

Általános algebra

2013 március 8.

1. Algebrai struktúra, izomorfizmus
2. Részalgebra, generálás
3. Kongruencia, faktoralgebra
4. Homomorfizmus, homomorfizmatétel

1. Algebrai struktúra, izomorfizmus

2. Részalgebra, generálás

3. Kongruencia, faktoralgebra

4. Homomorfizmus, homomorfizmatétel

Definíció

Algebrai struktúrán egy $\mathbb{A} = (A; F)$ párt értünk, ahol A nemüres halmaz, F pedig az A halmazon értelmezett műveletek egy halmaza. Az A halmazon értelmezett n -változós **művelet**:

$$f: A^n \rightarrow A, (a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n).$$

Példa

- ▶ Kétváltozós művelet: $f: A^2 \rightarrow A, (a_1, a_2) \mapsto a_1 * a_2$.
Az egész számok halmazán az összeadás (kivonás, szorzás) kétváltozós művelet:

$$+: \mathbb{Z}^2 \rightarrow \mathbb{Z}, (a_1, a_2) \mapsto a_1 + a_2.$$

- ▶ Egyváltozós művelet: $f: A \rightarrow A$.
A nemnulla determinánsú 2×2 -es valós mátrixok halmazán az inverzképzés egyváltozós művelet:

$$^{-1}: GL_2(\mathbb{R}) \rightarrow GL_2(\mathbb{R}), M \mapsto M^{-1}.$$

Nullaváltozós művelet (?!):

$$f: A^0 \rightarrow A, a \mapsto f(a).$$

Mivel $A^0 = \{\heartsuit\}$ (egyelemű halmaz), a nullaváltozós f műveletet egyértelműen meghatározza az $f(\heartsuit) \in A$ elem.

Tehát egy nullaváltozós művelet nem más, mint az alaphalmaz egy elemének kijelölése.

Példa

Az egész számok gyűrűje: $(\mathbb{Z}; \{+, \cdot\}) = (\mathbb{Z}; +, \cdot)$, ahol

$$+: \mathbb{Z}^2 \rightarrow \mathbb{Z}, (a_1, a_2) \mapsto a_1 + a_2,$$

$$\cdot: \mathbb{Z}^2 \rightarrow \mathbb{Z}, (a_1, a_2) \mapsto a_1 \cdot a_2.$$

Időnként hasznos az additív inverz képzését (egyváltozós művelet) és az additív egységelemet (nullaváltozós művelet) is belefoglalni a struktúrába: $(\mathbb{Z}; \{+, \cdot, -, 0\}) = (\mathbb{Z}; +, \cdot, -, 0)$, ahol

$$-: \mathbb{Z} \rightarrow \mathbb{Z}, a \mapsto -a,$$

$$0: \mathbb{Z}^0 \rightarrow \mathbb{Z}, \heartsuit \mapsto 0.$$



algebrai struktúrák



\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 struktúrák






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

\otimes		
		
		

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

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

$\xrightarrow{\text{átnevezés}}$

\otimes		
		
		

Ezt az „átnevezést” a

$$\varphi: \{\bar{0}, \bar{1}\} \rightarrow \{\text{tulipán}, \text{liliom}\}, \quad \bar{0} \mapsto \text{tulipán}, \quad \bar{1} \mapsto \text{liliom}$$

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

$$\forall a_1, a_2 \in \{\bar{0}, \bar{1}\} : (a_1 + a_2) \varphi = (a_1 \varphi) \otimes (a_2 \varphi).$$

Definíció

Legyen $\mathbb{A} = (A; *)$ és $\mathbb{B} = (B; \oplus)$ két **grupoid**, azaz egyetlen kétváltozós művelettel felszerelt halmaz. Azt mondjuk, hogy a $\varphi: A \rightarrow B$ leképezés **izomorfizmus** \mathbb{A} -ból \mathbb{B} -be, ha

1. φ bijektív leképezés, és
2. φ **felcserélhető a műveletekkel**, azaz

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

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

Megjegyzés

Az izomorfizmus tetszőleges algebrákra hasonló módon definiálható: a φ leképezésnek az algebrák minden műveletével felcserélhetőnek kell lennie.

Például $\mathbb{A} = (A; +, \cdot)$ és $\mathbb{B} = (B; +, \cdot)$ esetén:

$$\forall a_1, a_2 \in A : (a_1 + a_2) \varphi = a_1 \varphi + a_2 \varphi, \text{ és}$$

$$\forall a_1, a_2 \in A : (a_1 \cdot a_2) \varphi = a_1 \varphi \cdot a_2 \varphi.$$

Tétel

Izomorfizmusok szorzata (azaz egymásutánja), valamint izomorfizmus inverze szintén izomorfizmus.

Biz.

HF [Sz] X. fejezet, 1.14. Tétel. □

Következmény

Az izomorfia ekvivalenciareláció (pl. grupoidok bármely halmazán).

Biz.

HF [Sz] X. fejezet, 1.15. Következmény. □

Az izomorfizmusok minden „algebrai” tulajdonságot megőriznek. Ha két algebra izomorf, akkor a szerkezetük teljesen egyforma, legfeljebb csak az elemeik „természetében” különbözhetnek. Ezért az algebrai vizsgálatokban izomorf struktúrákat nem szükséges/érdemes/lehetséges egymástól megkülönböztetni.

Példa

Izomorf-e egymással a következő két grupoid?

$\mathbb{A} =$	$*$	a	b	c	$\mathbb{B} =$	\oplus	1	2	3
	a	a	c	c		1	3	2	2
	b	b	b	b		2	2	2	2
	c	c	a	c		3	2	2	3

- ▶ Nem, mert \oplus **kommutatív** művelet ($\forall x, y \in A : x * y = y * x$), míg $*$ nem az. (HF)
- ▶ Nem, mert \mathbb{A} -ban a **baloldali egységelem** ($\forall x \in A : a * x = x$), míg \mathbb{B} -ben nincs ilyen elem. (HF)
- ▶ Nem, mert \mathbb{B} -ben 2 **zéruselem** ($\forall x \in B : b * 2 = 2 * x = 2$), míg \mathbb{A} -ban nincs ilyen elem. (HF)
(Vegyük észre, hogy b csak **jobb oldali zéruselem** \mathbb{A} -ban.)
- ▶ Nem, mert $*$ **idempotens** művelet ($\forall x \in A : x * x = x$), míg \oplus nem az. (HF)

Példa

Izomorf-e egymással a következő két grupoid?

$$\mathbb{A} =$$

\circ	a	b	c	d
a	a	c	a	b
b	b	c	d	d
c	d	d	c	b
d	a	c	b	d

$$\mathbb{B} =$$

\diamond	α	β	γ	δ
α	α	β	α	γ
β	γ	β	δ	δ
γ	α	γ	β	δ
δ	β	δ	γ	α

Nem, mert \mathbb{A} -ban az a elem csak úgy bontható „szorzatra”, hogy az egyik tényező maga a :

$$\forall x, y \in A : x \circ y = a \implies x = a \text{ vagy } y = a,$$

míg \mathbb{B} -ben nincs ilyen tulajdonságú elem. (HF)

Példa

Izomorf-e egymással a következő két grupoid?

	\cdot	a	b	c	d		\cdot	p	q	r	s
	a	a	b	c	d		p	q	p	s	s
$\mathbb{A} =$	b	b	b	b	b	$\mathbb{B} =$	q	p	q	r	s
	c	c	b	c	a		r	q	r	r	s
	d	d	b	b	a		s	s	s	s	s

Talán igen ... Tegyük fel, hogy $\varphi: \mathbb{A} \rightarrow \mathbb{B}$ izomorfizmus.

