Algebra és számelmélet előadás

Waldhauser Tamás
2016. november 3.

4. Csoportok

A csoport fogalma, izomorfia

A csoport definíciója

4.1. Definíció.

(0) Az egyetlen kétváltozós művelettel rendelkező algebrát grupoidnak nevezzük. Tehát $\mathbb{A} = (A; *)$ grupoid, ha A nemüres halmaz és $*\colon A^2 \to A$ kétváltozós művelet A-n.

(1) Ha egy grupoid művelete asszociatív, akkor félcsoportnak nevezzük.

(2) Ha egy félcsoportotban van egységelem, akkor monoidnak nevezzük. Tehát az $\mathbb{A} = (A; *)$ félcsoport akkor monoid, ha létezik olyan $e \in A$ elem, amelyre

$$\forall a \in A : \ a * e = e * a = a.$$

(3) Ha egy monoidban minden elemnek van inverze, akkor csoportnak nevezzük. Tehát az $\mathbb{A} = (A; *)$ monoid (e egységelemmel) akkor csoport, ha

$$\forall a \in A\ \exists b \in A : \ a * b = b * a = e.$$

(4) Ha egy csoport művelete kommutatív,akkor Abel-csoportnak nevezzük.

Egységelem és inverz unicitása

4.2. Állítás.

1. Bármely grupoidban legföljebb egy egységelem létezhet.
2. Bármely monoidban egy elemnek legföljebb egy inverze lehet.

Bizonyítás.

1. Ha e_1 és e_2 is egységelem az $(A;*)$ grupoidban, akkor
   - $e_1 * e_2 = e_1$ (mert e_2 egységelem), és
   - $e_1 * e_2 = e_2$ (mert e_1 egységelem).
   - Tehát $e_1 = e_2$.
2. Ha az a elemnek inverze b és c is, akkor
   - $(b * a) * c = e * c = c$, és
   - $b * (a * c) = b * e = b$.
   - Tehát $b = b * (a * c) = (b * a) * c = c$. $\square$

4.3. Megjegyzés.

Ha a művelet nem asszociatív, akkor létezhet egy elemnek több inverze is.
(HF: Keressünk ilyen példákat!)

Csoport-e?

Példa.

Csoport-e az alábbi művelettáblázattal megadott $(\{a, b, c, d\}\,; *)$ grupoid?

$$
\begin{array}{c|cccc}
* & a & b & c & d \\
\hline
a & a & b & c & d \\
b & b & c & d & a \\
c & c & d & a & b \\
d & d & a & b & c
\end{array}
\quad \cong \quad
\begin{array}{c|cccc}
 & 0 & 1 & 2 & 3 \\
\hline
0 & 0 & 1 & 2 & 3 \\
1 & 1 & 2 & 3 & 0 \\
2 & 2 & 3 & 0 & 1 \\
3 & 3 & 0 & 1 & 2
\end{array}
$$

(0) Minden $x, y \in \{a, b, c, d\}$ esetén $x * y$ értelmezett, és $x * y \in A$. ✓

(1) Az asszociativitást körülményes ellenőrizni, de teljesül. ✓

(2) Egységelem: a. ✓

(3) Inverzek: a inverze a, b inverze d, c inverze c, d inverze b. ✓

Tehát ez egy Abel-csoport.

Nevezzük át az elemeket: $a \mapsto 0$, $b \mapsto 1$, $c \mapsto 2$, $d \mapsto 3$.
Így már látható, hogy a $(\mathbb{Z}_4; +)$ csoporttal van dolgunk (álruhában):
$(\{a, b, c, d\}\,; *)$ és $(\mathbb{Z}_4; +)$ izomorfak.

Invertálhatóság és kancellativitás

4.4. Definíció.

Legyen $*$ egy kétváltozós művelet a nemüres A halmazon.

1. $*$ invertálható művelet, ha bármely $a, b \in A$ elemek esetén az $a * x = b$, illetve $y * a = b$ egyenleteknek legalább egy megoldása van.

