Általános algebra

2013 március 8.

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

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**:

$$f\colon A^n \to A,\ \ (a_1, \ldots, a_n) \mapsto f(a_1, \ldots, a_n).$$

Példa

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

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

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

  $$^{-1}\colon \mathrm{GL}_2(\mathbb{R}) \to \mathrm{GL}_2(\mathbb{R}),\ \ M \mapsto M^{-1}.$$

Nullaváltozós művelet (?!):

$$f\colon A^0 \to A,\ \ a \mapsto f(a)\,.$$

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

$$+\colon \mathbb{Z}^2 \to \mathbb{Z},\ \ (a_1, a_2) \mapsto a_1 + a_2,$$
$$\cdot\colon \mathbb{Z}^2 \to \mathbb{Z},\ \ (a_1, a_2) \mapsto a_1 \cdot a_2.$$

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

$$-\colon \mathbb{Z} \to \mathbb{Z},\ \ a \mapsto -a,$$
$$0\colon \mathbb{Z}^0 \to \mathbb{Z},\ \ \heartsuit \mapsto 0.$$

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

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\otimes$	🌷	💐
🌷	🌷	💐
💐	💐	🌷

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

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\xrightarrow{\text{átnevezés}}$

$\otimes$	🌷	💐
🌷	🌷	💐
💐	💐	🌷

Ezt az „átnevezést” a

$$\varphi\colon \{\overline{0}, \overline{1}\} \to \{\,🌷\,, 💐\,\},\quad \overline{0} \mapsto 🌷\,,\ \overline{1} \mapsto 💐$$

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

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

Definíció

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

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

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

Ha létezik $\varphi\colon \mathbb{A} \to \mathbb{B}$ 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:

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

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
a	a	c	c
b	b	b	b
c	c	a	c

$\mathbb{B} =$

$\oplus$	1	2	3
1	3	2	2
2	2	2	2
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 **jobboldali 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?

$\mathbb{A} =$

$\cdot$	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	q	r	r	s
s	s	s	s	s

Talán igen ... Tegyük fel, hogy $\varphi\colon \mathbb{A} \to \mathbb{B}$ 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 $\varphi\colon \mathbb{A} \to \mathbb{B}$ izomorfizmus, akkor ez csak a következő lehet:

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

Próbáljuk ki, hogy ez a leképezés izomorfizmus-e:

$\mathbb{A} =$

$\cdot$	a	b	c	d
a	a	b	c	d
b	b	b	b	b
c	c	b	c	**a**
d	d	b	**b**	a

$\xrightarrow{\varphi}$ $\mathbb{A}\varphi =$

$\cdot$	q	s	r	p
q	q	s	r	p
s	s	s	s	s
r	r	s	r	**q**
p	p	s	**s**	q

$\|$

$\mathbb{B} =$

$\cdot$	p	q	r	s
p	q	p	**s**	s
q	p	q	r	s
r	**q**	r	r	s
s	s	s	s	s

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, $\varphi\colon \mathbb{R} \to \mathbb{R}^+$, $x \mapsto e^x$ 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:

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

Ha $\varphi\colon (\mathbb{Q}; +) \to (\mathbb{Q}^+; \cdot)$ 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 $\sqrt{2}$ irracionalitásának.

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?

$\mathbb{A} =$

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

- $B = \emptyset$: 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:

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

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:

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

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

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

□

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.

$\mathbb{A} =$

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

- $[\emptyset] = \emptyset$, 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.

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

Definíció

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

Megjegyzés

Ha $\mathbb{A}$-nak nincs nullaváltozós művelete, akkor $\emptyset \in \mathrm{Sub}(\mathbb{A})$, 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 $B, C \in \mathrm{Sub}(\mathbb{A})$ 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 részalgebrahálót.

$\mathbb{A} =$

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

Először számítsuk ki az egyes elemek generátumait:

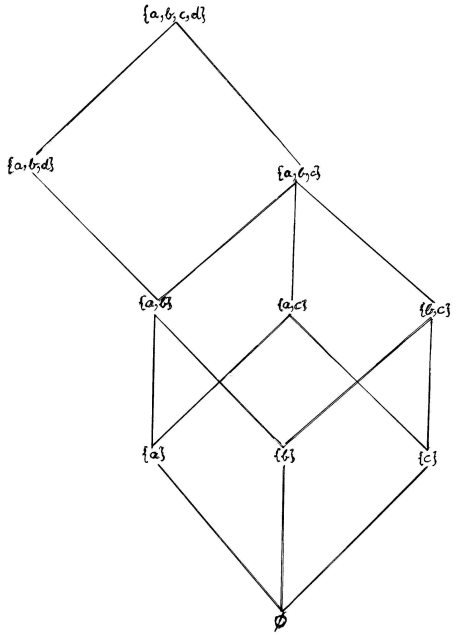
$$[a] = \{a\}, \quad [b] = \{b\}, \quad [c] = \{c\}, \quad [d] = \{a, b, d\}.$$

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

$$[u_1, \ldots, u_k] = [u_1] \vee \cdots \vee [u_k].$$

Példa (folyt.)

