MBLK12: Halmazok, Leképezések (levelező)

(előadásvázlat)

Maróti Miklós

Jelölje $\mathbb{Z}$ az egész számok halmazát, $\mathbb{N}$ a pozitív egészek halmazát, $\mathbb{Q}$ a racionális számok halmazát, $\mathbb{R}$ a valós számok halmazát, és $\mathbb{R}_0^+$ a nem negatív valós számok halmazát.

1. Halmazok

1. Megjegyzés. A halmaz és a halmaz eleme alapfogalmak, nem definiáljuk. Az $a \in A$ jelölést használjuk annak kifejezésére, hogy a eleme A-nak. A $\neg(a \in A)$ formula helyett $a \notin A$-t írunk. Megjegyezzük, hogy egy elem nem lehet többször eleme egy halmaznak, azaz csak az számít, hogy az adott elem eleme-e a halmaznak vagy sem. A halmazelmélet axiomatikus felépítésében csak azt tesszük fel, hogy $\in$ kétváltozós predikátumjel, és az individuumtartományunk a halmazok összessége.

2. Definíció. Ha az A és B halmazoknak ugyan azok az elemei, azaz $(\forall x)(x \in A \leftrightarrow x \in B)$, akkor azt mondjuk, hogy egyenlők, és azt írjuk, hogy $A = B$. Ha A minden eleme B-nek is eleme, azaz $(\forall x)(x \in A \rightarrow x \in B)$, akkor azt mondjuk, hogy A részhalmaza B-nek, és azt írjuk hogy $A \subseteq B$. Az A halmaz valódi részhalmaza B-nek, amelyet $A \subset B$-vel jelölünk, ha $A \subseteq B$, de $A \neq B$.

3. Definíció. Azt a halmazt, melynek nincsen eleme, üreshalmaznak nevezzük és $\emptyset$-el jelöljük, azaz $\neg(\exists x)(x \in \emptyset)$ teljesül.

4. Tétel. Tetszőleges A, B, C halmazokra

(1) $A \subseteq A$ és $\emptyset \subseteq A$;
(2) ha $A \subseteq B$ és $B \subseteq C$, akkor $A \subseteq C$;
(3) $A = B$ akkor és csak akkor, ha $A \subseteq B$ és $B \subseteq A$.

5. Definíció. Legyenek $a_1, \dots, a_n$ nem feltétlen különböző elemek. Ekkor $\{a_1, \dots, a_n\}$ azt az A halmazt jelöli, amelynek pontosan $a_1, \dots, a_n$ az elemei, azaz $(\forall x)(x \in A \leftrightarrow (x = a_1 \vee \dots \vee x = a_n))$.

6. Példa. Tekintsük a következő halmazokat:

$$A = \{1, 2\}; \quad B = \{1, 3-1\}; \quad C = \{1, 1, 2\}; \quad D = \{\emptyset, 1, 2\}; \quad E = \{\{1\}, 2\}; \quad F = \{\{1, 2\}\}.$$

Ekkor $A = B = C$, a többi mind különböző. D-nek három, F-nek egy eleme van, a többinek kettő. $\{1\}$ részhalmaza A, B, C és D-nek, de E és F-nek nem. $\{1\}$ csak E-nek eleme, a többinek nem.

7. Definíció. Legyen F olyan formula, melynek csak x a szabad változója. Ekkor $\{\, x : F \,\}$ azt az A halmazt jelöli, amelyre $(\forall x)(F \leftrightarrow x \in A)$ teljesül. Ha nem világos, hogy x milyen U individuumtartomány eleme lehet, akkor az $\{\, x \in U : F \,\}$ jelölést használjuk. Formula helyett sokszor csak szöveges predikátumot írunk amelyet megfelelően lehetne formalizálni.

