MBLK13E: Műveletek és algebrák

(előadásvázlat, 2023. február 10.)

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, $\mathbb{R}^n$ az n komponensű valós vektorok halmazát, $\mathbb{R}^{m\times n}$ az $m \times n$-es valós mátrixok halmazát. 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 permutációinak halmazát.

1. Műveleti tulajdonságok, algebrák

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: $(\mathbb{Z}; +, \cdot)$, $(\mathbb{Z}; -)$, $(\mathbb{N}; 1, \cdot)$, $(\mathbb{R}^3; +)$, $(\mathbb{R}^{2\times 3}; +)$, $(\mathbb{C}; +, \cdot)$, $(A^A; \cdot), (S_n; \mathrm{id}, \cdot)$.

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

7. Példa. A 5. Példában megadott algebrák közül a következők grupoidok: $(\mathbb{Z}; -)$, $(\mathbb{R}^3; +)$, $(\mathbb{R}^{2\times 3}; +)$, $(A^A; \cdot), (S_n; \mathrm{id}, \cdot)$.

1.1. Műveleti tulajdonságok

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

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

(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}.

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

1.2. Grupoidok hierarchiája

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. Legyen $GL_n(\mathbb{R})=\{M\in\mathbb{R}^{n\times n}:|M|\neq 0\}$, azaz az $n\times n$-es invertálható valós mátrixok halmaza, $(GL_n(\mathbb{R});\cdot)$ csoportot alkot, melynek neve általános lineáris csoport, ha $n>1$, akkor nem Abel-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) $(ab)^{-1}=b^{-1}a^{-1}$.

2. Csoportok

22. Definíció. Legyen $\circ$ egy kétváltozós művelet a nemüres A halmazon.

(1) A $*$ művelet invertálható, ha bármely $a,b\in A$ elemek esetén az $a*x=b$, illetve $y*a=b$ egyenleteknek **legalább** egy megoldása van.

(2) A $*$ művelet kancellatív, ha bármely $a, b \in A$ elemek esetén az $a * x = b$, illetve $y * a = b$ egyenleteknek **legfeljebb** egy megoldása van.

23. Megjegyzés. A kancellativitás így is megfogalmazható:

$$\forall a, u, v \in A\colon \quad a * u = a * v \implies u = v \quad \text{és} \quad u * a = v * a \implies u = v.$$

24. Tétel. Csoport művelete mindig invertálható és kancellatív.

25. Állítás. Véges alaphalmaz esetén az invertálhatóság és a kancellativitás egymással ekvivalens.

26. Megjegyzés. Sok esetben, ha egyértelmű, hogy mi a csoportban a művelet, akkor a műveleti jelet nem írjuk ki, csak az alaphalmazt. Például, ha azt írjuk, hogy $\mathbb{Z}$ csoport, akkor $+$ a művelet, hiszen $\cdot$ esetén nincs minden elemnek inverze. Hasonlóan a teljes szimmetrikus csoport esetén csak annyi írunk, hogy S_n, hiszen tudjuk, hogy a művelet a permutációk szorzása.

2.1. Hatványozás, elemrend

27. 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:

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

28. 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 $(ab)^n = a^n b^n$.

29. 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.

30. 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 $o(1 + \sqrt{3}i) = \infty$.

31. 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 $n \equiv m \pmod{o(a)}$.

32.* Tétel. Legyen $(A; \cdot)$ csoport, és $a, b \in A$ felcserélhető elemek, azaz $ab = ba$. Ekkor $o(ab) = o(a)o(b)$ akkor és csak akkor, ha $\text{lnko}(o(a), o(b)) = 1$.

2.2. Részcsoport, izomorfia

33. Definíció. Legyen $(G; \cdot)$ csoport Ha $H \subseteq G$ és $(H; \cdot)$ csoport, akkor azt mondjuk, hogy $(H; \cdot)$ részcsoportja $(G; \cdot)$-nek. Továbbá ha $H \neq G$, akkor $(H; \cdot)$ valódi részcsoportja $(G; \cdot)$-nek.

