Diszkrét matematika 1. középszint

6. előadás

Nagy Gábor
nagygabr@gmail.com
nagy@compalg.inf.elte.hu
compalg.inf.elte.hu/∼ nagy
Mérai László diái alapján

Komputeralgebra Tanszék

2017. ősz

Monoton függvények

Definíció

Legyenek $(X; \preceq_1)$, $(Y; \preceq_2)$ részbenrendezett halmazok. Az $f : X \to Y$ függvény

1. monoton növekedő, ha $\forall x, y \in X$, $x \preceq_1 y \Rightarrow f(x) \preceq_2 f(y)$;
2. szigorúan monoton növekedő, ha $\forall x, y \in X$, $x \prec_1 y \Rightarrow f(x) \prec_2 f(y)$;
3. monoton csökkenő, ha $\forall x, y \in X$, $x \preceq_1 y \Rightarrow f(y) \preceq_2 f(x)$;
4. szigorúan monoton csökkenő, ha $\forall x, y \in X$, $x \prec_1 y \Rightarrow f(y) \prec_2 f(x)$.

Példa

- Legyen $X = \mathbb{R}$ a szokásos rendezéssel. Ekkor az $f(x) = x$; $g(x) = x^3$ szigorúan monoton növekedő függvények.
- Legyen X az $\{a, b, c\}$ hatványhalmaza a részhalmaza részbenrendezéssel.
  Ekkor az $f(A) = A \setminus \{a\}$ monoton növekedő: $A \subseteq B \Rightarrow f(A) = A \setminus \{a\} \subseteq B \setminus \{a\} = f(B)$;
  A $g(A) = \overline{A}$ szigorúan monoton csökkenő: $A \subsetneq B \Rightarrow \overline{B} \subsetneq \overline{A}$.

Monoton függvények

Megjegyzés

- Ha $(X; \preceq_1)$, $(Y; \preceq_2)$ rendezett halmazok, akkor egy szigorúan monoton növekedő (ill. csökkenő) függvény injektív is:
  $x \neq y \Rightarrow (x \prec_1 y \vee y \prec_1 x) \Rightarrow (f(x) \prec_2 f(y) \vee f(y) \prec_2 f(x)) \Rightarrow$
  $\Rightarrow f(x) \neq f(y)$.
- Ha $(X; \preceq_1)$, $(Y; \preceq_2)$ rendezett halmazok, és f szigorúan monoton növekedő (ill. csökkenő) függvény, akkor f^{-1} szigorúan monoton növekedő (ill. csökkenő) függvény:
  Mivel f injektív, f^{-1} is függvény.
  Ha $f(x) \prec_2 f(y)$, akkor nem lehet $y \preceq_1 x$, hiszen $y = x$ esetén $f(y) = f(x)$, $y \prec_1 x$ esetén $f(y) \prec_2 f(x)$ teljesülne.

Példa

Legyen $X = \mathbb{R}$ a szokásos rendezéssel. Ekkor az $f(x) = \sqrt[3]{x}$ szigorúan monoton növekedő függvény.

Műveletek

Definíció

Egy X halmazon értelmezett binér (kétváltozós) művelet egy $* : X \times X \to X$ függvény. Gyakran $*(x, y)$ helyett $x * y$-t írunk.
Egy X halmazon értelmezett unér (egyváltozós) művelet egy $* : X \to X$ függvény.

Példa

- $\mathbb{C}$ halmazon az $+$, $\cdot$ binér, $z \mapsto -z$ (ellentett) unér művelet.
- $\mathbb{C}$ halmazon az $\div$ (osztás) nem művelet, mert $\mathrm{dmn}(\div) \neq \mathbb{C} \times \mathbb{C}$.
- $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ halmazon az $\div$ binér, az $x \mapsto 1/x$ (reciprok) unér művelet.
- $\mathbb{C}$ halmazon a 0 illetve 1 konstans kijelölése nullér művelet.