A részalgebraháló:



A számelméleti kongruenciareláció fontos tulajdonságai:

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

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

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:

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

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

Az eredmény nem függ a reprezentánsok választásától.

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

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

■ $=\{\ldots,-3,0,3,6,9,\ldots\}$

■ $=\{\ldots,-2,1,4,7,10,\ldots\}$

■ $=\{\ldots,-1,2,5,8,11,\ldots\}$

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?

$\mathbb{G} =$

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

Nem, pl. $a \sim b$ és $c \sim d$, de $a * c \nsim b * d$
(azaz ■ $*$ ■ nem jóldefiniált).

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

$\mathbb{G} =$

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

Igen, bármely két szín szorzata jóldefiniált:

■ $*$ ■ $=$ ■, ■ $*$ ■ $=$ ■, ■ $*$ ■ $=$ ■, ■ $*$ ■ $=$ ■.

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

$$\overline{a_1} \circledast \overline{a_2} = \overline{a_1 * a_2}.$$

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.

$\mathbb{G} =$

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

$\mathbb{G}/\sim =$

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

Példa

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

$\mathbb{G} =$

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

$\mathbb{G}/\sim =$

$*$	A	B
A	B	B
B	A	B

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

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

Példa

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

$\mathbb{G} =$

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

$*$	■	■	■
■	■	■	■
■	■	■	■
■	■	■	■

Példa

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

$\mathbb{G} =$

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

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

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

Példa

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

$\mathbb{G} =$

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

$\mathbb{G}/\sim =$

$*$	A	B	D
A	A	B	A
B	A	A	B
D	A	D	D

, 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.

$\mathbb{G} =$

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

$*$	■	■
■	■	■
■	?	■

Ez nem kongruencia, pl. $d \sim d$ és $a \sim b$, de $d * a \nsim d * b$.

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 $C_1 \circledast C_2$ 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 $C_1 * C_2 \subseteq C_1 \circledast C_2$ (HF), de itt néha valódi tartalmazás is lehetséges.

VESZÉLYES JELÖLÉS!

$\mathbb{G} =$

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

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

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

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

Példa

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

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

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

$(\mathbb{R};\cdot)/\!\sim =$

$\cdot$	$\{0\}$	$\mathbb{R}^+$	$\mathbb{R}^-$
$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
$\mathbb{R}^+$	$\{0\}$	$\mathbb{R}^+$	$\mathbb{R}^-$
$\mathbb{R}^-$	$\{0\}$	$\mathbb{R}^-$	$\mathbb{R}^+$

$\cong$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$= (\mathbb{Z}_3;\cdot)$

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

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

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

Definíció

Legyen $\mathbb{A} = (A; *)$ és $\mathbb{B} = (B; \oplus)$ két grupoid. Azt mondjuk, hogy a $\varphi\colon A \to B$ leképezés **homomorfizmus** $\mathbb{A}$-ból $\mathbb{B}$-be, ha 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 homorfizmus, akkor azt mondjuk, hogy $\mathbb{B}$ **homomorf képe** $\mathbb{A}$-nak.

Speciális homomorifzmusok:

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

Példa

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

Példa

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

- $4\varphi = (2+2)\,\varphi = 2\varphi + 2\varphi = 10 + 10 = 20$
- $6\varphi = (2+2+2)\,\varphi = 2\varphi + 2\varphi + 2\varphi = 10 + 10 + 10 = 30$
- $(2n)\,\varphi = (2+\cdots+2)\,\varphi = 2\varphi+\cdots+2\varphi = 10+\cdots+10 = 10n$
- $6\varphi = (3+3)\,\varphi = 3\varphi + 3\varphi = 9 + 9 = 18$
- $9\varphi = (3+3+3)\,\varphi = 3\varphi + 3\varphi + 3\varphi = 9 + 9 + 9 = 27$
- $(3n)\,\varphi = (3+\cdots+3)\,\varphi = 3\varphi + \cdots + 3\varphi = 9 + \cdots + 9 = 9n$
- $\ldots$

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 $\varphi\colon (\mathbb{N};+) \to (\mathbb{N};+)$ 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

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

Példa (másik megoldás)

Gondoltam egy $\varphi\colon (\mathbb{N};+) \to (\mathbb{N};+)$ 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

$$n\varphi = (1+\cdots+1)\,\varphi = 1\varphi + \cdots + 1\varphi = 1\varphi \cdot n.$$

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

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

Példa

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

Mennyi lehet 1φ?

