

Diszkrét matematika

Kurdics János

Kurdics János

Diszkrét matematika

Egyetemi jegyzet
Nyíregyházi Egyetem, 2018
A kiadást támogatta az EFOP-3.5.1-16-2017-00017
„NYE-DUÁL- Új utakon a duális felsőoktatással a Nyíregyházi Egyetemen,
az Északkelet-Magyarországi térség felemelkedéséért” pályázat

Előszó

A matematika a gyakorlati alkalmazások szerszámkészlete, de egyúttal a természettudományok szolgálóleánya, sőt, önálló tudományág is saját kérdésfelvetésekkel. Az infokommunikációs technológia szempontjából a számtalan forrásból keletkező sokféle szempontból hasznos, de még nem eladható nyers adatok feldolgozásához szolgál módszerekkel, amelyek kimenetei egyéb tudományágak - közgazdaságtan, médiatudományok, élettudományok, és í. t. - eszközei által válnak materiális vagy szellemi termékekké. Emellett a matematika tanulmányozása olyan kompetenciákkal is szolgál, mint például absztrakt fogalmak kialakítása illetve megértése, ezek attribútumainak pontos megfogalmazása, ezekből eredő fogas kérdések elmezése és válasz keresése pontos állítások belátása által ragaszkodva a logika törvényeinek betartásához. A Tisztelt Hallgatóság számára ezt szép de egyben nehéz kihívásnak szánom. A jegyzet forrásai az Egyetemünkön 2006 óta tartott előadásaim anyaga és az azóta írt jegyzeteim [5,6,7,8], és egyéb jegyzetek mint [1,3,11,13], az előadást átalakítottam a többszöri tantervváltozásoknak megfelelően; figyelembe véve, hogy a számonkérés most már gyakorlati jegy az eredeti vizsgajegy helyett, a legfőbb rendező elvnek a praktikusságot tettem. Ennélfogva a bizonyításokat pár helyen mellőztem, hogy az anyag mennyisége egy félév alatt elsajátítható legyen. Az infokommunikációs-technológiai alkalmazásokban centrális tudás hangsúlyozott, több algoritmus igen részletesen van megadva aképpen, hogy az aktuális programnyelven való kódolás gyorsan történhet, csak a szintaktikai finomságokat kell átformálni. Avégett, hogy a Tisztelt Hallgatóság hozzáférését az éppen keresett dologhoz megkönnyítsem, a fogalmakat és állításokat indexekbe foglaltam. Magas színvonalú forrásokat talál a T. Olvasó a témakörökben történő további elmélyülésre a [2,4,10,14] könyvekben. A [12] cikkben a Gallai-Erdős tétel frappáns bizonyítását találjuk, amely egyben polinomiális algoritmust is ad a grafikus listához a realizáció megkonstruálásához. Az automatikus szedést a L^AT_EX makrócsomag felhasználásával végeztem.

1. fejezet

Halmazok, struktúrák

1.1. Alapfogalmak

1.1.1. Halmazok.

Fogalmak: A modern matematika a **halmaz** fogalom kiépítésén alapul, alapfogalom, szemléletesen dolgok összességét jelenti. Eleve adottnak tekintjük az **univerzum** halmazt, amelyben összegyűjtünk minden dolgot, amelyet vizsgálatnak vetünk alá. Adott a objektum és A halmaz között az eleme összefüggés állhat fenn, ekkor A **halmazelem**éről beszélünk, jelölés: $a \in A$, és mindig eldönthető, hogy vagy $a \in A$ vagy $a \notin A$ teljesül. Lerögzítjük, hogy az univerzumnak nincs olyan eleme, amely halmaz. Az $\emptyset$ **üreshalmaz**ra az teljesül, hogy nincsen egyetlen eleme sem. A B halmaz az A egy **részhalmaza**, ha B minden eleme eleme az A halmaznak is, jelölés: $B \subseteq A$. B kétféleképpen adható meg, ha az elemek száma véges felsorolással, $B = \{a_1, a_2, a_3, a_4, \dots, a_n\}$, illetve A elemeknek valamely $P(x)$ tulajdonságával, amely pontosan B elemeire teljesül, $B = \{a \in A | P(a)\}$. A összes részhalmaza alkotja a $\mathcal{P}(A)$ **hatványhalmazt**. Az A és B **halmazok egyenlőek**, azaz $A = B$, ha $A \subseteq B$ és $B \subseteq A$. B **valódi része** A -nak, ha $B \subseteq A$ de $B \neq A$, jelölés: $A \subset B$.

Fogalmak: unió, metszet, különbség, komplementer, szimmetrikus különbség, diszjunkt halmazok

A régről jól ismert **halmazműveletek** az alábbiak, legyen $A, B \subseteq X$.

(1) **Unió** $A \cup B = \{x \in X | x \in A \text{ vagy } x \in B\};$

(2) **Metszet** $A \cap B = \{x \in X | x \in A \text{ és } x \in B\};$

- (3) **Különbség** $A \setminus B = \{x \in X | x \in A \text{ és } x \notin B\}$;
- (4) A -nak X -re vonatkoztatott **komplementere** $\bar{A} = \{x \in X | x \notin A\}$;
- (5) **Szimmetrikus különbségük** $A \triangle B = (A \setminus B) \cup (B \setminus A)$.

Ha $A \cap B = \emptyset$, akkor azt mondjuk, hogy **diszjunkt halmazok**.

Ha $\mathcal{A} \subseteq \mathcal{X}$ **halmazrendszer**, akkor elemeinek **uniója** $\cup \mathcal{A} = \{x \in X | x \in A \text{ valamely } A \in \mathcal{A} \text{ esetén}\}$, **metszete** $\cap_{A \in \mathcal{A}} A = \{x \in X | x \in A \text{ minden } A \in \mathcal{A} \text{ esetén}\}$. Ha $\mathcal{A} = \{A_1, A_2, \dots, A_n\}$ véges n elemszámú halmazrendszer, akkor a szokásos jelölések $\cup_{i=1}^n A_i$ illetve $\cap_{i=1}^n A_i$.

Fogalmak:
halmazrendszer
uniója,
halmazrendszer
metszete

1.1.2. Relációk, függvények

Ha $A \neq \emptyset$ és $B \neq \emptyset$ halmazok, akkor egy új halmaz az $A \times B$ **Descartes-szorzat**, amelynek elemei az (a, b) **rendezett elempárok**, a -t az elempár **első** és b -t az elempár **második tagjának** nevezzük, két **elempár egyenlő**, ha megegyeznek első és második tagjaik is. Ha $A_1, A_2, \dots, A_n$ nemüres halmaz, akkor új halmaz az $A_1 \times A_2 \times \dots \times A_n$ **Descartes-szorzat**, amelynek elemei az $(a_1, a_2, \dots, a_n)$ **rendezett elem n-esek**, $a_i \in A_i$ -t az elem n -es i -edik tagjának nevezzük ($i = 1, 2, \dots, n$), két **elem n-es egyenlő**, ha rendre megegyeznek i -edik tagjaik ($i = 1, 2, \dots, n$).

Fogalmak:
Descartes-szorzat,
rendezett
elempár, elem
n-es elempár
(n-es) első,
második,...
tagja,
elempárok
egyenlőek, elem
n-esek
egyenlőek

Az $R \subseteq A \times B$ reláció **értelmezési tartománya** a $\text{Dom}(R) = \{a \in A | \text{létezik } b \in B \text{ úgy, hogy } (a, b) \in R\}$ halmaz., $\text{Rng}(R) = B$ -t **értékkészletének**, az $\text{Im}(R) = R(A) = \{b \in B | \text{létezik } a \in A \text{ úgy, hogy } (a, b) \in R\}$ halmazt **képhalmazának** nevezzük. Az $a \in A$ **elem képe** a $R(a) = \{b \in B | (a, b) \in R\}$.

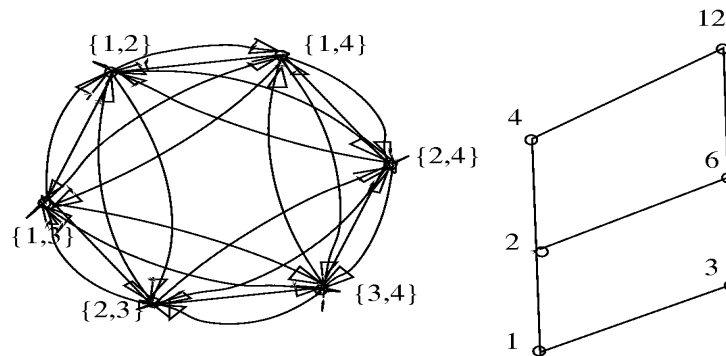
Az $R^{-1} = \{(b, a) \in B \times A | (a, b) \in R\}$ relációt az R **reláció inverzének** nevezzük. Homogén $R \subset A \times A$ kétváltozós relációk fontos típusai.

Fogalmak:
értelmezési
tartomány,
értékkészlet,
képhalmaz,
elem képe,
inverz, reflexív,
transzitiv,
antiszimmetrikus,
rendezés,
lineáris vagy
teljes,
ekvivalencia,
osztályozás

- (1) R **reflexív**, ha minden $a \in A$ esetén $(a, a) \in R$;
- (2) R **transzitiv**, ha $(a, b) \in R$ és $(b, c) \in R$ esetén $(a, c) \in R$;
- (3) R **szimmetrikus**, ha $(a, b) \in R$ esetén $(b, a) \in R$;
- (4) R **antiszimmetrikus**, ha $(a, b) \in R$ és $(b, a) \in R$ esetén $a = b$
- (5) R **rendezési reláció**, ha reflexív, antiszimmetrikus és transzitiv;

- (6) R rendezési reláció **lineáris vagy teljes**, ha $a \in A$ és $b \in B$ esetén $(a, b) \in R$;
- (7) R **ekvivalenciareláció**, ha reflexív, szimmetrikus és tranzitív.

Az $A \neq \emptyset$ halmazon adott **osztályozás** egy $\mathcal{C} \subseteq A$ halmazrendszer, amelynek elemeit **osztály**oknak nevezzük, hogy $\cup_{C \in \mathcal{C}} C = A$, és ha $C_1, C_2 \in \mathcal{C}$, $C_1 \neq C_2$ akkor $C_1 \cap C_2 = \emptyset$.



1.1. ábra. Az $\{1, 2, 3, 4\}$ halmaz kételemű részhalmazain a „metszet egyelemű” reláció nyíldiagramja és a 12 pozitív osztói halmazán az oszthatóság Hasse-diagramja

EKVIVALENCIA
RELÁCIÓ ÉS
OSZTÁLYOZÁS
Bizonyítás.

Ha $S \subseteq A \times A$ ekvivalenciareláció, akkor $\mathcal{C} = \{S(a) \times S(a) \mid a \in A\}$ az A halmaz osztályozását. Megfordítva, ha adva van egy $\mathcal{C} \subseteq \mathcal{P}(A)$ osztályozás, akkor $\cup\{C \times C \mid C \in \mathcal{C}\} \subseteq A \times A$ ekvivalenciareláció.

Hiszen, S reflexív és $\cup\{S(a) \mid a \in A\} = A$. Ha $c \in S(a) \cap S(b)$, lássuk be, hogy $S(a) = S(b)$. A szimmetria miatt $(a, c), (c, b) \in S$, a tranzitivitás miatt $(a, b) \in S$, és ismét a szimmetria miatt $(b, a) \in S$; így ha $d \in S(a)$ akkor $(d, a), (a, b) \in S$, a tranzitivitás és a szimmetria miatt $(b, d) \in S$ és $S(a) \subseteq S(b)$. Hasonlóan $S(b) \subseteq S(a)$.

Megfordítva, közvetlenül kapjuk, hogy az $R = \cup\{C \times C \mid C \in \mathcal{C}\}$ reláció reflexív, szimmetrikus és tranzitív.

Q.E.D.

Az R ekvivalenciareláció osztályainak A/R halmazát **faktorhalmaz**-nak nevezzük. Az $f \subseteq A \times B$ relációról azt mondjuk, hogy (egyváltozós) **függvény** vagy **leképezés**, ha $\text{Dom}(f) = A$ és minden $a \in A$ elem $f(a) = \{b\}$ képe egyelemű, ekkor azt mondjuk, hogy f az a **elemhez** az $f(a) = b$ **elemet rendeli**. Jelölés: $f : A \rightarrow B, a \mapsto f(a) = b$. A többváltozós függvény fogalma analóg. Az f és g **függvények egyenlőek**, ha $\text{Dom}(f) = \text{Dom}(g)$, $\text{Rng}(f) = \text{Rng}(g)$ és ha $f : a \mapsto b$ akkor $g : a \mapsto b$. Nevezetes fogalmakat tekintsünk át az $f : A \rightarrow B$ függvényre vonatkozóan.

Fogalmak:
faktorhalmaz,
függvény, kép,
egyenlőség
Fogalmak:
identikus
leképezés,
injektív,
szürjektív,
bijektív

- (i) **Identikus leképezés** $1_A : A \rightarrow A, a \mapsto a;$ (iii) **szürjektív**, ha $\text{Im}(f) = B;$
- (ii) f **injektív**, ha $f(a) = f(a')$ -ből $a = a'$ következik; (iv) f **bijektív**, ha injektív és szürjektív.

Legyen $f : A \rightarrow B$ és $g : B \rightarrow C$, **kompozíciósor** $g \circ f : A \rightarrow C, a \mapsto g \circ f(a) = g(f(a))$ függvény. Ha egy függvény mint reláció inverze is függvény, akkor azt mondjuk, hogy **invertálható függvény**. Könnyen látjuk:

Fogalmak:
kompozíció
sorzat,
invertálható
függvény

Ha $f : A \rightarrow B, g : B \rightarrow C$ és $h : C \rightarrow D$ függvények, akkor $(h \circ g) \circ f = h \circ (g \circ f)$.

ÁTZÁRÓJELEZÉS

Ha $f : A \rightarrow B$ függvény, akkor . az alábbi állítások ekvivalensek:

INVERTÁLHATÓSÁG

(i) f invertálható függvény;

(ii) létezik $g : B \rightarrow A$ függvény úgy, hogy $f \circ g = 1_B$ és $g \circ f = 1_A;$

(iii) f bijektív függvény.

Hiszen, tekintsük először az (i) $\implies$ (ii) implikációt. Legyen g az f inverzfüggvénye, így teljesül (ii).

Bizonyítás.

(ii) $\implies$ (iii) Ha $f(a) = f(a')$ akkor $g \circ f = 1_A$ miatt $a = 1_A(a) = g(f(a)) = g(f(a')) = 1_A(a') = a'$, és az injektivitás teljesül. Az $f \circ g = 1_B$ tulajdonság miatt $f(A) \supseteq f(g(B)) = 1_B(B) = B$, és a szürjektivitás világos.

(iii) $\implies$ (i) f függvény szürjektív, így az f^{-1} inverzreláció értelmezési tartománya az egész B . Az injektivitás miatt pedig az $f^{-1}(b)$ halmaz egyelemű.

Q.E.D.

Az A és B halmazokat **meg egyező számosságúnak** hívunk, ha létezik $f : A \rightarrow B$ bijekció. Ha A számossága egyetlen valódi részhalmazáéval sem egyezik meg, A -t **véges számosságú**, ellenkező esetben A **végtelen számosságú halmaz**ként eméltjük.

Fogalmak:
számosság,
véges halmaz,
végtelen
halmaz, , ,
Fogalmak:
egyváltozós,
kétváltozós,
 n -változós
művelet,
algebrai
struktúra

1.1.3. Műveletek.

Legyen $A \neq \emptyset$ halmaz.

- (1) $*$ **egyváltozós (unér) művelet** $* : A \rightarrow A, a \mapsto a^*$ függvény;

- (2) * **kétváltozós (binér) művelet** $*$: $A \times A \rightarrow A$, $(a, b) \mapsto a * b$ függvény;
- (3) * **n -változós (n -ér) művelet** $*$: $\underbrace{A \times A \times \dots \times A}_{n\text{-szer}} \rightarrow A$,
 $(a_1, a_2, \dots, a_n) \mapsto *(a_1, a_2, \dots, a_n)$ függvény;
- (4) Ha az A halmazon adva van m darab $*, \circ, \dots$ művelet, akkor az $(A, *, \circ, \dots)$ rendezett elem $m + 1$ -est **m -műveletes algebrai struktúrának** nevezzük.

Egy- és kétváltozós műveletekre láttunk példákat fentebb a halmazműveleteknél. Művelet alatt kétváltozós műveletet fogunk érteni. Az alábbi műveleti tulajdonságokat szokás tanulmányozni. Legyen $(A, *)$ algebrai struktúra a $*$ művelettel.

Fogalmak:
 asszociatív,
 kommutatív,
 idempotens,
 invertálható,

- (1) * **asszociatív**, ha minden $a, b, c \in A$ -ra $(a * b) * c = a * (b * c)$;
- (2) * **kommutatív**, ha minden $a, b \in A$ elemre $a * b = b * a$;
- (3) * **idempotens**, ha minden $a \in A$ elemre $a * a = a$;
- (4) * **invertálható**, ha minden $a, b \in A$ elemhez létezik $u, v \in A$ elem úgy, hogy $a * u = b$ és $v * a = b$.

Fogalmak:
 neutrális elem,
 zéruselem,
 zérusosztó,
 inverz

Kitüntetett elem az

- (1) $e \in A$ **neutrális elem**: minden $a \in A$ elem esetén $e * a = a * e = a$;
- (2) $z \in A$ **zéruselem**: minden $a \in A$ elem esetén $z * a = a * z = z$;
- (3) $a \in A$ **zérusosztó**: létezik $b \in A$ úgy, hogy $b \neq z$ és $a * b = z$ vagy $b * a = z$, ahol z zéruselem;
- (4) az $a \in A$ **elem** $b \in A$ **inverze**: $a * b = b * a = e$, ahol e neutrális elem.

Azokat az elemeket, amelyeknek létezik inverzük, **invertálható elem**-eknek vagy **egységeknek** nevezzük. Azt mondjuk, hogy egy zéruselemet tartalmazó struktúra **zérusosztómentes**, ha az egyedüli zérusosztó a zéruselem. Az $a \in A$ **elemmel lehet egyszerűsíteni**, ha minden $b, c \in A$ elem esetén abból, hogy $a * b = a * c$ vagy $b * a = c * a$ következik $b = c$.

Legyen $(A, *, \circ)$ algebrai struktúra. Azt mondjuk, hogy

- (1) $a * \text{ művelet }$ **disztributív** $a \circ \text{ műveletre nézve}$, ha minden $a, b, c \in A$ elemre $a * (b \circ c) = (a * b) \circ (a * c)$ és $(a \circ b) * c = (a * c) \circ (b * c)$;
- (2) $a * \text{ művelet }$ **abszorbtív** $a \circ \text{ műveletre nézve}$, ha minden $a, b \in A$ elemre $a * (a \circ b) = a$ és $(b \circ a) * a = a$

Fogalmak:
disztributív,
abszorbtív

$(A, *)$ struktúráról azt mondjuk, hogy

- (1) **félcsoport**, ha $*$ asszociatív;
- (2) **monoid**, ha félcsoport, és létezik neutrális eleme;
- (3) **kommutatív félcsoport**, ha félcsoport, és a művelet kommutatív;
- (4) **félháló**, ha kommutatív félcsoport és a művelet idempotens;
- (5) **csoport**, ha monoid és minden elemnek van inverze;
- (6) **Abel- (kommutatív) csoport**, ha csoport és a művelet kommutatív.

Fogalmak:
félcsoport,
monoid, ,
kommutatív
félcsoport,
félháló, csoport,
kommutatív
csoport

Ha művelet az összeadás illetve a szorzás, $(A, +)$ -t **additív struktúrá**-nak, $(A, \cdot)$ -t **multiplikatív struktúra**-nak nevezzük, szokás az additív neutrális elemet **nullá**nak nevezni és 0-val jelölni; az a elem additív inverzét **ellentett**jének nevezni és $-a$ -val jelölni; a multiplikatív neutrális elemet **egységelem**nek nevezni és 1-gyel jelölni; az a elem multiplikatív inverzét **reciprok**ának nevezni és a^{-1} -gyel jelölni.

Az $(A, +, \cdot)$ algebrai struktúráról azt mondjuk, hogy

- (1) **gyűrű**, ha $(A, +)$ Abel-csoport, $(A, \cdot)$ félcsoport és a szorzás disztributív az összeadásra nézve;
- (2) **kommutatív gyűrű**, ha gyűrű és a szorzás kommutatív;
- (3) **egységelemes gyűrű**, ha legalább kételemű gyűrű és $(A, \cdot)$ monoid;
- (4) **ferdetest**, ha egységelemes gyűrű és $A \setminus \{0\}, \cdot$ csoport;
- (5) **test**, ha kommutatív egységelemes gyűrű és $A \setminus \{0\}, \cdot$ csoport.

Fogalmak:
additív
struktúra,
multiplikatív
struktúra,
nulla, ellentett,
egységelem,
reciprok, gyűrű,
kommutatív
gyűrű,
egységelemes
gyűrű,
ferdetest, test

Legyen $(A, \cdot)$ félcsoporth. Ekkor

ASSZOCIATIVITÁS
KÖVETKEZMÉNYEI

(i) *Tetszőleges számú A -beli tényezőből álló szorzat értéke független a zárójelezéstől.*

(ii) *Ha $(A, \cdot)$ monoid, akkor egyetlen neutrális eleme van, és ha az $a \in A$ elem egység, akkor inverze egyértelmű.*

Bizonyítás.

Hiszen, lássuk be (i)-et. Legyen az $a_1, \dots, a_n \in A$ elemek tetszőlegesen zárójelezett szorzata t_n , és legyen $l_n = (\dots((a_1 a_2) a_3) \dots) a_n$ a balrarendezett szorzat. Indukcióval n szerint belátjuk, hogy $t_n = l_n$. $n = 3$ esetén az állítás éppen a szorzás asszociativitása. Tegyük fel, hogy n -nél kisebb tényezős szorzatok ($n > 3$) tetszőlegesen zárójelezhetők. Ha $t_n \neq l_n$ akkor $t_n = t_k u$, ahol u az $a_{k+1}, \dots, a_n$ elemek valamely szorzata. Indukció alapján $t_k = l_k$ és $u = a_{k+1}(a_{k+2}(\dots(a_{n-1} a_n) \dots)) = r_{n-k}$ jobbrarendezett szorzat, azaz az asszociativitás többszöri alkalmazásával

$$\begin{aligned} t_n &= l_k(a_{k+1}(a_{k+2}(\dots(a_{n-1} a_n) \dots))) = \\ &= (l_k a_{k+1})(a_{k+2}(a_{k+3}(\dots(a_{n-1} a_n) \dots))) = \\ &= l_{k+1}(a_{k+2}(\dots(a_{n-1} a_n) \dots)) = \dots = l_{n-2}(a_{n-1} a_n) = l_{n-1} a_n \end{aligned}$$

$= l_n$, amit be kellett látni.

(ii) Legyen e, f neutrális elem. Ekkor mivel f neutrális elem, $ef = e$, de mivel e is neutrális elem, $ef = f$, azaz $e = f$. Ha $aa^{-1} = a^{-1}a = e$ és $ab = ba = e$, akkor $b = eb = (a^{-1}a)b = a^{-1}(ab) = a^{-1}e = a^{-1}$.

Q.E.D.