Műveletek

Egy véges halmazon bármely binér művelet megadható a műveleti táblájával.

$\wedge$	I	H
I	I	H
H	H	H

$\vee$	I	H
I	I	I
H	I	H

XOR	I	H
I	H	I
H	I	H

$\neg$	I	H
	H	I

Definíció (Műveletek függvényekkel)

Legyen X tetszőleges halmaz, Y halmaz a $*$ művelettel, $f, g : X \to Y$ függvények. Ekkor

$$(f * g)(x) = f(x) * g(x).$$

Példa

$(\sin + \cos)(x) = \sin x + \cos x$

Műveleti tulajdonságok

Definíció

A $* : X \times X \to X$ művelet
asszociatív, ha $\forall a, b, c \in X : (a * b) * c = a * (b * c)$;
kommutatív, ha $\forall a, b \in X : a * b = b * a$.

Példa

- $\mathbb{C}$-n az $+$ ill. a $\cdot$ műveletek asszociatívak, kommutatívak.
- A függvények halmazán a kompozíció művelete asszociatív: $(f \circ g) \circ h = f \circ (g \circ h)$.
- Az $\mathbb{R} \to \mathbb{R}$ függvények halmazán a kompozíció művelete nem kommutatív: $f(x) = x + 1$, $g(x) = x^2$: $x^2 + 1 = (f \circ g)(x) \neq (g \circ f)(x) = (x + 1)^2$.
- Az osztás nem asszociatív $\mathbb{C}^*$-on: $\frac{a}{bc} = (a \div b) \div c \neq a \div (b \div c) = \frac{ac}{b}$.

Művelettartó leképezések

Definíció

Legyen X halmaz a $*$ művelettel, Y a $\diamond$ művelettel. Az $f : X \to Y$ függvény művelettartó, ha $\forall x, y \in X$ esetén

$$f(x * y) = f(x) \diamond f(y).$$

Példa

- Legyen $X = \mathbb{R}$ az $+$ művelettel, $Y = \mathbb{R}^+$ a $\cdot$ művelettel. Ekkor az $x \mapsto a^x$ művelettartó: $a^{x+y} = a^x \cdot a^y$.
- Legyen $X = Y = \mathbb{C}$ az $+$ művelettel. Ekkor a $z \mapsto \overline{z}$ művelettartó: $\overline{z + w} = \overline{z} + \overline{w}$.

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. $(S \subseteq \mathbb{N}, 0 \in S, (n \in S \Rightarrow n^+ \in S)) \Rightarrow S = \mathbb{N}$.

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, például $n+1 := n^+$, $n+2 := (n^+)^+$, ...

Állítás

Bármely k, m, $n \in \mathbb{N}$ esetén

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).

Algebrai struktúrák

Definíció

A $(H; M)$ pár algebrai struktúra, ha H egy halmaz, M pedig H-n értelmezett műveletek halmaza.
Az egy binér műveletes struktúrát grupoidnak nevezzük.

Példa

- $(\mathbb{N}; +)$ algebrai struktúra, mert természetes számok összege természetes szám, és grupoid is.
- $(\mathbb{N}; -)$ nem algebrai struktúra, mert például $0 - 1 = -1 \notin \mathbb{N}$.
- $(\mathbb{N}; +, ^+)$ algebrai struktúra, mert természetes számok összege, és rákövetkezője természetes szám, de nem grupoid.

Félcsoportok

Definíció

A $(G; *)$ grupoid félcsoport, ha $*$ asszociatív G-n.
Ha létezik $s \in G$: $\forall g \in G : s * g = g * s = g$,
akkor az s semleges elem (egységelem), $(G; *)$ pedig semleges elemes félcsoport (egységelemes félcsoport, monoid).