2. $*$ kancellatív művelet, ha bármely $a, b \in A$ elemek esetén az $a * x = b$, illetve $y * a = b$ egyenleteknek legfeljebb egy megoldása van.

4.5. Megjegyzés.

A kancellativitás így is megfogalmazható: $\forall a, u, v \in A:$

$$a * u = a * v \implies u = v;$$

$$u * a = v * a \implies u = v.$$

Megjegyzés.

Az invertálhatóság azt jelenti, hogy a művelettáblázat minden sorában és minden oszlopában az A halmaz minden eleme legalább egyszer fellép.
A kancellativitás pedig azt jelenti, hogy minden sorban és minden oszlopban minden elem legfeljebb egyszer lép fel.

Invertálhatóság és kancellativitás

4.7. Állítás.

Véges alaphalmaz esetén az invertálhatóság és a kancellativitás egymással ekvivalens.

Bizonyítás.

Skatulya-elv. (HF) $\square$

4.6. Tétel.

Csoport művelete mindig invertálható és kancellatív. Fordítva, minden invertálható művelettel rendelkező félcsoport csoport.

Bizonyítás.

Tfh. $(A; *)$ csoport, és legyen $a, b \in A$. Ekkor

$$a * x = b \quad \Longrightarrow \quad x = a^{-1} * b \quad \ldots\ldots\text{(balról beszorzunk } a^{-1}\text{-zel);}$$

$$x = a^{-1} * b \quad \Longrightarrow \quad a * x = b \quad \ldots\ldots\ldots\text{(balról beszorzunk } a\text{-val).}$$

Tehát az $a * x = b$ egyenlet egyetlen megoldása $x = a^{-1} * b$.
Hasonlóan: az $y * a = b$ egyenlet egyetlen megoldása $y = b * a^{-1}$.

A másik állítást nem bizonyítjuk. $\square$

Nyolcadik házi feladat az előadásra

Egészítse ki a táblázatot úgy, hogy egy csoport művelettáblázatát kapjuk. (Melyik ismert csoporttal izomorf ez a csoport?)

$\cdot$	e	a	b	x	y	z
e	e					
a		b	e	y		
b						
x		z		e		
y						
z						

- beküldendő emailben: `twaldha@math.u-szeged.hu`
- pdf fájl legyen (lehet szkennelt is)
- fájlnév: `EHA-eahf8.pdf` (például `WATHAAS-eahf8.pdf`)
- határidő: november 16, reggel 8 óra

Izomiaúrfizmus

$\leftrightarrow$	igaz	hamis
igaz	igaz	hamis
hamis	hamis	igaz

$\cdot$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$
$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$
$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$

izomorf csoportok

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\otimes$		
		
		

Izomiaúrfizmus

Az $\mathbb{A} = (\{$  ,  $\}; \otimes)$ és a $\mathbb{B} = (\{\bar{0}, \bar{1}\}\,; +)$ csoportok szerkezete ugyanaz: ha $\mathbb{A}$ művelettáblázatában
minden -t átnevezünk $\bar{0}$-ra , és minden -t átnevezünk $\bar{1}$-re,
akkor éppen $\mathbb{B}$ művelettáblázatát kapjuk:

$\otimes$		
		
		

$\xrightarrow{\text{átnevezés}}$

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

Ezt az „átnevezést” a

$\varphi\colon \{$  ,  $\} \to \{\bar{0}, \bar{1}\}$,  $\mapsto \bar{0}$,  $\mapsto \bar{1}$

leképezéssel írhatjuk le. Az átnevezés „jogossága” pedig a következőképpen fogalmazható meg:

$\forall a_1, a_2 \in \{$  ,  $\} : \quad (a_1 \otimes a_2)\,\varphi \;=\; (a_1\varphi) + (a_2\varphi)\,.$

Izomorfizmus

4.8. Definíció.

Legyen $\mathbb{A} = (A; *)$ és $\mathbb{B} = (B; \oplus)$ két csoport (vagy csak grupoid).
Azt mondjuk, hogy a $\varphi \colon A \to B$ leképezés izomorfizmus $\mathbb{A}$-ból $\mathbb{B}$-be, ha

- φ bijektív leképezés, és
- φ felcserélhető a műveletekkel, azaz

$$\forall a_1, a_2 \in A : \quad (a_1 * a_2)\,\varphi \;=\; a_1\varphi \oplus a_2\varphi.$$

Ha létezik $\varphi \colon \mathbb{A} \to \mathbb{B}$ szürjektív izomorfizmus, akkor azt mondjuk, hogy
$\mathbb{A}$ és $\mathbb{B}$ *izomorf* (jelölés: $\mathbb{A} \cong \mathbb{B}$).