Fogalmak:
egységcsoporth
egységcsoporth,
permutáció,
szimmetrikus
csoporth,
transzpozíció

Mivel (multiplikatív írt) monoidban ha az a és b elemnek van inverze akkor az ab elemnek is van, $b^{-1}a^{-1}$, monoid egységei csoportot alkotnak, az úgynevezett **egységcsoporthot**. Ha A egy halmaz, akkor az összes $A \rightarrow A$ függvény halmazán a kompozíciószorzás művelet, amelyre nézve a függvények halmaza félcsoporth, amelyben az identikus leképezés neutrális elem. Ezek közül az egységek a bijektív leképezések, az (ismétlés nélküli) **permutációk**, ezeknek a csoportja az A halmaz **szimmetrikus csoportja**, ha A rendje véges n , akkor jelölés S_n , az n -edfokú szimmetrikus csoport. Gyakori a permutációk úgynevezett kétsoros jelölése: legyen

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 3 & 4 & 6 & 9 & 5 & 2 & 1 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 1 & 9 & 4 & 7 & 6 & 3 & 2 \end{pmatrix}$$

kilenc elem két permutációja. Nyilván a felső sor eleméhez a permutáció az alatta levő elemet rendeli. Minden elem mindkét sorban egyszer

és csak egyszer szerepel. A permutációk közötti művelet a függvény-szorzás. Ezt háromsoros alakban végezhetjük el:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 5 & 1 & 9 & 1 & 7 & 6 & 3 & 2 \\ 2 & 6 & 7 & 1 & 4 & 5 & 9 & 3 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 6 & 7 & 1 & 4 & 5 & 9 & 3 & 8 \end{pmatrix},$$

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 3 & 4 & 6 & 9 & 5 & 2 & 1 \\ 6 & 3 & 1 & 9 & 7 & 2 & 4 & 5 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 3 & 1 & 9 & 7 & 2 & 4 & 5 & 8 \end{pmatrix}.$$

Figyeljük meg, hogy a $\sigma\tau$ szorzatban a második sorba a τ permutáció második sora került, mivel a kompozíció-szorzásnál az $(f \circ g)(x) = f(g(x))$ konvenciót használjuk. Látjuk azt is, hogy $n \geq 3$ -ra az S_n szimmetrikus csoport nemkommutatív. Nyilván n elem permutációinak szorzása asszociatív, az identikus permutáció neutrális elem, és permutációnak létezik inverze, mivel bijektív leképezés, és az is permutáció. Számítsuk ki a σ permutáció összes hatványát! Ehhez az úgynevezett egysoros jelölést alkalmazzuk. Egy permutációt **ciklusnak** nevezünk, ha összes mozgatott elemét egymás között ciklikusan $i_1 \rightarrow i_2 \rightarrow \dots \rightarrow i_l \rightarrow i_1$ alakban permutálja, ahol a mozgatott elemek l számát a **ciklus hosszának** nevezzük; a ciklus jelölése $(i_1 i_2 \dots i_l)$. Egy $(G, \cdot)$ csoportban a $g \in G$ **elem rendjének** nevezzük azt legkisebb pozitív n természetes számot, hogy $g^n = 1$, ha ilyen nincs, azt mondjuk, hogy g **végtelenrendű elem**, jelölés $|g|$. Ciklus rendje nyilván megegyezik a hosszával. Permutáció egymás között mozgatott elemeinek halmazát **pályának** nevezzük, ezek osztályozást alkotnak. Diszjunkt nemtriviális pályákkal rendelkező ciklusokat **diszjunkt ciklusoknak** nevezzük. Egy ciklust ily módon többféleképpen jelölhetünk:

Fogalmak:
ciklus,
diszjunkt
ciklusok, ciklus
hossza, elem
rendje, pálya,
transzpozíció

$$(i_1 i_2 \dots i_l) = (i_2 i_3 \dots i_l i_1) = \dots = (i_l i_1 i_2 \dots i_{l-1}).$$

Nemidentikus permutáció felírható sorrendtől eltekintve egyértelműen diszjunkt ciklusok szorzataként. Az eljárás a σ permutáción alkalmazva a következő. Kiindulunk valahonnan, például az 1-ből (célszerű a természetes sorrendhez ragaszkodni): $1 \rightarrow 7 \rightarrow 5 \rightarrow 6 \rightarrow 9 \rightarrow 1$ azaz (17569), bejártuk az első pályát a σ permutációnak, megkatuk a felbontás első 5 hosszú ciklusát. Vegyük észre, hogy mindegy, hogy

EGYSOROS
ALAK

honnan indultunk ki: $(17569) = (75691) = (56917) = (69175) = (91756)$. A második (nemtriviális) pálya (28). Kimaradt a 3 és a 4, amiket σ fixál, ezek önmagukban úgynevezett triviális pályákat alkotnak, nem veszünk bele a felírásba. Így $\sigma = (17569)(28)$ az egysoros alak. Ebben az alakban könnyű invertálni: vegyük észre, hogy a diszjunkt ciklusok egymással felcserélhetőek, mivel más-más elemeket mozgatnak. így lehet az eredeti sorrendben tényezőnként invertálni, ciklus inverzét pedig a nyilakat megfordítva kapjuk: $\sigma^{-1} = (19657)(28)$. A (28) kettő hosszú ciklus, úgynevezett **transzpozíció**, inverze önmaga.

Visszatérve a σ permutáció összes hatványa kiszámításának a kérdéséhez vegyük észre, hogy mivel diszjunkt ciklusok egymással felcserélhetőek, lehet az egysoros felírásban tényezőnként hatványozni, és ciklust k -adik hatványra úgy lehet emelni, hogy a ciklusban nem egyenként, hanem k lépésenként megyünk körbe, amíg el nem értük a kiindulási pontot. Azaz $\sigma^2 = (19675)^2(28)^2 = (16597)$, $\sigma^3 = (17956)(28)$, $\sigma^4 = (19657)$, $\sigma^5 = (28)$, $\sigma^6 = (19675)(28)\sigma^5 = (19675)$, $\sigma^7 = (16597)(28)$, $\sigma^8 = (17956)$, $\sigma^9 = (19657)(28)$, $\sigma^{10} = (1)$, a magasabb hatványok ezután ciklikusan ismétlődnek. A σ permutáció összes különböző hatványainak a száma 10, ezek szorzata szintén σ -hatvány, és a negatív kitevőseket is kimerítik, $\sigma^{-1} = \sigma^9$), azaz $|\sigma| = 10$. $\sigma \in S_n$ permutáció rendje megegyezik egysoros alakjában a diszjunkt faktorok hosszainak legkisebb közös többszörösével.

PERMUTÁCIÓ
RENDJE

Fogalmak: Legyen $(G, \cdot)$ csoport, $a, b \in G$. Ha létezik $g \in G$ elem úgy, hogy konjugált, $b = g^{-1}ag$, akkor azt mondjuk, hogy b az a **elem konjugáltja**, és a csoportban, $b = a^g$ jelölést alkalmazzuk. A konjugált reláció nyilván ekvivalencia, konjugáltság konjugáltsági osztály

Legyen $\sigma, \tau \in S_n$ permutáció, $\sigma = \sigma_1\sigma_2 \cdots \sigma_k$ egysoros alak, $\sigma_1 = (i_1 \dots i_{l_1})$. Ekkor a $\tau(i) = i^\tau$ jelöléssel élve,

PERMUTÁCIÓ
KONJUGÁLTJA

$$\sigma_1^\tau = (i_1^{\tau^{-1}} \dots i_{l_1}^{\tau^{-1}}), \quad \sigma^\tau = \sigma_1^\tau \sigma_2^\tau \cdots \sigma_k^\tau$$

Továbbá, S_n egy konjugált osztályában az összes olyan permutáció van, amelynek egysoros alakja ugyanolyan típusú, azaz ugyanolyan hosszú ciklus faktorból ugyanannyi van a felbontásokban.

Az előző példa permutációira

$$\sigma^\tau = (17569)^\tau(28)^\tau = (1^{\tau^{-1}}7^{\tau^{-1}}5^{\tau^{-1}}6^{\tau^{-1}}9^{\tau^{-1}})(2^{\tau^{-1}}8^{\tau^{-1}}) = (36274)(91)$$

Legyen A egy halmaz, az úgynevezett **ábécé**, elemei a **betűk**. Képezzünk a betűkből (véges hosszú) szavakat, ezek közötti művelet legyen a **konkatenáció**, az egymásutánírás, amelyet asszociatívnak tekintünk. Kaptuk az úgynevezett **szabad félcsoporthot**. Bővítsük ki az A ábécét újabb betűkkel az $A \cup A^{-1}$ ábécévé, ahol $A^{-1} = \{a^{-1} \mid a \in A\}$. Tekintsük az $A \cup A^{-1}$ ábécé betűiből képzett szavak W halmazát, amelybe beleértjük az üres szót is. Egy W -beli szót **redukált alakúnak** nevezünk, ha benne nem áll egymás mellett a illetve a^{-1} alakú betű. Tetszőleges W -beli szóhoz tartozik redukált alakú szó, az aa^{-1} illetve $a^{-1}a$ alakú szórészek helyébe az üres szót írva, esetleg több lépésben. Legyen F a redukált alakú szavak halmaza (az üres szóval együtt). Két F -beli szó konkatenáltja legyen az egymásutánírt szó (ami W eleme) redukált alakja (ez már biztosan F -beli), a konkatenációt ismét asszociatívnak tekintve. Ekkor a konkatenáció művelet a redukált alakú szavak F halmazán, amely erre a műveletre nézve csoport, amelyet az A ábécé feletti **szabad csoportnak** nevezünk.

Fogalmak:
ábécé,
konkatenáció,
szabad
félcsoporthot,
redukált alak,
szabad csoport

Legyen $(A, +, \cdot)$ gyűrű. Ekkor:

- (i) az additív neutrális elem multiplikatív zéruselem;
- (ii) minden $a \in A$ elemre $(-a)b = a(-b) = -(ab)$ és $(-a)(-b) = ab$;
- (iii) ha $(A, +, \cdot)$ egységelemes gyűrű, akkor minden $a \in A$ elemre $-a = (-1)a$.

DISZTRIBUTIVITÁS
KÖVETKEZMÉNYEI

Hiszen, egyen $a \in A$. Ekkor, mivel 0 additív neutrális elem, és a disztributív törvény teljesül, $0a = (0 + 0)a = 0a + 0a$, és mindkét oldalhoz hozzáadva $-0a$ -t kapjuk, hogy $0 = 0a$. Hasonlóan adódik, hogy $0 = a0$, kapjuk (i)-et. (ii) és (iii) hasonlóan egyszerűen látható.

Bizonyítás.

Q.E.D.

Ferdetest, test zérusosztómentes. A kommutatív, egységelemes és zérusosztómentes gyűrűt **integritástartomány**nak nevezzük.

Fogalmak:
integritás
tartomány

1.1.4. A természetes számoktól a valós számokig

Feltesszük, hogy adva van az univerzumnak egy $\mathbb{N}$ részhalmaza, a **természetes számok halmaza**, elemei a **természetes számok**, és teljesülnek az alábbi úgynevezett **Peano-axiómák**:

Az (5) axiómán alapul a rekurzív definíció és a teljes indukciós bizonyítás módszere. A szokásos jelölések és elnevezések: $0' = 1$ egy, $1' = 2$ kettő, $2' = 3$ három, és így tovább. Mivel a rákövetkezés leképezés a (3) és (4) axiómák alapján $\mathbb{N} \rightarrow \mathbb{N}^+$ ($\mathbb{N}^+ = \mathbb{N} \setminus \{0\}$) a **pozitív**

Fogalmak:
természetes
számok
halmaza,
pozitív, Peano-
axiómák,
megszámlálható,
megszámlálhatatlan,
rend

- (1) létezik $0 \in \mathbb{N}$ nullának nevezett elem;
- (2) létezik $' : \mathbb{N} \rightarrow \mathbb{N}$, $a \mapsto a'$ leképezés, a' -t az a rákövetkezőjének nevezzük;
- (3) nem létezik $a \in \mathbb{N}$, hogy $a' = 0$
- (4) a rákövetkezés leképezés injektív;
- (5) ha $A \subseteq \mathbb{N}$, $0 \in A$, továbbá ha $a \in A$ maga után vonja $a' \in A$ -t, akkor $A = \mathbb{N}$.

természetes számok) bijekció, a $\mathbb{N}$ halmaz végtelen. $\mathbb{N}$ részhalmazával megegyező számosságú halmazokról azt mondjuk, hogy számosságuk megszámlálható. Az összes többi halmazról azt mondjuk, hogy számosságuk megszámlálhatatlan. Ha A véges halmaz, akkor számossága megegyezik valamely $n \in \mathbb{N}$ -re az $\underline{n} = \{1, 2, \dots, n\}$ halmazéval, ekkor azt mondjuk, hogy A számossága n . A számosságra a $|B|$ jelölést alkalmazzuk, gyakran azt is mondjuk, hogy B rendje $|B|$.

Fogalmak: Az utolsó Peano-axiómán alapul a rekurzív definíció módszere. összeadás, Természetes számot, mint paramétert tartalmazó fogalmakat vagy elemeket határozunk meg oly módon, hogy megadjuk a 0-hoz tartozót, szorzás és azt, hogy tetszőleges n természetes szám esetén az n -hez tartozó fogalom illetve elem ismeretében hogyan határozható meg az n' rákövetkezőhöz tartozó. A természetes számok közötti összeadás és szorzás műveletét így definiáljuk rekurzíve: tetszőleges $a \in \mathbb{N}$ -re legyen $a + 0 = a$, $a \cdot 0 = 0$, továbbá ha $b \in \mathbb{N}$, akkor legyen $a + b' = (a + b)'$ és $ab' = ab + a$. Teljesülnek a megszokott műveleti tulajdonságok, mint azt látni fogjuk. Azt mondjuk, hogy az $(A, *)$ struktúrában lehet egyszerűsíteni, ha minden $a, b, c \in A$ -ra $a*b = a*c$ vagy $b*a = c*a$ -ból $a = b$ következik. A bizonyítás módszere a teljes indukció.

A
TERMÉSZETES
SZÁMOK
STRUKTÚRÁJA

- (i) $(\mathbb{N}, +)$ struktúra kommutatív félcsoporth, amelyben lehet egyszerűsíteni, neutrális eleme a 0;
- (ii) $(\mathbb{N}, \cdot)$ kommutatív félcsoporth, neutrális eleme az 1, $(\mathbb{N}^+, \cdot)$ struktúrában lehet egyszerűsíteni;
- (iii) a szorzás az összeadásra nézve disztributív.

Bizonyítás. Hiszen, lássuk be először, hogy 0 neutrális elem. A definíció szerint $a + 0 = a$. Nyilván $0 + 0 = 0$, és tegyük föl, hogy $0 + a = a$ (az ün. indukciós feltevés). Be kell látni, hogy az állítás igaz a' -re is. Valóban,

$0 + a' = (0 + a)' = a'$. Ezzel beláttuk az állítást tetszőleges $a \in \mathbb{N}$ -re. Most tekintsük a kommutativitást. Mivel 0 neutrális elem, $a + 0 = 0 + a$, és tegyük föl, hogy $a + b = b + a$. Ekkor $a + b' = (a + b)' = (b + a)' = b + a'$, így elegendő belátni, hogy $b + a' = b' + a$, újbóli indukcióval. Nyilván $b + 0' = (b + 0)' = b' = b' + 0$, és tegyük föl, hogy $b + a' = b' + a$. Ekkor $b + a'' = (b + a')' = (b' + a)' = b' + a'$. A többi tulajdonság hasonlóan adódik indukcióval.

Q.E.D.

Azt mondjuk, hogy az a természetes szám kisebb vagy egyenlő mint a b természetes szám, ha valamely $c \in \mathbb{N}$ -re $b = a + c$, jelölés: $a \leq b$, illetve az éles egyenlőtlenségé $a < b$.

Fogalmak:
rendezés

$\mathbb{N}$ -en $\leq$ lineáris rendezés, $\mathbb{N}$ tetszőleges nemüres halmazában van legkisebb elem. 0 a rendezés minimális eleme.

 $\mathbb{N}$ RENDEZÉSE

Az $\mathbb{N}$ számkörön belül a négy alpművelet közül kettőt el lehet végezni. Ahhoz, hogy a kivonást is el lehessen végezni, bővíteni kell a számhalmazt. Legyen a_1 és a_2 természetes szám. Az $a_1 - a_2$ különbséget (ami nem biztos, hogy természetes szám) jelképezze az (a_1, a_2) kisebbítendő – kivonandó elempár. Ennek megfelelően két elempár megegyezik, ha ugyanannyi az $a_1 - a_2 = b_1 - b_2$ különbségük, azaz $a_1 + b_2 = a_2 + b_1$. Az összeadást és a szorzást is elvégezhetjük a kisebbítendő – kivonandó elempárok között: $(a_1 - a_2) + (b_1 - b_2) = (a_1 + b_1) - (a_2 + b_2)$ illetve $(a_1 - a_2)(b_1 - b_2) = (a_1 b_1 + a_2 b_2) - (a_1 b_2 + a_2 b_1)$. Ezeket az észrevételeket szem előtt tartva konstruálhatjuk meg az egész számokat.

Legyen $Z = \mathbb{N} \times \mathbb{N}$ $\rho \subseteq Z \times Z$ a következőképpen meghatározva: $(a_1, a_2) \rho (b_1, b_2)$ ha $a_1 + b_2 = a_2 + b_1$. Ekkor ρ ekvivalencia-reláció, (a_1, a_2) ekvivalencia-osztályát jelölje $\overline{(a_1, a_2)}$, az ekvivalencia-osztályok faktorhalmazát jelölje Z . Legyen továbbá $a = \overline{(a_1, a_2)}$, $b = \overline{(b_1, b_2)} \in Z$,

AZ EGÉSZÉK
STRUKTÚRÁJA

$$a + b = \overline{(a_1 + b_1, a_2 + b_2)}, \quad a \cdot b = \overline{(a_1 b_1 + a_2 b_2, a_1 b_2 + a_2 b_1)}.$$

Ekkor a $(Z, +, \cdot)$ integritástartomány.

A $(Z, +, \cdot)$ struktúrát az egész számok gyűrűjének, elemeit egész számoknak nevezzük. Az $a \in \mathbb{N}$ természetes számot azonosítsuk az $\overline{(a, 0)} \in Z$ egész számmal úgy tekinthetjük, hogy $\mathbb{N} \subset Z$, és $Z = Z^- \cup \{0\} \cup \mathbb{N}^+$, ahol Z^- elemei a negatív egészek, $\mathbb{N}^+ = Z^+$ elemeinek ellentettjei. Teljesül a kiterjesztési elv: két természetes számot összeadva és szorozva ugyanazt kapjuk, akár természetes akár egész számként tesszük. . A $\mathbb{N} \leq$ rendezését kiterjeszthetjük az egész Z -re figyelembe véve, hogy -1 -gyel szorozva az egyenlőtlenség iránya megfordul.

Fogalmak:
egész számok
gyűrűje,
negatív egész
számok

Z -n $\leq$ lineáris rendezés, továbbá, ha $a, b, c \in Z$, $a \leq b$ és $d \in Z^+$ akkor $a + c \leq b + c$ és $ad \leq bd$.

Az egész számkörben a negyedik alapművelet, az osztás nem mindig végezhető el. Ezért kiterjesztjük a számfogalmat a racionális számokkal. A racionális számokat egész számokból alkotott számláló – nevező rendezett elempárnak tekintjük, ahol a nevező nem lehet nulla. Két tört, $\frac{a_1}{a_2}$ és $\frac{b_1}{b_2}$ egyenlő, ha $a_1b_2 = a_2b_1$. Az összeadás műveletét közös nevezőre hozás után végezhetjük el, a szorzást pedig a megszokott „számlálót a számlálóval, nevezőt a nevezővel” szabály szerint. Mivel az eljárás során csak azt használjuk ki, hogy $\mathbb{Z}$ integritástartomány, teljesen általánosan járhatunk el.

HÁNYADOSTEST Legyen $(A, +, \cdot)$ integritástartomány, $B = A \times A \setminus \{0\}$, $\rho \subseteq B \times B$ reláció a következőképpen meghatározva: $((a_1, a_2), (b_1, b_2)) \in \rho$ ha $a_1b_2 = a_2b_1$. Ekkor ρ ekvivalencia-reláció, tekintsük a $Q = B/\rho$ faktorhalmazt. Jelölje (a_1, a_2) ekvivalenciaosztályát $\frac{a_1}{a_2} \in Q$. Legyen

$$\frac{a_1}{a_2} + \frac{b_1}{b_2} = \frac{a_1b_2 + a_2b_1}{a_2b_2}, \quad \frac{a_1}{a_2} \frac{b_1}{b_2} = \frac{a_1b_1}{a_2b_2}.$$

Ekkor $(Q, +, \cdot)$ test.

Fogalmak: A Q testet az A integritástartomány **hányadostest**ének, a $\mathbb{Z} \subset Q$ hányadostestét a **racionális számtest**nek, elemeit **racionális számok**nak nevezzük. Azonosíthatjuk az $a \in \mathbb{Z}$ számot az $\frac{a}{1} \in Q$ számmal, így tekinthetjük úgy, hogy $\mathbb{Z} \subset Q$ és az összeadás és szorzás Q -n az egész számok közötti műveletek kiterjesztései, és minden racionális szám előáll két egész szám hányadosaként. $\mathbb{Z} \leq$ rendezését kiterjeszthetjük Q -ra.

REDUKÁLT ALAK Minden $r \in Q$ -hoz létezik egyértelműen $a \in \mathbb{Z}$, $b \in \mathbb{Z}^+$, hogy $r = \frac{a}{b}$, a és b relatív prímek.

Ekkor az $\frac{a}{b}$ alakot **redukált alak**nak nevezzük.

Legyen $r, s \in Q$, $r = \frac{a}{b}$ és $s = \frac{c}{d}$ redukált alakok, és legyen $r \leq s$ ha $ad \leq bc$. Ekkor Q -n $\leq$ lineáris rendezés, továbbá, ha $r, s, t \in Q$, $r \leq s$ és $u \in Q^+$ akkor $r + t \leq s + t$ és $ru \leq su$.

Érdekes tulajdonság, hogy míg az egész számhoz van előző és rákövetkező egész szám, addig bármely két különböző racionális szám között van egy harmadik racionális szám, figyelembe véve, hogy számtani közepük mindig egy harmadik szám a kettő között. Ismeretes, hogy vannak nem összemérhető szakaszok, azaz amelyek hossza nem racionális szám, például az egységnégyzet átlójának hossza, az egységkör kerülete. A számegyenes nem fedik le teljesen a racionális számok, noha minden pontja tetszőlegesen közelíthető racionális ponttal.

Tekintsük a racionális sorozatokat, azaz az $a : \mathbb{N} \rightarrow \mathbb{Q}, n \mapsto a_n$ leképezéseket. Ezek között vannak konvergensek, azaz olyanok, amelyekhez létezik olyan $u \in \mathbb{Q}$ racionális szám, hogy tetszőleges $\varepsilon \in \mathbb{Q}^+$ -hoz létezik $N \in \mathbb{N}$, hogy $|u - a_n| < \varepsilon$ hacsak $n > N$. Ilyenkor azt mondjuk, hogy az a_n sorozat határértéke $u \in \mathbb{Q}$, jelölés: $\lim_{n \rightarrow \infty} a_n = u$. a_n -t nullsorozatnak nevezzük, ha $\lim_{n \rightarrow \infty} a_n = 0$. nullához konvergáló racionális sorozatot.

Fogalmak:
sorozat,
konvergens,
sorozat
határértéke,
nullsorozat,

Az a_n racionális sorozatot Cauchy-sorozatnak hívjuk, ha minden $\varepsilon \in \mathbb{Q}^+$ -hoz létezik $N \in \mathbb{N}$, hogy $|a_n - a_m| < \varepsilon$ hacsak $n, m > N$. Nyilván racionális konvergens sorozat Cauchy-tulajdonságú, a megfordítás nem teljesül: bizonyos racionális Cauchy-sorozatok „irracionális” számokhoz konvergálnak.

Legyen R a racionális Cauchy-sorozatok halmaza, és legyen a $\rho \subseteq R \times R$ reláció a következőképpen meghatározva: $(a_n, b_n) \in \rho$ ha $a_n - b_n$ nullsorozat. Ekkor a ρ reláció ekvivalenciareláció, az ekvivalenciaosztályok halmazát jelölje $\mathbb{R}$. A műveleteket az $\mathbb{R}$ halmazon definiáljuk az alábbi módon: $\overline{a_n} + \overline{b_n} = \overline{a_n + b_n}$; $\overline{a_n} \overline{b_n} = \overline{a_n b_n}$. Ekkor az $(\mathbb{R}, +, \cdot)$ test.

A VALÓS
SZÁMOK
STRUKTÚRÁJA

Hiszen, legyen a_n, b_n, c_n, d_n racionális Cauchy-sorozat. ρ ekvivalenciareláció Nyilván a ρ reláció reflexív és szimmetrikus. Legyen $a_n - b_n$ és $b_n - c_n$ nullsorozat, és legyen ε pozitív racionális szám, N_1 és N_2 olyan természetes szám, hogy $|a_n - b_n| < \frac{\varepsilon}{2}$ hacsak $n > N_1$ és $|b_n - c_n| < \frac{\varepsilon}{2}$ hacsak $n > N_2$. Ekkor $|a_n - c_n| = |(a_n - b_n) + (b_n - c_n)| \leq |a_n - b_n| + |b_n - c_n| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$ hacsak $n > \max\{N_1, N_2\}$, azaz $a_n - c_n$ nullsorozat, és a ρ reláció tranzitív.

Bizonyítás.

