Diszkrét matematika I. középszint

5. előadás

Mérai László diái alapján

Komputeralgebra Tanszék

2014. ősz

Számfogalom bővítése

A természetes számokból kiindulva megkonstruálhatók a

- természetes számok: $\mathbb{N} = \{0, 1, \dots\}$;
- egész számok: $\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$;
- racionális számok: $\mathbb{Q} = \{p/q : p, q \in \mathbb{Z}, q \neq 0\}$;
- valós számok: $\mathbb{R} = ?$;
- komplex számok: $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$.

Kérdések

- Milyen fontos tulajdonságokkal rendelkeznek az adott számhalmazok?
- Mik a valós számok?
- Mi a pontos kapcsolat a műveletek és a számhalmazok között?

  $\mathbb{N}$-ben nincs kivonás, de $\mathbb{Z}$-ben van,

  $\mathbb{Z}$-ben nincs osztás, de $\mathbb{Q}$-ban van...

Természetes számok

Peano-axiómák

Legyen $\mathbb{N}$ egy halmaz, $^+$ egy unér művelet (rákövetkező). Ekkor

1. $0 \in \mathbb{N}$;
2. $n \in \mathbb{N} \Rightarrow n^+ \in \mathbb{N}$;
3. $n \in \mathbb{N} \Rightarrow n^+ \neq 0$;
4. $n, m \in \mathbb{N}$ esetén $n^+ = m^+ \Rightarrow n = m$;
5. $(S \subset \mathbb{N}, 0 \in S, (n \in S \Rightarrow n^+ \in S)) \Rightarrow S = \mathbb{N}$.

Megjegyzések

- Az axiómák egyértelműen definiálják $\mathbb{N}$-et.
- Mindegyik axióma szükséges.
- $\mathbb{N}$ halmaz megkonstruálható: $0 := \emptyset$, $0^+ := \{\emptyset\}$, $(0^+)^+ := \{\emptyset, \{\emptyset\}\}$,...
- $1 := 0^+$, $2 := 1^+$, ...

Műveletek természetes számokkal

$\mathbb{N}$-en természetes módon definiálhatjuk az összeadást (HF), például $n+1 := n^+$, $n+2 := (n^+)^+$, ...

Állítás

Ha k, m, $n \in \mathbb{N}$, akkor

1. $(k+m)+n = k+(m+n)$ (asszociativitás);
2. $k+m = m+k$ (kommutativitás);
3. $0+n = n+0 = n$ (van nullelem/egységelem/semleges elem).

Félcsoportok

Definíció

A G halmaz a $*$ művelettel félcsoport, ha $*$ asszociatív G-n.
Ha létezik $n \in G$: $\forall g \in G : n * g = g * n = g$, akkor az n egységelem (nullelem, neutrális elem), G pedig egységelemes félcsoport.

Példa

- $\mathbb{N}$ az $+$ művelettel egységelemes félcsoport $n = 0$ egységelemmel.
- $\mathbb{Q}$ a $\cdot$ művelettel egységelemes félcsoport $n = 1$ egységelemmel.
- $\mathbb{C}^{k \times k}$ a mátrixszorzással egységelemes félcsoport az egységmátrixszal, mint egységelemmel.

Egész számok

Az $\mathbb{N}$ halmazon nem (mindig) tudjuk a kivonást elvégezni.
A kivonás elvégzéséhez elég (lenne), hogy a 0-ból ki tudjuk vonni az adott n számot (ellentett):

Definíció

Legyen G egy egységelemes félcsoport a $*$ művelettel és n egységelemmel. A $g \in G$ elem inverze (ellentettje) a $g^{-1} \in G$ elem, melyre $g * g^{-1} = g^{-1} * g = n$.
Ha minden $g \in G$ elemnek létezik inverze, akkor G csoport. Ha $*$ kommutatív, akkor G Abel-csoport.

Állítás

$\mathbb{Z}$ a legszűkebb olyan (Abel-) csoport, mely tartalmazza $\mathbb{N}$-et.

Megjegyzés
$\mathbb{Z}$ megkonstruálható $\mathbb{N}$-ből: az $(r, s) \sim (p, q)$, ha $r + q = p + s$ ekvivalenciareláció osztályai az egész számok.