- ▶ \mathbb{A} -ban a az egységelem, \mathbb{B} -ben pedig q , ezért $a\varphi = q$. (HF)
- ▶ \mathbb{A} -ban b a zéruselem, \mathbb{B} -ben pedig s , ezért $b\varphi = s$. (HF)
- ▶ \mathbb{A} -ban $c^2 = c$, míg d^2 az egységelem.
 \mathbb{B} -ben $r^2 = r$, míg p^2 az egységelem.
Ezért $c\varphi = r$ és $d\varphi = p$. (HF)

Példa (folyt.)

Tehát ha létezik egyáltalán $\varphi: \mathbb{A} \rightarrow \mathbb{B}$ izomorfizmus, akkor ez csak a következő lehet:

$$a\varphi = q, \quad b\varphi = s, \quad c\varphi = r, \quad d\varphi = p.$$

Próbáljuk ki, hogy ez a leképezés izomorfizmus-e:

$$\begin{array}{c}
 \mathbb{A} = \\
 \cdot \mid a \quad b \quad c \quad d \\
 \hline
 a \mid a \quad b \quad c \quad d \\
 b \mid b \quad b \quad b \quad b \\
 c \mid c \quad b \quad c \quad \mathbf{a} \\
 d \mid d \quad b \quad \mathbf{b} \quad a
 \end{array}
 \xrightarrow{\varphi}
 \begin{array}{c}
 \mathbb{A}\varphi = \\
 \cdot \mid q \quad s \quad r \quad p \\
 \hline
 q \mid q \quad s \quad r \quad p \\
 s \mid s \quad s \quad s \quad s \\
 r \mid r \quad s \quad r \quad \mathbf{q} \\
 p \mid p \quad s \quad \mathbf{s} \quad q
 \end{array}
 \parallel
 \begin{array}{c}
 \mathbb{B} = \\
 \cdot \mid p \quad q \quad r \quad s \\
 \hline
 p \mid q \quad p \quad \mathbf{s} \quad s \\
 q \mid p \quad q \quad r \quad s \\
 r \mid \mathbf{q} \quad r \quad r \quad s \\
 s \mid s \quad s \quad s \quad s
 \end{array}$$

Példa

Izomorf-e egymással a következő két grupoid?

$$\mathbb{A} =$$

\cdot	a	b	c	d
a	a	b	c	d
b	b	b	b	b
c	c	b	c	a
d	d	b	b	a

$$\mathbb{B} =$$

\cdot	p	q	r	s
p	q	p	s	s
q	p	q	r	s
r	s	r	r	s
s	s	s	s	s

Az előbbi megfigyeléseink most is érvényesek, ezért φ -re megint csak ugyanaz az egy lehetőség van. De ez a φ leképezés most nem lesz izomorfizmus (HF leellenőrizni).

Már csak azért sem lehet a két grupoid izomorf, mert \mathbb{B} kommutatív, de \mathbb{A} nem az.

Példa

Izomorf-e egymással $(\mathbb{R}; +)$ és $(\mathbb{R}^+; \cdot)$?

Igen, $\varphi: \mathbb{R} \rightarrow \mathbb{R}^+, x \mapsto e^x$ izomorfizmus közöttük.

Példa

Izomorf-e egymással $(\mathbb{Q}; +)$ és $(\mathbb{Q}^+; \cdot)$?

Nem, mert az $x * x = a$ egyenlet az első grupoidban minden a -ra megoldható, a másodikban pedig nem:

$$\forall a \in \mathbb{Q} \exists x \in \mathbb{Q} : x + x = a \quad \text{teljesül,}$$

$$\text{de } \forall a \in \mathbb{Q}^+ \exists x \in \mathbb{Q}^+ : x \cdot x = a \quad \text{nem teljesül.}$$

Ha $\varphi: (\mathbb{Q}; +) \rightarrow (\mathbb{Q}^+; \cdot)$ izomorfizmus lenne, akkor létezne olyan $u \in \mathbb{Q}$ szám, amelyre $u\varphi = 2$ (mert φ szürjektív).

Ekkor a $v = \frac{u}{2}\varphi \in \mathbb{Q}^+$ számra azt kapnánk, hogy

$$v^2 = v \cdot v = \frac{u}{2}\varphi \cdot \frac{u}{2}\varphi = \left(\frac{u}{2} + \frac{u}{2}\right)\varphi = u\varphi = 2,$$

ami ellentmond $\sqrt{2}$ irracionálisának.

1. Algebrai struktúra, izomorfizmus

2. Részalgebra, generálás

3. Kongruencia, faktoralgebra

4. Homomorfizmus, homomorfizmatétel

Definíció

Legyen $\mathbb{A} = (A; *)$ egy grupoid, és $B \subseteq A$. Azt mondjuk, hogy a B halmaz **zárt** a $*$ műveletre, ha

$$\forall b_1, b_2 \in B : b_1 * b_2 \in B.$$

Ha B **nemüres** zárt halmaz, akkor B grupoidot alkot a $*$ művelettel (pontosabban annak B -re való megszorításával).

Ezt a $\mathbb{B} = (B; *)$ grupoidot \mathbb{A} **részgrupoidjának** nevezzük.

Jelölés $\mathbb{B} \leq \mathbb{A}$.

Megjegyzés

- ▶ Tetszőleges algebra esetén hasonlóan definiálható a zárt részhalmaz (zárt minden műveletre) és a **részalgebra** fogalma.
- ▶ Ha $a \in A$ egy nullaváltozós művelet, akkor minden zárt részhalmaznak tartalmaznia kell az a elemet. Ebben az esetben a zárt részhalmazok ugyanazok, mint a részalgebrák tartóhalmazai.
- ▶ Ha viszont az \mathbb{A} algebrának nincs nullaváltozós művelete, akkor az üres halmaz zárt, de nem alkot részalgebrát.

Példa

Részalgebrát alkot-e a B halmaz az alábbi grupoidban?

$$\mathbb{A} = \begin{array}{c|cccc} \cdot & a & b & c & d \\ \hline a & a & b & c & b \\ b & b & b & b & b \\ c & c & b & c & a \\ d & d & b & b & a \end{array}$$

- ▶ $B = \emptyset$: zárt, de nem részalgebra.
- ▶ $B = \{c, d\}$: nem, mert $c \cdot d = a \notin \{c, d\}$.
- ▶ $B = \{a, b\}$: igen, mert $a \cdot a, a \cdot b, b \cdot a, b \cdot b \in \{a, b\}$.
- ▶ $B = \{a, b, d\}$: igen, mert ...
- ▶ $B = \{a, c, d\}$: nem, mert $d \cdot c = b \notin \{a, c, d\}$.
- ▶ $B = \{d\}$: nem, mert $d \cdot d = a \notin \{d\}$.

Tétel

Zárt részhalmazok metszete is zárt. Precízebben:

Ha \mathbb{A} egy algebra, és $B_i \subseteq A$ zárt részhalmaz minden $i \in I$ indexre, akkor $\bigcap_{i \in I} B_i$ is zárt.

Biz.

Csak grupoidra: legyen $\mathbb{A} = (A; *)$.

Legyenek $b_1, b_2 \in \bigcap_{i \in I} B_i$ tetszőleges elemek.

Ekkor minden i -re $b_1, b_2 \in B_i$ teljesül.

Mivel B_i zárt, ebből $b_1 * b_2 \in B_i$ következik.

Ez minden $i \in I$ esetén fennáll, ezért $b_1 * b_2$ benne van a B_i halmazok metszetében. □

Definíció

Legyen $\mathbb{A} = (A; *)$ egy grupoid, és $\emptyset \neq B \subseteq A$. A B halmaz által **generált részgrupoidon** azt a $([B]; *)$ grupoidot értjük, melynek tartóhalmaza a B halmazt tartalmazó összes zárt halmazok metszete:

$$[B] = \bigcap_{\substack{B \subseteq S \subseteq A \\ \overline{S} \text{ zárt}}} S.$$

Megjegyzés

Hasonló módon definiálható a **generált részalgebra** fogalma.

Ha nincsenek nullaváltozós műveletek, akkor $[\emptyset] := \emptyset$,

ha pedig vannak, akkor $[\emptyset]$ legyen a nullaváltozós műveletek által kijelölt elemek halmaza.