Az összeadás és a szorzás művelet. Be kell látni, hogy Cauchy-sorozatok összege és szorzata is Cauchy-tulajdonságú. Legyen az N_1 természetes szám olyan, hogy $|a_n - a_m| < \frac{\varepsilon}{2}$ hacsak $n, m > N_1$, és az N_2 olyan, hogy $|b_n - b_m| < \frac{\varepsilon}{2}$ hacsak $n, m > N_2$. Ekkor, ha $n, m > \max\{N_1, N_2\}$, $|(a_n + b_n) - (a_m + b_m)| = |(a_n - a_m) + (b_n - b_m)| \leq |a_n - a_m| + |b_n - b_m| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon$, és az $a_n + b_n$ sorozat Cauchy-tulajdonságú.

Most lássuk be, hogy az a_n Cauchy-sorozat korlátos, azaz van olyan A pozitív racionális szám, hogy $|a_n| \leq A$ minden n természetes számra. Valóban, legyen az N természetes szám olyan, hogy $|a_n - a_m| < 1$ hacsak $n, m > N$. Világos, hogy $A = \max\{|a_1|, |a_2|, \dots, |a_N|, |a_{N+1}| + 1\}$ megfelelő korlát.

Legyen az a_n sorozat korlátja az A racionális szám és a b_n sorozat korlátja a B racionális szám. Legyen továbbá az N_1 természetes szám olyan, hogy $|a_n - a_m| < \frac{\varepsilon}{2B}$ hacsak $n, m > N_1$, és az N_2 olyan, hogy

$|b_n - b_m| < \frac{\varepsilon}{2A}$ ha csak $n, m > N_2$. Ekkor, ha $n, m > \max\{N_1, N_2\}$,

$$\begin{aligned} |a_n b_n - a_m b_m| &= |a_n b_n - a_m b_n + a_m b_n - a_m b_m| = \\ &= |(a_n - a_m)b_n + a_m(b_n - b_m)| \leq \\ &= |(a_n - a_m)b_n| + |a_m(b_n - b_m)| = |a_n - a_m||b_n| + |a_m||b_n - b_m| \\ &< \frac{\varepsilon}{2B}B + A\frac{\varepsilon}{2A} = \varepsilon, \end{aligned}$$

azaz az $a_n b_n$ sorozat is Cauchy-tulajdonságú.

Legyen $\alpha = \overline{a_n}$, $\beta = \overline{b_n}$, $\gamma = \overline{c_n}$, $\delta = \overline{d_n}$ az $\mathbb{R}$ halmaz elemei.

Az összeadás és a szorzás jóldefiniált. Be kell látni, hogy ha $\alpha = \gamma$, azaz $a_n - c_n$ nullsorozat, és $\beta = \delta$, azaz $b_n - d_n$ nullsorozat, akkor $\alpha + \beta = \gamma + \delta$, azaz $(a_n + b_n) - (c_n + d_n) = (a_n - c_n) + (b_n - d_n)$ nullsorozat; illetve $\alpha\beta = \gamma\delta$, azaz $a_n b_n - c_n d_n = a_n(b_n - d_n) + (a_n - c_n)d_n$ nullsorozat. Ez a két tulajdonság azokból a nyilvánvaló tényekből adódik, hogy nullsorozatok összege nullsorozat, és egy korlátos sorozat és egy nullsorozat szorzata nullsorozat.

Az összeadás asszociatív. Nyilván $(\alpha + \beta) + \gamma = \overline{a_n + b_n} + \gamma = \overline{a_n + b_n + c_n}$ és $\alpha + (\beta + \gamma) = \alpha + \overline{b_n + c_n} = \overline{a_n + b_n + c_n}$.

Az összeadás kommutatív. Nyilván $\alpha + \beta = \overline{a_n + b_n} = \overline{b_n + a_n} = \beta + \alpha$. Neutrális elem, ellentett. Nyilván a konstans 0 sorozat osztálya (azaz a nullsorozatok halmaza) neutrális elem, és $-\alpha = \overline{-a_n}$.

A szorzás asszociatív. Nyilván $(\alpha\beta)\gamma = \overline{a_n b_n} \gamma = \overline{a_n b_n c_n}$ és $\alpha(\beta\gamma) = \alpha \overline{b_n c_n} = \overline{a_n b_n c_n}$.

A szorzás kommutatív. Nyilván $\alpha\beta = \overline{a_n b_n} = \overline{b_n a_n} = \beta\alpha$.

Neutrális elem, inverz. Nyilván a konstans 1 sorozat osztálya (azaz az 1-hez konvergáló sorozatok halmaza) neutrális elem. Legyen α nemnulla elem, azaz nem a nullsorozatok halmaza. Be kell látni, hogy van olyan sorozat az α halmazban, amelynek egyik tagja sem 0. Valóban, vegyünk egy sorozatot az α halmazból. Nem lehet végtelen sok tagja 0, mivel azonnal látjuk, hogy ekkor, Cauchy sorozat lévén, konvergálna a 0-hoz. Így csak véges sok tagja 0, ezek mindegyike a sorozat N -nél kisebbik indexű tagja. Ekkor az az a_n sorozat, amelyik első N tagja 1, a többi megegyezik az eredeti sorozattal, eleme az α osztálynak, és egyik tagja sem 0. Nyilván $\frac{1}{a_n}$ is Cauchy-sorozat, és $\frac{1}{\alpha} = \overline{\frac{1}{a_n}}$ a keresett reciprok.

Q.E.D. A disztributivitás belátása nem nehéz.

Fogalmak: A $\mathbb{R}$ testet a **valós számok testének**, elemeit **valós számoknak** nevezzük. Azonosíthatjuk a racionális konstans sorozatok osztályait és a racionális számokat, így tekinthetjük úgy, hogy $\mathbb{Q} \subseteq \mathbb{R}$, és a

teste, rendezés,
zárt interv.

valós számok közötti összeadás és szorzás a racionális számok közötti műveletének kiterjesztése. Minden valós szám valamely racionális sorozat határértéke, és minden valós Cauchy sorozat konvergens. A $\mathbb{Q}$ rendezése kiterjeszthető $\mathbb{R}$ **rendezés**évé: $\alpha, \beta \in \mathbb{R}$ esetén $\alpha \leq \beta$, ha létezik $a_n \in \alpha$, $b_n \in \beta$ sorozat, hogy $a_n \leq b_n$ minden n számra. Ha $a, b \in \mathbb{R}$, $a < b$, akkor az $[a, b] = \{r \in \mathbb{R} | a \leq r \leq b\}$ halmazt **zárt intervallumnak** nevezzük.

$\mathbb{R}$ RENDEZÉSE

- (i) $\mathbb{R}$ -en $\leq$ lineáris rendezés;
- (ii) ha $r, s, t \in \mathbb{R}$, $r \leq s$ és $u \in \mathbb{R}^+$, akkor $r + t \leq s + t$ és $ru \leq su$;
- (iii) ha $r, s \in \mathbb{R}^+$, $r < s$ akkor létezik $n \in \mathbb{N}$, hogy $s < nr$;
- (iv) ha a_n, b_n valós sorozatok, hogy minden $n \in \mathbb{N}$ -re $a_n < b_n$, $[a_n, b_n] \supset [a_{n+1}, b_{n+1}]$, $\lim_{n \rightarrow \infty} (b_n - a_n) = 0$, akkor a $\bigcap_{n=0}^{\infty} [a_n, b_n]$ halmaz egyelemű.

Szokás kalkulusban a valós számok Cantor-féle axiómarendszeréből kiindulni, ez nem más, mint hogy $\mathbb{R}$ test, $\mathbb{N} = \{n \in \mathbb{R} | n = 0, 1, \text{ vagy } n = 1 + 1 + \dots + 1 \text{ alakú}\}$, $\mathbb{R}$ -en adott $\leq$ lineáris rendezés amelyre teljesül (ii)-(iv).

1.2. Hálók, Boole algebrák

1.2.1. Hálóelméleti lapfogalmak

- | | | |
|---|---|---|
| <p>(1) Az $(A, \vee, \wedge)$ struktúra háló, ha $(A, \vee)$ és $(A, \wedge)$ félháló, és mindkét művelet abszorbtív a másikkra nézve.</p> <p>(2) A $\vee$ műveletet diszjunkciónak nevezzük.</p> | <p>(3) Az $(A, \vee, \wedge)$ struktúra disztributív háló, ha háló, és mindkét művelet disztributív a másikkra nézve.</p> <p>(4) A $\wedge$ műveletet konjunkciónak nevezzük.</p> | <p>Fogalmak:
háló,
disztributív háló,
diszjunkció,
konjunkció</p> |
|---|---|---|

A hálók és a rendezett struktúrák között szoros kapcsolat áll fenn. Legyen A rendezett halmaz a $\leq$ relációra nézve. Ha $a, b \in A$, és $\min\{a, b\}$ olyan elem, hogy $\min\{a, b\} \leq a$, $\min\{a, b\} \leq b$, és ha $c \leq a$, $c \leq b$ akkor $c \leq \min\{a, b\}$, akkor azt mondjuk, hogy $\min\{a, b\}$ az a és b elemek **minimuma**. Ha $a, b \in A$, és $\max\{a, b\}$ olyan elem, hogy

Fogalmak:
minimum,
maximum,
hálószerűen
rendezett

$a \leq \max\{a, b\}$, $b \leq \max\{a, b\}$, és ha $a \leq c$, $b \leq c$ akkor $\max\{a, b\} \leq c$, akkor azt mondjuk, hogy $\max\{a, b\}$ az a és b elemek **maximuma**. Azt mondjuk, hogy a A **hálószerűen rendezett halmaz**, ha bármely két elemnek létezik minimuma és maximuma.

RENDEZÉS ÉS HÁLÓ Ha $(A, \vee, \wedge)$ háló, akkor az $a \leq b$ ha $a \vee b = b$ relációval A hálószerűen rendezett halmaz. Megfordítva, ha A hálószerűen rendezett halmaz a $\leq$ relációra nézve, akkor az $(A, \max, \min)$ struktúra háló.

Bizonyítás. Hiszen, legyen $(A, \vee, \wedge)$ háló. Az idempotencia miatt $a \vee a = a$ és $a \leq a$ reláció reflexív. Ha $a \leq b$ és $b \leq a$ azaz $a \vee b = b$ és $b \vee a = a$ akkor a kommutativitás miatt $a = b$, és a $\leq$ reláció antiszimmetrikus. Ha $a \leq b$, $b \leq c$ azaz $a \vee b = b$ és $b \vee c = c$ akkor $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$ és $a \leq c$, a tranzitivitás is világos. Legyen $\max\{a, b\} = a \vee b$. Ekkor $a \vee \max\{a, b\} = a \vee (a \vee b) = (a \vee a) \vee b = a \vee b = \max\{a, b\}$, és $a \leq \max\{a, b\}$; hasonlóan $b \leq \max\{a, b\}$. Ha $a \leq c$ és $b \leq c$ azaz $a \vee c = c$ és $b \vee c = c$ akkor $\max\{a, b\} \vee c = (a \vee b) \vee c = a \vee (b \vee c) = a \vee c = c$ és $\max\{a, b\} \leq c$, a maximalitás teljesül. Hasonlóan kapjuk, hogy $a \wedge b$ minimum.

Megfordítva, legyen A hálószerűen rendezett halmaz. Az $(A, \min)$ pár nyilván algebrai struktúra.

Asszociativitás. Legyen $u = \min\{\min\{a, b\}, c\}$ és $v = \min\{a, \min\{b, c\}\}$. Ekkor $u \leq \min\{a, b\}$ és $u \leq c$, ahonnan $u \leq a$, $u \leq b$ és $u \leq c$. Innen $u \leq a$ és $u \leq \min\{b, c\}$, adódik, hogy $u \leq v$. Analóg módon $v \leq u$, és az antiszimmetria miatt $u = v$.

Kommutativitás, idempotencia. Ezek a tulajdonságok nyilvánvalóak a művelet definíciójából.

Az $(A, \min)$ pár valóban félháló. Hasonlóan kapjuk, hogy az $(A, \max)$ pár is félháló.

A két abszorbtív tulajdonságból csak az egyiket tekintjük. a másik hasonlóan kapható. Legyen $c = \min\{a, \max\{a, b\}\}$. Ekkor nyilván $c \leq a$. Továbbá $a \leq a$ és $a \leq \max\{a, b\}$ miatt $a \leq \min\{a, \max\{a, b\}\} = c$, így az antiszimmetriából adódik, hogy $a = c$.

Q.E.D.

Legyen 0 illetve 1 az $(A, \vee, \wedge)$ háló eleme úgy, hogy minden $a \in A$ elemre $0 \vee a = a$ illetve $1 \wedge a = a$. Ekkor 0 -t a **háló zéruselemének** illetve 1 -et a **háló egységelemének** nevezzük. Könnyen látható, hogy az indukált rendezésre nézve a 0 a legkisebb, 1 a legnagyobb elem. Ha $a, \bar{a} \in A$ olyan elemek, hogy $a \vee \bar{a} = 1$ és $a \wedge \bar{a} = 0$ akkor azt mondjuk, hogy $\bar{a}$ az a elem **komplementuma**. **Boole-algebrának** nevezzük az olyan disztributív hálót, amelyben létezik zéruselem és egységelem, és minden elemnek van komplementuma. Minimális Boole-algebra az igaz és hamis logikai értékek **2** halmaza a „vagy” és az „és” műveletekkel.

Fogalmak:
zéruselem
hálóé,
egységelem,
hálóé
komplementum,
Boole-algebra

Boole-algebra a, b elemeire $\overline{a \vee b} = \bar{a} \wedge \bar{b}$ és $\overline{a \wedge b} = \bar{a} \vee \bar{b}$.

Hiszen,

$$(a \vee b) \vee (\bar{a} \wedge \bar{b}) = a \vee (b \vee \bar{a} \wedge \bar{b}) = a \vee ((b \vee \bar{a}) \wedge (b \vee \bar{b}))$$

$$= a \vee ((b \vee \bar{a}) \wedge 1) = a \vee (b \vee \bar{a}) = (a \vee \bar{a}) \vee b =$$

$1 \vee b = 1$, illetve

$$(a \vee b) \wedge (\bar{a} \wedge \bar{b}) = ((a \vee b) \wedge \bar{a}) \wedge \bar{b} = ((a \wedge \bar{a}) \vee (b \wedge \bar{a})) \wedge \bar{b} =$$

$$(0 \vee (b \wedge \bar{a})) \wedge \bar{b} = (b \wedge \bar{a}) \wedge \bar{b} = (b \wedge \bar{b}) \wedge \bar{a} = 0 \wedge \bar{a} = 0.$$

Innen következik az első De Morgan-törvény, a másik hasonlóan mutatható meg.

Legyen H egy halmaz, $\emptyset \neq T \subseteq \mathcal{P}(H)$ zárt az unió és metszet műveletekre. A $(T, \cup, \cap)$ algebrai struktúrát **halmaztest**nek nevezzük, ha zárt a komplementer képzésére nézve is. .

A $(T, \cup, \cap)$ halmaztest Boole-algebra.

Hiszen, h'arom halmaz uniójának (metszetének) elemei, akárhogyan zárójellezve, azok az elemek, amelyek legalább az egyik (mindhárom) halmazban benne vannak, így az unió- (metszet) képzés asszociatív. Két halmaz uniójának (metszetének) elemei, bármilyen sorrendben, azok az elemek, amelyek legalább az egyik (mindkét) halmazban benne vannak, így az unió- (metszet) képzés kommutatív. Egy halmaznak önmagával vett uniójának (metszetének) elemei nyilván a halmaz elemei, így az unió- (metszet) képzés idempotens. A $(T, \cup)$ $(T, \cap)$ struktúra félháló.

A két abszorbtív tulajdonságból az egyiket tekintjük, a másik ellenőrzése analóg. Legyen $a \in A \cup (A \cap B)$. Ekkor $a \in A$ vagy $a \in A \cap B$, de $A \cap B$ részhalmaza A -nak, így mindenképpen $a \in A$, azaz $A \cup (A \cap B) \subseteq A$. A fordított $A \subseteq A \cup (A \cap B)$ tartalmazás nyilvánvaló, és $A = A \cup (A \cap B)$. Eddig beláttuk, hogy $(T, \cup, \cap)$ háló.

A két disztributivitásból csak az egyiket látjuk be, a másik analóg. Legyen $a \in A \cup (B \cap C)$. Ekkor $a \in A$ vagy $a \in B \cap C$. Innen világos, hogy az a elem benne van az $A \cup B$ halmazban és az $A \cup C$ -ben is. Így $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Legyen most $a \in (A \cup B) \cap (A \cup C)$. Ekkor $a \in A \cup B$ és $a \in A \cup C$. Ha $a \in A$ akkor nyilván $a \in A \cup (B \cap C)$. Ha $a \notin A$ akkor szükségképpen $a \in B$ és $a \in C$ is teljesül, azaz $a \in B \cap C \subseteq A \cup (B \cap C)$. Így $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. A kétoldali tartalmazás miatt a két halmaz megegyezik. Az unió kommutativitása

DE MORGAN
TÖRVÉNYEK

Bizonyítás.

Q.E.D.

Fogalmak:
halmaztest

HALMAZTESTEK

Bizonyítás.

Q.E.D. miatt $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

Fogalmak: Nyilvánvaló, $\emptyset, H \in T$, $\emptyset$ a háló zéruselemee, H egységeleme.

atom Ennek a tételnek van megfordítása, először néhány fogalmat tekintünk, legyen $(A, \vee, \wedge)$, $(B, \vee, \wedge)$ Boole-algebra. $0 \neq a \in A$ elemet **atomnak** nevezünk, ha $b \leq a$ -ból $b = 0$ vagy $b = a$ következik. A $\varphi : A \rightarrow B$ leképezést **Boole-algebrák homomorfizmusának** nevezünk, ha bármely $a, b \in A$ -re $\varphi(a \vee b) = \varphi(a) \vee \varphi(b)$, $\varphi(a \wedge b) = \varphi(a) \wedge \varphi(b)$ és $\varphi(\bar{a}) = \overline{\varphi(a)}$. A bijektív homomorfizmust **izomorfizmus**ként említjük. A -t és B -t are **izomorf Boole algebrák**nak nevezzük, ha létezik közöttük izomorfizmus.

STONE-TÉTEL Boole-algebra izomorf valamely halmaztesttel.

VÉGES Véges Boole-algebra véges halmaz hatványhalmazával izomorf.

BOOLE-ALGEBRÁK Hiszen, legyen $(A, \vee, \wedge)$ Boole-algebra A véges halmaz, $\downarrow 0 = \emptyset$, ha $0 \neq x \in A$, $\downarrow x = \{a \in A \mid a \leq x, a \text{ atom}\}$. Ha $s = \bigvee \downarrow x$, lássuk be, **Bizonyítás.** hogy $x = s$. Világos, $s \leq x$. Tegyük fel, hogy $x \wedge \bar{s} = 0$. Ekkor

$$\begin{aligned} x \wedge s &= (x \wedge s) \vee (x \wedge \bar{s}) = x \wedge (s \vee (x \wedge \bar{s})) \\ &= x \wedge (x \vee s) = x, \end{aligned}$$

így $x \leq s$. Most tegyük fel, hogy $x \wedge \bar{s} \neq 0$. Mivel A véges, létezik $b \leq x \wedge \bar{s}$ atom. Mivel $b \leq \bar{s}$, $b \leq s$ az $b = 0$ ellentmondáshoz vezet. Következésképp $b \notin \downarrow x$, ami ellentmond $b \leq x$ -nak. Ezért $x \wedge \bar{s} = 0$ nem lehet és $s = x$.

Legyen $\varphi : A \rightarrow \mathcal{P}(\downarrow 1)$, $x \mapsto \downarrow x$. Az előzőekből világos, hogy ez bijekció. Csak azt kell még belátni, hogy a három Boole-művelet és φ elvégzésének sorrendje felcserélhető. Ha x vagy y 0 akkor $\downarrow (x \vee y) = \downarrow x \cup \downarrow y$ nyilvánvaló, $x \neq 0$ és $y \neq 0$ feltehető. Látjuk, hogy $\downarrow x \cup \downarrow y \subseteq \downarrow (x \vee y)$. Tegyük fel, hogy $a \leq x \vee y$ atom és $a \not\leq x$. Ekkor

$$a \wedge x = 0, \quad a = a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y) = a \wedge y$$

és ezért $a \leq y$ és a fordított $\downarrow (x \vee y) \subseteq \downarrow x \cup \downarrow y$ a tartalmazás is teljesül. Azaz, $\varphi(x \vee y) = \varphi(x) \cup \varphi(y)$. A másik két $\varphi(x \wedge y) = \varphi(x) \cap \varphi(y)$ és

Q.E.D. $\varphi(\bar{x}) = \overline{\varphi(x)}$ tulajdonság belátása sem nehéz.

A véges Boole-algebra rendje 2-hatvány, végtelen esetben vannak atommentes Boolean algebrák is.

1.2.2. Boole műveletek

Tekintsük az igazságértékek **2** Boole-algebráját a logikai diszjunkció (vagy) és konjunkció (és) műveletével. Legyen $x_1, x_2, \dots, x_n$ változók. A **minterm** $y_{i_1} \wedge y_{i_2} \wedge \dots \wedge y_{i_k}$ alakú kifejezés, ahol $y_{i_j} = x_{i_j}$ or $y_{i_j} = \overline{x_{i_j}}$ ($1 \leq i_j \leq n$). A **diszjunktív normálforma (d.n.f.)** $c_1 \vee c_2 \vee \dots \vee c_r$ alakú kifejezés, ahol a c_j -k mintermek. A **maxterm** $y_{i_1} \vee y_{i_2} \vee \dots \vee y_{i_k}$ alakú kifejezés, ahol $y_{i_j} = x_{i_j}$ vagy $y_{i_j} = \overline{x_{i_j}}$ ($1 \leq i_j \leq n$). A **konjunktív normálforma (k.n.f.)** $d_1 \wedge d_2 \wedge \dots \wedge d_r$ alakú kifejezés, ahol a d_j -k maxtermek. Egy $f : 2^n \rightarrow 2$ függvényt **n -ér Boole-művelet**nek nevezzük

Fogalmak:
minterm, d.n.f.,
maxterm,
k.n.f.,
Boole-művelet

Tetszőleges Boole-műveletnek van d.n.f.-je és k.n.f.-je.

Hiszen, legyen $f : 2^n \rightarrow 2$ Boole-művelet, $x_1, x_2, \dots, x_n$ Boole változók. Be kell látni, hogy létezik $c_1 \vee c_2 \vee \dots \vee c_r$ d.n.f.-je ($d_1 \wedge d_2 \wedge \dots \wedge d_r$ k.n.f.-je). hogy minden $(x_1, x_2, \dots, x_n) \in 2^n$, $f(x_1, x_2, \dots, x_n) = c_1 \vee c_2 \vee \dots \vee c_r$ ($f(x_1, x_2, \dots, x_n) = d_1 \wedge d_2 \wedge \dots \wedge d_r$).

Szerkesszük meg az f művelet Quine-táblázatát. Minden sor amelynek utolsó eleme 1 meghatároz egy c_j mintermet: x_i -t vagy $\overline{x_i}$ -t vegyünk bele a mintermbe annak megfelelően, hogy 1 vagy 0 van-e az i -dik oszlopban. Ezeknek a mintermeknek diszjunkcióját véve $f(x_1, x_2, \dots, x_n) = c_1 \vee c_2 \vee \dots \vee c_r$. Meghatározva a komplementert $\overline{f} = c_1 \vee c_2 \vee \dots \vee c_r$ d.n.f.-jét, majd mindkét oldalnak a komplementerét véve $f(x_1, x_2, \dots, x_n) = d_1 \wedge d_2 \wedge \dots \wedge d_r$, ami a k.n.f.

D.N.F. és
K.N.F D.N.F.
és K.N.F

Bizonyítás.

Q.E.D.

A két unér Boole művelet az identikus leképezés **1₂** vagy **puffer**, a komplementer vagy **negáció** $\neg$. További nevezetes Boole műveletek:

Fogalmak:
puffer, negáció,
or, and, xor,
nor, nand,
implikáció,
ekvivalencia,
klón,
függvényteljes

- | | |
|---|--|
| <p>(1) diszjunkció, or művelet $\vee$;</p> <p>(2) konjunkció, and művelet $\wedge$;</p> <p>(3) xor művelet $+$, értéke 1 pontosan akkor, ha pontosan egy argumentuma értéke 1;</p> <p>(4) nor művelet $\downarrow$, értéke 1 pontosan akkor, ha mindkét argumentuma értéke 0;</p> | <p>(5) nand művelet $$, értéke 1 pontosan akkor, ha legalább egy argumentuma értéke 0;</p> <p>(6) implikáció művelet $\supset$, értéke 0 pontosan akkor, ha első argumentuma értéke 1, a másodiké 0;</p> <p>(7) ekvivalencia művelet $\leftrightarrow$, értéke 1 pontosan akkor, ha két argumentuma értéke megegyező;</p> |
|---|--|

Boole műveletek egy halmazát **klón**nak nevezzük, ha tartalmazza

az összes $\pi_i : (x_1, x_2, \dots, x_n) \mapsto x_i$ projekciót és zárt a helyettesítésre. Boole műveletek egy M halmazát **függvényteljes**nek nevezzük, ha a B -t tartalmazó egyetlen klón az összes Boole művek halmaza.