34. Tétel. Tetszőleges G csoport és $\emptyset \neq H \subseteq G$ esetén H akkor és csak akkor részcsoportja G-nek, ha

(1) H tartalmazza G egységelemét: $1_G \in H$;
(2) H zárt a szorzásra: $\forall h_1, h_2 \in H : \ h_1 \cdot h_2 \in H$;
(3) H zárt az inverzképzésre: $\forall h \in H : \ h^{-1} \in H$.

35. Példa. Az S_4 csoportban a $V = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$ részcsoportot alkot, amit Klein-féle csoportnak nevezünk.

36. Példa. Az S_n csoportban a páros permutációk halmaza, A_n részcsoportot alkot, amit alternáló csoportnak nevezünk.

37. Példa. A $GL_n(\mathbb{R})$ általános lineáris csoportban az $SL_n(\mathbb{R}) = \{M \in \mathbb{R}^{n\times n} : |M| = 1\}$, az úgynevezett speciális lineáris csoport, részcsoportot alkot.

38. Példa. A sík összes egybevágósági transzformációi csoportot alkotnak a leképezésszorzás műveletével, egy adott síkidomot önmagába képező egybevágóságok pedig részcsoportot alkotnak ebben a csoportban a síkidom szimmetriacsoportja.

39. Definíció. A szabályos n-szög szimmetriacsoportját n-edfokú diédercsoportnak nevezzük és D_n-nel jelöljük.

40.* Tétel. A D_n csoportnak $2n$ eleme van: $D_n = \{\mathrm{id}, a, a^2, \dots, a^{n-1}, t, at, a^2t, \dots, a^{n-1}t\}$, ahol a jelöli a szabályos n-szög középpontja körüli $\frac{2\pi}{n}$ szögű forgatást, t pedig egy tetszőleges szimmetriatengelyre való tükrözést. Ekkor a^k a középpont körüli $\frac{2k\pi}{n}$ szögű forgatás ($0 \le k \le n-1$), a $t, at, a^2t, \dots, a^{n-1}t$ transzformációk pedig tengelyes tükrözések (két „szomszédos" tengely $\frac{\pi}{n}$ szöget zár be egymással). Fennáll továbbá a $ta = a^{-1}t$ összefüggés.

41. Definíció. Legyen $\mathbb{A} = (A; *)$ és $\mathbb{B} = (B; \oplus)$ két csoport (vagy csak grupoid). Azt mondjuk, hogy a $\varphi\colon A \to B$ leképezés izomorfizmus $\mathbb{A}$-ból $\mathbb{B}$-be, ha φ bijektív leképezés, és φ felcserélhető a műveletekkel, azaz

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

Ha létezik $\varphi\colon \mathbb{A} \to \mathbb{B}$ izomorfizmus, akkor azt mondjuk, hogy $\mathbb{A}$ és $\mathbb{B}$ izomorf, jelölése: $\mathbb{A} \cong \mathbb{B}$.

42. Példa. A D_3 csoport izomorf az S_3 csoporttal ($D_3 \cong S_3$), ugyanis megadható izomorfizmus közöttük. Például, a D_3-ban szereplő $\frac{2\pi}{3}$ szögű forgatást megfeleltethetjük az $(1\ 2\ 3) \in S_3$ permutációnak, valamint a t tükrözést $(1\ 2) \in S_3$-nak, ezek szorzataiként pedig a többi elemet is megkaphatjuk a megfelelő módon. Igazolható, hogy így izomorfizmust kapunk.

43. Megjegyzés. Csoportok közötti izomorfizmus megadásánál nagy segítséget jelent, ha ismerjük az elemek rendjét, ugyanis az egymásnak megfeleltett elemek rendjének meg kell egyeznie.

2.3. Modulo n maradékosztályok

44. Definíció. Az a egész szám modulo n maradékosztályán az $\overline{a} = \{\, b \in \mathbb{Z} \mid b \equiv a \pmod n \,\}$ halmazt értjük. A modulo n maradékosztályok halmazát $\mathbb{Z}_n$ jelöli, azaz $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$.

45. Tétel. A $\mathbb{Z}_n$ halmazon művelet a következőképpen definiált összeadás, kivonás és szorzás:

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} - \overline{b} = \overline{a-b}, \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

46. Példa. Tekintsük $\mathbb{Z}_8$-at, ekkor $\overline{3} + \overline{6} = \overline{3+6} = \overline{1}$, valamint $\overline{2} \cdot \overline{4} = \overline{2 \cdot 4} = \overline{0}$.