Definíció

Ha $[B] = A$, akkor azt mondjuk, hogy B **generátorrendszere** az \mathbb{A} algebrának.

Tétel

Tetszőleges \mathbb{A} algebra és $\emptyset \neq B \subseteq A$ esetén $[B]$ a **legszűkebb** olyan zárt halmaz, ami B -t tartalmazza.

Biz.

Az világos, hogy $[B]$ zárt és tartalmazza B -t. Azt kell belátnunk, hogy $[B]$ része minden B -t tartalmazó zárt halmaznak.

Emlékeztetőül:

$$[B] = \bigcap_{\substack{B \subseteq S \subseteq A \\ \overline{S} \text{ zárt}}} S.$$

Legyen C egy tetszőleges zárt halmaz, ami tartalmazza B -t. Ekkor C szerepel a $[B]$ -t definiáló fenti metszetben, ezért

$$[B] = \bigcap_{\substack{B \subseteq S \subseteq A \\ \overline{S} \text{ zárt}}} S \subseteq C.$$



Tétel

Tetszőleges \mathbb{A} algebra és $\emptyset \neq B \subseteq A$ esetén $[B]$ mindazon elemekből áll, amelyek B elemeiből kiindulva megkaphatók az \mathbb{A} algebra műveleteinek (véges számú) alkalmazásával.

Biz.

Csak grupoidra: legyen $\mathbb{A} = (A; *)$. Jelöljük \widehat{B} -pal azon elemek halmazát, amelyek megkaphatók B elemeiből. Megmutatjuk, hogy \widehat{B} nem más, mint a B -t tartalmazó legszűkebb zárt halmaz.

1. $\widehat{B} \supseteq B$: Világos.
2. \widehat{B} zárt: Tfh. $b_1, b_2 \in \widehat{B}$, mondjuk b_i megkapható B elemeiből kiindulva a $*$ művelet k_i -szer történő alkalmazásával ($i = 1, 2$). Ekkor $b_1 * b_2$ megkapható B elemeiből kiindulva a $*$ művelet $(k_1 + k_2 + 1)$ -szer történő alkalmazásával. Tehát $b_1 * b_2 \in \widehat{B}$.
3. \widehat{B} a legszűkebb: Tfh. $B \subseteq C \subseteq A$ és C zárt. Mivel C zárt, és tartalmazza B elemeit, tartalmaznia kell az összes olyan elemet, ami megkapható B elemeiből kiindulva a $*$ művelet véges sokszori alkalmazásával. Tehát $\widehat{B} \subseteq C$. □

Példa

Határozzuk meg a megadott halmazok által generált részgrupoidot az alábbi grupoidban.

$$\mathbb{A} = \begin{array}{c|cccc} \cdot & a & b & c & d \\ \hline a & a & b & c & b \\ b & b & b & b & b \\ c & c & b & c & a \\ d & d & b & b & a \end{array}$$

- ▶ $[\emptyset] = \emptyset$, de ez nem alkot grupoidot.
- ▶ $[c, d] = \{c, d, a, b\}$ ($a = d \cdot d$, $b = d \cdot c$)
- ▶ $[a, b] = \{a, b\}$ (már eleve zárt volt)
- ▶ $[a, b, d] = \{a, b, d\}$ (már eleve zárt volt)
- ▶ $[a, c, d] = \{a, c, d, b\}$ ($b = a \cdot d$)
- ▶ $[d] = \{d, a, b\}$ ($a = d \cdot d$, $b = a \cdot d$)

Példa

Határozzuk meg a B részhalmaz által generált részgrupoidot az \mathbb{A} grupoidban.

- ▶ $B = \{2\}$, $\mathbb{A} = (\mathbb{Z}; \cdot)$
 $[B] = \{2, 4, 8, 16, \dots\}$
- ▶ $B = \{\text{prímszámok}\}$, $\mathbb{A} = (\mathbb{Z}; \cdot)$
 $[B] = \{2, 3, 4, 5, \dots\}$
- ▶ $B = \{\text{prímszámok}\}$, $\mathbb{A} = (\mathbb{Z}; +)$
 $[B] = \{2, 3, 4, 5, \dots\}$
- ▶ $\mathbb{A} = (\mathcal{P}(\mathbb{N}); \cap)$ $B = \{\text{kételemű halmazok}\}$,
 $[B] = \{\text{legfeljebb kételemű halmazok}\}$
- ▶ $\mathbb{A} = (\mathcal{P}(\mathbb{N}); \Delta)$ $B = \{\text{kételemű halmazok}\}$,
 $[B] = \{\text{páros elemszámú véges halmazok}\}$

Definíció

Tetszőleges \mathbb{A} algebra esetén $\text{Sub}(\mathbb{A})$ jelöli \mathbb{A} összes zárt részhalmazainak halmazát. A $(\text{Sub}(\mathbb{A}); \subseteq)$ részbenrendezett halmazt \mathbb{A} **részalgebrahálójának** nevezzük.

Megjegyzés

Ha \mathbb{A} -nak nincs nullaváltozós művelete, akkor $\emptyset \in \text{Sub}(\mathbb{A})$, de \emptyset nem részalgebra. Ennek ellenére — az egyszerűség kedvéért — ilyenkor is részalgebrahálóról beszélünk.

Általában **hálónak** olyan részbenrendezett halmazt neveznek, amelyben bármely két elemnek létezik legkisebb közös felső korlátja (supremuma) és legnagyobb közös alsó korlátja (infimuma).

Bármely $B, C \in \text{Sub}(\mathbb{A})$ esetén

$$\sup(B, C) = [B \cup C] =: B \vee C,$$

$$\inf(B, C) = B \cap C =: B \wedge C.$$

Példa

Határozzuk meg az alábbi grupoid összes részalgebráját, és rajzoljuk fel a részalgebraháálót.

$$\mathbb{A} = \begin{array}{c|cccc} \cdot & a & b & c & d \\ \hline a & a & b & c & b \\ b & b & b & b & b \\ c & c & b & c & a \\ d & d & b & b & a \end{array}$$

Először számítsuk ki az egyes elemek generátumait:

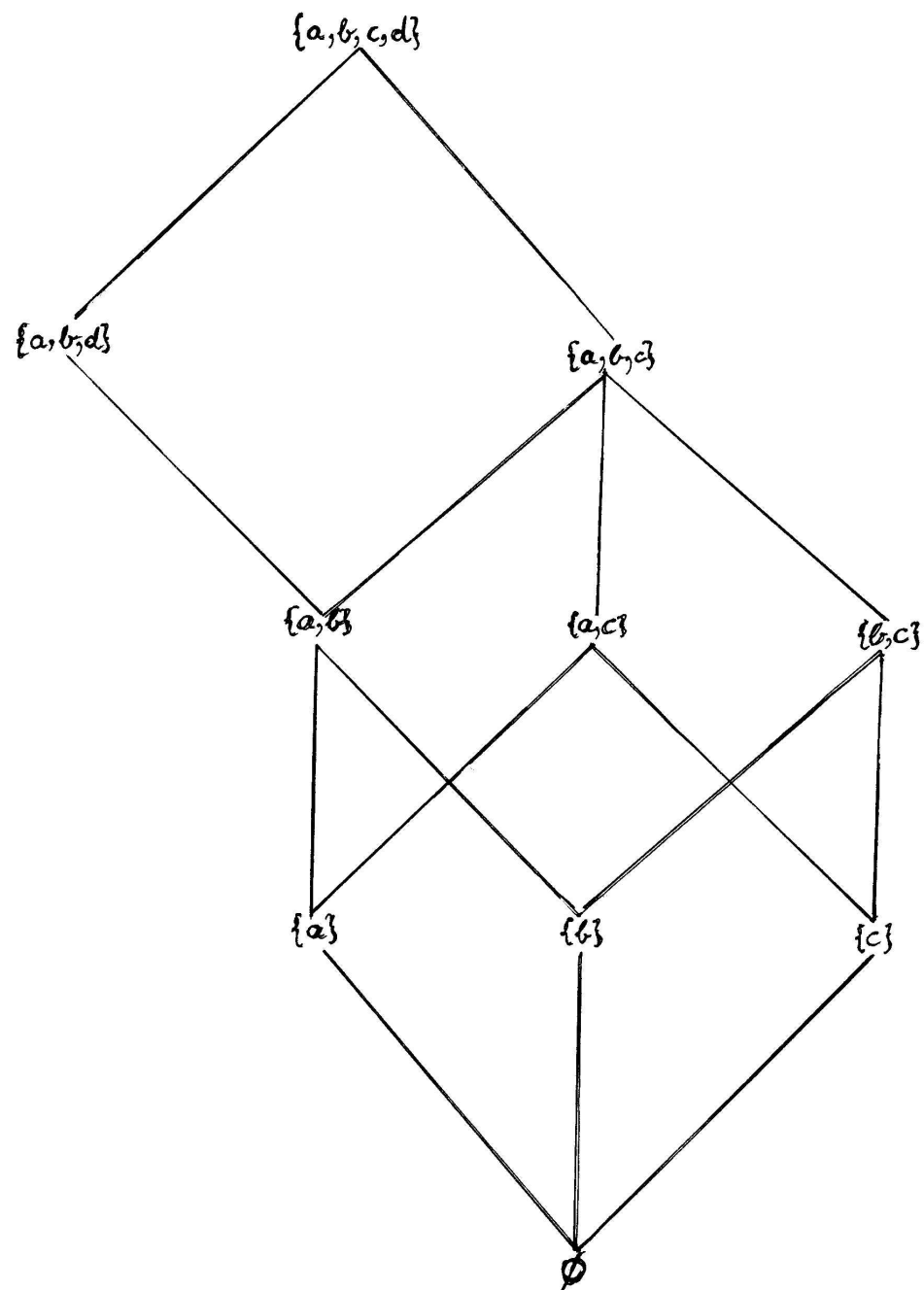
$$[a] = \{a\}, \quad [b] = \{b\}, \quad [c] = \{c\}, \quad [d] = \{a, b, d\}.$$

Ezután építsük fel alulról a részalgebraháálót a következő általános észrevételre támaszkodva:

$$[u_1, \dots, u_k] = [u_1] \vee \dots \vee [u_k].$$

Példa (folyt.)

A részalgebrahááló:



1. Algebrai struktúra, izomorfizmus

2. Részalgebra, generálás

3. Kongruencia, faktoralgebra

4. Homomorfizmus, homomorfizmatétel

A számelméleti kongruenciareláció fontos tulajdonságai:

- ▶ ekvivalenciareláció (reflexív, szimmetrikus, tranzitív);
- ▶ „szabad” kongruenciákat összeadni és összeszorozni:

$$\left. \begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array} \right\} \implies \begin{array}{l} a_1 + a_2 \equiv b_1 + b_2 \pmod{m}, \\ a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}. \end{array}$$

A fenti **kompatibilitási** tulajdonság lehetővé teszi, hogy maradékosztályokat **reprezentánsaik** segítségével adjunk és szorozzunk össze, és ezek a műveletek **jóldefiniáltak** lesznek.

Példa

Modulo 7 maradékosztályok összeadása:

$$\{\dots, -5, \mathbf{2}, 9, 16, \dots\} + \{\dots, -3, \mathbf{4}, 11, 18, \dots\} = \bar{2} + \bar{4} = \bar{6} = \\ = \{\dots, -1, \mathbf{6}, 13, 20, \dots\}$$

$$\{\dots, -5, 2, \mathbf{9}, 16, \dots\} + \{\dots, -3, 4, \mathbf{11}, 18, \dots\} = \bar{9} + \bar{11} = \bar{20} = \\ = \{\dots, -1, 6, 13, \mathbf{20}, \dots\}$$

Az eredmény nem függ a reprezentánsok választásától.

Példa

A $(\mathbb{Z}_3; +, \cdot)$ gyűrű művelet táblázatai:

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, \dots\}$$

+	■	■	■
■	■	■	■
■	■	■	■
■	■	■	■

·	■	■	■
■	■	■	■
■	■	■	■
■	■	■	■

$$\blacksquare = \{\dots, -3, 0, 3, 6, 9, \dots\}$$

$$\blacksquare = \{\dots, -2, 1, 4, 7, 10, \dots\}$$

$$\blacksquare = \{\dots, -1, 2, 5, 8, 11, \dots\}$$

Definíció

Legyen $\mathbb{A} = (A; *)$ egy grupoid, és legyen \sim egy ekvivalenciareláció az A halmazon.

Azt mondjuk, hogy \sim **kongruenciarelációja** az \mathbb{A} algebrának, ha tetszőleges $a_1, a_2, b_1, b_2 \in A$ elemek esetén

$$\left. \begin{array}{l} a_1 \sim b_1 \\ a_2 \sim b_2 \end{array} \right\} \implies a_1 * a_2 \sim b_1 * b_2.$$

Definíció

Legyen $\mathbb{A} = (A; *)$ egy grupoid, és legyen \mathcal{C} egy osztályozás az A halmazon.

Azt mondjuk, hogy \mathcal{C} **kompatibilis osztályozása** az \mathbb{A} algebrának, ha tetszőleges $C_1, C_2 \in \mathcal{C}$ osztályokhoz létezik egy olyan $D \in \mathcal{C}$ osztály, amelyre

$$C_1 * C_2 := \{ a_1 * a_2 \mid a_1 \in C_1, a_2 \in C_2 \} \subseteq D.$$

Tétel

*Egy ekvivalenciareláció akkor és csak akkor kongruencia,
ha a hozzá tartozó osztályozás kompatibilis.*

Biz.

Triviális. (?) De legalábbis HF.



Példa

Kompatibilis osztályozása-e $\mathcal{C} = \{\{a, b\}, \{c, d\}, \{e\}\}$ az alábbi grupoidnak?

$$\mathbb{G} =$$

*	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>c</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>
<i>c</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>d</i>	<i>a</i>	<i>d</i>	<i>c</i>	<i>d</i>	<i>d</i>
<i>e</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>

Nem, pl. $a \sim b$ és $c \sim d$, de $a * c \not\sim b * d$
(azaz $\blacksquare * \blacksquare$ nem jóldefiniált).

Példa

Kompatibilis osztályozása-e $\mathcal{C} = \{\{a\}, \{b, c, d, e\}\}$ az alábbi grupoidnak?

$$\mathbb{G} =$$

*	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>c</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>
<i>c</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>d</i>	<i>a</i>	<i>d</i>	<i>c</i>	<i>d</i>	<i>d</i>
<i>e</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>

Igen, bármely két szín szorzata jóldefiniált:

$$\blacksquare * \blacksquare = \blacksquare, \quad \blacksquare * \blacksquare = \blacksquare, \quad \blacksquare * \blacksquare = \blacksquare, \quad \blacksquare * \blacksquare = \blacksquare.$$

Definíció

Legyen $\mathbb{A} = (A; *)$ egy grupoid, legyen \sim egy kongruenciarelációja \mathbb{A} -nak, és legyen $\mathcal{C} = A/\sim$ a megfelelő kompatibilis osztályozás. Értelmezzük a kongruenciaosztályok halmazán a \circledast műveletet a következőképpen: tetszőleges $C_1, C_2 \in A/\sim$ esetén legyen $C_1 \circledast C_2$ az az egyértelműen meghatározott $D \in A/\sim$ kongruenciaosztály, amelyre

$$\{ a_1 * a_2 \mid a_1 \in C_1, a_2 \in C_2 \} \subseteq D.$$

Az így kapott $\mathbb{A}/\sim = (A/\sim; \circledast)$ algebrát nevezzük az \mathbb{A} algebra \sim kongruencia szerinti **faktoralgebrájának**.