8. Példa. A következő halmazok mind egyenlők: $\{1, 2, 3, 6\}$, $\{\, x \in \mathbb{N} : x \mid 6 \,\}$, $\{\, x \in \mathbb{Z} : x \geq 1 \text{ és } x \mid 6 \,\}$, $\{\, \text{hat pozitív osztói} \,\}$.

9. Definíció. Tetszőleges A és B halmazokra definiáljuk az egyesítésüket és metszetüket:

$$A \cup B = \{\, x : x \in A \vee x \in B \,\}, \qquad A \cap B = \{\, x : x \in A \wedge x \in B \,\}.$$

Azt mondjuk, hogy A és B diszjunktak, ha $A \cap B = \emptyset$.

10. Definíció. Legyen rögzítve egy U univerzum. Ekkor tetszőleges $A \subseteq U$ halmazra definiáljuk az A komplementerét:

$$\overline{A} = \{\, x \in U : x \notin A \,\}.$$

11. Definíció. Tetszőleges A és B halmazokra definiáljuk a különbségüket és szimmetrikus különbségüket:

$$A \setminus B = \{\, x : x \in A \wedge x \notin B \,\}, \qquad A \bigtriangleup B = \{\, x : x \in A \leftrightarrow x \notin B \,\}.$$

12. Tétel. Tetszőleges $A, B, C \subseteq U$ halmazokra

$$\begin{aligned}
A \cap A &= A, & A \cup A &= A, && \text{(idempotencia)}\\
A \cap B &= B \cap A, & A \cup B &= B \cup A, && \text{(kommutativitás)}\\
(A \cap B) \cap C &= A \cap (B \cap C), & (A \cup B) \cup C &= A \cup (B \cup C), && \text{(asszociativitás)}\\
(A \cup B) \cap A &= A, & (A \cap B) \cup A &= A, && \text{(abszorptivitás)}\\
(A \cup B) \cap C &= (A \cap C) \cup (B \cap C), & (A \cap B) \cup C &= (A \cup C) \cap (B \cup C), && \text{(disztibutivitás)}
\end{aligned}$$

$$\begin{aligned}
& & \overline{\overline{A}} &= A, && \text{(dupla tagadás)}\\
\overline{A \cap B} &= \overline{A} \cup \overline{B}, & \overline{A \cup B} &= \overline{A} \cap \overline{B}, && \text{(De Morgan szabályok)}\\
A \cap \overline{A} &= \emptyset, & A \cup \overline{A} &= U, &&\\
A \cap U &= A, & A \cup U &= U, &&\\
A \cap \emptyset &= \emptyset, & A \cup \emptyset &= A &&
\end{aligned}$$

$$A \setminus B = A \cap \overline{B} \qquad A \triangle B = (A \setminus B) \cup (B \setminus A).$$

13. Definíció. Tetszőleges a, b elemekre definiáljuk az (a, b) rendezett elempárt. Az (a, b) rendezett elempárnak a és b az első, illetve a második koordinátája. Két rendezett elempár akkor és csak akkor egyenlő, ha a megfelelő koordinátáik egyenlők.

14. Definíció. Tetszőleges A, B halmazokra definiáljuk a Descartes-szorzatukat:

$$A \times B = \{\,(a, b) : a \in A \wedge b \in B\,\}.$$

15. Példa. Az $A = \{1, 2\}$ kételemű és $B = \{3, 4, 5\}$ háromelemű halmazok Descartes-szorzata $A \times B = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}$ hatelemű halmaz. Vegyük észre, hogy $\emptyset \times B = \emptyset$, mert ha (a, b) eleme lenne a Descartes-szorzatnak, akkor $a \in \emptyset$ lenne, ami nem lehet.