47. Tétel. Tetszőleges $n \in \mathbb{N}$ esetén $(\mathbb{Z}_n; +)$ csoport, $(\mathbb{Z}_n; \cdot)$ monoid. A $(\mathbb{Z}_n \setminus \{0\}; \cdot)$ grupoid pontosan akkor csoport, ha n prímszám.

48. Definíció. Az $\overline{a}$ modulo n maradékosztály redukált maradékosztály, ha $\mathrm{lnko}(a, n) = 1$. A modulo n redukált maradékosztályok halmazát $\mathbb{Z}_n^*$ jelöli, azaz $\mathbb{Z}_n^* = \{\, \overline{a} \in \mathbb{Z}_n \mid \mathrm{lnko}(a, n) = 1 \,\}$.

49. Példa. $\mathbb{Z}_9^* = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$.

50. Tétel. $(\mathbb{Z}_n^*; \cdot)$ csoport.

51. Megjegyzés. A 47. Tétel alapján, ha $n > 1$, akkor, ha azt mondjuk, hogy Z_n csoport, a $+$ a művelet. A 50. Tétel alapján a $\mathbb{Z}_n^*$ csoport esetén a $\cdot$ a művelet.

2.4. Generálás, ciklikus csoprot

52. Definíció. A $(G; \cdot)$ csoport X részhalmaza által generált részcsoportja:

$$[X] = \{x_1^{\varepsilon_1} \cdots x_k^{\varepsilon_k} : k \in \mathbb{N}_0, x_i \in X, \varepsilon_i = \pm 1\}.$$

Ha $X = \{a\}$, azaz 1-elemű halmaz, akkor az a elem által generált részcsoport $[a] = \{a^k : k \in \mathbb{Z}\}$.

53. Példa. A $\mathbb{Z}_8$ csoportban $[\overline{4}, \overline{6}] = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$. Ugyanis a generált részcsopotban mindig szerepelnek a generáló elemek, továbbá $\overline{4}+\overline{4} = \overline{0}$, $\overline{4}+\overline{6} = \overline{2}$, és további elemeket már nem tudunk előállítani a csoportban. Ez a részcsoport egy elem segítségével is előállítható, ugyanis $[\overline{2}] = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$, tehát $[\overline{4}, \overline{6}] = [\overline{2}]$

54. Példa. Tekintsük a $\mathbb{Z}_{10}^*$ csopotot, mivel redukált maradékosztályokról van szó $\mathbb{Z}_{10}^* = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$, és a $\cdot$ a művelet. Ekkor $[\overline{9}] = \{\overline{1}, \overline{9}\}$ és $[\overline{3}] = [\overline{7}] = \mathbb{Z}_{10}^*$

55. Példa. Az S_3 csoportban $[(1\ 2\ 3)] = \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}$ részcsoport, ami az A_3 alternáló csoport, $A_3 = [(1\ 2\ 3)]$.

56. Tétel. Legyen G csoport, $a \in G$. Ha $o(a) = n$, akkor $[a] \cong \mathbb{Z}_n$. Ha $o(a) = \infty$, akkor $[a] \cong \mathbb{Z}$.

57. Definíció. Ha a G csoportra és $X \subseteq G$-re $G = [X]$, akkor azt mondjuk, hogy G-t generálja az X halmaz. Ekkor X-et a G csoport generátorrendszerének nevezzük.

58. Példa. A 54. Példa alapján $\mathbb{Z}_{10}^*$-ot generátorrendszere például a $\{\overline{3}\}$ halmaz.

59. Definíció. A G csoportot ciklikusnak nevezzük, ha van egyelemű generátorrendszere, azaz $G = [a]$ valamely $a \in G$-re.

60. Példa. A 54. Példa alapján $\mathbb{Z}_{10}^*$ cikliku csoport, ugyanis $[\overline{7}] = \mathbb{Z}_{10}^*$.

61. Példa. Az S_3 csoport nem ciklikus csoport, mert a transzpozíciók rendje 2, a 3-hosszú ciklusoké pedig 3, tehát egyik elem sem állítja elő a csoport összes elemét.