Megjegyzés

Általában \bar{a} jelöli az $a \in A$ elem \sim szerinti ekvivalenciaosztályát. Ezzel a jelöléssel a faktoralgebra művelete így definiálható:

$$\bar{a}_1 \circledast \bar{a}_2 = \overline{a_1 * a_2}.$$

Az osztályozás kompatibilitása garantálja, hogy ez a művelet jóldefiniált, azaz az eredmény nem függ a reprezentánsok választásától.

Példa

Határozzuk meg a \mathbb{G}/\sim faktorgrupoidot, ahol \sim a $\mathcal{C} = \{\{a\}, \{b, c, d, e\}\}$ osztályozáshoz tartozó kongruencia.

$$\mathbb{G} =$$

*	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>c</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>
<i>c</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>d</i>	<i>a</i>	<i>d</i>	<i>c</i>	<i>d</i>	<i>d</i>
<i>e</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>

*	■	■
■	■	■
■	■	■

Példa

Határozzuk meg a \mathbb{G}/\sim faktorgrupoidot, ahol \sim a $\mathcal{C} = \{\{a\}, \{b, c, d, e\}\}$ osztályozáshoz tartozó kongruencia.

$$\mathbb{G} =$$

*	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>c</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>
<i>c</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>d</i>	<i>a</i>	<i>d</i>	<i>c</i>	<i>d</i>	<i>d</i>
<i>e</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>

$$\mathbb{G}/\sim =$$

*	<i>{a}</i>	<i>{b, c, d, e}</i>
<i>{a}</i>	<i>{b, c, d, e}</i>	<i>{b, c, d, e}</i>
<i>{b, c, d, e}</i>	<i>{a}</i>	<i>{b, c, d, e}</i>

Példa

Határozzuk meg a \mathbb{G}/\sim faktorgrupoidot, ahol \sim a $\mathcal{C} = \{\{a\}, \{b, c, d, e\}\}$ osztályozáshoz tartozó kongruencia.

$$\mathbb{G} =$$

	*	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>c</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>	<i>c</i>
<i>c</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>d</i>	<i>a</i>	<i>d</i>	<i>c</i>	<i>d</i>	<i>d</i>	<i>d</i>
<i>e</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>	<i>c</i>

$$\mathbb{G}/\sim =$$

	*	<i>A</i>	<i>B</i>
<i>A</i>	<i>B</i>	<i>B</i>	
<i>B</i>	<i>A</i>	<i>B</i>	

, ahol $A = \{a\}$ és $B = \{b, c, d, e\}$

Pl. $B * B = \bar{b} * \bar{b} = \overline{b * b} = \bar{c} = B.$

Példa

Határozzuk meg a \mathbb{G}/\sim faktorgrupoidot, ahol \sim a $\mathcal{C} = \{\{a, c\}, \{b, e\}, \{d\}\}$ osztályozáshoz tartozó kongruencia.

$$\mathbb{G} =$$

*	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>c</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>
<i>c</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>d</i>	<i>a</i>	<i>d</i>	<i>c</i>	<i>d</i>	<i>d</i>
<i>e</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>

*	■	■	■
■	■	■	■
■	■	■	■
■	■	■	■

Példa

Határozzuk meg a \mathbb{G}/\sim faktorgrupoidot, ahol \sim a $\mathcal{C} = \{\{a, c\}, \{b, e\}, \{d\}\}$ osztályozáshoz tartozó kongruencia.

$$\mathbb{G} =$$

*	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>c</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>
<i>c</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>d</i>	<i>a</i>	<i>d</i>	<i>c</i>	<i>d</i>	<i>d</i>
<i>e</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>

$$\mathbb{G}/\sim =$$

*	$\{a, c\}$	$\{b, e\}$	$\{d\}$
$\{a, c\}$	$\{a, c\}$	$\{b, e\}$	$\{a, c\}$
$\{b, e\}$	$\{a, c\}$	$\{a, c\}$	$\{b, e\}$
$\{d\}$	$\{a, c\}$	$\{d\}$	$\{d\}$

Példa

Határozzuk meg a \mathbb{G}/\sim faktorgrupoidot, ahol \sim a $\mathcal{C} = \{\{a, c\}, \{b, e\}, \{d\}\}$ osztályozáshoz tartozó kongruencia.

$$\mathbb{G} =$$

*	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>c</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>
<i>c</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>d</i>	<i>a</i>	<i>d</i>	<i>c</i>	<i>d</i>	<i>d</i>
<i>e</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>

$$\mathbb{G}/\sim =$$

*	<i>A</i>	<i>B</i>	<i>D</i>
<i>A</i>	<i>A</i>	<i>B</i>	<i>A</i>
<i>B</i>	<i>A</i>	<i>A</i>	<i>B</i>
<i>D</i>	<i>A</i>	<i>D</i>	<i>D</i>

, ahol $A = \{a, c\}$, $B = \{b, e\}$ és $D = \{d\}$

Példa

Határozzuk meg a \mathbb{G}/\sim faktorgrupoidot, ahol \sim a $\mathcal{C} = \{\{a, b, c, e\}, \{d\}\}$ osztályozáshoz tartozó kongruencia.

$$\mathbb{G} =$$

*	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>c</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>
<i>c</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>d</i>	<i>a</i>	<i>d</i>	<i>c</i>	<i>d</i>	<i>d</i>
<i>e</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>

*	■	■
■	■	■
■	?	■

Ez nem kongruencia, pl. $d \sim d$ és $a \sim b$, de $d * a \not\sim d * b$.



VESZÉLYES JELÖLÉS!

Tetszőleges $C_1, C_2 \subseteq A$ esetén szokás definiálni a $C_1 * C_2$ **komplexusszorzatot**:

$$C_1 * C_2 := \{a_1 * a_2 \mid a_1 \in C_1, a_2 \in C_2\} \subseteq A.$$

Ha \sim kongruencia, és $C_1, C_2 \in A/\sim$, akkor $C_1 \otimes C_2$ értelmezett az \mathbb{A}/\sim faktoralgebrában (és megállapodtunk abban, hogy ezt egyszerűen csak $C_1 * C_2$ jelöli).

Ez a két „szorzat” nem ugyanaz: minden $C_1, C_2 \in A/\sim$ esetén teljesül $C_1 * C_2 \subseteq C_1 \otimes C_2$ (HF), de itt néha valódi tartalmazás is lehetséges.



VESZÉLYES JELÖLÉS!

$$G =$$

*	<i>a</i>	<i>b</i>	<i>c</i>	<i>d</i>	<i>e</i>
<i>a</i>	<i>c</i>	<i>b</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>b</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>
<i>c</i>	<i>a</i>	<i>e</i>	<i>c</i>	<i>c</i>	<i>e</i>
<i>d</i>	<i>a</i>	<i>d</i>	<i>c</i>	<i>d</i>	<i>d</i>
<i>e</i>	<i>a</i>	<i>c</i>	<i>c</i>	<i>e</i>	<i>c</i>

$$\{a\} * \{b, c, d, e\} = \{b, c, e\} \quad (\text{komplexusszorzat}),$$

$$\{a\} \circledast \{b, c, d, e\} = \{b, c, d, e\} \quad (\text{faktoralgebra}).$$

Jó hír: komplexusszorzattal csak csoportoknál fogunk foglalkozni, és ott a faktoralgebrában kiszámolt szorzat mindig megegyezik a komplexusszorzattal.