Példa.

- $\varphi \colon\ (\mathbb{C}; +) \to (\mathbb{C}; +)\,,\ z \mapsto \overline{z}$
- $\varphi \colon\ (\mathbb{C}; \cdot) \to (\mathbb{C}; \cdot)\,,\ z \mapsto \overline{z}$
- $\varphi \colon\ (\mathbb{R}^+; \cdot) \to (\mathbb{R}; +)\,,\ x \mapsto \log x$

Házi feladat a gyakorlatra

25. feladat. Döntse el, hogy a művelettáblázat által meghatározott $\mathbb{A}$ grupoid izomorf-e a $\mathbb{B}$ grupoiddal.

(a)

$\cdot$	u	v	x	y
u	y	u	v	x
v	u	v	x	y
x	v	x	y	u
y	x	y	u	v

$\mathbb{B} = (\mathcal{P}(\{a, b\}); \cup)$

Nem, mert $\forall z \in B\colon z \cup z = z$, de $\exists z \in A\colon z \cdot z \neq z$.

(b)

$\cdot$	u	v	x	y
u	y	u	v	x
v	u	v	x	y
x	v	x	y	u
y	x	y	u	v

$\mathbb{B} = (\mathbb{Z}_4; +)$

Igen, pl. $u \mapsto \overline{3}, v \mapsto \overline{0}, x \mapsto \overline{1}, y \mapsto \overline{2}$.

Házi feladat a gyakorlatra

25. feladat. Döntse el, hogy a művelettáblázat által meghatározott $\mathbb{A}$ grupoid izomorf-e a $\mathbb{B}$ grupoiddal.

(c)

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\mathbb{B} = (\{1, i, -1, -i\}; \cdot)$

(d)

$\circ$	α	β	γ	δ
α	δ	β	α	γ
β	β	β	β	β
γ	α	β	γ	δ
δ	γ	β	δ	δ

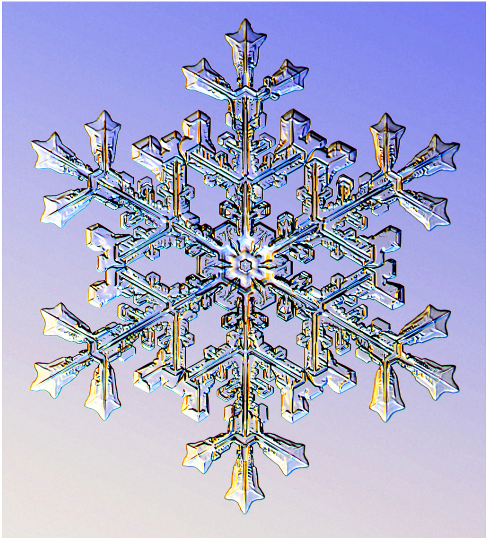
$\mathbb{B} = (\mathbb{Z}_5^*; \cdot)$

(e)

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\mathbb{B} = (\{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}; \cdot)$

Nevezetes példák



Gyűrűből csoport

4.9. Példa.

Tetszőleges gyűrű Abel-csoportot alkot az összeadás műveletével, és tetszőleges egységelemes gyűrű egységei csoportot alkotnak a szorzás műveletével.
(HF: Keressünk konkrét példákat!).

4.10. Definíció.

Ha G egy csoport, és a $H \subseteq G$ halmaz is csoportot alkot a G-ből „örökölt" művelettel, akkor azt mondjuk, hogy H *részcsoportja* G-nek. (Pontosabban lásd a 4.43. Definícióban.)

