MTNM113E: Műveletek és algebrák

(előadásvázlat, 2022. november 11.)

Kátai-Urbán Kamilla

Jelölje $\mathbb{Z}$ az egész számok halmazát, $\mathbb{N}$ a pozitív egészek halmazát, $\mathbb{N}_0$ a nem negatív egészek halmazát, $\mathbb{Q}$ a racionális számok halmazát, $\mathbb{R}$ a valós számok halmazát, $\mathbb{R}_0^+$ a nem negatív valós számok halmazát, $\mathbb{C}$ a komplex számok halmazát, $\mathbb{R}^{m\times n}$ az $m\times n$-es valós mátrixok halmazát, továbbá $GL(n,\mathbb{R}) = \{M \in \mathbb{R}^{n\times n} : |M| \neq 0\}$, azaz az $n\times n$-es invertálható valós mátrixok halmazát jelöli. Valamint jelölje B^A az A halmazból B halmazba menő leképzések halmazát, S_n pedig tetszőleges pozitív n egész esetén az $\{1,\dots,n\}$ halmaz összes permutációjának halmazát.

1. Műveleti tulajdonságok

1. Jelölés. Legyen A egy tetszőleges halmaz, jelölje A^n az n-tényezős $A\times A\times\cdots\times A$ Descartes-szorzatot.

2. Definíció. Legyen A tetszőleges nemüres halmaz, és $n\in\mathbb{N}_0$. Az A-n értelmezett n-változós műveleten egy $A^n\to A$ leképezést értünk, n-et a művelet változószámának (aritásának) nevezzük.

3. Megjegyzés. Az előző definíció $n=0$ esetén egy elem kijelölését jelenti az A halmazból.

4. Definíció. Legyen A tetszőleges nemüres halmaz, $\mathcal{F}$ pedig jelölje az A-n értelmezett műveletek egy halmazát, ekkor az $(A;\mathcal{F})$ párt algebrának nevezzük.

5. Példa. Ha az előző definícióban szereplő $\mathcal{F}$ véges halmaz, akkor elemeit felsoroljuk a halmaz jelet elhagyva, például algebrák a következők: $(\mathbb{Z};+,\cdot)$, $(\mathbb{Z};-)$, $(\mathbb{N};1,\cdot)$, $(\mathbb{R}^3;+)$, $(\mathbb{R}^{2\times3};+)$, $(GL(2,\mathbb{R});\cdot)$, $(\mathbb{C};+,\cdot)$, $(A^A;\cdot)$, $(S_n;\mathrm{id},\cdot)$.

6. Definíció. Azokat az algebrákat, amelyeknek egy kétváltozós művelete van grupoidnak nevezzük.

7. Példa. A 5. példában megadott algebrák közül a következők grupoidok: $(\mathbb{Z};-)$, $(\mathbb{R}^3;+)$, $(\mathbb{R}^{2\times3};+)$, $(GL(2,\mathbb{R});\cdot)$, $(A^A;\cdot)$.

8. Definíció. (Grupoid műveleti tulajdonságai)

(1) Az $(A;\circ)$ grupoid asszociatív, ha $(\forall a,b,c\in A)\big(a\circ(b\circ c)=(a\circ b)\circ c\big)$.
(2) Az $(A;\circ)$ grupoid kommutatív, ha $(\forall a,b\in A)(a\circ b=b\circ a)$.
(3) Az $(A;\circ)$ grupoidban van zéruselem, ha $(\exists o\in A)(\forall a\in A)(a\circ o=o\circ a=o)$.
(4) Az $(A;\circ)$ grupoidban van egységelem, ha $(\exists e\in A)(\forall a\in A)(a\circ e=e\circ a=a)$.
(5) Ha az $(A;\circ)$ grupoidban e egységelem, és $(\forall a\in A)(\exists b\in A)(a\circ b=b\circ a=e)$, akkor minden elemnek van inverze.

9. Tétel. Bármely grupoidban legfeljebb egy egységelem és legfeljebb egy zéruselem van.

10. Definíció. Ha a grupoidnak van egységeleme, egységelemes, ha van zéruseleme, zéruselemes grupoidnak nevezzük.

11. Példa. Olyan grupoidokra adunk példát, melyek a 8. definícióban szereplő tulajdonságokkal rendelkeznek.

(1) Asszociatív grupoidok: $(\mathbb{N};\cdot)$, $(\mathbb{R}^3;+)$, $(GL(n,\mathbb{R});\cdot)$, $(A^A;\cdot)$, $(S_n;\cdot)$.
(2) Kommutatív grupoidok: $(\mathbb{N};\cdot)$, $(\mathbb{R}^3;+)$, $(\mathbb{C};+)$, $(\mathbb{R}^{2\times3};+)$.
(3) Zéruselemes grupoidok: $(\mathbb{Z};\cdot)$ zéruseleme a 0, $(\mathbb{C};\cdot)$ zéruseleme a 0, $(\mathbb{R}^{2\times2};\cdot)$ zéruselme a 2×2-es zérómátrix.