Példa

Határozzuk meg az $(\mathbb{R}; \cdot)$ algebra \sim szerinti faktoralgebráját, ahol

$$a \sim b \iff \text{sgn } a = \text{sgn } b.$$

$$\mathbb{R}/\sim = \{ \mathbb{R}^+, \mathbb{R}^-, \{0\} \}$$

$$(\mathbb{R}; \cdot) / \sim = \begin{array}{c|ccc} \cdot & \{0\} & \mathbb{R}^+ & \mathbb{R}^- \\ \hline \{0\} & \{0\} & \{0\} & \{0\} \\ \mathbb{R}^+ & \{0\} & \mathbb{R}^+ & \mathbb{R}^- \\ \mathbb{R}^- & \{0\} & \mathbb{R}^- & \mathbb{R}^+ \end{array} \cong \begin{array}{c|ccc} \cdot & \bar{0} & \bar{1} & \bar{2} \\ \hline \bar{0} & \bar{0} & \bar{0} & \bar{0} \\ \bar{1} & \bar{0} & \bar{1} & \bar{2} \\ \bar{2} & \bar{0} & \bar{2} & \bar{1} \end{array} = (\mathbb{Z}_3; \cdot)$$

Példa

Határozzuk meg az $(\mathbb{R}; +)$ algebra \sim szerinti faktoralgebráját, ahol

$$a \sim b \iff \operatorname{sgn} a = \operatorname{sgn} b.$$

Ez nem kongruencia, mert az összeg előjelét nem határozza meg egyértelműen az összeadandók előjele.

Például $2 \sim 5$ és $-6 \sim -4$, de $(2 + (-6)) \not\sim (5 + (-4))$.

Példa

Határozzuk meg a $(\mathcal{P}(\mathbb{N}); \cup)$ algebra \mathcal{C} kompatibilis osztályozáshoz tartozó faktoralgebráját, ahol

$$\mathcal{C} = \{ \{ \text{véges halmazok} \}, \{ \text{végtelen halmazok} \} \}.$$

$$(\mathcal{P}(\mathbb{N}); \cup) / \sim = \begin{array}{c|cc} \cup & \{ \text{véges} \} & \{ \text{végtelen} \} \\ \hline \{ \text{véges} \} & \{ \text{véges} \} & \{ \text{végtelen} \} \\ \{ \text{végtelen} \} & \{ \text{végtelen} \} & \{ \text{végtelen} \} \end{array} \cong (\mathbb{Z}_2; \cdot)$$

1. Algebrai struktúra, izomorfizmus

2. Részalgebra, generálás

3. Kongruencia, faktoralgebra

4. Homomorfizmus, homomorfizmatétel

Definíció

Legyen $\mathbb{A} = (A; *)$ és $\mathbb{B} = (B; \oplus)$ két grupoid. Azt mondjuk, hogy a $\varphi: A \rightarrow B$ leképezés **homomorfizmus** \mathbb{A} -ból \mathbb{B} -be, ha φ felcserélhető a műveletekkel, azaz

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

Ha létezik $\varphi: \mathbb{A} \rightarrow \mathbb{B}$ szürjektív homomorfizmus, akkor azt mondjuk, hogy \mathbb{B} **homomorf képe** \mathbb{A} -nak.

Speciális homomorfizmusok:

- ▶ bijektív homomorfizmus = **izomorfizmus**,
- ▶ injektív homomorfizmus = **beágyazás**,
- ▶ $\mathbb{A} \rightarrow \mathbb{A}$ homomorfizmus = **endomorfizmus**,
- ▶ bijektív $\mathbb{A} \rightarrow \mathbb{A}$ homomorfizmus = **automorfizmus**.

Példa

- ▶ $\varphi: (\mathbb{R}^+; \cdot) \rightarrow (\mathbb{R}; +)$, $x \mapsto \log x$ izomorfizmus
- ▶ $\varphi: (\mathbb{C}; +, \cdot) \rightarrow (\mathbb{C}; +, \cdot)$, $z \mapsto \bar{z}$ automorfizmus
- ▶ $\varphi: (\mathbb{C}; +) \rightarrow (\mathbb{C}; +)$, $z \mapsto \operatorname{Re} z$ endomorfizmus
- ▶ $\varphi: (\mathbb{C}; +) \rightarrow (\mathbb{R}; +)$, $z \mapsto \operatorname{Re} z$ szürjektív homomorfizmus
- ▶ $\varphi: (\mathbb{C}; \cdot) \rightarrow (\mathbb{R}; \cdot)$, $z \mapsto \operatorname{Re} z$ nem homomorfizmus
- ▶ $\varphi: (\mathbb{R}; +, \cdot) \rightarrow (\mathbb{C}; +, \cdot)$, $x \mapsto x$ beágyazás
- ▶ $\varphi: (\mathbb{R}^{n \times n}; \cdot) \rightarrow (\mathbb{R}; \cdot)$, $M \mapsto \det M$ szürjektív homomorfizmus
- ▶ $\varphi: (C[0, 1]; +) \rightarrow (\mathbb{R}; +)$, $f \mapsto \int_0^1 f(x) dx$
szürjektív homomorfizmus

Példa

Gondoltam egy $\varphi: (\mathbb{N}; +) \rightarrow (\mathbb{N}; +)$ homomorfizmust. Annyit elárulok, hogy $2\varphi = 10$ és $3\varphi = 9$. Mi lehet ez a homomorfizmus?

- ▶ $4\varphi = (2 + 2)\varphi = 2\varphi + 2\varphi = 10 + 10 = 20$
- ▶ $6\varphi = (2 + 2 + 2)\varphi = 2\varphi + 2\varphi + 2\varphi = 10 + 10 + 10 = 30$
- ▶ $(2n)\varphi = (2 + \dots + 2)\varphi = 2\varphi + \dots + 2\varphi = 10 + \dots + 10 = 10n$
- ▶ $6\varphi = (3 + 3)\varphi = 3\varphi + 3\varphi = 9 + 9 = 18$
- ▶ $9\varphi = (3 + 3 + 3)\varphi = 3\varphi + 3\varphi + 3\varphi = 9 + 9 + 9 = 27$
- ▶ $(3n)\varphi = (3 + \dots + 3)\varphi = 3\varphi + \dots + 3\varphi = 9 + \dots + 9 = 9n$
- ▶ ...

Átverés!

$$6\varphi = 2\varphi + 2\varphi + 2\varphi = 30 \neq 18 = 3\varphi + 3\varphi = 6\varphi$$

Ilyen homomorfizmus nem létezik!

Példa

Gondoltam egy $\varphi: (\mathbb{N}; +) \rightarrow (\mathbb{N}; +)$ homomorfizmust. Annyit elárulok, hogy $2\varphi = 4$ és $3\varphi = 6$. Mi lehet ez a homomorfizmus?

- ▶ $4\varphi = (2 + 2)\varphi = 2\varphi + 2\varphi = 4 + 4 = 8$
- ▶ $5\varphi = (2 + 3)\varphi = 2\varphi + 3\varphi = 4 + 6 = 10$
- ▶ $6\varphi = (2 + 2 + 2)\varphi = 2\varphi + 2\varphi + 2\varphi = 4 + 4 + 4 = 12$
- ▶ $7\varphi = (2 + 2 + 3)\varphi = 2\varphi + 2\varphi + 3\varphi = 4 + 4 + 6 = 14$
- ▶ $8\varphi = (2 + 2 + 2 + 2)\varphi = 2\varphi + 2\varphi + 2\varphi + 2\varphi = 4 + 4 + 4 + 4 = 16$
- ▶ $9\varphi = (2 + 2 + 2 + 3)\varphi = 2\varphi + 2\varphi + 2\varphi + 3\varphi = 4 + 4 + 4 + 6 = 18$

Sejtés: $n\varphi = 2n$ minden $n \in \mathbb{N}$ -re.

Ez valóban homomorfizmus? Igen, mert minden $a, b \in \mathbb{N}$ esetén

$$(a + b)\varphi = 2(a + b) = a\varphi + b\varphi = 2a + 2b.$$

Példa (másik megoldás)

Gondoltam egy $\varphi: (\mathbb{N}; +) \rightarrow (\mathbb{N}; +)$ homomorfizmust. Annyit elárulok, hogy $2\varphi = 4$ és $3\varphi = 6$. Mi lehet ez a homomorfizmus?