FÜGGVÉNY
TELJESSÉG

A $\{\vee, \neg\}, \{\wedge, \neg\}, \{\mid\}, \{\downarrow\}$ halmazok függvényteljesek.

Bizonyítás.

Hiszen, a d.n.f. és k.n.f., illetve De Morgan tételek alapján $\{\vee, \neg\}$ és $\{\wedge, \neg\}$ függvényteljesek. Az első esetben alkalmazzuk a $a \wedge b = \overline{\overline{a} \vee \overline{b}}$ összefüggést hogy eltávolítsuk a d.n.f.-ben $\wedge$ összes előfordulását. A harmadik esetben alkalmazzuk a $\overline{a} = a \mid a$, $a \vee b = (a \mid a) \mid (b \mid b)$ és $a \wedge b = (a \mid b) \mid (a \mid b)$ összefüggéseket a d.n.f.-ben a $\vee, \wedge$ és $\neg$ összes előfordulását. A negyedik esetben alkalmazzuk az $\overline{a} = a \downarrow a$, $a \vee b = (a \downarrow b) \downarrow (a \downarrow b)$, $a \wedge b = (a \downarrow a) \downarrow (b \downarrow b)$ összefüggéseket a d.n.f.-ben a $\vee, \wedge$ and összes előfordulását.

Q.E.D.

Fogalmak:
karakterisztika,
Boole-gyűrű

Legyen $A, +, \cdot$ egységelemes gyűrű. Ha $n \in \mathbb{N}^+$ a legkisebb pozitív szám, hogy $\underbrace{1 + 1 + \dots + 1}_{n\text{-szer}} = 0$ teljesül, akkor azt mondjuk, hogy az

A gyűrű **karakterisztikája** n . Ha ez semmilyen $n \in \mathbb{N}^+$ -re sem teljesül, akkor azt mondjuk, hogy az A gyűrű **karakterisztikája** 0 (ilyen $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$). Az egységelemes gyűrűt, amelyben a multiplikatív struktúra félháló, **Boole-gyűrű**nek nevezzük.

BOOLE-GYŰRŰ

Legyen $(B, \vee, \wedge)$ Boole-algebra. Ekkor $(B, +, \wedge)$ Boole-gyűrű.

2. fejezet

Kombinatorika

2.1. Alapesetek

2.1.1. Rendezett kiválasztás, ismétlés nélkül

Legyen $\underline{k} = \{1, 2, \dots, k\}$, A egy n elemű halmaz. Az $l : \underline{k} \rightarrow A$ leképezést **k hosszú listának**, az $l(i)$ elemet a **lista i . tagjának**, ha l bijektív, l -et n elem **ismétlés nélküli permutációjának** nevezzük, az összes $l : \underline{n} \rightarrow A$ ismétlés nélküli permutáció halmazát $\mathcal{P}_n$ -nel jelöljük, legyen $P_n = |\mathcal{P}_n|$.

$$P_n = 1 \cdot 2 \cdot 3 \cdots n = n!$$

Hiszen, alkalmazzuk a skatulya módszert. $l(1)$ értékének kiválasztására n lehetőségünk van, $l(2)$ értékének kiválasztására $n - 1$, és í.t., $l(n)$ -re 1 lehetőségünk marad. A lehetőségek számait nyilván össze kell szorozni.

Fentebb alternatív definíciót adtunk n elem (ismétlés nélküli) permutációjára, nevezetesen mint $A \rightarrow A$ bijekció. Ha $1 \leq k \leq n$, akkor n elem k -adosztályú **ismétlés nélküli variációjának** nevezünk egy injektív $l : \underline{k} \rightarrow A$ listát. Aaz összes $l : \underline{k} \rightarrow A$ ismétlés nélküli variáció halmazát $\mathcal{V}_n^k$ -val jelöljük, legyen $V_n^k = |\mathcal{V}_n^k|$.

$$V_n^k = n - k + 1 \cdot n - k + 2 \cdot n - k + 3 \cdots n = \frac{n!}{(n-k)!}$$

Hiszen, ismét a skatulya módszerrel $l(1)$ értékének kiválasztására n lehetőségünk van, $l(2)$ értékének kiválasztására $n - 1$, és í.t., $l(k)$ -ra $n - k + 1$ lehetőségünk marad. A lehetőségek számait nyilván összeszorozva kapjuk V_n^k -t.

Fogalmak:
ismétlés nélküli
permutáció,
lista, lista i .
tagja, ismétlés
nélküli variáció

P_n ÉRTÉKE

Bizonyítás.

Q.E.D.

V_n^k ÉRTÉKE

Bizonyítás.

Q.E.D.

2.1.2. Rendezett kiválasztás, ismétléses

Fogalmak: Legyen $A = \{a_1, a_2, \dots, a_r\}$, $|A| = r$, $2 \leq r \leq n$. $0 \leq k : i \leq n$ ($i = 1, 2, \dots, r$), $k_1 + k_2 + \dots + k_r = n$. Az $l : \underline{n} \rightarrow A$ listát n elem $k_1, k_2, \dots, k_r$ osztályú **ismétléses permutáció**jának nevezzük ha a_i éppen k_i -szer tagja a listának ($i = 1, 2, \dots, r$). Az összes $l : \underline{n} \rightarrow A$ ismétléses permutáció halmazát $\mathcal{P}_n^{k_1, k_2, \dots, k_r}$ -rel jelöljük, legyen $P_n^{k_1, k_2, \dots, k_r} = |\mathcal{P}_n^{k_1, k_2, \dots, k_r}|$.

$P_n^{k_1, k_2, \dots, k_r}$ ÉRTÉKE
$$P_n^{k_1, k_2, \dots, k_r} = \frac{n!}{k_1! \cdot k_2! \cdot \dots \cdot k_r!}.$$

Bizonyítás. Hiszen, különböztessük meg a lista összes n elemét, ekkor ismétlés nélküli permutációkat kapunk, számuk $n!$. Mivel egy ismétléses permutációhoz $k_1! \cdot k_2! \cdot \dots \cdot k_r!$ számú ismétlés nélküli tartozik, és minden ismétlés nélkülit pontosan egyszer kapunk meg így, a formula teljesül.

Q.E.D. Most legyen k , $n \in \mathbb{N}^+$. n elem k -adosztályú **ismétléses variáció**jának nevezzük egy $l : \underline{k} \rightarrow A$ listát. Aaz összes $l : \underline{k} \rightarrow A$ ismétléses variáció halmazát $\mathcal{V}_n^{k,i}$ -val jelöljük, legyen $V_n^{k,i} = |\mathcal{V}_n^{k,i}|$.

$V_n^{k,i}$ ÉRTÉKE
$$V_n^{k,i} = n^k.$$

Bizonyítás. Ismét a skatulya módszerrel $l(i)$ értékének kiválasztására n lehetőségünk van ($1 \leq i \leq k$), a lehetőségek számai nyilván összeszorozandók.

Q.E.D.

2.1.3. Rendezetlen kiválasztás, ismétlés nélküli

Fogalmak: Legyen $A = \{a_1, a_2, \dots, a_n\}$, $n \in \mathbb{N}^+$, $0 \leq k \leq n$. n elem k -adosztályú **ismétlés nélküli kombináció**jának nevezzük egy $m : A \rightarrow \{0, 1\}$ leképezést ha $\sum_{i=1}^n m(a_i) = k$. Aaz összes ilyen $m : \underline{k} \rightarrow A$ ismétlés nélküli kombináció halmazát $\mathcal{C}_n^k$ -val jelöljük, legyen $C_n^k = |\mathcal{C}_n^k|$.

C_n^k ÉRTÉKE
$$C_n^k = \frac{n!}{k!(n-k)!} = \binom{n}{k}.$$

Bizonyítás. Hiszen, $A = \underline{n}$ választással $\mathcal{C}_n^k$ elemei $\mathcal{P}_n^{k, n-k}$ elemeinek is tekinthetők.

Q.E.D.

Az $\binom{n}{k}$ számokat **binomiális együtthatók**nak hívjuk (ha nem $0 \leq k \leq n$, akkor legyen $\binom{n}{k} = 0$). Alternatív definíció az $\binom{n}{k}$ számokra: n elemű halmaz k elemű részhalmazainak száma. Ha $B \subseteq A$, $|B| = k$, akkor ennek **karakterisztikus (tagsági) függvénye** $m : A \rightarrow \{0, 1\}$, $m(a) = 1$ pontosan akkor, ha $a \in B$, visszaadja az eredeti szemléletet. Megegyezés: $a^0 = 1$.

BINOMIÁLIS
EGYÜTTHATÓK
TULAJDONSÁGAI

Legyen $n, k \in \mathbb{N}$, $k \leq n$.

Bizonyítás. Hiszen, (i) nyilvánvaló a definícióból. (ii)-ben

$$j.o. = \frac{(n-1)!}{(k-1)!(n-k)!} + \frac{(n-1)!}{k!(n-k-1)!} = \frac{(n-1)!}{k!(n-k)!} (k + n - k) = b.o.$$

- (i) $\binom{n}{k} = \binom{n}{n-k}$;
- (ii) ha $n, k \geq 1$, $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$; (v) $\sum_{k=0}^n (-1)^k \binom{n}{k} = 2^n$;
- (iii) (binomiális tétel) ha a, b gyűrűbeli elemek, $ab = ba$ akkor $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$; (vi) ha $k \leq m \leq n$, $\binom{n}{m} \binom{m}{k} = \binom{n}{k} \binom{n-k}{m-k}$;
- (vii) ha $m, r \in \mathbb{N}$, $k \leq r \leq n$, $k \leq m$, $\sum_{k=0}^r \binom{m}{k} \binom{n}{r-k} = \binom{m+r}{r}$.
- (iv) $\sum_{k=0}^n \binom{n}{k} = 2^n$;

(iii)-at abból láthatjuk, hogy az $a^k b^{n-k}$ tagot akkor kapjuk, ha a baloldali szorzatban k -szor a -t, $n-k$ -szor b -t választjuk. ezt $\binom{n}{k}$ féleképpen tehetjük meg. (iv)-e és (v)-öt megkapjuk (iii)-ból az $a = 1$, $b = 1$ illetve az $a = 1$, $b = -1$ helyettesítéssel. (vi) baloldala azt adja, hogy n emberből m tagú bizottságot, majd k tagú albizottságot választunk, a jobboldali ugyanezt, de úgy, hogy először a k tagú albizottságot választjuk ki, majd a maradék $n-k$ emberből a hiányzó $m-k$ bizottsági tagot. (vii) A jobboldal m férfiből és n nőből álló r tagú bizottságok számát adja. A baloldal ugyanezt, de k tagú férfi és $r-k$ tagú női bizottságokra lebontva.

Q.E.D.

Legyenek az A egységelemes gyűrű egymással felcserélhető elemei $a_1, a_2, \dots, a_r$, $r, n \in \mathbb{N}$, $r, n > 1$. Ekkor

POLINOMIÁLIS
TÉTEL

$$(a_1 + a_2 + \dots + a_r)^n = \sum_{\substack{\rightarrow \\ 0 \leq k_i \leq n \\ k_1 + k_2 + \dots + k_r = n}} \frac{n!}{k_1! k_2! \dots k_r!} a_1^{k_1} a_2^{k_2} \dots a_r^{k_r}.$$

Hiszen, a baloldali szorzás elvégzésekor a $a_1^{k_1} a_2^{k_2} \dots a_r^{k_r}$ tagot akkor kapjuk, ha k_1 -szer a_1 -et, k_2 -szer a_2 -t, és í. t., k_r -szer a_r -et választjuk, ezt nyilván $P_n^{k_1, k_2, \dots, k_r} = \frac{n!}{k_1! k_2! \dots k_r!}$ féleképpen tehetjük meg.

Bizonyítás.

Q.E.D.

2.1.4. Rendezetlen kiválasztás, ismétléssel

Legyen $A = \{a_1, a_2, \dots, a_n\}$, $|A| = n$, $k \in \mathbb{N}$. Az $m : A \rightarrow \{0, 1, \dots, k\}$ leképezést n elem k -ad osztályú **ismétléses kombinációj**ának nevezzük ha $\sum_{i=1}^n m(a_i) = k$. Szokás még m -t tagsági függvénynek is mondani, ami megmondja hogy az adott táskában, **multihalmaz**ban

Fogalmak:
ismétléses
kombináció,
multihalmaz

az a_i elem hányszor szerepel. Az összes $m : A \rightarrow \{0, 1, \dots, k\}$ k -adosztályú ismétléses permutáció halmazát $\mathcal{C}_n^{k,i}$ -vel jelöljük, legyen

$$C_n^{k,i} = |\mathcal{C}_n^{k,i}|.$$

$$C_n^{k,i} = \binom{n+k-1}{k}.$$

Bizonyítás.

Hiszen, legyen $A = \underline{n}$, $m \in \mathcal{C}_n^{k,i}$. Tekintsük m -et multihalmaznak, elemei $i_0 \leq i_1 \leq \dots \leq i_{k-1} \in \underline{n}$. Legyen $\widetilde{m}(i_j + j) = 1$ ($0 \leq j \leq k-1$), egyébként $\widetilde{m}(l) = 0$ ($0 \leq l \leq n+k-1$). Kaptuk, hogy $\widetilde{m} \in \mathcal{C}_{n+k-1}^k$. Nyilván bijekciót határoztunk meg a $\mathcal{C}_n^{k,i}$ és $\mathcal{C}_{n+k-1}^k$ halmazok között.

Q.E.D.
 $x_1 + x_2 + \dots +$
 $x_n = k$

MEGOLDÁSAI

Bizonyítás.

Az $x_1 + x_2 + \dots + x_n = k$ egyenlet $\mathbb{N}$ -beli megoldásainak száma $C_n^{k,i}$. Hiszen, gondoljunk arra, hogy a táskánkba n féle gyümölcsből $A = \underline{n}$ kell összesen k darabot vásárolnunk a piacon, az i -edik fajtából $x_i = m(i)$ darabot. Ekkor $m : A \rightarrow \{0, 1, \dots, k\} \in \mathcal{C}_n^{k,i}$. Bijekciót határoztunk meg az egyenlet megoldásai és n elem k -ad osztályú ismétléses kombinációi között.

Q.E.D.

2.1.5. Szita formula

SZITA
FORMULA

Legyen $\emptyset \neq A$ véges halmaz, $\emptyset \neq A_i \subseteq A$ ($i = 1, 2, \dots, r$). Ekkor

$$\begin{aligned} |\overline{A_1 \cup A_2 \cup \dots \cup A_r}| &= |A| - (|A_1| + |A_2| + \dots + |A_r|) + \\ &+ (|A_1 \cap A_2| + |A_1 \cap A_3| + \dots + |A_{r-1} \cap A_r|) - \dots + \dots \\ &+ (-1)^k \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq r} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}| + \dots - \dots + \\ &(-1)^r |A_1 \cap A_2 \cap \dots \cap A_r|. \end{aligned}$$

Bizonyítás.

Hiszen, érveljünk indukció alapján. Az $r = 2$ esetben a nyilvánvaló $|\overline{A_1 \cup A_2}| = |A| - (|A_1| + |A_2|) + |A_1 \cap A_2|$ összefüggést adja a formula. Jelölje a_r a formula jobb oldalának az értékét. Tegyük fel, hogy a formula teljesül $r-1$ -re. Látjuk, hogy $a_{r-1} - a_n =$

$$\begin{aligned} |A_r| - (|A_1 \cap A_r| + |A_2 \cap A_r| + \dots + |A_{r-1} \cap A_r|) + \dots - \dots + \\ (-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \dots < i_{k-1} \leq r-1} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_{k-1}} \cap A_r| + \dots - \\ \dots + (-1)^{n-1} |A_1 \cap A_2 \cap \dots \cap A_r|. \end{aligned}$$

Alkalmazva a formulát az $A = A_r$ halmazra és az $A_i \cap A_r$ részhalmazaira ($i = 1, 2, \dots, r-1$) kapjuk, hogy $a_{r-1} - a_r$ a $B = A_r \setminus (A_1 \cup A_2 \cup \dots \cup A_{r-1})$ halmaz elemeinek a száma. Világos, hogy az $\overline{A_1 \cup A_2 \cup \dots \cup A_{r-1}}$ halmaz az $\overline{A_1 \cup A_2 \cup \dots \cup A_r}$ és a B halmazok diszjunkt uniója, és

Q.E.D. emiatt $a_{r-1} = |\overline{A_1 \cup A_2 \cup \dots \cup A_r}| + a_{r-1} - a_r.$

2.2. Alkalmazások

2.2.1. Euler-féle φ -függvény

Legyen $\varphi : \mathbb{N}^+ \rightarrow \mathbb{R}$ Euler-féle φ -függvény a következő: $\varphi(1) = 1$, ha $m > 1$, $m = p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$ (a p_i -k különböző prímszámok, $k_i \in \mathbb{N}^+$) legyen $\varphi(m)$ az $A = \{0, 1, \dots, m-1\}$ halmazban az m -hez relatív prímek száma.

Ha $m > 1$, akkor $\varphi(m) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \cdots (p_n^{k_n} - p_n^{k_n-1})$.

Hiszen, legyen A_i az A halmazban a p_i prímszám többszöröseinek a halmaza. Ekkor a szita-formula szerint $\varphi(m) = |\overline{A_1 \cup A_2 \cup \cdots \cup A_n}| =$

$$\begin{aligned} & m - \left(\frac{m}{p_1} + \frac{m}{p_2} \cdots \frac{m}{p_n} \right) + \left(\frac{m}{p_1 p_2} + \frac{m}{p_1 p_3} \cdots \frac{m}{p_{n-1} p_n} \right) + \cdots - \cdots + \\ & (-1)^k \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \frac{m}{p_{i_1} p_{i_2} \cdots p_{i_k}} + \cdots - \cdots + (-1)^n \frac{m}{p_1 p_2 \cdots p_n} \\ & = \frac{m}{p_1 p_2 \cdots p_n} (p_1 - 1)(p_2 - 1) \cdots (p_n - 1) = j.o. \end{aligned}$$

Fogalmak: ,
Euler-féle φ ,
átrendezés

φ
KISZÁMÍTÁSA
Bizonyítás.

Q.E.D.

2.2.2. Átrendezések

Legyen $|A| = n \in \mathbb{N}^+$. A egy átrendezés olyan $A \rightarrow A$ permutáció, amely egyetlen elemet sem fixál. Legyen $\mathcal{D}_n$ A összes átrendezésének halmaza, $D_n = |\mathcal{D}_n|$. Megegyezés: $0! = 1$.

$$D_n = n! \sum_{i=0}^n (-1)^i \frac{1}{i!}.$$

Hiszen, legyen $A = \underline{n}$, $B_i = \{\sigma \in S_n | \sigma(i) = i\}$ ($i \in \underline{n}$). Nyilván $|B_{i_1} \cap B_{i_2} \cap \cdots \cap B_{i_k}| = (n-k)!$, az $1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n$ k-asra $\binom{n}{k}$ lehetőség van, $(n-k)! \binom{n}{k} = \frac{n!}{k!}$, alkalmazzuk a szita-formulát!

ÁTRENDEZÉSEK
SZÁMA

Bizonyítás.

Q.E.D.

2.2.3. Színezések

Legyen A , $|A| = n$, a színezendő objektumok (pl. csúcspontok, élek, oldalak), $C = \{c_1, c_2, \dots, c_m\}$ a színek halmaza, G $A \rightarrow A$ permutációk csoportja (szimmetriák csoportja). Az $s : A \rightarrow C$ leképezést az A egy színezésének vagy mintázatának nevezzük, az összes ilyen mintázat halmaza legyen S . A $g \in G$ permutáció indukál egy $\tilde{g} : S \rightarrow S$ leképezést, $\tilde{g}(s)(a) = s(g(a))$. Azt mondjuk, hogy az r, s mintázatok G -kongruensek, ha létezik $g \in G$, hogy $\tilde{g}(r) = s$, jelölés: $(r, s) \in \kappa_G$.

Fogalmak:
színezés v.
mintázat,
 G -kongruens

A G -
KONGRUENCIÁRÓL

$\kappa_G \subseteq S \times S$ ekvivalencia reláció.

Bizonyítás.

Hiszen, a reflexivitás nyilvánvaló, mivel $\widetilde{1}_A(r) = r$ minden $r \in S$ -re. Ha $(r, s) \in \kappa_G$ akkor valamely $g \in G$ -re $r(g(a)) = s(a)$ minden $a \in A$ -ra, de ekkor $s(g^{-1}(a)) = r(a)$ és $(s, r) \in \kappa_G$, kaptuk a szimmetriát. A tranzitivitáshoz legyen $(r, s), (s, t) \in \kappa_G$, valamely $g, h \in G$ -re $r(g(a)) = s(a)$ és $s(h(a)) = t(a)$ minden $a \in A$ -ra. Következésképp $r(gh(a)) = s(h(a)) = t(a)$ minden $a \in A$ -ra és $(r, t) \in \kappa_G$.

Q.E.D.

BURNSIDE-
LEMMA

Ha $f : H \rightarrow H$, akkor legyen $\psi(f) = \{h \in H \mid f(h) = h\}$.

$$|S/\kappa_G| = \frac{1}{|G|} \sum_{g \in G} |\psi(\tilde{g})|$$

Fogalmak:
ciklikus csoport

A $(G, \cdot)$ csoportról azt mondjuk, hogy a $g \in G$ által generált **ciklikus csoport**, ha G minden eleme g egész kitevős hatványa. Legyen $A = \{b_1, b_2, \dots, b_6\}$ nyakláncba kötendő gyöngyszemek halmaza, $C = \{f, p, k\}$ a színek halmaza, fehér, piros és kék. Két nyakláncot azonosnak tekintünk, ha az egyik nyakláncot alkalmasan elforgatva a gyöngyök színsorrendje ugyanaz lesz, azaz $G = \langle (123456) \rangle$, a $g = (123456)$ permutáció által generált ciklikus csoport, elemei a hatványok, azaz $g^2 = (135)(246)$, $g^3 = (14)(25)(36)$, $g^4 = (153)(264)$, $g^5 = (165432)$. $|S| = 3^6$,

$$|S/\kappa_G| = \frac{1}{|G|} \sum_{g \in G} |\psi(\tilde{g})| = \frac{1}{6} (3^6 + 3 + 9 + 27 + 9 + 3) = 780/6 = 130.$$

Legyen most $A = \{P_1, P_2, P_3, P_4\}$ adott négyzet csúcspontjainak halmaza, $C = \{f, p, k\}$ a színek halmaza. Két mintázatot azonosnak tekintünk, ha az egyik színezést alkalmasan mozgatva, tükrözve a színezés ugyanaz lesz, azaz $G = \langle a, b \rangle$ a négyzet szimmetriacsoportja, ahol a a 90° -os elforgatás és b a P_1P_2 szakasz felezőpontján átmenő szimmetriatengelyre történő tükrözés, G -t szokás 8-adrendű diédercsoportnak hívni és D_4 -gyel jelölni. Ezeket most a csúcspontok permutációinak tekintjük, G nemidentikus elemei $a = (1234)$, $a^2 = (13)(24)$, $a^3 = (1432)$ az elforgatások, $b = (12)(34)$, $ab = (13)$, $a^2b = (14)(23)$, $a^3b = (24)$ a tükrözések. $|S| = 3^4$,

$$|S/\kappa_G| = \frac{1}{|G|} \sum_{g \in G} |\psi(\tilde{g})| = \frac{1}{8} (3^4 + 3 + 9 + 3 + 9 + 27 + 9 + 27) = 168/8 = 21.$$

Látjuk, hogy $\psi(\tilde{g}) = m^w$, ahol w g (esetleg triviális) pályáinak száma.

Fogalmak:
egysoros alak
típusa,
permutáció
típuselőállítása,
ciklusindex

$g \in G$ **egysoros alakjának típusa** $(k_1, k_2, \dots, k_n)$, ha az egysoros alakban l hosszú ciklusból k_l darab van, nyilván $\sum_{l=1}^n k_l l = n$. A $g \in G$ **permutáció típuselőállítása** $Z_g(x_1, x_2, \dots, x_n) = x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$. A G csoport ciklusindexe $Z_G(x_1, x_2, \dots, x_n) = \frac{1}{|G|} \sum_{g \in G} Z_g(x_1, x_2, \dots, x_n)$.

$$|S/\kappa_G| = Z_G(m, m, \dots, m)$$

Ha $G = \langle (123456) \rangle$ akkor $Z_G(x_1, x_2, \dots, x_n) = \frac{1}{6}(x_1^6 + x_2^3 + 2x_3^2 + 2x_6)$
és $Z_G(3, 3, \dots, 3) = \frac{1}{6}(3^6 + 27 + 18 + 6) = 130$.