Példa

- $(\mathbb{N}; +)$ egységelemes félcsoport $s = 0$ egységelemmel.
- $(\mathbb{Q}; \cdot)$ egységelemes félcsoport $s = 1$ 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 e egységelemmel.
A $g \in G$ elem inverze a $g^{-1} \in G$ elem, melyre $g * g^{-1} = g^{-1} * g = e$.
Ha minden $g \in G$ elemnek létezik inverze, akkor G csoport.
Ha $*$ kommutatív is, 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:

- $(\mathbb{Q}; +)$: a 0 egységelem, minden szám inverze az ellentettje.
- $(\mathbb{Q}^*; \cdot)$: az 1 egységelem, minden szám inverze a reciproka. $(\mathbb{Q}^* = \mathbb{Q} \setminus \{0\})$
- $\{M \in \mathbb{C}^{k \times k} : \det M \neq 0\}$ 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 $\cdot$ művelettel 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: $k \cdot (l + m) = k \cdot l + k \cdot m$, illetve $(k + m) \cdot l = k \cdot l + m \cdot l$.

Gyűrűk

Definíció

Legyen $(R; *, \diamond)$ algebrai struktúra, ahol $*$ és $\diamond$ binér műveletek. Azt mondjuk, hogy teljesül a $\diamond$-nak a $*$-ra vonatkozó bal oldali disztributivitása, illetve jobb oldali disztributivitása, ha
$\forall k, l, m \in R$-re: $k \diamond (l * m) = (k \diamond l) * (k \diamond m)$, illetve
$\forall k, l, m \in R$-re: $(k * l) \diamond m = (k \diamond m) * (l \diamond m)$.

Példa

$(\mathbb{Z}; +, \cdot)$ esetén teljesül a szorzás összeadásra vonatkozó mindkét oldali disztributivitása.

Elnevezés

$(R; *, \diamond)$ két binér műveletes algebrai struktúra esetén a $*$-ra vonatkozó semleges elemet nullelemnek, a $\diamond$-ra vonatkozó semleges elemet egységelemnek nevezzük. A nullelem szokásos jelölése 0, az egységelemé 1, esetleg e.

Gyűrűk

Definíció

Az $(R; *, \diamond)$ két binér műveletes algebrai struktúra gyűrű, ha

- $(R; *)$ Abel-csoport;
- $(R; \diamond)$ félcsoport;
- teljesül a $\diamond$-nak a $*$-ra vonatkozó mindkét oldali disztributivitása.

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

Példa

- $(\mathbb{Z}; +, \cdot)$ egységelemes kommutatív gyűrű.
- $(2\mathbb{Z}; +, \cdot)$ gyűrű, de nem egységelemes.
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ a szokásos műveletekkel egységelemes kommutatív gyűrűk.
- $\mathbb{C}^{k\times k}$ a szokásos műveletekkel egységelemes gyűrű, de nem kommutatív, ha $k > 1$.

Nullosztómentes gyűrűk

Definíció

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

Példa

Nem nullosztómentes gyűrű

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

A gyűrűkben nem mindig 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

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

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

Az $(R; *, \diamond)$ gyűrű ferdetest, ha $(R \setminus \{0\}; \diamond)$ csoport. A kommutatív ferdetestet testnek nevezzük.

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.

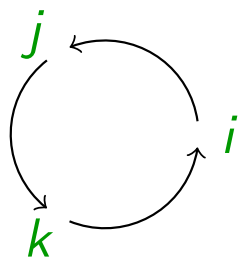
Testek

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: $\frac{p}{q} < \frac{r}{s}$ $(0 < q, s)$, 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 $\emptyset \neq Y \subseteq X$ 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 úgy az m, n párt, hogy $(m, n) = 1$. 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 halmazának definíciója

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 $\mathbb{Q}$ kezdőszeleteinek halmaza:
  Egy $A \subseteq \mathbb{Q}$ 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;
- $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N})$;
- $\mathbb{Q} = \{r/s \in \mathbb{R} : r, s \in \mathbb{Z}, s \neq 0\}$.