Egy ötlet: ha tudnánk, hogy mennyi 1φ , akkor készen lennénk, mert minden $n \in \mathbb{N}$ -re

$$n\varphi = (1 + \dots + 1)\varphi = 1\varphi + \dots + 1\varphi = 1\varphi \cdot n.$$

$$6 = 3\varphi = (1 + 2)\varphi = 1\varphi + 2\varphi = 1\varphi + 4 \implies 1\varphi = 2$$

Tehát $\forall n \in \mathbb{N} : n\varphi = 2n$.

Példa

Gondoltam egy $\varphi: (\mathbb{N}; +) \rightarrow (\mathbb{N}; +)$ homomorfizmust. Annyit elárulok, hogy $2\varphi = 25$. Mi lehet ez a homomorfizmus?

Mennyi lehet 1φ ?

$$25 = 2\varphi = (1 + 1)\varphi = 1\varphi + 1\varphi \implies 1\varphi = \frac{25}{2} \notin \mathbb{N}$$

Ilyen homomorfizmus nem létezik!

Példa

Gondoltam egy $\varphi: (\mathbb{N}; +) \rightarrow (\mathbb{N}; \cdot)$ homomorfizmust. Annyit elárulok, hogy $2\varphi = 25$. Mi lehet ez a homomorfizmus?

Mennyi lehet 1φ ?

$$25 = 2\varphi = (1 + 1)\varphi = 1\varphi \cdot 1\varphi \implies 1\varphi = 5$$

$$n\varphi = (1 + \dots + 1)\varphi = 1\varphi \cdot \dots \cdot 1\varphi = 5 \cdot \dots \cdot 5 = 5^n$$

Ez valóban homomorfizmus? Igen, mert minden $a, b \in \mathbb{N}$ esetén

$$(a + b)\varphi = 5^{a+b} = a\varphi \cdot b\varphi = 5^a \cdot 5^b.$$

Példa

Gondoltam egy $\varphi: \mathbb{A} \rightarrow \mathbb{B}$ homomorfizmust. Annyit elárulok, hogy $b\varphi = v$ és $c\varphi = w$. Mi lehet ez a homomorfizmus?

$$\mathbb{A} = \begin{array}{c|cccc} * & a & b & c & d \\ \hline a & d & d & a & a \\ b & d & d & b & b \\ c & a & a & c & c \\ d & a & b & c & d \end{array} \xrightarrow{\varphi} \begin{array}{c|ccc} \otimes & u & v & w \\ \hline u & v & u & w \\ v & w & w & v \\ w & u & v & w \end{array} = \mathbb{B}$$

$$a\varphi = (c * b)\varphi = c\varphi \otimes b\varphi = w \otimes v = v$$

$$d\varphi = (b * b)\varphi = b\varphi \otimes b\varphi = v \otimes v = w$$

Ez valóban homomorfizmus?

Igen, de körülményes lenne ellenőrizni. (Majd később, a homomorfizmatétel segítségével könnyebb lesz.)

Példa

Gondoltam egy $\varphi: \mathbb{A} \rightarrow \mathbb{B}$ homomorfizmust. Annyit elárulok, hogy $a\varphi = u$. Mi lehet ez a homomorfizmus?

$$\mathbb{A} = \begin{array}{c|ccccc} \cdot & a & b & c & d & e \\ \hline a & b & c & a & a & a \\ b & a & a & c & e & e \\ c & b & d & c & d & d \\ d & b & e & e & c & c \\ e & b & d & e & d & e \end{array} \xrightarrow{\varphi} \begin{array}{c|ccc} \circ & u & v & w \\ \hline u & v & w & u \\ v & u & u & w \\ w & v & w & w \end{array} = \mathbb{B}$$

$$b\varphi = (a \cdot a)\varphi = a\varphi \circ a\varphi = u \circ u = v$$

$$c\varphi = (a \cdot b)\varphi = a\varphi \circ b\varphi = u \circ v = w$$

$$d\varphi = (c \cdot b)\varphi = c\varphi \circ b\varphi = w \circ v = w$$

$$e\varphi = (b \cdot d)\varphi = b\varphi \circ d\varphi = v \circ w = w$$

Ez valóban homomorfizmus? Igen, semmi átverés!

Az előző két példában azért sikerült a homomorfizmust egyértelműen meghatározni, mert egy **generátorrendszeren** meg volt adva.

A legutolsó példában $\{a\}$ generátorrendszer:

$$b\varphi = (a \cdot a)\varphi = a\varphi \circ a\varphi$$

$$c\varphi = (a \cdot (a \cdot a))\varphi = a\varphi \circ (a\varphi \circ a\varphi)$$

$$d\varphi = ((a \cdot (a \cdot a)) \cdot (a \cdot a))\varphi = (a\varphi \circ (a\varphi \circ a\varphi)) \circ (a\varphi \circ a\varphi)$$

$$\begin{aligned} e\varphi &= \left((a \cdot a) \cdot ((a \cdot (a \cdot a)) \cdot (a \cdot a)) \right)\varphi = \\ &= (a\varphi \circ a\varphi) \circ ((a\varphi \circ (a\varphi \circ a\varphi)) \circ (a\varphi \circ a\varphi)) \end{aligned}$$

Tétel

Homomorfizmust egyértelműen meghatározza egy generátorrendszerre való megszorítása. Precízebben:

Legyen T generátorrendszere az \mathbb{A} algebrának, és legyenek $\varphi, \psi: \mathbb{A} \rightarrow \mathbb{B}$ homomorfizmusok. Ha φ és ψ megegyezik a T halmazon (azaz $\forall t \in T: t\varphi = t\psi$), akkor φ és ψ mindenütt megegyezik (azaz $\forall a \in A: a\varphi = a\psi$).

Biz.

Könnyű ellenőrizni, hogy az

$$E = \{a \in A \mid a\varphi = a\psi\} \subseteq A$$

halmaz zárt (HF, lásd [Sz] X. fejezet, 8. feladat).

Mivel E tartalmazza T -t,

$$E = [E] \supseteq [T] = A.$$

Tehát $E = A$, vagyis φ és ψ valóban mindenütt megegyezik. □

Definíció

Legyen \sim kongruenciája az \mathbb{A} algebrának. Ekkor a

$$\nu: \mathbb{A} \rightarrow \mathbb{A}/\sim, a \mapsto \bar{a}$$

leképezés homomorfizmus (HF), amelyet a \sim kongruenciához tartozó **természetes homomorfizmusnak** nevezünk.

Példa

\mathbb{G}	a	b	c	d	e		\mathbb{G}/\sim	A	B	D
a	c	b	c	c	e	$\xrightarrow{\nu}$	A	A	B	A
b	a	c	c	e	c		B	A	A	B
c	a	e	c	c	e		D	A	D	D
d	a	d	c	d	d					
e	a	c	c	e	c					

$$a\nu = A, b\nu = B, c\nu = A, d\nu = D, e\nu = B,$$

$$\text{ahol } A = \{a, c\}, B = \{b, e\} \text{ és } D = \{d\}$$

Tétel

Ha $\varphi: \mathbb{A} \rightarrow \mathbb{B}$ homomorfizmus, akkor φ értékkészlete részalgebrát alkot \mathbb{B} -ben: $\mathbb{A}\varphi \leq \mathbb{B}$.

Biz.

HF [Sz] X. fejezet, 2.10. Tétel. □

Következmény

Ha $\varphi: \mathbb{A} \rightarrow \mathbb{B}$ beágyazás, akkor $\mathbb{A} \cong \mathbb{A}\varphi \leq \mathbb{B}$.

Tétel

Ha $\varphi: \mathbb{A} \rightarrow \mathbb{B}$ homomorfizmus és $S \leq \mathbb{B}$, akkor az

$$S\varphi^{-1} = \{ a \in \mathbb{A} \mid a\varphi \in S \}$$

halmaz (S teljes inverz képe) zárt \mathbb{A} -ban (lehet, hogy üres).