A mintázat leltár olyan

$$P_G(c_1, c_2, \dots, c_m) = \sum_{k_1 + \dots + k_m = n} d_{k_1, k_2, \dots, k_m} c_1^{k_1} c_2^{k_2} \dots c_m^{k_m}$$

polinom, hogy $d_{k_1, k_2, \dots, k_m}$ az összes olyan G-inkongruens mintázatok száma, amelyekben a c_i színből k_i darab van.

$$P_G(c_1, c_2, \dots, c_m) = Z_G(\sum_{i=1}^m c_i, \sum_{i=1}^m c_i^2, \dots, \sum_{i=1}^m c_i^n).$$

A 6 szemes nyaklánc példájánál

$$P_G(f, p, k) = (f^6 + \dots) + (f^5 p + \dots) + 3(f^4 p^2 + \dots) + 10(f^4 p k + \dots) \\ + 4(f^3 p^3 + \dots) + 10(f^3 p^2 k + \dots) + 16 f^2 p^2 k^2,$$

azaz 3 fehér, 2 piros és 1 kék gyöngyből 10 különböző nyaklánc fűzhető.

SZÍNEZÉSI
BURNSIDE
LEMMA

Fogalmak:
mintázat leltár

PÓLYA-
REDFELD

3. fejezet

Elemi számelmélet és polinomelmélet

3.1. Oszthatóság az egész számok körében

3.1.1. Oszthatósági alapfogalmak

Fogalmak: Azt mondjuk, hogy az a egész szám osztja a b egész számot, ha létezik c egész szám, hogy $b = ac$, jelölés: $a|b$. Azt mondjuk, hogy a b egész szám az a egész szám asszociáltja, ha $b = ac$, ahol c egység, azaz 1 vagy -1 ; jelölés: $a \sim b$. Az asszociáltság ekvivalenciareláció, oszthatósági szempontból asszociáltak között különbséget tenni nem tudunk.

Legyen $a, b, c, d \in \mathbb{Z}$.

OSZTHATÓSÁGI
TULAJDONSÁGOK

- (i) $a|a$;
- (ii) ha $a|b$ és $b|a$ akkor $a \sim b$;
- (iii) ha $a|b$ és $b|c$ akkor $a|c$;
- (iv) ha $a|b$ és $a|c$ akkor $a|bu + cv$ ($u, v \in \mathbb{Z}$);
- (v) ha $a|c$ és $b|d$ akkor $ab|cd$;

Bizonyítás. Hiszen, $a = a1$ (i) -et adja. Ha $b = as$ és $c = bt$, ahol $s, t \in \mathbb{Z}$, akkor $c = (as)t = a(st)$, és $a|c$, (ii) teljesül. Ha $b = as$ és $a = bt$, ahol $s, t \in \mathbb{Z}$, akkor $b = bts$. Ha $b = 0$, akkor $a = bt = 0t = 0$; ha $b \neq 0$ akkor $b(1 - ts) = 0$ és a zérusosztómentesség miatt $ts = 1$, azaz t és s egységek, $a \sim b$, (iii) teljesül. Ha $b = as$ és $c = at$, ahol $s, t \in \mathbb{Z}$, akkor $bu + cv = asu + atv = a(su + tv)$ és $a|bu + cv$, ami (iv)-et adja. Végül, *Q.E.D.* $c = as$ és $d = bt$, ahol $s, t \in \mathbb{Z}$, akkor $cd = asbt = ab(st)$ és $ab|cd$.

A fentiek tetszőleges integritástartományban igazak analóg bizonyítással. Az első három állítás azt jelenti, hogy az oszthatóság rendezési reláció az asszociáltsági osztályok halmazán; az egészek esetén a természetes számok halmazán.

Az $a, b \in \mathbb{Z} \setminus \{0\}$ -hoz egyértelműen létezik $q, r \in \mathbb{Z}$ hogy $b = aq + r$ és $0 \leq r < |a|$.

MARADÉKOS
OSZTÁS

Hiszen, legyen $a\mathbb{Z} = \{ai | i \in \mathbb{Z}\}$. A rendezés linearitása miatt vagy $b \in a\mathbb{Z}$ és akkor $b = aq + 0$ a keresett előállítás, vagy $aq < b < a(q+1)$ és $0 \leq r = b - aq < |a|$. Az egzisztencia világos. Az unicitáshoz vegyük észre, hogy az aq többszörösénél kisebb aq' értékekre $b - aq' > |a|$, és nagyobb aq' értékekre $b - aq' < 0$.

Bizonyítás.

Q.E.D.

ALGORITMUS:
MARADÉKOS
OSZTÁS

```
mo:=function(a,b) 1
  local r, q; integer a,b;
  if a =0 or b=0 then return("hiba"); else
    if a>0 and b>0 then q=int(b/a); fi;
    if a>0 and b<0 then q=-(int(abs(b)/a))-1; fi;
    if a<0 and b>0 then q=-(int(b/abs(a))); fi;
    if a<0 and b<0 then q=int(abs(b)/abs(a))+1; fi;
  return([q,b-a*q]);fi; end;
```

Algoritmusokat szokás pszeudokóddal megadni, átírásuk bármelyik kedvenc programnyelvre egyszerű. A maradékos osztás tételében szereplő a számot **osztónak**, a b számot **osztandónak**, a q számot **hányadosnak**, az r számot **maradéknak** nevezzük.

Fogalmak:
osztó, osztandó,
hányados,
maradék

```
eu:=function(a,b)
  local q=[],r=[], i=2; integer a,b;
  if a =0 or b=0 then return("hiba"); else
    append(q,mo(a,b)[1]); append(r,mo(a,b)[2]);
    if r[1]=0 then return(q,r); else
      append(q,mo(r[1],a)[1]); append(r,mo(r[1],a)[2]);
      while r[i]>0 do
        append(q,mo(r[i],r[i-1])[1]);
        append(r,mo(r[i],r[i-1])[2]); i=i+1;
      od; return([q,r]); fi; fi;end;
```

ALGORITMUS:
EUKLIDESZI

¹Az algoritmusok ellenőrzése a [9] programcsomaggal történt

Az euklideszi algoritmus maradékos osztások sorozata, az új osztás a régi osztót osztja a régi maradékkal.

$$b = aq_1 + r_1, \quad 0 < r_1 < |a|$$

$$a = r_1q_2 + r_2, \quad 0 < r_2 < r_1$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_2$$

.....

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2}$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 = r_n < r_{n-1}.$$

Fogalmak: Ha $a, b \in \mathbb{Z} \setminus \{0\}$, akkor **legnagyobb közös osztójuknak** nevezzük azt a $d = (a, b) \in \mathbb{N}$ számot, amelyre teljesül, hogy $d|a$ és $d|b$, és ha $c \in \mathbb{Z}$ -re $c|a$ és $c|b$, akkor $c|d$.

L.N.K.O. LÉTEZÉSE Ha $a, b \in \mathbb{Z} \setminus \{0\}$, akkor egyértelműen létezik (a, b) legnagyobb közös osztójuk, a rajtuk végrehajtott euklideszi algoritmus utolsó nemnulla maradéka.

KIBŐVÍTETT EUKLIDESZI ALGORITMUS Ha $a, b \in \mathbb{Z} \setminus \{0\}$, akkor létezik $u, v \in \mathbb{Z}$, hogy $(a, b) = au + bv$.

```
eux:=function(a,b)
  local q, m[2,3],u,v;integer a,b;
  if a=0 or b=0 then return("hiba"); else
    m=[[1,0,a],[0,1,b]];
    while m[1,3]<>0 and m[2,3]<>0 do
      if abs(m[1,3])>=abs(m[2,3]) then
        q=mo(m[2,3],m[1,3])[1];
        for i=1 to 3 do m[1,i]=m[1,i]-q*m[2,i];od;
      else q=mo(m[1,3],m[2,3])[1];
        for i=1 to 3 do m[2,i]=m[2,i]-q*m[1,i];od;fi;od;
    if m[1,3]=0 then return([m[2,1],m[2,2],m[2,3]]);
    else return([m[1,1],m[1,2],m[1,3]]); fi;fi;end;
```

Azaz, az euklideszi algoritmust elvégzése során behelyettesítéseket alkalmazva minden lépésben kifejezzük a maradékot $r_i = au_i + bv_i$ alakban, az utolsó lépésben a legnagyobb közös osztóval egyenlő r_{n-1} -et fejezzük ki a keresett $(a, b) = au + bv$ alakban.

- Legyen $a, b, c \in \mathbb{N}^+$.
- (i) $(\mathbb{N}^+, (,))$ félháló;
- (ii) $(ac, bc) = (a, b)c$;
- (iii) $(a, b) = (a + bc, b)$;
- (iv) $(a, b) = a$ pontosan akkor, ha $a \mid b$;
- (v) ha $a \mid bc$ és $(a, b) = 1$ akkor $a \mid c$

L.N.K.O.
TULAJDONSÁGAI

Hiszen, a kommutativitás és az idempotencia nyilvánvaló. Az asszociativitás belátásához legyen $a, b, c \in \mathbb{N}^+$, $u = ((a, b), c)$, $v = (a, (b, c))$. Mivel $u \mid (a, b)$, és $u \mid c$, teljesül $u \mid a$, $u \mid b$ és c . Ezért $u \mid a$ és $u \mid (b, c)$, ahonnan $u \mid v$. Hasonlóan adódik, hogy $v \mid u$, kaptuk (i)-et.

(ii) Mivel $(a, b) \mid a$, $(a, b) \mid b$, látjuk, hogy $(a, b)c \mid ac$ és $(a, b)c \mid bc$, következésképp $(a, b)c \mid (ac, bc)$ azaz $(ac, bc) = (a, b)ct$ valamely $t \in \mathbb{N}^+$ -ra. Nyilván $(ac, bc)r = ac$ és $(ac, bc)s = bc$ valamely r, s természetes számokra, így $(a, b)ctr = ac$ és $(a, b)cts = bc$, ahonnan egyszerűsítés után $(a, b)tr = a$ és $(a, b)ts = b$ adódik. Ekkor az $(a, b)t \mid a$ és $(a, b)t \mid b$ közös osztó, így $(a, b)t \mid (a, b)$, ami csak akkor lehetséges, ha $t = 1$. A többi állítás belátása hasonló megfontolásokat igényel.

Bizonyítás.

Q.E.D.

A fenti tulajdonságok érvényben maradnak egész számokra is, ha a tulajdonságokban az egyenlőséget a $\sim$ relációra cseréljük ki. Azt mondjuk, hogy az $a, b \in \mathbb{Z} \setminus \{0\}$ **relatív prímek**, ha $(a, b) = 1$. Nyilvánvaló, hogy az $\frac{a}{(a,b)}$ és a $\frac{b}{(a,b)}$ számok relatív prímek. Azt mondjuk, hogy $a, b \in \mathbb{Z} \setminus \{0\}$ számok **legkisebb közös többszöröse** az $[a, b] = m \in \mathbb{N}$ szám, ha az $a \mid m$ és $b \mid m$, és ha a $a \mid c$ és $b \mid c$, akkor $m \mid c$.

Fogalmak:
relatív prímek,
l.k.k.t.

- (i) Ha $a, b \in \mathbb{Z} \setminus \{0\}$, akkor $m = \frac{ab}{(a,b)}$ szám az $[a, b]$ legkisebb közös többszörös;

- (ii) $(\mathbb{N}^+, [,])$ félháló;

- (iii) Tetszőleges $a, b, c \in \mathbb{N}^+$ -ra $[ac, bc] = [a, b]c$.

L.K.K.T.
TULAJDONSÁGAI

Hiszen, az $m = a \mid \frac{b}{(a,b)} = b \mid \frac{a}{(a,b)}$ szám közös többszörös. Legyen a $a \mid c$, $b \mid c$, azaz $c = as = bt$ valamely $s, t \in \mathbb{Z}$ -re. Ekkor az $\frac{a}{(a,b)} \mid \frac{b}{(a,b)}t$ számot, és, mivel az $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$, látjuk, hogy $\frac{a}{(a,b)} \mid t$, azaz $t = \frac{a}{(a,b)}u$ valamely $u \in \mathbb{Z}$ -re, ahonnan $c = b \frac{a}{(a,b)}u = \pm mu$ következik, azaz az $m \mid c$. Valóban, $m = [a, b]$, (i) világos. A másik két állítás belátása sem bonyolult.

Bizonyítás.

Q.E.D.

A (ii) és (iii) tulajdonságok érvényben maradnak $\mathbb{Z} \setminus \{0\}$ -n, ha a tulajdonságokban az egyenlőséget $\sim$ -re cseréljük. Belátható, hogy az l.n.k.o. és az l.k.k.t. kölcsönösen abszorbtívák és disztributívák.

L.K.K.T,
L.N.K.O. HÁLÓ

Az $(\mathbb{N} \setminus \{0\}, [,], (,))$ struktúra disztributív háló, az indukált rendezés az oszthatóság.

Fogalmak:
prímszám,
törzsszám,
prímelem,
irreducibilis
elem

3.1.2. Egyértelmű prímfaktorizáció

Legyen $a, b, p \in \mathbb{N}$, $p, q > 1$, p -ről azt mondjuk, hogy **prímszám**, ha $p|ab$ -ből $p|a$ vagy $p|b$ következik; q -ről azt mondjuk, hogy **törzsszám**, ha $q = ab$ -ből $a = 1$ vagy $b = 1$ következik. Ellentettjeikkel együtt **prímelem**ekről illetve **irreducibilis elem**ekről beszélünk.

PRÍMSZÁM ÉS
A TÖRZSSZÁM
Bizonyítás.

$p \in \mathbb{N}$ prímszám pontosan akkor, ha törzsszám.

Hiszen, legyen p prímszám, $p = ab$, $a, b \in \mathbb{N}$. Mivel az $p|ab$, a prím tulajdonság szerint $p|a$ vagy $p|b$, az általánosság megszorítása nélkül föltehetjük, hogy $p|a$, azaz $a = ps$ valamely $s \in \mathbb{N}$ -re, és a $p = psb$ egyenlőségből egyszerűsítés után $sb = 1$ következik, azaz $s = b = 1$, p törzsszám is. Megfordítva, legyen most q törzsszám, $q|ab$. Az általánosság megszorítása nélkül föltehetjük, hogy $q \nmid a$. Mivel q törzsszám, $(q, a) = 1$ és az l.n.k.o. (v) tulajdonsága miatt $q|b$ és u prímszám.

Q.E.D.

Az egészekben nyilván a prímelem és az irreducibilis elem fogalma is egybeesik.

SZÁMELMÉLET
ALAPTÉTELE
Bizonyítás.

Tetszőleges $a \in \mathbb{N}$, $a > 1$ szám sorrendtől eltekintve egyértelműen bontható fel prímszámok $a = p_1 p_2 \cdots p_r$ ($r \in \mathbb{N}^+$) alakú szorzatára.

Hiszen, tekintsük az egzisztenciát, legyen $a \in \mathbb{N}$, $a > 1$. Lássuk be először, hogy a -nak létezik prímosztója. Tegyük fel indirekte, hogy nincs neki ilyen. Ekkor a nem prímszám, így nem is törzsszám, ezért létezik $a = a_1 t_1$ valódi faktorizációja, $a_1, t_1 \in \mathbb{N}$, $a_1, t_1 > 1$. a_1 nem lehet prímszám, így a_1 nem is törzsszám, ezért létezik $a_1 = a_2 t_2$ valódi faktorizációja, $a_2, t_2 > 1$. És így tovább, ez az eljárás természetes számok $a > a_1 > a_2 > \cdots$ végtelen szigorú monoton csökkenő sorozatát eredményezi, ami lehetetlen. Ezért az a számnak van prímosztója.

Tegyük fel most, hogy a -nak nem létezik prímfaktorizációja. Legyen u_1 az a szám prímosztója. Ekkor $a = u_1 b_1$, $b_1 > 1$, nem lehet prímszám. De ekkor b_1 -nek van u_2 valódi prímosztója, $a = u_1 u_2 b_2$ és $b_2 > 1$, b_2 nem prímszám, és így tovább, ez az eljárás végtelen sok lépésig folytatható, ami lehetetlen, mivel $a > b_1 > b_2 > \cdots$ természetes számok szigorú monoton csökkenő sorozata. a -nak létezik prímfaktorizációja.

Az unicitás belátásához legyen $a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ kétféle

prímtényező felbontás, $r \leq s$. Mivel az $p_1 | q_1 q_2 \cdots q_s$ prímszám, $p_1 | q_{i_1}$ valamely i_1 -re, de q_{i_1} törzsszám, így $p_1 = q_{i_1}$, átindexelés és egyszerűsítés után $p_1 p_2 \cdots p_{r-1} = q_1 q_2 \cdots q_{s-1}$. Ezt az eljárást folytatva $r - 1$ lépés után kapjuk, hogy $p_1 = q_1 q_2 \cdots q_{s-r+1}$, de p_1 törzsszám, ez csak úgy lehetséges, ha $r = s$ és (az átindexelések után) $p_1 = q_1$.

Q.E.D.

Értelmeszerűen az egész számok prímtényező felbontásában a tényezők lehetnek negatív prímelemek is, és a felbontás egyértelműségében az egységtényezőktől is el kell tekinteni. Legyen a és b nemnulla nem egység egész szám, $|a| = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ és $|b| = p_1^{l_1} p_2^{l_2} \cdots p_r^{l_r}$ felbontás, ahol $p_1, p_2, \dots, p_r$ különböző prímszámok, a nem közös prímosztók egyik kitevője zérus. Ekkor:

$$(a, b) = p_1^{\min\{k_1, l_1\}} p_2^{\min\{k_2, l_2\}} \cdots p_r^{\min\{k_r, l_r\}},$$

$$[a, b] = p_1^{\max\{k_1, l_1\}} p_2^{\max\{k_2, l_2\}} \cdots p_r^{\max\{k_r, l_r\}}.$$

PRÍMSZÁMOK
SZÁMA

A prímszámok halmaza végtelen.

Hiszen, érveljünk indirekte. Legyen az összes prímszám $p_1, p_2, \dots, p_r$, ahol $r \in \mathbb{N}^+$. Ekkor az $1 + p_1 p_2 \cdots p_r$ számnak egyrészt létezik prímosztója a számelmélet alaptétele miatt, másrészt a $p_1, p_2, \dots, p_r$ prímszámok közül egyik sem osztja, ellentmondás.

Q.E.D.

ERATOSZTHENÉSZI
SZITA

```
era:=function(n)
local a,p; integer n; boolean a; a[1]=0; p[1]=[2];
for i=2 to n do a[i] =1;od;
for i=2 to int(sqrt(n)) do
  for j=2 to int(n/i) do a[i*j]=0; od; od;
for i=3 to n do if a[i] =1 then append(p,i); fi; od;
return(p);end;
```

3.2. Diofantoszi egyenlet, kongruencia

Egy egyenletet **diofantoszi egyenlet**nek nevezünk, ha egész megoldásait keressük. Sokféle ilyen egyenletet vizsgáltak, itt az **elsőfokú kétismeretlenes diofantoszi egyenlet**tel foglalkozunk, **általános alakja** $ax + by = c$, ahol $a, b \in \mathbb{Z} \setminus \{0\}$, $c \in \mathbb{Z}$. Ha $c = 0$ akkor homogén egyenletről beszélünk.

Fogalmak:
diofantoszi
egyenlet,
elsőfokú
kétismeretlenes
d.e.

A D. E.
MEGOLDÁSA

Legyen $a, b \in \mathbb{Z} \setminus \{0\}$, $c \in \mathbb{Z}$. Az $ax + by = c$ diofantoszi egyenlet megoldható pontosan akkor, ha az $(a, b) | c$, ekkor ha $ax_0 + by_0 = c$, tetszőleges (x, y) megoldás

$$x = x_0 + \frac{b}{(a, b)} t \quad y = y_0 - \frac{a}{(a, b)} t$$

alakú valamely $t \in \mathbb{Z}$ egészre, és minden ilyen (x, y) számpár megoldás.

Bizonyítás. Hiszen, ha $ax_0 + by_0 = c$ akkor $(a, b) | b.o.$ és így a j.o.-t is azaz $(a, b) | c$. Megfordítva, ha $(a, b) | c$, akkor a kiterjesztett euklideszi algoritmus következtében $au + bv = (a, b)$ valamely $u, v \in \mathbb{Z}$ -re, ezt beszorozva a $\frac{c}{(a, b) \in \mathbb{Z}}$ számmal kapjuk, hogy $a \frac{uc}{(a, b)} + b \frac{vc}{(a, b)} = c$.

Ha $ax_0 + by_0 = c$ és $ax + by = c$, akkor $a(x - x_0) + b(y - y_0) = 0$.

Nyilvánvaló, hogy az általános megoldást megkapjuk, ha az inhomogén egyenlet (x_0, y_0) partikuláris megoldásához hozzáadjuk a homogén egyenlet általános megoldását, ami persze $(\frac{b}{(a, b)}t, -\frac{a}{(a, b)}t)$ ($t \in \mathbb{Z}$).

Q.E.D.

ALGORITMUS

```
1ide:=function(a,b,c)
  local d,u,v,x0,y0,ee,rr,r; integer a,b,c;
  if a=0 or b=0 then return("hiba") else
    ee=eux(a,b); u=ee[1]; v=ee[2]; d=ee[3];
    rr=mo(d,c); r=rr[2];
    If r<>0 then return("nincs megoldás") else
      x0=u*c/d; y0=v*c/d;
      print("x=",x0,"+",b/d,"t,   ", "y=",y0,"-",a/d,"t");
      return(x0,y0);fi;fi;end;
```

Fogalmak: Legyen $m \in \mathbb{N}$, $m > 1$, $a, b \in \mathbb{Z}$. Azt mondjuk, hogy a **kongruens a b -vel modulo m** , ha $m | b - a$. Jelölés: $a \equiv b \pmod{m}$. Az m számot a kongruencia **modulusának** nevezzük.

KONGRUENCIA TULAJDONSÁGAI Legyen $m, m' \in \mathbb{N}$, $m > 1$, $m' > 1$, $a, b, c, d \in \mathbb{Z}$. Ekkor az alábbi állítások teljesülnek:

Bizonyítás. Hiszen, a reflexivitás és a szimmetria világos. Legyen $a \equiv b \pmod{m}$ és $b \equiv c \pmod{m}$, azaz $m | b - a$ és $m | c - b$, de ekkor $m | (c - b) + (b - a) = c - a$, kaptuk, $a \equiv c \pmod{m}$, ami a tranzitivitást mutatja. (i) kész.

(ii) Legyen $a \equiv c \pmod{m}$ és $b \equiv d \pmod{m}$, azaz $m | c - a$ és $m | d - b$, de ekkor, mivel $m | (c - a) + (d - b) = (c + d) - (a + b)$ és $m | c(d - b) + (c - a)b = cd - ab$. Kaptuk, hogy $a + b \equiv c + d \pmod{m}$

- (i) a modulo m kongruencia ekvivalenciareláció $\mathbb{Z}$ -n;
 (ii) ha $a \equiv c \pmod{m}$ és $b \equiv d \pmod{m}$, akkor $a + b \equiv c + d \pmod{m}$ és $ab \equiv cd \pmod{m}$;
 (iii) ha az $m \nmid c$ és $ac \equiv bc \pmod{m}$, akkor $a \equiv b \pmod{\frac{m}{(m,c)}}$;
 (iv) ha $a \equiv b \pmod{m}$ és $a \equiv c + d \pmod{m}$ és $ab \equiv cd \pmod{m}$, akkor $a \equiv b \pmod{[m, m']}$.

és $ab \equiv cd \pmod{m}$.

(iii) Legyen $ac \equiv bc \pmod{m}$, azaz $m \mid bc - ac = (b - a)c$ és $\frac{m}{(m,c)} \mid (b - a) \frac{c}{(m,c)}$. Mivel $(\frac{m}{(m,c)}, \frac{c}{(m,c)}) = 1$, a kívánt $\frac{m}{(m,c)} \mid b - a$ oszthatóságot kapjuk.

Legyen $a \equiv b \pmod{m}$ és $a \equiv b \pmod{m'}$, azaz az $m \mid b - a$ és $m' \mid b - a$, ahonnan az l.k.k.t. definíciója miatt az $[m, m'] \mid b - a$, amit kívántunk.

