

MBNK13E: Műveletek és algebrák

(előadásvázlat, 2025. február 17.)

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 leképezések 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 $A \times A \times \dots \times A$ Descartes-szorzatot.
- 2. Definíció.** Legyen A tetszőleges nemüres halmaz, és $n \in \mathbb{N}_0$. Az A -n értelmezett **n -változós művelet**en egy $A^n \rightarrow A$ 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: $(\mathbb{Z}; +, \cdot)$, $(\mathbb{Z}; -)$, $(\mathbb{N}; 1, \cdot)$, $(\mathbb{R}^3; +)$, $(\mathbb{R}^{2 \times 3}; +)$, $(\mathbb{C}; +, \cdot)$, $(A^A; \cdot)$, $(S_n; \text{id}, \cdot)$.
- 6. Definíció.** Azokat az algebrákat, amelyeknek egy kétváltozós művelete van **grupoidnak** nevezzük.
- 7. Példa.** A 5. Példában megadott algebrák közül a következők grupoidok: $(\mathbb{Z}; -)$, $(\mathbb{R}^3; +)$, $(\mathbb{R}^{2 \times 3}; +)$, $(A^A; \cdot)$, $(S_n; \text{id}, \cdot)$.

1.1. Műveleti tulajdonságok

8. Definíció. (Grupoid műveleti tulajdonságai)

- (1) Az $(A; \circ)$ grupoid **asszociatív**, ha $(\forall a, b, c \in A)(a \circ (b \circ c) = (a \circ b) \circ c)$.
- (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, $(\mathbb{R}^{2 \times 2}; \cdot)$ zéruseleme a 2×2 -es zérómátrix.

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

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

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

- (5) Egységelméletes 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 permutáció 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 kétváltozós 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 **félcsoporthnak** nevezzük. Az egységelméletes félcsoporthokat **monoidnak** nevezzük. Azokat a monoidokat, ahol minden elemnek van inverze **csoportoknak** hívjuk. A kommutatív csoportokat **Abel-csoportoknak** nevezzük.

16. Példa. Az $(\mathbb{N}; +)$ félcsoporth, 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) $(ab)^{-1} = b^{-1}a^{-1}$.

22. Megjegyzés. Teljes indukcióval igazolható, hogy a szorzat inverze n tényező esetén az előzőhöz hasonlóan számolható, azaz $(A; \cdot)$ monoid esetén ha az $a_1, \dots, a_n \in A$ elemeknek van inverze, akkor $(a_1 \dots a_n)^{-1} = a_n^{-1} \dots a_1^{-1}$.

2. CSOPORTOK

23. Definíció. Legyen $*$ 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.

24. Megjegyzés. A kancellativitás így is megfogalmazható:

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

25. Tétel. Csoport művelete mindig invertálható és kancellatív.

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

27. 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

28. 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:

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

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

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

30. 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.

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

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

33.* 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 $\text{lko}(o(a), o(b)) = 1$.

2.2. Részcsoport, izomorfia

34. Definíció. Legyen $(G; \cdot)$ csoport. Ha $H \subseteq G$ és $(H; \cdot)$ csoport, akkor azt mondjuk, hogy $(H; \cdot)$ **részcsoportja** $(G; \cdot)$ -nek. Jele: $(H; \cdot) \leq (G; \cdot)$. Továbbá ha $H \neq G$, akkor $(H; \cdot)$ **valódi részcsoportha** $(G; \cdot)$ -nek.

35. Tétel. Tetszőleges G csoport és $\emptyset \neq H \subseteq G$ esetén H akkor és csak akkor részcsoportha 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: $\forall h \in H : h^{-1} \in H$.

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

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

38. 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.

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

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

41.* Tétel. A D_n csoportnak $2n$ eleme van: $D_n = \{\text{id}, a, a^2, \dots, a^{n-1}, t, at, a^2t, \dots, a^{n-1}t\}$, 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 ($0 \leq k \leq n-1$), 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 $ta^k = a^{-k}t$ összefüggés.

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

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

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

43. 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.

44. 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

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

46. Tétel. A $\mathbb{Z}_n$ halmazon művelet a következőképpen definiált összeadás, kivonás és szorzás:
$$\bar{a} + \bar{b} = \overline{a+b}, \quad \bar{a} - \bar{b} = \overline{a-b}, \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

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

48. 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.

49. Definíció. Az $\bar{a}$ modulo n maradékosztály **redukált maradékosztály**, ha $\text{lko}(a, n) = 1$. A modulo n redukált maradékosztályok halmazát $\mathbb{Z}_n^*$ jelöli, azaz $\mathbb{Z}_n^* = \{\bar{a} \in \mathbb{Z}_n \mid \text{lko}(a, n) = 1\}$.

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

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

52. Megjegyzés. A 48. Tétel alapján, ha $n > 1$, akkor, ha azt mondjuk, hogy $\mathbb{Z}_n$ csoport, a $+$ művelet. A 51. Tétel alapján a $\mathbb{Z}_n^*$ csoport esetén a $\cdot$ művelet.

2.4. Generálás, ciklikus csoport

53. 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 $[a] = \{a^k : k \in \mathbb{Z}\}$.

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

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

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

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

58. 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.

59. Példa. A 55. Példa alapján $\mathbb{Z}_{10}^*$ -ot generátorrendszere például a $\{\bar{3}\}$ halmaz.

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

61. Példa. A 55. Példa alapján $\mathbb{Z}_{10}^*$ ciklikus csoport, ugyanis $[\bar{7}] = \mathbb{Z}_{10}^*$.

62. 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.

63. Megjegyzés. A 57. Tétel alapján a ciklikus csoportok izomorfiától eltekintve a $\mathbb{Z}_n$ ($n \in \mathbb{N}$) és $\mathbb{Z}$.

64. Tétel. Ciklikus csoport bármely részcsoportja ciklikus.

2.5. Lagrange tétel

65. Tétel. Legyen G csoport, $H \leq G$, 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 $aH = \{ah : h \in H\}$.

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

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

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

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

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

71. Következmény. Tetszőleges G véges csoport és $H \leq G$ részcsoport esetén $|H|$ osztója $|G|$ -nak.

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

73.* 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

74. Definíció. Az $(A; +, \cdot)$ algebrát **gyűrűnek** nevezzük, ha $(A; +)$ Abel-csoport, $(A; \cdot)$ félcsoporth, és $a \cdot$ disztributív az $+$ -ra. Az $(A; +)$ Abel-csoportot a **gyűrű additív csoportjának**, az $(A; \cdot)$ félcsoporthot a **gyűrű multiplikatív félcsoporthjának** nevezzük.

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

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

77. 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.

78. 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 $n > 1$.

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

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

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

82. Példa. A 75. Példában felsorolt gyűrűk közül testek: $(\mathbb{R}; +, \cdot)$, $(\mathbb{C}; +, \cdot)$, $(\mathbb{Z}_5; +, \cdot)$.

83. 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**.

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

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

85. Állítás. Minden test integritástartomány.

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

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