16. Definíció. Tetszőleges A halmaz esetén az A összes részhalmazainak halmazát az A hatványhalmazának nevezzük és $\mathcal{P}(A)$-val jelöljük, azaz

$$\mathcal{P}(A) = \{\,X : X \subseteq A\,\}.$$

17. Példa. Az $A = \{1, 2, 3\}$ háromelemű halmaz hatványhalmaza

$$\mathcal{P}(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

8-elemű. Az üreshalmaznak csak az üreshalmaz a részhalmaza, ezért $\mathcal{P}(\emptyset) = \{\emptyset\}$, azaz egy olyan halmaz, amelynek egyetlen eleme van, az üreshalmaz. Gondoljuk át, hogy $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.

2. Leképezések

18. Definíció. Tetszőleges A, B halmazokra a $\varrho \subseteq A \times B$ részhalmazt leképezésnek nevezzük, ha minden $a \in A$ elemre pontosan egy $b \in B$ elem létezik, amelyre $(a, b) \in \varrho$. Ilyenkor a $\varrho\colon A \to B$ jelölés használjuk, továbbá $(a, b) \in \varrho$ helyett azt mondjuk hogy az a elem ϱ melletti képe b, és azt írjuk, hogy $a\varrho = b$ vagy $a \mapsto b$. Az A halmazból B-be menő összes leképezés halmazát B^A-val jelöljük.

19. Példa. Minden leképezés elempárok halmaza. Vegyük például az $A = \{-2, -1, 0, 1, 2\}$ halmazon az abszolútérték függvényt. Ekkor ez leképezés amely egyenlő a $\{(-2, 2), (-1, 1), (0, 0), (1, 1), (2, 2)\}$ halmazzal.

20. Definíció. A $\varrho\colon A \to B$ és a $\sigma\colon B \to C$ leképezések szorzatán azt a $\varrho\sigma\colon A \to C$ leképezést értünk, amelyre $a \in A$ elem képe a $c \in C$ pontosan akkor, ha létezik $b \in B$, amelyre $a\varrho = b$ és $b\sigma = c$.

21. Tétel. Ha $\varrho\colon A \to B$ és $\sigma\colon B \to C$ leképezések, akkor $\varrho\sigma\colon A \to C$ is leképezés és tetszőleges $a \in A$ elemre $a(\varrho\sigma) = (a\varrho)\sigma$.

22. Definíció. Tetszőleges A halmazon definiáljuk az identikus leképezést:

$$\mathrm{id}_A = \{\,(a,b) \in A \times A : a = b\,\},$$

más jelölést használva:

$$\mathrm{id}_A\colon A \to A, \quad a\,\mathrm{id}_A = a$$

23. Tétel. Tetszőleges $\varrho\colon A \to B$ leképezésre $\mathrm{id}_A\,\varrho = \varrho$ és $\varrho\,\mathrm{id}_B = \varrho$.

24. Tétel. Tetszőleges $\varrho\colon A \to B$, $\sigma\colon B \to C$ és $\tau\colon C \to D$ leképezésekre $(\varrho\sigma)\tau = \varrho(\sigma\tau)$, azaz a szorzás asszociatív.

25. Példa. Vegyük az $A = \{1,2,3\}$ halmazon a $\varrho = \{(1,2),(2,3),(3,1)\}$ és $\sigma = \{(1,2),(2,1),(3,3)\}$ leképezéseket. Ekkor $\varrho\sigma = \{(1,1),(2,3),(3,2)\}$ és $\sigma\varrho = \{(1,3),(2,2),(3,1)\}$, azaz a szorzás nem kommutatív.

26. Definíció. A $\varrho\colon A \to B$ leképezés szürjektív (vagy ráképezés), ha minden elem előfordul képelemként, azaz ha

$$(\forall b \in B)(\exists a \in A)(a\varrho = b).$$

A $\varrho\colon A \to B$ leképezés injektív (vagy kölcsönösen egyértelmű), ha különböző elemek képe különböző, azaz ha

$$(\forall a_1, a_2 \in A)(a_1\varrho = a_2\varrho \to a_1 = a_2).$$

A ϱ leképezés bijektív (vagy kölcsönösen egyértelmű ráképezés), ha szürjektív és injektív is.