A modulo m kongruencia ekvivalenciaosztályait **maradékosztály**oknak nevezzük, egy osztályban azok az elemek vannak, amelyek ugyanazt a maradékot adják m -mel osztva. Így a modulo m maradékosztályok száma éppen m : $\overline{0}, \overline{1}, \dots, \overline{m-1}$.

Legyen $m \in \mathbb{N}$, $m > 1$, Z_m a modulo m maradékosztályok halmaza, $\overline{a} + \overline{b} = \overline{a+b}$ és $\overline{a}\overline{b} = \overline{ab}$. Ekkor $(Z_m, +, \cdot)$ kommutatív egységelemes gyűrű, amely test pontosan akkor, ha m prímszám. $U(Z_m) = \{\overline{a} \in Z_m \mid (a, m) = 1\}$, az $U(Z_m)$ egységcsoport rendje $\varphi(m)$.

A Z_m gyűrűt **modulo m maradékosztálygyűrű**nek nevezzük.

Az $ax \equiv b \pmod{m}$, $m \nmid a$ **egyszeres elsőfokú kongruencia egyenlet** megoldását vezessük vissza az $ax + my = b$ kétismeretlenes diofantoszi egyenlet megoldására.

Legyen $a, b, m \in \mathbb{Z}$, $m \nmid a$, $m > 1$. Az $ax \equiv b \pmod{m}$ kongruencia egyenlet megoldható pontosan akkor, ha az $(a, m) \mid b$. A modulo m inkongruens összes megoldása $x \equiv x_0 + \frac{m}{(a, m)}t \pmod{m}$, ahol $ax_0 \equiv b \pmod{m}$ partikuláris megoldás és $t = 0, 1, \dots, (a, m) - 1$.

```
like:=function(a,b,m)
  local rr,r,d,u,ee; integer a,b,m;
  rr=mo(m,a); r=rr[2];
  if r=0 or m<2 then return("hiba") else
    ee=eux(a,m); u=ee[1]; d=ee[3];
    rr=mo(d,b); r=rr[2];
    if r<>0 then return("nincs megoldás") else
      x0=u*b/d;
      print("x=",x0,"+",m/d,"t(mod m)  t=0,1,...,",d-1);
```

Q.E.D.

Fogalmak:
 maradék-
 osztály,
 maradék
 osztály gyűrű
 MARADÉK
 OSZTÁLY
 GYÜRŰ

Fogalmak:
 kongruencia
 egyenlet

KONGRUENCIA
 EGYENLET
 MEGOLDÁSA

ALGORITMUS:
 KONGRUENCIA
 EGYENLET

Fogalmak:	<code>return([x0,d]);fi;fi;end;</code>
redukált maradékosztály	Ha az a szám relatív prím az m modulusához, akkor az $\bar{a}$ maradékosztályt redukált maradékosztálynak nevezzük, számuk $\varphi(m)$.
EULER- FERMAT	Legyen $a, m \in \mathbb{Z}$, $m > 1$ 'es $(a, m) = 1$. Ekkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.
Bizonyítás.	Hiszen, legyen $U = \{\bar{a}_1, \bar{a}_2, \dots, \bar{a}_{\varphi(m)}\} \subset Z_m$ az összes redukált maradékosztály, mivel ezek csoportot alkotnak a szorzásra és $\bar{a} \in U$, ha $\bar{b} = \bar{a}_1 \bar{a}_2 \cdots \bar{a}_{\varphi(m)}$, akkor $(\bar{a} \bar{a}_1)(\bar{a} \bar{a}_2) \cdots (\bar{a} \bar{a}_{\varphi(m)}) = \bar{b}$, ahonnan kapjuk,
Q.E.D.	hogy $a^{\varphi(m)} b \equiv b \pmod{m}$, egyszerűsítés után készen vagyunk..

3.3. Számrendszerek, tizedes törtek

SZÁM RENDSZEREK	Legyen $a, u \in \mathbb{N}^+$, $u > 1$. Ekkor egyértelműen létezik $s, a_i \in \mathbb{N}$, $0 \leq a_i \leq u - 1$ ($i = 0, 1, \dots, s$), $a_s \neq 0$ úgy, hogy $a = \sum_{i=0}^s a_i u^i$.
Bizonyítás.	Hiszen, az egzisztenciához égezzük el maradékos osztások alábbi sorozatát:

$$\begin{aligned}
 a &= uq_0 + a_0, & 0 \leq a_0 < u \\
 q_0 &= uq_1 + a_1, & 0 \leq a_1 < u \\
 q_1 &= uq_2 + a_2, & 0 \leq a_2 < u \\
 &\dots\dots\dots \\
 q_{i-1} &= uq_i + a_i, & 0 \leq a_i < u \\
 &\dots\dots\dots
 \end{aligned}$$

Mivel $a > q_0 > q_1 > q_2 > \cdots > q_i > \cdots$ természetes számok szigorú monoton csökkenő sorozata, véges sok lépés után q_{s-1} kisebb lesz, mint u , és az utolsó lépésben $q_{s-1} = u0 + a_s$, az utolsó hányados $q_s = 0$. A végéről visszafelé haladva lépésenként kapjuk, hogy

$$\begin{aligned}
 q_{s-1} &= a_s \\
 q_{s-2} &= a_s u + a_{s-1} \\
 q_{s-3} &= a_s u^2 + a_{s-1} u + a_{s-2} \\
 &\dots\dots\dots \\
 q_0 &= a_s u^{s-1} + a_{s-1} u^{s-2} + \cdots + a_2 u + a_1 \\
 a &= a_s u^s + a_{s-1} u^{s-1} + \cdots + a_1 u + a_0
 \end{aligned}$$

Unicitás. Ha $a = \sum_{i=0}^t a'_i u^i$ egy másik ilyen felírás, akkor szükségképpen az a'_i értékek rendre a fenti maradékos osztások maradékaival kell,

hogy megegyezzenek, mivel $a = u \sum_{i=1}^t a'_i u^{i-1} + a'_0$, $\sum_{i=1}^t a'_i u^{i-1} = u \sum_{i=2}^t a'_i u^{i-2} + a'_1$, és így tovább. Következésképp $s = t$ és $a_i = a'_i$.

Q.E.D.

A tételben szereplő u számot a **számrendszer alapjának**, az a_i számot az a szám u^i **helyiértékű számjegyének** nevezzük, és az $a_s a_{s-1} \dots a_1 a_0$ $= a$ jelölést alkalmazzuk. Nevezetes számrendszerek a 2-alapú **bináris**, a 16-alapú **hexadecimális**, a 10-alapú **decimális**.

Fogalmak:
számrendszer
alapja,
helyiérték

Legyen $a, u, k \in \mathbb{N}^+$, $u > 1$, $a = a_s a_{s-1} \dots a_1 a_0$, $w|u - 1$.

OSZTHATÓSÁGI
SZABÁLYOK

- (i) legyen $v|u$; $v^k|a$ ha (iii) legyen $v|u + 1$; $v|a$ ha
 $v^k|a_{k-1} \dots a_1 a_0$; $v|\sum_{i=0}^s (-1)^i a_i$;
 (ii) legyen $v|u - 1$; $v|a$ ha (iv) legyen $v|u^2 - u + 1$; $v|a$ ha
 $v|\sum_{i=0}^s a_i$; $v|a_s a_{s-1} \dots a_1 a_0 - (u - 1)a_0$.

Legyen $a \in \mathbb{Q}$, $0 < a < 1$ redukált alakja $a = \frac{p}{q}$. Végezzük el a maradékos osztások alábbi sorozatát (nyilván $a_0 = 0$, $r_0 = p$).

Fogalmak:
tisztá szakaszos
t.t., vegyes
szakaszos
szakaszos t.t.,
véges t.t.,
ismétlődő
szakasz,
előszakasz

$$\begin{aligned} p &= qa_0 + r_0 \\ 10r_0 &= qa_1 + r_1 \\ 10r_1 &= qa_2 + r_2 \\ &\dots\dots\dots \\ 10r_{k-1} &= qa_k + r_k \\ &\dots\dots\dots \end{aligned}$$

A hányadosokra $0 \leq a_i \leq 9$ teljesül. Ekkor, lépésenként visszahelyettesítve,

$$\begin{aligned} \frac{p}{q} &= a_1 10^{-1} + \frac{r_1}{10q} = a_1 10^{-1} + a_2 10^{-2} + \frac{r_2}{10^2 q} = \dots = \\ &a_1 10^{-1} + a_2 10^{-2} + \dots + a_k 10^{-k} + \frac{r_k}{10^k q} = \dots \end{aligned}$$

Mivel az r_i maradékok 0 és q közé esnek, létezik egy legkisebb i index és $t \in \mathbb{N}$, hogy $r_i = r_{i+t}$, és a többi maradék már ismétlődik, azaz $j \geq i$ indexekre $r_j = r_{j+t}$. Ha $i = 0$ akkor azt mondjuk, hogy az a **racióális szám tiszta szakaszos tizedes tört alakba írható**, és az $a = 0, \dot{a}_1 \dot{a}_2 \dots \dot{a}_t$ jelölést alkalmazzuk. A fenti összefüggésekből világos, hogy

$$a = \frac{a_1 10^{t-1} + a_2 10^{t-2} + \dots + a_t}{10^t} \sum_{i=0}^{\infty} \frac{1}{10^{it}} =$$

$$\frac{a_1 10^{t-1} + a_2 10^{t-2} + \dots + a_t}{10^t} \frac{10^t}{10^t - 1} = \frac{a_1 10^{t-1} + a_2 10^{t-2} + \dots + a_t}{10^t - 1}$$

a mértani sor összegképlete alapján.

TISZTA
SZAKASZOSBÓL
KÖZÖNSÉGES

Tiszta szakaszos tizedes törtet úgy írunk át közösleges tört alakba, hogy a számláló a szakasz számjegyeiből képzett szám, a nevező pedig annyi 9-esből képzett szám, ahány számjegyből áll a szakasz.

Ha $i > 1$ akkor azt mondjuk, hogy az a **racióális szám vegyes szakaszos tizedes tört alakba írható**, és az $a = 0, a_1 a_2 \dots a_{i-1} \dot{a}_i a_{i+1} \dots a_{i+t-1}$ jelölést alkalmazzuk, ahol $a_1 a_2 \dots a_{i-1}$ az **előszakasz** illetve $\dot{a}_i a_{i+1} \dots a_{i+t-1}$ a **szakasz**. A fenti összefüggésekből világos, hogy

$$\begin{aligned} a &= \frac{a_1 10^{i-2} + a_2 10^{i-3} + \dots + a_{i-1}}{10^{i-1}} + \\ &\quad \frac{a_i 10^{t-1} + a_{i+1} 10^{t-2} + \dots + a_{i+t-1}}{10^{t+i-1}} \sum_{i=0}^{\infty} \frac{1}{10^{it}} = \\ &\quad \frac{a_1 10^{i-2} + a_2 10^{i-3} + \dots + a_{i-1}}{10^{i-1}} + \\ &\quad \frac{a_i 10^{t-1} + a_{i+1} 10^{t-2} + \dots + a_{i+t-1}}{10^{t+i-1}} \frac{10^t}{10^t - 1} = \\ &= \frac{a_1 10^{i+t-2} + \dots + a_{i+t-1} - (a_1 10^{i-2} + \dots + a_{i-1})}{(10^t - 1) 10^{i-1}}. \end{aligned}$$

VEGYES
SZAKASZOSBÓL
KÖZÖNSÉGES

Vegyes szakaszos tizedes törtet úgy írunk át közösleges tört alakba, hogy a számláló az előszakasz és a szakasz számjegyeiből képzett számból kivonva az előszakasz számjegyeiből képzett szám, a nevező pedig annyi 9-esből illetve utána annyi 0-ból képzett szám, ahány számjegyből áll a szakasz illetve az előszakasz.

Speciálisan ha a szakasz a 0 számjegy, akkor azt mondjuk, hogy a racionális szám **véges tizedes tört alakba írható**, és az $a = 0, a_1 a_2 \dots a_{i-1}$ jelölést alkalmazzuk. Az előállítás nem egyértelmű, véges tizedes törtnek van végtelen tizedes tört alakjuk is, például $1, 5 = 1, 49$.

Nemnegatív racionális szám egész része a nála nem nagyobb legnagyobb természetes szám, törtrésze a szám és egészrészének különbsége. Az egész részt tizes számrendszerbe, a törtrészt tizedes tört alakba írva kapjuk a szám

$$a_s a_{s-1} \dots a_0, a_{-1} a_{-2} \dots$$

tizedes tört alakját. Az előjelet elírva határozhatjuk meg ellentettjének tizedes tört alakját.

Legyen $a \in \mathbb{Q}$, $0 < a < 1$ redukált közönséges tört alakja $\frac{p}{q}$. Ekkor a következő állítások teljesülnek:

SZAKASZOS
TIZEDES TÖRT
ALAK

- (i) a tiszta szakaszos tizedes tört alakba írható pontosan akkor ha a $(q, 10) = 1$;
- (ii) a vegyes szakaszos tizedes tört alakba írható pontosan akkor ha $a(q, 10) \neq 1$;
- (iii) a véges tizedes tört alakba írható pontosan akkor ha $q = 2^r 5^s$ valamely $r, s \in \mathbb{N}$ -re.

Azt mondjuk, hogy az α **valós szám tizedes tört alakja** $c, a_1 a_2 \dots$, ahol c egy decimális alakban felírt egész szám és $a_1, a_2, \dots$ tizedesjegyek, ha az $u_0 = c, u_1 = c, a_1, u_2 = c, a_1 a_2, \dots$ racionális számsorozat tartalmazza az α osztály (másszóval az u_n sorozat valós határértéke α).

Fogalmak:
valós szám t.t.
alakja

Minden valós szám egyértelműen felírható végtelen tizedes tört alakban, ezek közül a racionálisak pontosan a szakaszos tizedes törtök.

VALÓS SZÁM
T.T. ALAKJA

3.4. A polinomgyűrű

Legyen A kommutatív egységelemes gyűrű, $x \notin A$ **határozatlan**nak nevezett szimbólum. Az $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ alakú formális összeget, ahol az a_i együtthatók az A gyűrű elemei, $a_n \neq 0$, n természetes szám, **az A gyűrű feletti egyhatározatlanú polinomnak**, n -et, ha nem minden együttható 0, a **polinom fokszámának** nevezzük és f° -rel jelöljük. Ha az a_n együttható 1, akkor **főpolinom**ról beszélünk. Két polinomot akkor tekintjük egyenlőnek, ha megfelelő együtthatóik rendre megegyeznek. Ha c az A gyűrű eleme, akkor az $f(x)$ kifejezésben az x határozatlan helyére behelyettesítve a c elemet, az $f(c)$ kifejezésben a kijelölt műveleteket A gyűrűbelinek tekintve, az $f(c)$ értéket az $f(x)$ **polinom c helyen vett helyettesítési értékének** nevezzük.

Fogalmak:
határozatlan,
egyhatározatlanú
polinom,
polinom
fokszáma,
főpolinom,
polinom
helyettesítési
értéke

Legyen A kommutatív egységelemes gyűrű. Legyen $A[x] = \{a : \mathbb{N} \rightarrow A, n \mapsto a_n, \text{ csak véges sok } n\text{-re } a_n \neq 0\}$. Legyen $a, b \in A[x]$,

POLINOMGYŰRŰ

$$(a + b)_n = a_n + b_n, \quad (ab)_n = \sum_{i=0}^n a_i b_{n-i}.$$

Ekkor az $(A[x], +, \cdot)$ struktúra kommutatív egységelemes gyűrű, továbbá ha A integritástartomány, akkor $A[x]$ is integritástartomány és $U(A[x]) = U(A)$.

Bizonyítás. Hiszen, legyen $a, b, c \in A[x]$, ekkor nyilván $a + b, ab \in A[x]$. Minden nyilvánvaló, kivéve a szorzás asszociativitását, a zérusosztómentességet és az egységek meghatározását. Egyrészt

$$\begin{aligned} ((ab)c)_n &= \sum_{i=0}^n (ab)_i c_{n-i} = \sum_{i=0}^n \sum_{j=0}^i a_j b_{i-j} c_{n-i}, \text{ másrészt} \\ (a(bc))_n &= \sum_{i=0}^n a_i (bc)_{n-i} = \sum_{i=0}^n \sum_{j=0}^{n-i} a_i b_j c_{n-i-j}, \end{aligned}$$

mindkét kapott kifejezés egyenlő a $\sum_{i+j \leq n} a_i b_j c_{n-i-j}$ összeggel. Ha A zérusosztómentes, akkor látjuk, hogy szorzásnál a fokszámok összeadódnak, ahonnan következik $A[x]$ zérusosztómentessége és hogy $U(A[x]) = U(A)$.

Q.E.D.

Fogalmak: A sorozatok fenti szorzatát szokás **konvolúciósorzásnak** nevezni. Az $A[x]$ struktúrát **az A gyűrű feletti egyhatározatlanú polinomgyűrűnek** nevezzük. Azonosítsuk az $a \in A$ elemet azzal a sorozattal, amelynek nulladik tagja a , a többi 0; jelölje x^n azt a sorozatot, amelynek n . tagja 1 a többi 0. Így az $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ formális összegben levő „műveletek” az $A[x]$ gyűrűbeli műveletekként értelmezhetők, és minden $A[x]$ halmazbeli sorozat felírható ilyen alakban. A továbbiakban a polinomokat ilyen előállításban fogjuk tekinteni.

Fogalmak: Ezután csak test feletti polinomokat fogunk tekinteni. Legyen K test. Azt mondjuk, hogy az $a(x) \in K[x]$ **polinom osztja a $b(x) \in K[x]$ polinomot**, ha létezik $c(x) \in K[x]$ polinom, hogy $b(x) = a(x)c(x)$, jelölés: $a(x) | b(x)$. A polinomok oszthatóságának tulajdonságai analógok az egész számokéval. Azt mondjuk, hogy a $b(x) \in K[x]$ **polinom az $a(x) \in K[x]$ polinom asszociáltja**, ha $b(x) = a(x)c(x)$, ahol $c(x) \in U(K)$, jelölés: $a(x) \sim b(x)$. Az asszociáltság nyilván ekvivalenciareláció.

POLINOM OSZTÁSA POLINOMMAL Legyen K test, $0 \neq g(x), f(x) \in K[x]$. Ekkor egyértelműen létezik $q(x), r(x) \in K[x]$, hogy $g(x) = f(x)q(x) + r(x)$, és $r(x) = 0$ vagy $r^\circ < f^\circ$.

Bizonyítás. Hiszen, legyen $f(x) = a_m x^m + a_{m-1} x^{m-1} + \dots + a_1 x + a_0$, $g(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$, $f^\circ = m$, $g^\circ = n$. Ha $n < m$ akkor a $q(x) = 0$ és $r(x) = g(x)$ választás megfelelő. Legyen most $n \geq m$, $c_{n-m} = \frac{b_n}{a_m}$. Ekkor a $g_1(x) = g(x) - f(x)c_{n-m}x^{n-m}$ polinom fokszáma kisebb, mint $g(x)$ -é, $n-1$ -edfokú tagjának együtthatója legyen $b_{1,n-1}$ (lehet 0 is), Legyen $c_{n-m-1} = \frac{b_{1,n-1}}{a_m}$, ekkor $g_2(x) = g_1(x) - f(x)c_{n-m-1}x^{n-m-1}$

fokszáma kisebb, mint $n - 1$. És í. t., ezt az eljárást alkalmazva kapjuk a $q(x) = c_{n-m}x^{n-m} + c_{n-m-1}x^{n-m-1} + \dots + c_1x + c_0$ hányadost és $r(x) = g_{n-m+1}(x)$ maradékot, mivel $r(x) = 0$ vagy $r^\circ < f^\circ$, és visszahelyettesítések után látható, hogy $f(x) = g(x)q(x) + r(x)$. Az egzisztencia kész. Az unicitáshoz indirekte érvelve legyen

$$g(x) = f(x)q(x) + r(x), \quad g(x) = f(x)t(x) + w(x)$$

két maradékos osztás, $q(x) \neq t(x)$. A két egyenlőséget kivonva egymásból $0 = f(x)(q(x) - t(x)) + (r(x) - w(x))$ azaz $f(x)(t(x) - q(x)) = r(x) - w(x)$, ahol a bal oldal fokszáma legalább n , a jobboldal fokszáma kisebb, mint n , ami ellentmondás.

Az egészekhez hasonló elnevezéseket használunk: **osztandó, osztó, hányados, maradék**.

```
mop:=function(a,m,b,n)
  local q,af,bf,c;q=0;
  if n<m then return(0,b) else
    af=coeff(x^m,a);
    if af=0 then return("hiba") else
      for i=0 to n-m do
        bf=coeff(x^(n-i),b);
        c=(bf/af)*x^(n-m-i); q=q+c;
        b=b-c*a; od;
  return([q,b-a*q]);fi;fi; end;
```

A maradékos osztáson alapuló **euklideszi algoritmus** is analóg módon végezhető el az $a(x), b(x) \in K[x]$ polinomokon:

```
eup:=function(a,m,b,n)
  local q=[],r=[], i=2,f1,f2,mm;
  if coeff(x^m,a)=0 then return("hiba"); else
    append(q,mop(a,m,b,n)[1]);
    append(r,mo(a,m,b,n)[2]);
    if r[1]=0 then return(q,r); else
      f2=m; for j=min(m,n) to 0 step -1 do
        if coeff(x^j,r[1]) <> 0 then f1=j;j=-1;fi;od;
      append(q,mop(r[1],f1,a,f2)[1]);
      append(r,mop(r[1],f1,a,f2)[2]);
```

Q.E.D.

Fogalmak:
osztandó, osztó,
hányados,
maradék,
euklideszi
algoritmus
ALGORITMUS:
POLINOM
OSZTÁSA
POLINOMMAL

ALGORITMUS:
EUKLIDESZI

```

while r[i]<>0 do
  f2=f1, for j=min(m,n) to 0 step -1 do
    if coeff(x^j,r[i]) <>0 then f1=j;j=-1;fi;od;
  append(q,mo(r[i],f1,r[i-1],f2))[1];
  append(r,mo(r[i],f1,r[i-1],f2)[2]); i=i+1;
od; return([q,r]); fi; fi;end;

```

$$\begin{aligned}
b(x) &= a(x)q_1(x) + r_1(x), \quad r_1^\circ < a^\circ \\
a(x) &= r_1(x)q_2(x) + r_2(x), \quad r_2^\circ < r_1^\circ \\
r_1(x) &= r_2(x)q_3(x) + r_3(x), \quad r_3^\circ < r_2^\circ \\
&\dots\dots\dots : \\
r_{n-3}(x) &= r_{n-2}(x)q_{n-1}(x) + r_{n-1}(x), \quad r_{n-1}^\circ < r_{n-2}^\circ \\
r_{n-2}(x) &= r_{n-1}(x)q_n(x) + r_n(x), \quad r_n(x) = 0.
\end{aligned}$$

Fogalmak: Ha $0 \neq a(x), b(x) \in K[x]$, akkor $d(x) = (a(x), b(x))$ **legnagyobb**
 l.n.k.o., l.k.k.t., **közös osztó**juk olyan főpolinom, amelyre teljesül, hogy $d(x)|a(x)$ és
 prímpolinom, $d(x)|b(x)$, ha $c(x) \in K[x]$ -ra szintén $c(x)|a(x)$ és $c(x)|b(x)$, akkor $c(x)|d(x)$.
 irreducibilis
 polinom Ha K test, $0 \neq a(x), b(x) \in K[x]$, akkor létezik $(a(x), b(x))$ legnagyobb
 közös osztó, nevezetesen a rajtuk végrehajtott euklideszi algoritmus

L.N.K.O. utolsó nemnulla maradékával asszociált főpolinom.

LÉTEZÉSE Ha $a(x), b(x) \in K[x] \setminus \{0\}$, akkor létezik $u(x), v(x) \in K[x]$, hogy
 KIBŐVÍTETT $(a(x), b(x)) = a(x)u(x) + b(x)v(x)$.