grupoid	zéruselem
$(\mathbb{Z};\cdot)$	0
$(\mathbb{C};\cdot)$	0
$(\mathbb{R}^{2\times2};\cdot)$	$\left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$

(4) Egységelemes grupoidok: $(\mathbb{Z};\cdot)$ egységeleme az 1, $(\mathbb{C};+)$ egységeleme a 0, $(\mathbb{R}^{2\times 2};\cdot)$ egységelme a 2×2-es egységmátrix, $(A^A;\cdot)$ egységeleme id_A és $(S_n;\cdot)$ egységeleme id.

grupoid	egységelem
$(\mathbb{Z};\cdot)$	1
$(\mathbb{C};+)$	0
$(\mathbb{R}^{2\times 2};\cdot)$	$\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$
$(A^A;\cdot)$	id_A
$(S_n;+)$	id

(5) Egységelmeles grupoidok, ahol minden elemnek van inverze: $(\mathbb{Z};+)$-ban az a inverze $-a$, $(\mathbb{R}^3;+)$-ban a v inverze $-v$, $(\mathbb{Q}\setminus\{0\};\cdot)$-ban a inverze $1/a$, $(S_n;\cdot)$-ban az a permutációs inverze mindig kiszámítható (bijektív leképezéseknek van inverze), jelölje a^{-1}, $(GL(n,\mathbb{R});\cdot)$-ban az összes $n\times n$-es nemnulla determinánsú mátrix szerepel, így minden elemnek van inverze.

grupoid	a inverze
$(\mathbb{Z};+)$	$-a$
$(\mathbb{R}^3;+)$	$-a$
$(\mathbb{Q}\setminus\{0\};\cdot)$	$\frac{1}{a}$
$(S_n;\cdot)$	a^{-1}
$(GL(n,\mathbb{R});\cdot)$	a^{-1}

12. Példa. Olyan grupoidokra adunk példát, melyek NEM rendelkeznek a 8. definícióban szereplő tulajdonságokkal.

(1) Nem asszociatív grupoidok: $(\mathbb{Z};-),(\mathbb{Q}\setminus\{0\};:)$.
(2) Nem kommutatív grupoidok: $(\mathbb{Z};-),(\mathbb{Q}\setminus\{0\};:),(\mathbb{R}^{2\times 2};\cdot),(A^A;\cdot),(S_n;\cdot)$.
(3) Grupoidok, ahol nincs zéruselem: $(\mathbb{Z};-),(\mathbb{Z};+),(\mathbb{N};\cdot),(GL(n,\mathbb{R});\cdot),(S_n;\cdot)$.
(4) Grupoidok, ahol nincs egységelem: $(\mathbb{N};+),(\mathbb{Z};-),(\mathbb{Q}\setminus\{0\};:)$.
(5) Egységelemes grupoidok, ahol nincs minden elemnek inverze: $(\mathbb{N}_0;+),(\mathbb{Q};\cdot),(\mathbb{R}^{2\times 2};\cdot),(A^A;\cdot)$.

13. Definíció. Legyen $\circ$ és $\star$ két kétváltozó művelet az A halmazon. A $\circ$ disztributív a $\star$-ra nézve, ha $(\forall a,b,c\in A)((a\circ(b\star c)=(a\circ b)\star(a\circ c))\wedge((b\star c)\circ a=(b\circ a)\star(c\circ a)))$.

14. Példa. A $\mathbb{C},\mathbb{R},\mathbb{Q},\mathbb{Z},\mathbb{N},\mathbb{R}^{n\times n}$ halmazon a $\cdot$ disztributív a $+$-ra.

2. Félcsoport, csoport

15. Definíció. Az asszociatív grupoidokat félcsoportnak nevezzük. Az egységelmes félcsoportokat monoidnak nevezzük. Azokat a monoidokat, ahol minden elemnek van inverze csoportoknak hívjuk. A kommutatív csoportokat Abel-csoportoknak nevezzük.

16. Példa. Az $(\mathbb{N};+)$ félcsoport, de nem monoid.

17. Példa. A következők monoidok, de nem csoportok: $(\mathbb{N};\cdot)$, $(\mathbb{N}_0;+)$, $(\mathbb{R};\cdot)$, $(\mathbb{R}^{n\times n};\cdot)$, $(A^A;\cdot)$.

18. Példa. Nem (feltétlen) Abel-csoport az $(S_n;\cdot)$ csoport, melynek neve a teljes szimmetrikus csoport, továbbá a $(GL(n,\mathbb{R});\cdot)$ csoport, melynek neve az általános lineáris csoport.

19. Példa. A következők Abel-csoportok: $(\mathbb{Z};+)$, $(\mathbb{R}\setminus\{0\};\cdot)$, $(\mathbb{C};+)$, $(\mathbb{R}^{n\times m};+)$.