Biz.

HF [Sz] X. fejezet, 7. feladat. □

Tétel

Homomorfizmusok szorzata homomorfizmus.

Biz.

HF [Sz] X. fejezet, 1.13. Tétel. □

A természetes homomorfizmus mutatja, hogy minden faktoralgebra előáll homomorf képként. Ennek a fordítottja is igaz: minden homomorf kép faktoralgebra (legalábbis izomorfia erejéig).

Definíció

Tetszőleges $\varphi: A \rightarrow B$ leképezés esetén az

$$a_1 \sim a_2 \iff a_1\varphi = a_2\varphi$$

képlettel definiált reláció ekvivalenciareláció az A halmazon (HF), amelyet φ **magjának** nevezünk, és $\ker \varphi$ -vel jelölünk.

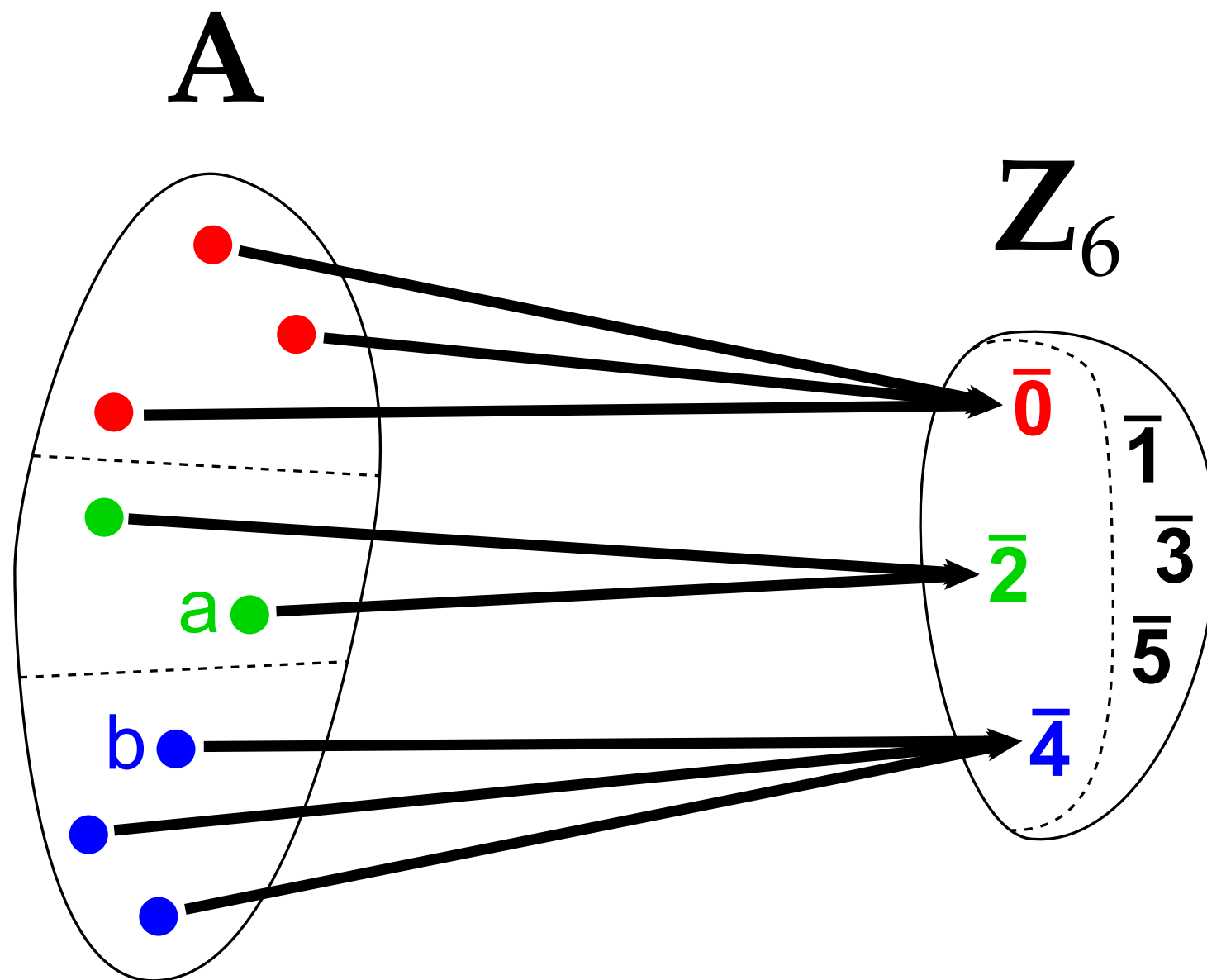
Tétel (Homomorfiatétel)

Ha $\varphi: \mathbb{A} \rightarrow \mathbb{B}$ homomorfizmus, akkor $\ker \varphi$ kongruencia \mathbb{A} -n, és

$$\mathbb{A}/\ker \varphi \cong \mathbb{A}\varphi \leq \mathbb{B}.$$

Bizonyítás helyett egy illusztráció, ami „majdnem” bizonyítás.
A precíz bizonyítást lásd: [Sz] X. fejezet, 3.12. Tétel.

Legyen $\varphi: (A; *) \rightarrow (\mathbb{Z}_6; +)$ homomorfizmus.



$$(a * b) \varphi = a\varphi + b\varphi = \bar{2} + \bar{4} = \bar{0} \implies a * b \text{ piros}$$

A homomorfia-tétel szerint minden homomorfizmus felfogható egy faktorizálás és egy beágyazás egymásutánjaként.

Példa

$$\mathbb{A} = \begin{array}{c|cccc} * & a & b & c & d \\ \hline a & d & d & a & a \\ b & d & d & b & b \\ c & a & a & c & c \\ d & a & b & c & d \end{array} \xrightarrow{\varphi} \begin{array}{c|ccc} \otimes & u & v & w \\ \hline u & v & u & w \\ v & w & w & v \\ w & u & v & w \end{array} = \mathbb{B}$$

$$a\varphi = v, \quad b\varphi = v, \quad c\varphi = w, \quad d\varphi = w$$

$$\mathbb{A}/\sim = \begin{array}{c|cc} * & \{a, b\} & \{c, d\} \\ \hline \{a, b\} & \{c, d\} & \{a, b\} \\ \{c, d\} & \{a, b\} & \{c, d\} \end{array} \cong \begin{array}{c|cc} \otimes & v & w \\ \hline v & w & v \\ w & v & w \end{array} \leq \begin{array}{c|ccc} \otimes & u & v & w \\ \hline u & v & u & w \\ v & w & w & v \\ w & u & v & w \end{array} = \mathbb{B}$$

Példa

Írjuk fel a homomorfizmatételt a

$$\text{sgn}: (\mathbb{R}; \cdot) \rightarrow (\mathbb{R}; \cdot)$$

homomorfizmusra.

Az értékkészlet: $\mathbb{R}_\varphi = \{-1, 0, +1\}$.

A maghoz tartozó osztályozás: $\mathbb{R} / \ker \text{sgn} = \{\mathbb{R}^-, \{0\}, \mathbb{R}^+\}$.

A mag szerinti faktor:

$$(\mathbb{R}; \cdot) / \ker \text{sgn} = \begin{array}{c|ccc} \cdot & \mathbb{R}^- & \{0\} & \mathbb{R}^+ \\ \hline \mathbb{R}^- & \mathbb{R}^+ & \{0\} & \mathbb{R}^- \\ \{0\} & \{0\} & \{0\} & \{0\} \\ \mathbb{R}^+ & \mathbb{R}^- & \{0\} & \mathbb{R}^+ \end{array} \cong \begin{array}{c|ccc} \cdot & -1 & 0 & +1 \\ \hline -1 & +1 & 0 & -1 \\ 0 & 0 & 0 & 0 \\ +1 & -1 & 0 & +1 \end{array} \cong (\mathbb{R}; \cdot)$$