27. Példa. A 19. példában szereplő leképezés nem szürjektív, mert például a -1 nem forul elő képként, és nem is injektív, mert a -2 és a 2 képe megegyezik.

28. Definíció. A $\varrho \subseteq A \times B$ leképezés inverze a

$$\varrho^{-1} = \{(b,a) \in B \times A\colon (a,b) \in \varrho\}.$$

29. Tétel. A $\varrho\colon A \to B$ leképezésnek az inverze akkor és csak akkor leképezés, ha ϱ bijektív.

30. Tétel. Tetszőleges $\varrho\colon A \to B$ és $\sigma\colon B \to C$ leképezésekre

(1) ha ϱ és σ szürjektív, akkor $\varrho\sigma$ is szürjektív;
(2) ha ϱ és σ injektív, akkor $\varrho\sigma$ is injektív;
(3) ha ϱ és σ bijektív, akkor $\varrho\sigma$ is bijektív;
(4) ha $\varrho\sigma$ szürjektív, akkor σ szürjektív;
(5) ha $\varrho\sigma$ injektív, akkor ϱ injektív;
(6) ha $\varrho\sigma$ bijektív, akkor ϱ injektív és σ szürjektív;
(7) ha ϱ bijektív, akkor ϱ^{-1} is bijektív.

31. Tétel. Tetszőleges $\varrho\colon A \to B$, $\sigma\colon B \to C$ bijektív leképezésre

(1) $\varrho\varrho^{-1} = \mathrm{id}_A$,
(2) $\varrho^{-1}\varrho = \mathrm{id}_B$,
(3) $(\varrho\sigma)^{-1} = \sigma^{-1}\varrho^{-1}$.

3. Halmazok elemszáma

32. Definíció. Azt mondjuk, hogy az A és B halmazok elemszáma megegyezik, és azt írjuk, hogy $|A| = |B|$, ha létezik bijektív leképezés A-ból B-re. Azt mondjuk, hogy az A halmaz n-elemű, és azt írjuk, hogy $|A| = n$, ha n nemnegatív egész és létezik A-ból bijektív leképezés az $\{1,2,\ldots,n\}$ halmazra.

33. Példa. Az $\emptyset$ halmaz nulla elemű. Az $\{\emptyset\}$ halmaz egyelemű, mert $\{(\emptyset,1)\}$ bijektív leképezés $\{\emptyset\}$-ból $\{1\}$-be.

34. Tétel. Tetszőleges A, B, C halmazokra

(1) $|A| = |A|$;

(2) ha $|A| = |B|$, akkor $|B| = |A|$;
(3) ha $|A| = |B|$ és $|B| = |C|$, akkor $|A| = |C|$;
(4) ha $|A| = |B|$, akkor $|A \times C| = |B \times C|$;
(5) ha $|A| = |B|$, akkor $|A^C| = |B^C|$;
(6) ha $|A| = |B|$, akkor $|C^A| = |C^B|$.

35. Tétel. Ha $|A| = n$, $|B| = m$ és az A és B halmazok diszjunktak, akkor $|A \cup B| = n + m$.

36. Tétel. Tetszőleges A halmazra $|\mathcal{P}(A)| = |\{0,1\}^A|$. Ha $|A| = n$, akkor $|\mathcal{P}(A)| = 2^n$.

37. Tétel. Ha $|A| = n$ és $0 \le k \le n$, akkor $|\{ B \in \mathcal{P}(A) : |B| = k \}| = \binom{n}{k}$.

38.* Tétel. Tetszőleges A, B halmazokra $|A \times B| = |B \times A|$. Ha $|A| = n$ és $|B| = m$, akkor $|A \times B| = nm$.