20. Tétel. Tetszőleges monoidban minden elemnek legfeljebb egy inverze van.

21. Tétel. Legyen $(A;\cdot)$ monoid. Ha az $a,b\in A$ elemnek van inverze: a^{-1},b^{-1}, akkor az a^{-1} és ab elemeknek is van inverze, mégpedig

(1) $(a^{-1})^{-1}=a$,
(2) $(ab)^{-1}=b^{-1}a^{-1}$.

22. Definíció. Legyen $(A;\cdot)$ tetszőleges csoport, és jelölje 1 az egységelemet. Az $a \in A$ elem n-edik hatványát ($n \in \mathbb{Z}$) a következőképpen definiáljuk:

$$a^n = \begin{cases} \underbrace{a \cdots a}_{n \text{ db}}, & \text{ha } n > 0, \\ 1, & \text{ha } n = 0, \\ \underbrace{a^{-1} \cdots a^{-1}}_{-n \text{ db}}, & \text{ha } n < 0. \end{cases}$$

23. Lemma. Legyen $(A;\cdot)$ tetszőleges csoport, $a \in A$ és $n \in \mathbb{Z}$. Ekkor $a^n \cdot a = a \cdot a^n = a^{n+1}$ és $a^{-1} \cdot a^n = a^n \cdot a^{-1} = a^{n-1}$.

24.* Tétel. Legyen $(A;\cdot)$ tetszőleges csoport. Bármely $m, n \in \mathbb{Z}$-re és $a, b \in A$-ra

(1) $a^m a^n = a^{m+n}$,
(2) $(a^m)^n = a^{mn}$,
(3) ha $ab = ba$, akkor $(ab)^n = a^n b^n$.

25. Definíció. Legyen $(A;\cdot)$ tetszőleges csoport, és jelölje 1 az egységelemet. Az $a \in A$ elem rendje az a legkisebb pozitív egész $n \in \mathbb{N}$, amelyre $a^n = 1$. Ha nincs ilyen n, akkor a rendje végtelen. Az elem rendjét $o(a)$-val jelöljük.

26. Példa. Az $(S_5;\cdot)$ csoportban $o((1\ 2\ 3)(4\ 5)) = 6$, mert a ciklusok függetlenek, azaz felcserélhetőek, így külön hatványozhatóak. A $(\mathbb{C} \setminus \{0\};\cdot)$ csoportban $o(i) = 4$ és $o(1 + \sqrt{3}i) = \infty$.

27. Tétel. Legyen $(A;\cdot)$ csoport, $a \in A$ véges rendű elem, és $n, m \in \mathbb{Z}$

(1) $a^n = 1$ akkor és csak akkor teljesül, ha $o(a) \mid n$,
(2) $a^n = a^m$ akkor és csak akkor teljesül, ha $o(a) \mid n - m$.

3. Gyűrű, test

28. Definíció. Az $(A;+,\cdot)$ algebrát gyűrűnek nevezzük, ha $(A;+)$ Abel-csoport, $(A;\cdot)$ félcsoport, és a $\cdot$ disztributív az $+$-ra. Az $(A;+)$ Abel-csoportot a gyűrű additív csoportjának, az $(A;\cdot)$ félcsoportot a gyűrű multiplikatív félcsoportjának nevezzük.

29. Példa. Gyűrűk: $(\mathbb{Z};+,\cdot)$, $(\mathbb{R};+,\cdot)$, $(\mathbb{R}^{2\times 2};+,\cdot)$, $(\mathbb{C};+,\cdot)$.

30. Tétel. Az $(A;+,\cdot)$ gyűrű esetén

(1) a 0 additív egységelem a szorzásra nézve zéruselem,
(2) tetszőleges $a, b \in A$ elemekre $(-a)b = a(-b) = -(ab)$.

31. Definíció. Az $(A;+,\cdot)$ gyűrűt egységelemesnek nevezzük, ha $(A;\cdot)$ monoidot alkot, azaz van a szorzásra nézve egységeleme.

32. Példa. A $(\mathbb{Z};+,\cdot)$, $(\mathbb{C};+,\cdot)$, $(\mathbb{R}^{n\times n};+,\cdot)$ gyűrűk mind egységelemesek, a $(\{\text{páros számok}\},+,\cdot)$ gyűrű nem egységelemes. Egységelemes gyűrűkben van értelme megkérdezni, hogy mely elemeknek van multiplikatív inverze.

33. Definíció. Az $(A;+,\cdot)$ gyűrűt testnek nevezzük, ha az $(A\setminus\{0\};\cdot)$ Abel-csoportot alkot, amelyet a test multiplikatív csoportjának nevezzük.

34. Példa. A 29. példában felsorolt gyűrűk közül testek: $(\mathbb{R};+,\cdot)$, $(\mathbb{C};+,\cdot)$.