EUKLIDESZI
 ALGORITMUS

```

euxp:=function(a,m,b,n)
  local q, ma[2,3],f1=m,f2=n;
  if a=0 or b=0 then return("hiba"); else
    ma=[[1,0,a],[0,1,b]];
    while ma[1,3]<>0 and ma[2,3]<>0 do
      if f1>f2 then q=mop(ma[2,3],f2,ma[1,3],f1)[1];
        for i=1 to 3 do ma[1,i]=ma[1,i]-q*ma[2,i];od;
      else q=mop(ma[1,3],f1,ma[2,3],f2)[1];
        for i=1 to 3 do ma[2,i]=ma[2,i]-q*ma[1,i];od;fi;
      for j=min(m,n) to 0 step -1 do
        if coeff(x^j,ma[1,3])<>0 then f1=j;j=-1;fi;od;
        for j=min(m,n) to 0 step -1 do
          if coeff(x^j,ma[2,3])<>0 then f2=j;j=-1;fi;od;od;
        if ma[1,3]=0 then return([ma[2,1],ma[2,2],ma[2,3]]);
        else return([ma[1,1],ma[1,2],ma[1,3]]); fi; fi; end;
    end;
  end;
end;

```

Azaz, az euklideszi algoritmust elvégzése során behelyettesítéseket alkalmazva minden lépésben kifejezzük a maradékot $r_i(x) = a(x)u_i(x) + b(x)v_i(x)$ alakban, az utolsó lépésben a legnagyobb közös osztóval egyenlő $r_{n-1}(x)$ -et fejezzük ki a keresett $(a(x), b(x)) = a(x)u(x) + b(x)v(x)$ alakban.

Az l.n.k.o. képzésének tulajdonságai főpolinomokra analógok a természetes számoknál kapottakkal. Azt mondjuk, hogy a $0 \neq a(x), b(x) \in K[x]$ polinomok **legkisebb közös többszöröse** az $m(x) = [a(x), b(x)] \in K[x]$ főpolinom, ha $a(x)|m(x)$ és $b(x)|m(x)$, és ha $c(x) \in K[x]$ ra $a(x)|c(x)$ és $b(x)|c(x)$, akkor $m(x)|c(x)$.

Ha K test, $0 \neq a(x), b(x) \in K[x]$, akkor az $\frac{a(x)b(x)}{(a(x), b(x))}$ polinommal asszociált $m(x)$ főpolinom az $a(x), b(x) \in K[x]$ nemnulla polinomok legkisebb közös többszöröse. L.K.K.T.
LÉTEZÉSE

A l.k.k.t. képzésének tulajdonságai főpolinomokra megegyeznek a természetes számoknál kapottakkal.

Nemnulla és nem egység $p(x) \in K[x]$ polinomról azt mondjuk, hogy **prímpolinom**, ha $p(x)|b(x)c(x)$ ($b(x), c(x) \in K[x]$) esetén $p(x)|b(x)$ vagy $p(x)|c(x)$. Nemnulla és nem egység $q(x) \in K[x]$ polinomról azt mondjuk, hogy **irreducibilis polinom**, ha $q(x) = a(x)b(x)$ ($a(x), b(x) \in K[x]$) esetén $a(x)$ egység vagy $b(x)$ egység, azaz nemnulla konstans polinom. Testfeletti polinom prím akkor és csak akkor, ha irreducibilis. Fogalmak:
prímpolinom,
irreducibilis
polinom

Tetszőleges nemnulla nem egység testfölötti polinom sorrendtől és egységtényezőtől eltekintve egyértelműen bontható fel prímpolinomok szorzatára. POLINOM
ELMÉLET
ALAPTÉTELE

4. fejezet

Testelmélet

4.1. Komplex számok

Fogalmak: Könnyen látható, hogy páratlan fokszámú valós együtthatós polinomnak mindig van valós gyöke, azonban például az $x^2 + 1$ polinomnak nincs valós gyöke. Jelölje az i szimbólum egy gyökét, és nevezzük el **képzetes egység**nek, mivel nem valós, hanem „elképzelt” számról van szó, hiszen négyzete -1 . Tekintsük az $a = a_1 + a_2i$ alakú formális összegeket, ahol az $a_1 = \operatorname{Re}(a) \in \mathbb{R}$ számot **valós rész**nek, az $a_2 = \operatorname{Im}(a) \in \mathbb{R}$ számot **képzetes rész**nek nevezzük. Az összeadás és a szorzás műveletét végezzük el ahogyan megszoktuk kéttagok esetén, a kapott struktúra minden, számoktól elvárt műveleti tulajdonsággal rendelkezik. A $0 \neq a = a_1 + a_2i$ elem reciprokának megkereséséhez alkalmazzuk a nevező gyöktelenítésének eljárását, legyen $\bar{a} = a_1 - a_2i$ az a **konjugáltja**, továbbá $\|a\| = a\bar{a} = (a_1 + a_2i)(a_1 - a_2i) = a_1^2 + a_2^2 \in \mathbb{R}^+$ az a **normája**, $|a| = \sqrt{\|a\|} \in \mathbb{R}^+$ az a **abszolútértéke**. Így kapjuk, hogy $\frac{1}{a} = \frac{1}{a} \frac{\bar{a}}{\bar{a}} = \frac{1}{\|a\|} \bar{a}$. A bizonyításhoz ezeket az „elképzelt” számokat valós rész – képzetes rész rendezett számpároknak tekintjük.

KOMPLEX
SZÁMOK
STRUKTÚRÁJA

Legyen $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, $a = (a_1, a_2)$, $b = (b_1, b_2) \in \mathbb{C}$, és a műveleteket a következőképpen határozzuk meg:

$$a + b = (a_1 + b_1, a_2 + b_2), \quad ab = (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1).$$

Ekkor $(\mathbb{C}, +, \cdot)$ test.

Bizonyítás. Hiszen, legyenek $a = (a_1, a_2)$, $b = (b_1, b_2)$, $c = (c_1, c_2) \in \mathbb{C}$. Világos, hogy $a+b, ab \in \mathbb{C}$ és minden megkívánt műveleti tulajdonságot közvetlen számolással megkaphatjuk. A szorzás asszociativitását példának tekintve,

egyrészt

$$\begin{aligned} a(bc) &= a(b_1c_1 - b_2c_2, b_1c_2 + b_2c_1) = (a_1b_1c_1 - a_1b_2c_2 - a_2b_1c_2 - a_2b_2c_1, \\ &\quad a_1b_1c_2 + a_1b_2c_1 + a_2b_1c_1 - a_2b_2c_2), \text{ másrészt} \\ (ab)c &= (a_1b_1 - a_2b_2, a_1b_2 + a_2b_1)c = (a_1b_1c_1 - a_2b_2c_1 - a_1b_2c_2 - a_2b_1c_2, \\ &\quad a_1b_1c_2 - a_2b_2c_2 + a_1b_2c_1 + a_2b_1c_1) = a(bc). \end{aligned}$$

Q.E.D.

A $\mathbb{C}$ struktúrát a **komplex számok testének**, elemeit **komplex számoknak** nevezzük. Azonosíthatjuk az $(a, 0)$ alakú komplex számokat az a valós számokkal, így $\mathbb{R} \subset \mathbb{C}$, és a komplex számok közötti összeadás és szorzás a valós számok közötti műveletek kiterjesztése. Legyen $i = (0, 1)$. Ekkor $a = (a_1, a_2) = (a_1, 0) + (a_2, 0)(0, 1) = a_1 + a_2i$ az $a_1 = (a_1, 0)$, $a_2 = (a_2, 0)$ azonosítást felhasználva, amely alakot a komplex szám **algebrai alakjának** nevezzük.

Fogalmak:
komplex
számok teste,
algebrai alak

Ha $a = a_1 + a_2i$, $b = b_1 + b_2i \in \mathbb{C}$, akkor:

KONJUGÁLÁS
TULAJDONSÁGAI

- (i) $\overline{a + b} = \bar{a} + \bar{b}$;
- (ii) $\overline{ab} = \bar{a}\bar{b}$;
- (iii) $\bar{\bar{a}} = a$;
- (iv) $a\bar{a} = a_1^2 + a_2^2 \in \mathbb{R}$, és $a = \bar{a}$ pontosan akkor, ha $a \in \mathbb{R}$.

Legyen $a, b \in \mathbb{C}$.

ABSZOLÚT
ÉRTÉK
TULAJDONSÁGAI

- (i) $|a| \geq 0$ és $a = 0$ pontosan akkor, ha $a = 0$;
- (ii) (háromszög-egyenlőtlenség) $|a + b| \leq |a| + |b|$;
- (iii) $|a - b| \geq ||a| - |b||$;
- (iv) $|ab| = |a| |b|$.

Hiszen, minden egyszerűen adódik, tekintsük (ii)-t. Az egyenlőtlenség teljesül, ha $||a + b|| \leq (|a| + |b|)^2$, azaz

Bizonyítás.

$$(a + b)\overline{a + b} = |a|^2 + |b|^2 + \bar{a}b + a\bar{b} \leq |a|^2 + |b|^2 + 2|a||b|,$$

ehhez elegendő, hogy $\bar{a}b + a\bar{b} \leq 2|a||b|$ legyen. Ez az egyenlőtlenség fennáll, ha $4(a_1b_1 + a_2b_2)^2 \leq 4|a|^2|b|^2$, azaz

$$a_1^2b_1^2 + a_2^2b_2^2 + 2a_1a_2b_1b_2 \leq a_1^2b_1^2 + a_2^2b_2^2 + a_1^2b_2^2 + a_2^2b_1^2.$$

Egyszerűsítés és átrendezés után a nyilvánvaló $0 \leq (a_1b_2 - a_2b_1)^2$ egyenlőtlenséget kapjuk.

Q.E.D.

Fogalmak: Azonosítsuk a Descartes-féle koordinátasík pontjait a valós rendezett számpárokkal, azaz a komplex számokkal, ilyenkor a síkot **Gauss-féle számsík**nak nevezzük. Ekkor $0 \neq a \in \mathbb{C}$ számot meghatározhatjuk az odamutató helyvektor $|a|$ hosszával és $\alpha = \arg a$ irányszögével, és kapjuk a **trigonometrikus alakot**: $a = a_1 + a_2i = |a|(\cos \alpha + i \sin \alpha)$ ahol a $\arg a$ a **komplex szám argumentuma**. Az áttérés a $0 \neq a = a_1 + a_2i \in \mathbb{C}$ algebrai alakról a trigonometrikus alakra a következőképpen lehetséges. Nyilván $a = |a|(\frac{a_1}{|a|} + \frac{a_2}{|a|}i)$, mivel az $\frac{a_1}{|a|}$ és az $\frac{a_2}{|a|}$ valós számok négyzetösszege 1, valamely α szögre $\cos \alpha = \frac{a_1}{|a|}$ és $\sin \alpha = \frac{a_2}{|a|}$. Ha $a_1 = 0$ és $a_2 > 0$ akkor $\alpha = \frac{\pi}{2}$; ha $a_1 = 0$ és $a_2 < 0$ akkor $\alpha = \frac{3\pi}{2}$; egyébként $\alpha = \begin{cases} \arctg \frac{a_2}{a_1}, & \text{ha } a_1 > 0; \\ \pi + \arctg \frac{a_2}{a_1}, & \text{ha } a_1 < 0 \end{cases}$ (Ez a visszakeresés $(-\frac{\pi}{2}, \frac{3\pi}{2}]$ intervallumbeli szöget ad meg.) A $0 \neq a \in \mathbb{C}$ **komplex n . gyökének** ($n \geq 2$) nevezzük az $x^n - a$ polinom komplex gyökeit, és $\sqrt[n]{a}$ -val jelöljük. Nevezetes tény, hogy ilyen komplex gyök n darab különböző van. A trigonometrikus alakban egyszerűen végezhető el a szorzás, osztás, hatványozás és

MŰVELETEK
TRIGONOMETRIKUS
ALAKBAN

Legyen $0 \neq a, b \in \mathbb{C}$, $n \in \mathbb{N}^+$. Ekkor:

- (iii) (Moivre képlete) $|a^n| = |a|^n$ és $\arg a^n = n \arg a$;
- (i) $|ab| = |a||b|$ és $\arg ab = \arg a + \arg b$;
- (iv) $|\sqrt[n]{a}| = \sqrt[n]{|a|} \in \mathbb{R}$, $\arg \sqrt[n]{a} = \frac{\arg a + 2k\pi}{n}$ ($k = 0, 1, 2, \dots, n-1$).
- (ii) $|\frac{a}{b}| = \frac{|a|}{|b|}$ és $\arg \frac{a}{b} = \arg a - \arg b$;

Fogalmak: Az úgynevezett **n -edik komplex egységgyökök** ($n \geq 2$) az 1 komplex n -edik gyökei, azaz a

$$\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \quad (k = 0, 1, \dots, n-1)$$

komplex számok, amelyek a Gauss-féle számsíkon az egységkörnek szabályos n -szöget alkotó pontjai. Ezek közül speciálisak azok, amelyek hatványaiként előáll az összes többi n -edik egységgyök: ezek a **primitív n -edik egységgyökök**.

KOMPLEX
EGYSÉGGYÖKÖK

Legyen $E_n = \{\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \in \mathbb{C} | k = 0, 1, \dots, n-1\}$. Az ε_k egységgyök primitív pontosan akkor, ha $(k, n) = 1$. Az $(E_n, \cdot)$ n -edrendű ciklikus csoport. Továbbá, $\sum_{k=0}^{n-1} \varepsilon_k = 0$.

Ha $(K, +, \cdot)$ és $(N, +, \cdot)$ test, $K \subseteq N$, K -beli elemek összege és szorzata mindkét testben ugyanazok, akkor azt mondjuk, hogy K az N **résztest**e, ill. N a K **bővítése**, és az $N|K$ testbővítéstől beszélünk. Ha $a \in N$, akkor a **transzcendens elem K fölött**, ha a nem gyöke egyetlen $K[x]$ -beli nemnulla polinomnak sem. Ha létezik $0 \neq f(x) \in K[x]$, hogy $f(a) = 0$, akkor a -ról azt mondjuk, hogy **algebrai elem a K test fölött**. Ha az N test összes eleme algebrai K fölött, akkor N -t a K **algebrai bővítésének** nevezzük. Ha K egyetlen algebrai bővítése önmaga, azt mondjuk, hogy **algebrailag zárt test**.

Fogalmak:
résztest,
testbővítés,
transzcendens
elem, algebrai
elem, algebrai
bővítés,
algebrailag zárt
test

- (i) Tetszőleges, legalább elsőfokú $\mathbb{C}[x]$ -beli komplex polinom sorrendtől és egységtényezőitől eltekintve egyértelműen bontható fel elsőfokú komplex polinomok szorzatára.
- (ii) $\mathbb{C}$ algebrailag zárt.

KLASSZIKUS
ALGEBRA
ALAPTÉTELE

4.2. Galois testek

Ha $(R, +, \cdot)$ és $(S, +, \cdot)$ gyűrű, $f : R \rightarrow S$, hogy bármely $a, b \in R$ -re $f(a + b) = f(a) + f(b)$, $f(ab) = f(a)f(b)$, akkor azt mondjuk, hogy f gyűrűk **homomorfizmusa**, ha még injektív, szürjektív ill. bijektív is, akkor **monomorfizmusnak**, **epimorfizmusnak**, ill. **izomorfizmusnak** hívjuk, és a legutóbbi esetben azt mondjuk, hogy R és S **izomorf gyűrűk**. Keressük a véges K testeket, amelyeket szokás **Galois-test**eknek is nevezni. Ilyenek a Z_p maradékosztálygyűrűk, p prímszám. Az olyan testet, amelynek részteste csak önmaga, **prímtestnek** hívjuk.

Fogalmak:
homomorfizmus,
monomorfizmus,
epimorfizmus,
izomorfizmus,
izomorf gyűrűk,
Galois-test,
prímtest

Az összes prímtest az alábbiak egyikével izomorf: $\mathbb{Q}$ és Z_p , ahol p prímszám.

PRÍMTESTEK

K -ban az 1 egész számú többszörösei alkotnak egy integritástartományt, ennek T hányadosteste egy prímtest, azaz $T = Z_p$ valamely p prímszámmra. K prímteste fölött véges n dimenziós vektortér, mint ilyen izomorf Z_p^n -nel, aminek rendje p^n . A $Z_p[x]$ polinomgyűrűben analóg elmélet építhető ki a modulo $m(x)$ kongruenciára mint az egészeknél, és könnyen látható, hogy ha $q(x) \in Z_p[x]$ n -edfokú irreducibilis polinom, akkor a $Z_p[x]/(q(x))$ faktorgyűrű test, rendje p^n .

Ha K véges test, akkor a K test karakterisztikája p prímszám és $|K| = p^n$ valamely $n \in \mathbb{N}^+$ -ra. Megfordítva, ha p prímszám és $n \in \mathbb{N}^+$, akkor izomorfíattól eltekintve egyértelműen létezik p^n -elemű $\text{GF}(p^n)$ test. $U(\text{GF}(p^n))$ $p^n - 1$ -edrendű ciklikus csoport.

VÉGES
TESTEK

Legyen $K = \text{GF}(5^3)$. Keresnünk kell egy harmadfokú irreducibilis polinomot Z_5 fölött, $q(x) = x^3 + x + 1 \in Z_5[x]$ ilyen. Ha $q(a) = 0$, akkor $K = Z_5 + aZ_5 + a^2Z_5$ 3-dimenziós vektortér. Legyen $u = a^2 + 3a + 4$, $v = a^2 + 2a + 1 \in K$. Ekkor $u(x)v(x) = x^4 + x^2 + x - 1$, ami modulo $q(x)$ -1-gyel kongruens, azaz $\frac{1}{u} = -v$. Hogyan lehet reciprokot számolni K -ban? Az $u(x)f(x) \equiv 1 \pmod{q(x)}$ kongruencia egyenletet kell megoldani. Hogyan lehet generálóelemet keresni a ciklikus csoportban? Olyan $g(x) \in Z_5[x]$ legfőbb másodfokú polinomot kell keresni, hogy $g(x)^{62} \equiv -1 \pmod{q(x)}$ (a próbálgatások $g(x) = x, x + 1, x + 2, x + 3, x + 4$ voltak). A kész rutinjainkkal ez egyszerű.

```
char =5;
q=x^3+x+1; u=x^2+3*x+4; v=x^2+2*x+1;
mop(q,3,u*v,4); [x+5,10*x^2+5*x-1]
euxp(u,2,q,3); [x^2+2*x+1,-x,-1]
mop(q,3,(x+4)^62,62); [3x^58+...,-1]
```

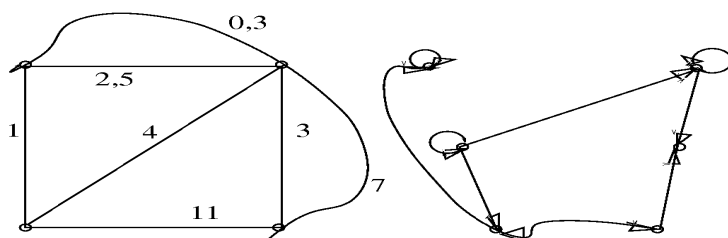
5. fejezet

Gráfelmélet

5.1. Alapfogalmak

Legyen $\emptyset \neq V$ és E halmazok, $g : E \rightarrow \{P \subseteq V \mid |P| = 1 \text{ vagy } 2\}$. Ekkor a $G = (V, E, g)$ hármaszt **gráfnak**, V elemeit a **gráf csúcspontjainak**, g -t az **incidencia leképezésnek**, $f \in E$ elemeket a **gráf éleinek**, $g(f)$ elemeit az **él csúcspontjainak**, ha $g(f)$ egyelemű, **hurokélnek** hívjuk. Azt a gráfot, amelyben Img minden eleme kételemű és g injektív, **egyszerű gráfnak**, amelyben V véges halmaz, **véges gráfnak** nevezzük. Véges gráfot szemléltethetjük diagrammjával, amely a csúcspontoknak a tér pontjait, éleinek a csúcspontokat összekötő görbeszakaszokat feleltet meg. A $G = (V, E, g, w)$ négyest **súlyozott gráfnak** nevezzük, ha (V, E, g) gráf és $g : E \rightarrow R$. A $w(e)$ számot az **e él súlyának** hívjuk. A $G = (V, E, g)$ hármaszt **irányított gráfként** említjük, ha $\emptyset \neq V$ és E halmazok, $g : E \rightarrow V \times V$. Ha $g(f) = (v_1, v_2)$, akkor azt mondjuk, hogy

Fogalmak: gráf, gráf csúcspontja, incidencialeképezés, gráf élei, él csúcspontjai, hurokél, egyszerű gráf, véges gráf, súlyozott gráf, él súlya, irányított gráf, él kezdő (vég-) pontja, fokszám, szomszédos csúcspontok



5.1. ábra. Súlyozott gráf és irányított gráf hurokélekkel

v_1 az f **él kezdőpontja**, v_2 az f **él végpontja**. A $G = (E, V, g)$ véges

gráfban a v pont $d(v)$ fokszáma azon f élek száma, hogy $v \in g(f)$, a hurokéleket kétszer számolva. Azt mondjuk, hogy $v, w \in V$ szomszédos csúcsponatok, ha $v = w$ vagy létezik $f \in E$, hogy $g(f) = \{v, w\}$.

EULER
TÉTELE

Véges gráfban a csúcsponatok fokszámainak összege $2|E|$.

Bizonyítás.

Hiszen, minden élt, köztük a hurokéleket is, kétszer számoljuk bele a $\sum_{v \in V} d(v)$ összegbe.

Q.E.D.

FOKSZÁM
REALIZÁCIÓ

Ha adva van fokszámnak $l : \underline{c} \rightarrow \mathbb{N}$ listája, pontosan akkor létezik $G = (V, E, g)$ gráf, hogy $V = \{v_1, v_2, \dots, v_c\}$, $d(v_i) = l(i)$ ($1 \leq i \leq c$), ha $\sum_{i \in \underline{c}} l(i)$ páros.

Bizonyítás.

Hiszen, a szükségesség következik az Euler tételből. Legyen $\sum_{i \in \underline{c}} l(i)$ páros. Ha $n = 1$, akkor $l(i)/2$ hurokélből álló gráf megfelel. Alkalmazzunk indukciót c -re. Tegyük fel, hogy $c > 2$, és $c - 1$ -re igaz az elégségesség. Ha $\sum_{i \in \underline{c-1}} l(i)$ és $l(c)$ is páratlan, akkor legyen $l(t) \neq 0$ valamely $1 \leq t \leq c - 1$ -re, és $l_0 : \underline{c-1} \rightarrow \mathbb{N}$ különbözzön l -től csak abban, hogy $l_0(t) = l(t) - 1$, és legyen G_0 az l_0 -hoz tartozó gráf. A keresett gráfot úgy kapjuk meg, hogy G_0 -t kiegészítjük a v_c ponttal, egy $\{v_t, v_c\}$ éllel és $\frac{l(c)-1}{2} \{v_c\}$ hurokéllal. Ha $\sum_{i \in \underline{c-1}} l(i)$ és $l(c)$ is páros, akkor az $l : \underline{c-1} \rightarrow \mathbb{N}$ leképezéshez tartozó gráfot kiegészítjük a v_c ponttal és $\frac{l(c)}{2}$ darab $\{v_c\}$ hurokéllal.

Q.E.D.

GALLAI-ERDŐS

Legyen $l : \underline{c} \rightarrow \mathbb{N}$ csökkenő lista. l -hez pontosan akkor létezik $G = (V, E, g)$ véges egyszerű gráf, hogy $V = \{v_1, v_2, \dots, v_c\}$, $d(v_i) = l(i)$ minden $1 \leq i \leq c$ -re, ha $\sum_{i \in \underline{c}} l(i)$ páros és $\sum_{i \in \underline{k}} l(i) \leq k(k-1) + \sum_{i=k+1}^c \min\{k, l(i)\}$ minden $1 \leq k \leq c$ -re.

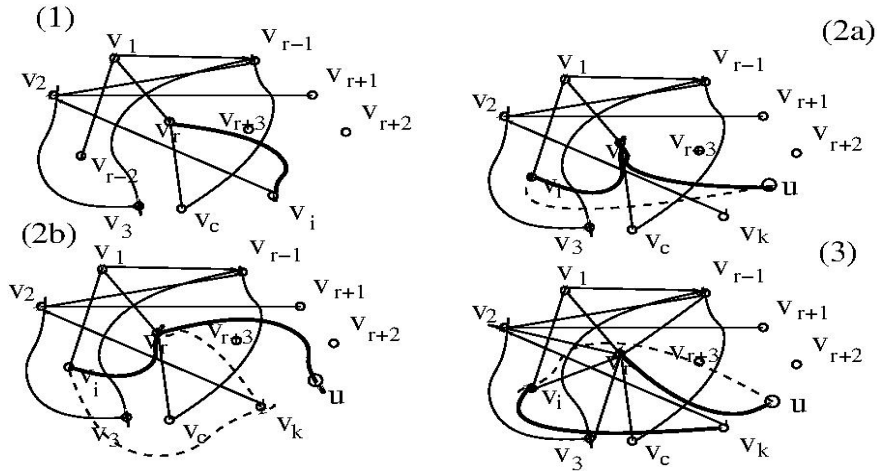
Bizonyítás.