39. Tétel. Ha $|A| = n$, akkor $|\operatorname{Sym}(A)| = n!$, speciálisan $|S_n| = n!$.

40.* Tétel. Tetszőleges A, B, C halmazokra ha B és C diszjunktak, akkor $|A^{B\cup C}| = |A^B \times A^C|$. Ha $|A| = n$ és $|B| = m$, akkor $|A^B| = n^m$.

41.* Tétel. Tetszőlegs A, B, C halmazokra $|(A^B)^C| = |A^{(B\times C)}|$.

42.* Tétel. $|\mathbb{N}| = |\mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{Z}[x]| = |\mathbb{Q}|$, ahol $\mathbb{Z}[x]$ az egészegyütthatós polinomok halmaza (egészek olyan $(a_0, a_1, a_2, \dots)$ végtelen sorozatai, amelyek egy idő után azonosan nullák).

43.* Tétel. $|\mathbb{R}| = |\{ x \in \mathbb{R} : 0 < x < 1 \}| = |\mathbb{R} \setminus \mathbb{Z}| = |\mathbb{R} \setminus \mathbb{Q}| = |\mathcal{P}(\mathbb{N})| \ne |\mathbb{N}|$.

44.* Tétel (Cantor-tétel). Tetszőleges A halmazra $|\mathcal{P}(A)| \ne |A|$.

45. Definíció. Az A halmaz véges, ha létezik olyan n nemnegatív egész, hogy $|A| = n$. Az A halmaz megszámlálhatóan végtelen, ha $|A| = |\mathbb{N}|$, ekkor azt írjuk, hogy $|A| = \aleph_0$. Az A halmaz megszámlálható, ha A véges vagy megszámlálhatóan végtelen. Az A halmaz kontinuum számosságú, ha $|A| = |\mathbb{R}|$, ekkor azt írjuk, hogy $|A| = \mathfrak{c}$.

46.* Tétel. Az A halmaz akkor és csak akkor véges, ha minden $f : A \to A$ injektív (szürjektív) leképezés bijektív.

47. Definíció. Ha létezik injektív leképezés A-ból B-be, akkor azt írjuk, hogy $|A| \le |B|$.

48.* Tétel (Schröder-Bernstein-tétel). Tetszőleges A, B halmazokra ha léteznek $f : A \to B$ és $g : B \to A$ injektív leképezések, akkor létezik $h : A \to B$ bijektív leképezés is. Tehát ha $|A| \le |B|$ és $|B| \le |A|$, akkor $|A| = |B|$.

49. Példa (Russel-paradoxon). A 7. definíciót felhasználva definiáljuk az

$$R = \{x : x \text{ halmaz, és } x \notin x\}$$

halmazt. Ekkor se $R \in R$, se $R \notin R$ nem teljesülhet, tehát R nem lehet halmaz.

50. Megjegyzés. A halmazelmélet axiomatikus felépítésében meg kell követelnünk, hogy a 7. definícióban szereplő U individuumtartomány csak halmaz lehet (például az összes halmaz összessége nem), és így elkerülhető a Russel-paradoxon.

51. Megjegyzés. Ha a 7. definíciót csak részhalmazok definiálására használhatjuk, akkor külön meg kell követelnünk, hogy létezik az üres halmaz, és tetszőleges A, B halmazokra léteznek a $\{A, B\}$, $A \cup B$ és $P(A)$ halmazok is.

52. Megjegyzés. Az előbb megkövetelt halmazok létezésén kívűl feltesszük még, hogy van végtelen halmaz (olyan A halmaz, hogy ha $x \in A$, akkor $x \cup \{x\} \in A$), és azt, hogy minden nemüres A halmaznak van olyan $x \in A$ eleme, hogy $A \cap x = \emptyset$.

4. Permutációk

53. Definíció. Az A halmaz permutációin a $\pi : A \to A$ bijektív leképezéseket értjük. Az A halmaz összes permutációinak halmazát $\mathrm{Sym}(A)$-val jelöljük, speciálisan tetszőleges n pozitív egészre az $\{1, \ldots, n\}$ halmaz összes permutációinak halmazát S_n jelöli.