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

$$n\varphi = (1+\cdots+1)\,\varphi = 1\varphi \cdot \ldots \cdot 1\varphi = 5 \cdot \ldots \cdot 5 = 5^n$$

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

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

Példa

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

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

$$\begin{aligned} a\varphi &= (c * b)\,\varphi = c\varphi \otimes b\varphi = w \otimes v = v \\ d\varphi &= (b * b)\,\varphi = b\varphi \otimes b\varphi = v \otimes v = w \end{aligned}$$

Ez valóban homomorfizmus?

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

Példa

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

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

$$\begin{aligned} b\varphi &= (a \cdot a)\,\varphi = a\varphi \circ a\varphi = u \circ u = v \\ c\varphi &= (a \cdot b)\,\varphi = a\varphi \circ b\varphi = u \circ v = w \\ d\varphi &= (c \cdot b)\,\varphi = c\varphi \circ b\varphi = w \circ v = w \\ e\varphi &= (b \cdot d)\,\varphi = b\varphi \circ d\varphi = v \circ w = w \end{aligned}$$

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:

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

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

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

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

Tétel

Homomorfizmust egyértelműen meghatározza egy generátorrendszerre való megszorítása. Precízebben:

Legyen T generátorrendszere az $\mathbb{A}$ algebrának, és legyenek $\varphi, \psi\colon \mathbb{A} \to \mathbb{B}$ 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

$$\nu\colon \mathbb{A} \to \mathbb{A}/\!\sim,\ a \mapsto \overline{a}$$

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

Példa

$\mathbb{G}$	a	b	c	d	e
a	c	b	c	c	e
b	a	c	c	e	c
c	a	e	c	c	e
d	a	d	c	d	d
e	a	c	c	e	c

$\xrightarrow{\nu}$

$\mathbb{G}/\!\sim$	A	B	D
A	A	B	A
B	A	A	B
D	A	D	D

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

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

Tétel

Ha $\varphi\colon \mathbb{A} \to \mathbb{B}$ 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 $\varphi\colon \mathbb{A} \to \mathbb{B}$ beágyazás, akkor $\mathbb{A} \cong \mathbb{A}\varphi \leq \mathbb{B}$.

Tétel

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

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

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 $\varphi\colon A \to B$ 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.

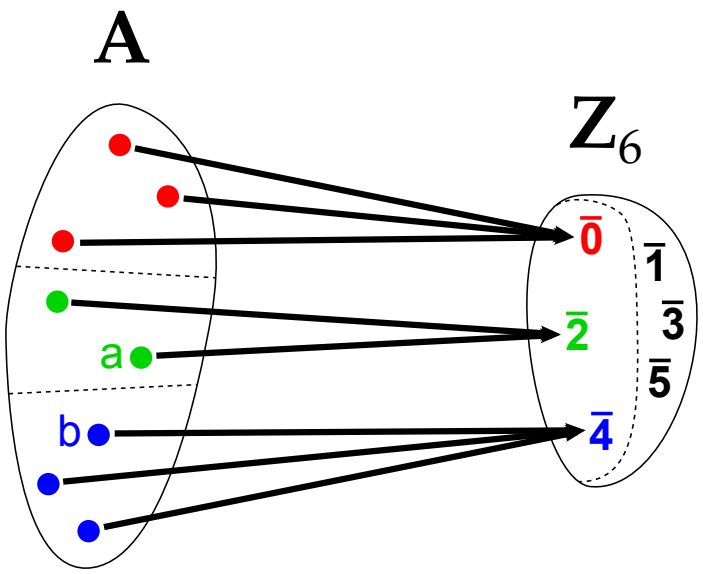
Tétel (Homomorfiatétel)

Ha $\varphi\colon \mathbb{A} \to \mathbb{B}$ 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 $\varphi\colon (A; *) \to (\mathbb{Z}_6; +)$ homomorfizmus.



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

A homomorfiatétel szerint minden homomorfizmus felfogható egy faktorizálás és egy beágyazás egymásutánjaként.

Példa

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

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

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

Példa

Írjuk fel a homomorfiatételt a

$$\operatorname{sgn}\colon (\mathbb{R};\cdot) \to (\mathbb{R};\cdot)$$

homomorfizmusra.

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

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

A mag szerinti faktor:

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