztálya, azaz $\ker(\varphi)$, normálosztó $\Rightarrow$

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

Lemma(faktorcsoporth) $\Rightarrow$

A tétel második fele.