Csoportok

További példák csoportokra:

- $\mathbb{Q}$ az $+$ művelettel, a 0 egységelemmel.
- $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ a $\cdot$ művelettel, az 1 egységelemmel.
- $\{M \in \mathbb{C}^{k \times k} : \det M \neq 0\}$ a mátrixszorzással, és az egységmátrixszal, mint egységelemmel.
- $X \to X$ bijektív függvények a $\circ$ művelettel, és az $id_X : x \mapsto x$ identikus leképzéssel, mint egységelemmel.

Egész számok szorzása

Az egész számok körében definiálhatjuk a $\cdot$ műveletet:

Ha $n \in \mathbb{N}$, $m \in \mathbb{Z}$, akkor legyen $n \cdot m = \underbrace{m + m + \cdots + m}_{n \text{ darab}}$.

Ha $n \notin \mathbb{N}$, akkor legyen $n \cdot m = -\big((-n) \cdot m\big)$.

Állítás

A $\mathbb{Z}$ a $\cdot$ műveletre kommutatív egységelemes félcsoport. (A $\cdot$ kommutatív, asszociatív, van egységelem.)

A két művelet nem ,,független'':

Állítás

$\mathbb{Z}$-n a $\cdot$ az $+$-ra nézve disztributív:
$\forall k, l, m \in \mathbb{Z}$-re: $k \cdot (l + m) = k \cdot l + k \cdot m$.

Gyűrűk

Definíció

Legyen R egy halmaz két binér művelettel: $*$, $\circ$. Ekkor az R gyűrű, ha

- R a $*$ művelettel Abel-csoport (0-val, mint egységelemmel);
- R a $\circ$ művelettel félcsoport;
- a $\circ$ a $*$-ra nézve disztributív:
  $r \circ (s * t) = (r \circ s) * (r \circ t)$; $\quad (s * t) \circ r = (s \circ r) * (t \circ r)$.

Az R egységelemes gyűrű, ha R-en a $\circ$ műveletre nézve van egységelem.
Az R kommutatív gyűrű, ha a $\circ$ művelet (is) kommutatív.

Példa

- $\mathbb{Z}$ az $(+, \cdot)$ műveletekre egységelemes kommutatív gyűrű.
- A páros számok halmaza gyűrű, de nem egységelemes.
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ egységelemes kommutatív gyűrűk.
- $\mathbb{C}^{k \times k}$ egységelemes gyűrű, de nem kommutatív.

Nullosztómentes gyűrűk

A gyűrűkben általában nem lehet elvégezni az osztást:

- $\mathbb{Z}$-ben nem oldható meg a $2x = 1$ egyenlet.
- $\mathbb{R}^{2\times 2}$-ben nem oldható meg az alábbi egyenlet

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

Definíció

Ha egy $(R, *, \circ)$ gyűrűben $\forall r, s \in R,\ r, s \neq 0$ esetén $r \circ s \neq 0$, akkor R nullosztómentes gyűrű.

Példa

Nem nullosztómentes gyűrű

- $\mathbb{R}^{2\times 2}$: $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

Testek

Szeretnénk $\mathbb{Z}$-ben az osztást elvégezni. Mivel az osztás nem ,,szép" művelet (nem asszociatív), ezért azt a reciprokkal (inverzzel) való szorzással helyettesítenénk.

Definíció

Legyen K egy halmaz, azon két művelet: $*$, $\circ$. A K ferdetest, ha

- K gyűrű;
- $K^* = K \setminus \{0\}$ a $\circ$ művelettel csoport.

Megjegyzés Ha K^* csoport, akkor minden elemnek létezik inverze (reciproka), így minden elemmel tudunk osztani.

Állítás

$\mathbb{Q}$ az $\mathbb{N}$-et tartalmazó legszűkebb test.

Megjegyzés

$\mathbb{Q}$ megkonstruálható $\mathbb{Z}$ segítségével: az $(r, s) \sim (p, q)$ $(s, q \neq 0)$, ha $r \cdot q = p \cdot s$ ekvivalenciareláció osztályai a racionális számok.

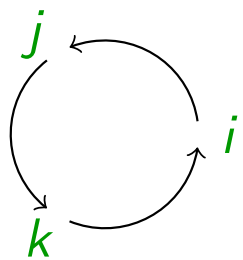
Testek

Példa

- $\mathbb{R}$, $\mathbb{C}$
- $\{r + s\sqrt{2} : \ r, s \in \mathbb{Q}\}$:

$$\frac{1}{r+s\sqrt{2}} = \frac{1}{r+s\sqrt{2}} \cdot \frac{r-s\sqrt{2}}{r-s\sqrt{2}} = \\ = \frac{r-s\sqrt{2}}{r^2-2s^2} = \frac{r}{r^2-2s^2} + \frac{-s}{r^2-2s^2}\sqrt{2}$$

- Kvaterniók $\mathbb{H} = \{a + bi + cj + dk : \ a, b, c, d \in \mathbb{R}\}$, továbbá $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$, ... Nemkommutatív ferdetest!