62. Megjegyzés. A 56. Tétel alapján a ciklikus csoportok izomorfiától eltekintve a $\mathbb{Z}_n$ ($n \in \mathbb{N}$) és $\mathbb{Z}$.

63. Tétel. Ciklikus csoport bármely részcsoportja ciklikus.

2.5. Lagrange tétel

64. Tétel. Legyen $H \leq G$, és definiáljunk a G halmazon egy $\sim$ relációt: $a \sim b \iff a^{-1}b \in H$. Ekkor $\sim$ ekvivalenciareláció, és egy $a \in G$ elem ekvivalenciaosztálya $aH = \{ah \colon h \in H\}$.

65. Definíció. Az aH halmazt az a elem H szerinti bal oldali mellékosztályának nevezzük.

66. Következmény. Egy $H \leq G$ részcsoport szerinti bal oldali mellékosztályok a G csoport egy osztályozását alkotják.

67. Megjegyzés. Hasonló módon definiálhatóak a Ha jobb oldali mellékosztályok, amelyek szintén osztályozást alkotnak.

68. Definíció. A G véges csoport H részcsoportja szerinti bal oldali (jobb oldali) mellékosztályok számát H indexének nevezzük. Jelölése: $[G : H]$.

69. Tétel (Lagrange tétele). Tetszőleges G véges csoport és $H \leq G$ részcsoport esetén $|G| = |H| \cdot [G : H]$.

70. Következmény. Ha G véges és $a \in G$, akkor $o(a)$ osztója G elemszámának.

71.* Tétel. A legfeljebb 7-elemű csoportok (izomorfia erejéig) a következők: $\{1\}$; $\mathbb{Z}_2$; $\mathbb{Z}_3$; $\mathbb{Z}_4, V$; $\mathbb{Z}_5$; $\mathbb{Z}_6, S_3$; $\mathbb{Z}_7$.

3. Gyűrű, test, integritástartomány

72. 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.

73. Példa. Gyűrűk: $(\mathbb{Z}; +, \cdot)$, $(\mathbb{R}; +, \cdot)$, $(\mathbb{R}^{2\times 2}; +, \cdot)$, $(\mathbb{C}; +, \cdot), (\mathbb{Z}_5; +, \cdot)$.

74. Tétel. Bármely $(A; +, \cdot)$ gyűrű additív egységeleme zéruselem a multiplikatív félcsoportban.

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

76. 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. Az $(\mathbb{R}^{n\times n}; +, \cdot)$ nem kommutatív gyűrű, ha $n > 1$.

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

78. Tétel. A $(\mathbb{Z}_n;+,\cdot)$ gyűrű, és pontosan akkor test, ha n prím.

79. Definíció. A $\mathbb{Z}_n$ gyűrű neve modulo n maradékosztály-gyűrű, illetve prím modulus esetén maradékosztálytest.

80. Példa. A 73. Példában felsorolt gyűrűk közül testek: $(\mathbb{R};+,\cdot)$, $(\mathbb{C};+,\cdot)$, $(\mathbb{Z}_5;+,\cdot)$.

81. Definíció. Ha egy gyűrű a,b elemeire $ab=0$ teljesül, de se a, se b nem nulla, akkor azt mondjuk, hogy a és b zérusosztók. Ha egy gyűrűben nincsenek zérusosztók (azaz nullától különböző elemek szorzata sosem nulla), akkor zérusosztómentes gyűrűnek nevezzük. A kommutatív, egységelemes, zérusosztómentes gyűrű neve integritástartomány.

82. Állítás. Integritástartományban lehet nemzéró elemmel egyszerűsíteni, azaz tetszőleges a,b,c $(c\neq 0)$ elemekre

$$ac=bc \implies a=b.$$

83. Állítás. Minden test integritástartomány.

84. Definíció. Gauss-egészeknek nevezzük azokat a komplex számokat, melyeknek valós és képzetes része is egész szám. A Gauss-egészek halmazát $\mathbb{Z}[i]$ jelöli: $\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$.

85. Állítás. A Gauss-egészek a komplex számok szokásos összeadásával és szorzásával integritástartományt alkotnak (de nem alkotnak testet).