54. Jelölés. A $\pi \in S_n$ permutációt megadhatjuk elempárok halmazaként: $\pi = \{(1, 1\pi), (2, 2\pi), \ldots, (n, n\pi)\}$, vagy kétsoros írásmóddal:

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1\pi & 2\pi & \cdots & n\pi \end{pmatrix}$$

55. Példa. Ha $\alpha \in S_3$ az a permutáció, amelyre $1\alpha = 2$, $2\alpha = 1$ és $3\alpha = 3$, akkor

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \{(1, 2), (2, 1), (3, 3)\}.$$

56. Példa. Számoljuk ki az

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ és } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

permutációk szorzatát. A 21. tétel alapján az elemek képe a következőképpen számolható:

$$\begin{aligned} 1(\alpha\beta) &= (1\alpha)\beta = 2\beta = 3, \\ 2(\alpha\beta) &= (2\alpha)\beta = 1\beta = 2, \\ 3(\alpha\beta) &= (3\alpha)\beta = 3\beta = 1, \end{aligned}$$

azaz

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Számoljuk ki β inverzét. Mivel

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \{(1, 2), (2, 3), (3, 1)\}$$

ezért

$$\beta^{-1} = \{(2, 1), (3, 2), (1, 3)\} = \{(1, 3), (2, 1), (3, 2)\} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

57. Definíció. A $\pi \in S_n$ permutáció az $x \in \{1, \ldots, n\}$ elemet mozgatja, ha $x\pi \neq x$. A $\pi \in S_n$ által mozgatott elemek halmazát M_π-vel jelöljük, azaz

$$M_\pi = \{\, x \in \{1, \ldots, n\} : x\pi \neq x \,\}.$$

58. Példa. Az

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

permutáció által mozgatott elemek halmaza $M_\alpha = \{1, 2\}$.

59. Definíció. A $\pi, \sigma \in S_n$ permutációkat idegennek nevezzük, ha $M_\pi \cap M_\sigma = \emptyset$.

60. Tétel. Ha a $\pi, \sigma \in S_n$ permutációk idegenek, akkor

(1) $\pi\sigma = \sigma\pi$, és
(2) $(\pi\sigma)^k = \pi^k \sigma^k$ minden k egészre.

61. Definíció. Legyen $n \geq k \geq 2$, és az $a_1, \ldots, a_k \in \{1, \ldots, n\}$ elemek páronként különbözőek. Ekkor azt a $\pi \in S_n$ permutációt, amelyre

$$a_1\pi = a_2, \quad a_2\pi = a_3, \quad \ldots \quad a_{k-1}\pi = a_k, \quad a_k\pi = a_1,$$

és $x\pi = x$ minden $x \in \{1, \ldots, n\} \setminus \{a_1, \ldots, a_k\}$ elemre, ciklusnak nevezzük és röviden így jelöljük:

$$\pi = (a_1\ a_2\ \cdots\ a_k).$$

A k számot a ciklus hosszának nevezzük. A 2 hosszúságú ciklusokat transzpozícióknak hívjuk.

62. Példa. Az
$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$
permutáció ciklus, mivel a $k = 2$, $a_1 = 1$ és $a_2 = 2$ választással éppen ezt a permutációt kapjuk, azaz $\alpha = (1\ 2)$. Mivel α hossza éppen 2, ezért α transzpozíció is. A
$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
permutáció szintén ciklus, és $\beta = (1\ 2\ 3)$.

63. Megjegyzés. Vegyük észre, hogy egy permutáció ciklusos alakban való megadása nem egyértelmű! Egyrészt ugyanazt a permutációt többféleképpen is felírhatjuk ciklusként:
$$(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2).$$
A másik probléma pedig az, hogy az $(1\ 2\ 3)$ permutációról nem tudjuk eldönteni, hogy az S_3 vagy esetleg az S_4 csoport eleme-e. Természetesen ha S_3-beli permutációkról beszélünk, akkor
$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$
viszont S_4-ben már
$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix},$$
és ez a két permutáció nem ugyanaz. Ugyan ez a probléma az identikus permutáció „id” jelölésével is, arról sem lehet eldönteni, hogy melyik permutációcsoportban használjuk.