Számok és rendezés

$\mathbb{Z}$-n a természetes módon definiálhatjuk a rendezést:

- Adott $n \in \mathbb{N}$, $n \neq 0$ esetén legyen $0 < n$.
- Legyen továbbá $n < m$, ha $0 < m - n$.

Ekkor a rendezés kompatibilis a műveletekkel:

Állítás

Ha k, m, $n \in \mathbb{Z}$, akkor

- $k < m \Rightarrow k + n < m + n$,
- $m, n > 0 \Rightarrow m \cdot n > 0$.

Definíció

Egy R gyűrű rendezett gyűrű, ha van az R-en definiálva egy rendezés, mely kielégíti a fenti tulajdonságokat.

Rendezett testek

A $\mathbb{Z}$-n definiált rendezés kiterjeszthető $\mathbb{Q}$-ra: $\frac{p}{q} < \frac{r}{s}$, ha $ps < rq$.

A kiterjesztés azonban nem lesz ,,teljes", $\mathbb{Q}$ nem lesz felső határ tulajdonságú.

Emlékeztető

Egy X halmaz felső határ tulajdonságú, ha minden $\emptyset \neq Y \subset X$ felülről korlátos részhalmaznak van supremuma.

Állítás

$\sqrt{2} \notin \mathbb{Q}$.

Speciálisan $\mathbb{Q}$ nem felső határ tulajdonságú: $\{r \in \mathbb{Q} : r \leq \sqrt{2}\}$ felülről korlátos, de nincs supremuma ($\sup = \sqrt{2} \notin \mathbb{Q}$).

Bizonyítás

Indirekt tfh $\exists n, m \in \mathbb{N}^+$: $(m/n)^2 = 2$. Válasszuk azt az m, n párt, ahol $(m, n) = 1$. Most $m^2 = 2n^2 \Rightarrow 2 \mid m$. Legyen $m = 2k \Rightarrow$ $m^2 = 4k^2 = 2n^2 \Rightarrow 2 \mid n \Rightarrow (m, n) \geq 2$. □

Valós számok

Valós számok axiómája

Legyen $\mathbb{R}$ az $\mathbb{N}$-et tartalmazó legszűkebb felső határ tulajdonsággal rendelkező rendezett test.

Megjegyzés

- A valós számok halmaza lényegében egyértelmű.
- $\mathbb{R}$ megkonstruálható: legyen $\mathbb{R}$ a $\mathbb{Q}$ kezdőszeletei:
  Egy $A \subset \mathbb{Q}$ kezdőszelet, ha $A \neq \mathbb{Q}$, és $r \in A$, $s < r \Rightarrow s \in A$;
  például $\sqrt{2} \leftrightarrow \{r \in \mathbb{Q} : r \leq \sqrt{2}\}$.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ definiálható $\mathbb{R}$ segítségével is:

- $\mathbb{N}$: a $0, 1 \in \mathbb{R}$ elemeket tartalmazó legszűkebb félcsoport;
- $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$;
- $\mathbb{Q} = \{r/s \in \mathbb{R} : r, s \in \mathbb{Z}, s \neq 0\}$.

Összefoglaló

Műveletek halmazokon

Struktúra	Példa
Peano axiómák	$\mathbb{N}$
félcsoport: van asszociatív művelet	$(\mathbb{N}, +)$, $(\mathbb{Z}, \cdot)$
csoport: van inverz	$(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{Z}_m, +)$, $(\mathbb{Z}_p^*, \cdot)$
gyűrű: két művelet,	$(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}_m, +, \cdot)$,
$*$-ra kommutatív csoport,	$(\mathbb{R}^{k\times k}, +, \cdot)$
$\circ$-re félcsoport, disztributivitás	
ferdetest: két művelet,	$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{Z}_p$
$*$-ra kommutatív csoport,	
$\circ$-re a 0 kivételével csoport,	
disztributivitás	

Összefoglaló

Műveletek és rendezés

Struktúra	**Példa**
rendezett gyűrű	$\mathbb{Z}$
rendezett test	$\mathbb{Q}$, $\mathbb{R}$
felsőhatár tulajdonságú test	$\mathbb{R}$