Számhalmazok az összeadás műveletével

Példa.

Az alábbi H számhalmazok közül melyek alkotnak csoportot a szokásos összeadásra nézve?

- $H = \emptyset$: nem (nem is grupoid)
- $H = \{0\}$: igen (Abel-csoport)
- $H = \mathbb{C},\ \mathbb{R},\ \mathbb{Q},\ \mathbb{Z}$: igen (Abel-csoport)
- $H = \mathbb{R}^+,\ \mathbb{Q}^+,\ \mathbb{N}$: nem (csak félcsoport)
- $H = \{\text{páros számok}\}$: igen (Abel-csoport)
- $H = \{\text{páratlan számok}\}$: nem (nem is grupoid)
- $H = \{\text{irracionális számok}\}$: nem (nem is grupoid)
- $H = \{\text{véges tizedestörtek}\}$: igen (Abel-csoport)

Számhalmazok a szorzás műveletével

Példa.

Az alábbi H számhalmazok közül melyek alkotnak csoportot a szokásos szorzásra nézve?

- $H = \emptyset$: nem (nem is grupoid)
- $H = \{1\}$: igen (Abel-csoport)
- $H = \mathbb{C},\ \mathbb{R},\ \mathbb{Q},\ \mathbb{Z}$: nem (csak monoid)
- $H = \mathbb{C} \setminus \{0\},\ \mathbb{R} \setminus \{0\},\ \mathbb{Q} \setminus \{0\}$: igen (Abel-csoport)
- $H = \mathbb{Z} \setminus \{0\}$: nem (csak monoid)
- $H = \mathbb{R}^+,\ \mathbb{Q}^+$: igen (Abel-csoport)
- $H = \mathbb{N}$: nem (csak monoid)
- $H = \{\text{irracionális számok}\}$: nem (nem is grupoid)
- $H = \{\text{véges tizedestörtek}\} \setminus \{0\}$: nem (csak monoid)

4.11. Példa.

Tetszőleges T test esetén a T feletti $n \times n$-es mátrixok gyűrűjének egységcsoportja a T feletti n-dimenziós *általános lineáris csoport* (jelölés: $\mathrm{GL}_n(T)$), ebben az 1 determinánsú mátrixok alkotta részcsoport a megfelelő *speciális lineáris csoport* (jelölés: $\mathrm{SL}_n(T)$):

$$\mathrm{GL}_n(T) = \{A \in T^{n \times n} : \det(A) \neq 0\},$$
$$\mathrm{SL}_n(T) = \{A \in T^{n \times n} : \det(A) = 1\}.$$

Házi feladat a gyakorlatra

26. feladat. Döntse el, hogy az alábbi halmazok grupoidot, félcsoportot, csoportot alkotnak-e a megadott művelettel.

(a) $(\mathcal{P}(\{a, b\}); \triangle)$, $(\mathbb{Z}_5^*; +)$

$(\mathcal{P}(\{a, b\}); \triangle)$ csoport, $(\mathbb{Z}_5^*; +)$ nem is grupoid

(b) $(\mathbb{R}^{2\times 2}; +)$, $(\mathbb{R}^{2\times 2}; \cdot)$

$(\mathbb{R}^{2\times 2}; +)$ csoport, $(\mathbb{R}^{2\times 2}; \cdot)$ csak monoid

(c) $(\mathbb{Z}_6 \setminus \{0\}; \cdot)$

(d) $(\mathcal{P}(\{a, b\}); \cap)$

(e) $(\mathbb{R}^4; +)$

Házi feladat a gyakorlatra

27. feladat. Adja meg az alábbi S_7-beli permutációkat páronként idegen ciklusok szorzataként.

(a) $((1342)(237))^{126}(3476)^{-1}$

(3674)

(b) $((13)(15)(276))^{-10}(125)(63)$

$(23)(567)$

(c) $(345)((7451)^{-1}(4256))^{83}$

(d) $((124)^{35}(134))^{-4}(27)$

(e) $((1247)^{-6}(154)^{103})^{-100}$