64. Példa. Természetesen nem minden permutáció ciklus, például a következő π permutáció sem ciklus, de előáll ciklusok szorzataként:
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1\ 2\ 3)(4\ 5).$$

65. Tétel. Minden S_n-beli permutáció előáll páronként idegen ciklusok szorzataként, és ez az előállítás a tényezők sorrendjétől eltekintve egyértelműen meghatározott. (Az identikus permutációt ciklusok üres szorzatának tekintjük.)

66. Példa. Adjuk meg a $\pi = (5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7)$ permutációt páronként idegen ciklusok szorzataként. Tekintsük azokat az elemeket, melyeket a szorzat valamely tényezője mozgat: $\{1, 2, 3, 4, 5, 7\}$. Vegyünk ki ezek közül egyet, mondjuk az 1-gyet, és számoljuk ki, hogy ezt a π permutáció milyen elemekbe viszi át:
$$1\pi = 1(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 1(1\ 3\ 5)(4\ 3\ 7) = 3(4\ 3\ 7) = 7.$$
Folytassuk a kapott elemekkel, azaz
$$7\pi = 7(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 7(1\ 3\ 5)(4\ 3\ 7) = 7(4\ 3\ 7) = 4,$$
$$4\pi = 4(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 5(1\ 3\ 5)(4\ 3\ 7) = 1(4\ 3\ 7) = 1.$$
Visszaértünk ahhoz az elemhez, amiből kiindultunk, tehát megvan az első ciklusunk: $(1\ 7\ 4)$. A maradék elemekből vegyük a következőt, mondjuk a 2-től, és számoljuk ki hogy ezt π milyen elemekbe viszi át, és így tovább folytatva megkapjuk a π permutációt páronként idegen ciklusok szorzatára bontott alakban:
$$\pi = (1\ 7\ 4)(2\ 5).$$

67. Tétel. Tetszőleges $\pi = (a_1\ a_2\ \cdots\ a_k) \in S_n$ ciklusra

(1) $\pi^{-1} = (a_k\ a_{k-1}\ \cdots\ a_1)$,
(2) $\pi^k = \mathrm{id}$,
(3) Ha $i \equiv j \pmod{k}$, akkor $\pi^i = \pi^j$.

68. Tétel. Tetszőleges ciklus felírható transzpozíciók szorzataként, mégpedig

$$(a_1\ a_2\ a_3\ \cdots\ a_k) = (a_1\ a_2)(a_1\ a_3)\cdots(a_1\ a_k).$$

Következésképpen, minden permutáció transzpozíciók szorzatára bontható (de ez általában nem egyértelmű).

69. Példa. $(1\ 2\ 3\ 4)(5\ 6) = (1\ 2)(1\ 3)(1\ 4)(5\ 6)$, de mivel $(1\ 2\ 3\ 4) = (2\ 3\ 4\ 1)$, ezért $(1\ 2\ 3\ 4)(5\ 6) = (2\ 3)(2\ 4)(2\ 1)(5\ 6)$, vagy $(1\ 2\ 3\ 4)(5\ 6) = (2\ 3)(5\ 6)(2\ 4)(2\ 1)$, mert idegen transzpozíciók felcserélhetők.

70.* **Tétel.** Minden permutáció vagy csak páros vagy csak páratlan sok transzpozíció szorzataként írható fel.

71. Definíció. A $\pi \in S_n$ permutációt párosnak nevezzük, ha felbontható páros sok transzpozíció szorzatára. A nempáros permutációkat páratlannak nevezzük.