Hiszen, a szükségesség nyilvánvaló az előző tételből és abból, hogy a jobb oldal az első k csúcsponat egymás közötti élekből adódó maximális foksámösszeg plusz a többi csúcsponat maximális hozzájárulása az első k csúcsponat foksámösszegéhez. Az elégségességhez legyen a $G_0 = (V_0, E_0, g_0)$ egyszerű gráf egy alsó realizációja az l foksámlistának ha $V_0 = \{v_1, v_2, \dots, v_c\}$, $d(v_i) \leq l(i)$ ($i \in \underline{c}$).

A kiinduló G_0 alsó realizációban ne legyen egyetlen él sem. Egy alsó realizációban a kritikus r index legyen a legnagyobb index, hogy $d(v_i) = l(i)$ ha $1 \leq i < r$. Feltehetjük, hogy l nem konstans 0. Kezdetben tehát $r = 1$, a következő alsó realizáció $G_1 = (V_1, E_1, g_1)$ olyan, hogy az $l(r) - d(v_r)$ eltérés csökken, míg a v_i , $i < r$ csúcsponatok foksámjai nem változnak. A folyamat csak akkor áll le, ha l realizációját kapjuk.

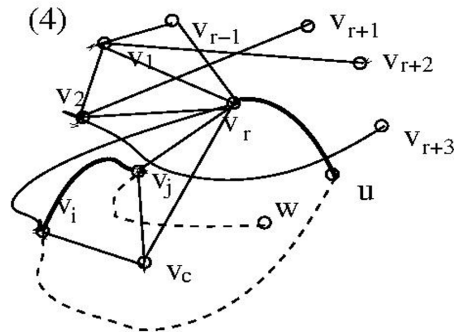
Legyen $S = \{v_{r+1}, v_{r+2}, \dots, v_c\}$. Fenntartjuk a feltételt, hogy S -en belül nincsenek élek.

(1) Van olyan v_r -rel nem szomszédos v_i , hogy $d(v_i) < l(i)$ (G_0 -ban). Legyen $E_1 = E_0 \cup \{g_1^{-1}(\{v_r, v_i\})\}$.



5.2. ábra. A G_1 alsó közelítés konstrukciójának esetei: (1) $v_i \neq v_r$, $d(v_i) < l(i)$; (2) $v_i \neq v_r$ ($i < r$), $l(r) - d(v_r) \geq 2$ vagy $= 1$; (3) $d(v_k) \neq \min\{r, l(k)\}$

(2) Valamely $i < r$ -re v_r és v_i nemszomszédosak. Mivel $d(v_i) =$



5.3. ábra. A G_1 alsó közelítés konstrukciójának (4) esete: minden $i < r$ -re $v_i - v_r$ de valamely $i < j < r$ -re $v_i \neq v_j$

$l(i) \geq l(r) > d(v_r)$, létezik u v_i -vel szomszédos csúcspont, amely nemszomszédos v_r -rel. Ha $l(r) - d(v_r) \geq 2$, akkor legyen $E_1 = (E_0 \cup \{g_1^{-1}(\{u, v_r\}), g_1^{-1}(\{v_i, v_r\})\}) \setminus \{g_0^{-1}(\{u, v_i\})\}$. Ha $l(r) - d(v_r) = 1$, akkor miivel $\sum_{i=1}^c l(i) - \sum_{i=1}^c d(v_i)$ páros, valamely $k > r$ indexre $d(v_k) < l(k)$. Az (1) eset alkalmazható kivéve ha v_r és v_k szomszédosak, ebben az esetben legyen $E_1 = (E_0 \cup \{g_1^{-1}(\{u, v_r\}), g_1^{-1}(\{v_i, v_r\})\}) \setminus \{g_0^{-1}(\{v_r, v_k\}), g_0^{-1}(\{u, v_i\})\}$.

(3) $v_1, \dots, v_{r-1}$ szomszédosak v_r -rel és $d(v_k) \neq \min\{r, l(k)\}$ valamely

$k > r$ -re. Mivel G_0 alsó realizáció, $d(v_k) \leq l(k)$. Mivel S -en belüli élek nincsenek, $d(v_k) \leq r$. Így $d(v_k) < \min\{r, l(k)\}$, és (1) alkalmazható, kivéve ha v_k és v_r szomszédosak. Mivel $d(v_k) < r$, létezik $i < r$ hogy v_k és v_i nemszomszédosak. Mivel $d(v_i) > d(v_r)$, létezik v_i -vel szomszédos de v_r -rel nemszomszédos u csúcspon, legyen $E_1 = (E_0 \cup \{g_1^{-1}(\{u, v_r\}), g_1^{-1}(\{v_i, v_k\})\}) \setminus \{g_0^{-1}(\{u, v_i\})\}$. (4) $v_1, \dots, v_{r-1}$ szomszédosak v_r -rel és létezik nemszomszédos v_i és v_j valamely $i < j < r$ -re. Mivel $d(v_i) \geq d(v_j) > d(v_r)$, létezik v_i -vel szomszédos $u \in S$ csúcspon, amely nemszomszédos v_r -rel, és létezik v_j -vel szomszédos $w \in S$ csúcspon, amely nemszomszédos v_r -rel, $u = w$ lehetséges. Legyen

$$E_1 = (E_0 \cup \{g_1^{-1}(\{v_i, v_j\}), g_1^{-1}(\{u, v_r\})\}) \setminus \{g_0^{-1}(\{u, v_i\}), g_0^{-1}(\{w, v_j\})\}.$$

(5) Ha (1)-(4) egyike sem alkalmazható, akkor $v_1, \dots, v_r$ páronként szomszédosak és $d(v_k) = \min\{r, l(k)\}$ hacsak $k > r$. Mivel S -en belül nincsenek élek, $\sum_{i=1}^r d(v_i) = r(r-1) + \sum_{k=r+1}^c \min\{r, l(k)\}$. A tétel feltétele szerint $\sum_{i=1}^r l(i)$ a jobb oldalnál nem nagyobb, ezért ekkor már eltűnt az $l(r) - d(v_r)$ eltérés. Növeljük eggyel r -t hacsak nem $r = c$.

Q.E.D.

Fogalmak: séta,
séta
kezdőpontja,
séta végpontja,
vonal, út, zárt
séta,
összekötött

Egy $s : \underline{2n+1} \rightarrow V \cup E$ listát $n \in \mathbb{N}^+$ hosszú $s(1)$ **kezdőpontú** és $s(2n+1)$ **végpontú sétának** nevezzük, ha

$$s = [v_1, e_2, v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1}] \text{ és } g(e_{2i}) = \{v_{2i-1}, v_{2i+1}\} \ (1 \leq i \leq n).$$

Ha az $s : \underline{2n+1} \rightarrow V \cup E$ séta élei között nincs ismétlődés, **vonálnak**, ha a séta csúcspontjai között nincs ismétlődés, **útnak** hívjuk. Ha $s(1) = s(2n+1)$, akkor a sétát **zárt sétának** nevezzük. Zárt út esetén v_1 -re és v_2 -re nem feltétel a különbözőség. Azt mondjuk, hogy $v, w \in V$ **összekötöttek**, ha $v = w$ vagy létezik v kezdőpontú és w végpontú út,

ÖSSZEFÜGGŐSÉG jelölés: $(v, w) \in P_G$.

RELÁCIÓ

Ha $G = (V, E, g)$ gráf, akkor P_G ekvivalencia.

Bizonyítás.

Hiszen, a reflexivitás nyilvánvaló. Legyen $(v, w) \in P_G$, $v \neq w$, $s = [v_1 = v, e_2, v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1} = w]$ út, vagyis a v_i -k különbözők. De ekkor az $s' = [v_{2n+1} = w, e_{2n}, v_{2n-1}, \dots, v_3, e_2, v_1 = v]$ útban is a v_i -k különbözők, és $(w, v) \in P_G$, a szimmetriát belátuk. Végül lássuk be a tranzitivitást, legyen $(v, w) \in P_G$, $(w, z) \in P_G$. Ha valamely kettő egybeesik, nincs mit belátni, ezért feltehető, hogy mindhárom különböző. Legyen $r = [u_1 = v, e_2, u_3, \dots, u_{2m-1}, e_{2m}, u_{2m+1} = w]$ $s = [v_1 = w, f_2, v_3, \dots, v_{2n-1}, f_{2n}, v_{2n+1} = z]$ utak hogy az u_i -k különbözők, és a v_i -k is különbözők. Ha w -t kivéve mind az összes csúcspon különböző, akkor a $\pi : \underline{2(m+n)+1} \rightarrow V \cup E$, $\pi(i) = r(i)$ ha $1 \leq$

$i \leq 2m + 1$, $\pi(2m + i) = s(i)$ ha $1 \leq i \leq 2n + 1$ szintén út, ahonnan $(v, z) \in P_G$. Legyen $1 \leq i_1 \leq 2m - 1$ a legkisebb index, hogy $u_{i_1} = v_{j_1}$ valamely j_1 -re, kapjuk, hogy $\pi = [v = u_1, e_1, \dots, e_{i_1-1}, u_{i_1} = v_{j_1}, f_{j_1+1}, \dots, f_{2n}, v_{2n+1} = z]$ út, $(v, z) \in P_G$.

Q.E.D.

A P_G reláció ekvivalenciaosztályait **gráf összefüggőségi komponenseinek** nevezzük, és ha egyetlen ilyen van, azaz $P_G = V \times V$, akkor G -t **összefüggő gráfnak** hívjuk. A $G_0 = (V_0, E_0, g_0)$ gráfról azt mondjuk, hogy a $G = (V, E, g)$ gráf **részgráfja**, ha $V_0 \subseteq V$, $E_0 \subseteq E$ és $f \in E_0$ -ra $g_0(f) = g(f)$.

Fogalmak:
összefüggőségi
komponens,
összefüggő gráf,
részgráf

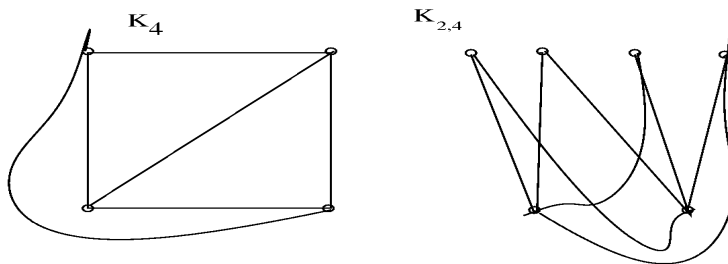
Legyen C a $G = (V, E, g)$ gráf egy összefüggőségi komponense, $E_C = \{e \in E \mid g(e) \cap C \neq \emptyset\}$, $e \in E_C$ -re $g_C(e) = g(e)$. Ekkor $G_C = (C, E_C, g_C)$ a G gráf részgráfja.

KOMPONENS
RÉSZGRÁF

Hiszen, ha $f \in E$ -re $g(f) \cap C \neq \emptyset$, akkor $g(e) \subseteq C$.

Bizonyítás.

Fogalmak: üres
gráf, teljes gráf,
közműgráf,
körgráf



5.4. ábra. A K_4 teljes gráf és a $K_{2,4}$ közműgráf

Speciális gráfok a $(V, \emptyset, \emptyset)$ az **üres gráf**, $K = (V, E, g)$ **teljes gráf**, ha $\text{Img} = \{P \subseteq V \mid |P| = 2\}$. Ha $|V| = c$, akkor a teljes gráf kelőlése K_c . $K_{c,d} = (V, E, g)$ **közműgráf** ha $V = V_1 \cup V_2$ diszjunkt unió, $|V_1| = c$, $|V_2| = d$ és $\text{Img} = \{\{v_1, v_2\} \mid v_1 \in V_1, v_2 \in V_2\}$. $C_c = (V, E, g)$ $n \in \mathbb{N}^+$ **hosszú körgráf**, ha $V = \{v_1, v_2, \dots, v_c\}$, $E = \{e_1, e_2, \dots, e_c\}$, $g(e_i) = \{v_i, v_{i+1}\}$ ($1 \leq i \leq c - 1$) és $g(e_c) = \{v_1, v_c\}$.

Tetszőleges véges egyszerű G gráfban, amelynek legalább két csúcspontja van, létezik két azonos fokszámú csúcspont.

KÉZFOGÁS

Hiszen, legyen $G = (V, E, g)$, $|V| = c$. Ha $|G| = 1$ akkor nincs mit belátni, feltehetjük, hogy $|G| > 1$. Legyen összefüggő, akkor nincs 0 fokszámú csúcspont, és $\text{Imd} \subseteq \underline{c-1}$, így a c számú csúcspont nem lehet mind különböző fokszámú. Ha G nem összefüggő, akkor nincs $c - 1$ fokszámú csúcspont, és $\text{Imd} \subseteq \{0, 1, \dots, c - 2\}$, így a c számú csúcspont ekkor sem lehet mind különböző fokszámú.

Bizonyítás.

Q.E.D.

5.2. Fák és erdők

Fogalmak: További speciális gráfokat tekintünk. A G gráfot **erdő**nek hívjuk, ha véges, egyszerű és nem tartalmaz kört, az összefüggő erdőt **fagráf**nak hívjuk. Azonnal látjuk, hogy erdő összefüggőségi komponense fagráf.

FAGRÁFOK
ÉLEI, CSÚCSAI

Legyen $G = (V, E, g)$ fagráf, $|V| = c > 1$, $|E| = e$.

(i) G -ben van legalább két elsőfokú csúcs;

(i) $e = c - 1$.

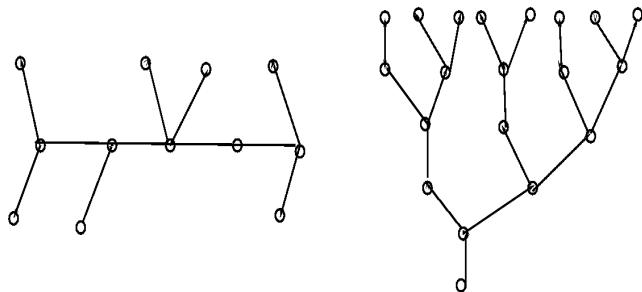
Bizonyítás. Hiszen, tegyük fel, hogy G -ben legföljebb egy csúcspont fokszáma 1. Legyen $s = [v_1, e_2, v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1}]$ maximális hosszú út G -ben, ami nem kör. Mivel egyszerre a kezdő és a végpont fokszáma nem lehet 1, valamelyikre, például a végpontra, $d(v_{2n+1}) > 1$, és lennie kell $w \in V$ csúcspontnak, hogy az $f = \{v_{2n+1}, w\} \in E$ él nem szerepel az s útban. Legyen $s' = [v_1, e_2, v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1}, f, w]$. Ha w csak egyszer fordul elő s' -ben, akkor s' eggyel hosszabb út, mint s ami lehetetlen. Ha $w = v_{2i+1}$ valamely $1 \leq i \leq n-1$ -re, akkor $[w, e_{2i+2}, v_{2i+3}, \dots, v_{2n-1}, e_{2n}, v_{2n+1}, f, w]$ kör, ami ellentmondás. (i)-gyel készen vagyunk.

(ii) Keressünk egy $s_1 = [v_1, e_2, v_3, \dots, v_{2m-1}, e_{2m}, v_{2m+1}]$ maximális utat G -ben, erre a részgráfra teljesül az állítás, nevezzük ezt ágnak. Az előző gondolatmenet szerint $d(v_1) = d(v_{2n}) = 1$. Ha $w_1 = v_{2i+1}$ ($1 < i < n$) fokszáma 2-nél nagyobb, akkor innen is kiindul egy $s_2 = [w_1, f_2, w_3, \dots, w_{2n-1}, f_{2n}, w_{2n+1}]$, az előzőleg bejárt részgráffal csak a w_1 közös csúcspontot tartalmazó maximális út, újabb ág, ami e -hez is és c -hez is n -nel járul hozzá, azaz a már bejárt ágakhoz ezt is hozzátevé a kapott részgráfra állítás továbbra is fennáll. Ezt az eljárást folytatva kimerítjük a teljes G gráfot.

Q.E.D.

Fogalmak:
minimálisan
összefüggő gráf,
maximálisan
körmentes gráf

A $G = (V, E, g)$ összefüggő gráfról azt mondjuk, hogy **minimálisan összefüggő gráf**, ha minden $e \in E$ -re igaz, hogy elhagyása után már kapottt gráf nem összefüggő. A $G = (V, E, g)$ körmentes gráfról azt mondjuk, hogy **maximálisan körmentes gráf**, bármely $v, w \in V$ -re a $\{v, w\}$ éllel kibővítve E -t kört kapnánk.



5.5. ábra. Hernyógráf és hím méhecske (csak anyjuk van) leszármazási gráfja, bináris fa, az n . szinten f_{n+1} felmenő van, ahol f_n a Fibonacci-sorozat

Legyen $G = (V, E, g)$ véges egyszerű gráf $|V| = c$, $|E| = e$. Ekkor a következő állítások ekvivalensek.

FÁK
JELLEMZÉSE

- (i) G fa;
- (ii) G minimálisan összefüggő;
- (iii) G maximális körmentes;
- (iv) G összefüggő és $e = c - 1$;
- (v) G körmentes és $e = c - 1$;

Hiszen, az eddigiekből világos, hogy fagra teljesül (ii)-(v). Nyilván $c > 1$ feltehető. Ha (ii) igaz, akkor csak azt kell belátni, hogy G körmentes. Ha G -ben van $s = [v = v_1, e_2, v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1} = v]$ kör, akkor a minimalitás miatt e_1 -et elvéve az összefüggőség már nem teljesülhetne, de a végpont is v ezért marad ugyanabban a komponensben mint volt, ami az egész V .

Ha (iii) igaz, akkor azt kell belátni, hogy G összefüggő. Tegyük fel, hogy C_1, C_2 két különböző összefüggőségi komponens, $v \in C_1, w \in C_2$. A maximalitás miatt E -t kibővítve az $\{v, w\}$ éllel kapunk egy $s = [v = v_1, e_2, w = v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1} = v]$ kört, ami lehetetlen, mivel $s_0 = [w = v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1} = v]$ út lenne G -ben, ami ellentmond annak, hogy v és w különböző komponensekből valók.

Ha (iv) igaz, be kell látni, hogy G körmentes. Legyen $p = [v = v_1, e_2, w = v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1} = v]$ kör G -ben, ebben n csúcspont és n él van. Ha p tartalmazza az összes csúcspontot, akkor $c = n$ és $e \geq n = c > c - 1$, ami ellentmondás. Ha p nem tartalmazza az összes csúcspontot, akkor először bővítsük az élek halmazát a p csúcspontjai közötti összes éllel, az élek száma nem lesz kisebb, mint

a csúcsok száma. Egyenként bővítsük a csúcspontok halmazát olyan csúcsponttal, ami szomszédos az eddig vizsgált pontokkal, az összefüggőség miatt ilyen létezik. Bővítsük az élek halmazát az új pont és a már vizsgált csúcspontok közötti összes éllel. Az a tulajdonság, hogy élék száma nem lesz kisebb, mint a csúcsok száma, fennmarad. Azonban ez ellentmond annak, hogy $e = c - 1$.

Ha (v) igaz, be kell látni, hogy G összefüggő. Tegyük fel, hogy G nem összefüggő, ekkor a G erdőnek $r > 1$ komponense van, és $e = c - k$, ami ellentmond annak, hogy $e = c - 1$.

Q.E.D.

A $G = (V, E, g)$ véges gráf $G_0 = (V_0, E_0, g_0)$ részgráfját a G feszítőfájának mondjuk, ha $V_0 = V$ és G_0 fa.

FESZÍTŐFA
LÉTEZÉSE

A $G = (V, E, g)$ véges gráfnak pontosan akkor létezik feszítőfája, ha G összefüggő.

Bizonyítás.

Hiszen, a szükségesség triviális. Legyen G összefüggő. A hurokéleket, többszörös éleket elhagyva egy egyszerű G_1 részgráfot kapunk V -n, tegyük fel, hogy tartalmaz kört. Ennek kell körmentes részgráfját konstruálni V -n. Ha az összefüggőséget fenntartva a körök számát élék elvételével csökkenteni tudjuk, készen vagyunk. Legyen $s = [v = v_1, e_2, w = v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1} = v]$ kör G_1 -ben. Ennek hagyjuk el tetszőleges élét, például e_2 -et, az összefüggőség fennmarad, a körök száma csökken.

Q.E.D.

Legyen $G = (V, E, g, w)$ véges egyszerű összefüggő súlyozott gráf. A Kruskal-algoritmus meghatározza G egy minimális összsúlyú feszítőfáját, amely gyakori feladat az alkalmazásokban.

ALGORITMUS:
KRUSKAL

```

ofk:=function(v,gr,n)
  local ko; real array gr[n,n]; ko=[v];
  if not(v<=n) then return("hiba") else
    if n=1 then return([1]) else
      for s=1 to n-1 do
        if length(ko)<s then s=n else
          for j=1 to n do
            if gr[ko[s],j]<>0 and not(j in ko)
              then append(j,ko);fi;od;fi;od;
  return(ko);fi;fi; end;
ofe:=function(gr,n)
  local ko=[]; real array gr[n,n];
  if n=1 then return(1) else ko=ofk(1,gr,n);
  if length(ko)<n then return(0)

```

```

else return(1); fi; fi; end;
kr:=function(gr,n)
  local fa=[], mn,gr1,mnw=0,ti=[],fl,ko;
  real array gr[n,n]; real array gr1[n,n];
  if not(ofe(gr,n)) then return("nem osszefuggo");
  else if n =1 then return([1],0); else
    for i=1 to n do for j=i to n do
      gr1[i,j]=0;gr1[j,i]=0; od; od;
    for i=1 to n do if gr[1,i]<>0 then mn=[1,i];break;fi;
    for s=1 to n-1 do
      fl=1; while fl do for i=1 to n do for j=i+1 to n do
        if gr[i,j]<>0 and gr[i,j]<gr[mn[1],mn[2]]
        and not([i,j] in ti) then mn=[i,j];fi; od; od;
        ko=ofk(mn[2],gr1,n); append(mn,ti);
        if not(mn[1] in ko) then append(mn,fa);
        mnw=mnw+gr[mn[1],mn[2]];
        gr1[mn[1],mn[2]]=1; gr1[mn[2],mn[1]]=1;
        for i=1 to n do for j=i+1 to n do
          if (gr[i,j]<>0 and not(i in ofk(j,gr1,n))
          and not([i,j] in ti)) then
            mn=[i,j];i=n+1;j=n+1;fi;od;od;
          fl=0; fi; od; od;
        return([fa,mnw]); fi; fi; end;

```

5.3. Euler vonal, Hamilton út, Euler formula

Leonard Euler a XVIII.sz-d-ban élt svájci matematikus volt, ő kezdeményezte a gráfelméleti vizsgálatokat. Königsbergben (a mai Kalinyingrád, Orosz Federáció) sétálgatott a Pregel folyó környékén, ahol két kis szigetet hidak kötöttek össze egymással és a belvárossal. Az ötlött eszébe séta közben, hogy be lehet-e járni a környéket úgy, hogy minden hídon pontosan egyszer megyünk át, és ugyanoda érkezünk vissza. A $G = (V, G, g)$ gráfban **Euler vonal**nak nevezünk egy vonalat, amelyik E mindegyik élén áthalad.

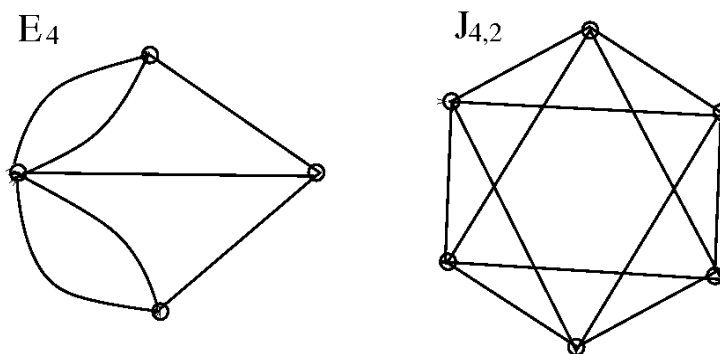
Véges összefüggő gráfban pontosan akkor létezik zárt Euler-vonal, ha minden csúcspont fokszáma páros.

Hiszen, legyen $G = (V, E, g)$ véges összefüggő gráf. Ha $\epsilon : 2n + 1 \rightarrow V \cup E$, $\epsilon = [v_1, e_2, v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1}]$ zárt Euler-vonal, akkor $E =$

Fogalmak:
Euler vonal,
zárt Hamilton
út

KÖNIGSBERGI
HIDAK

Bizonyítás.

5.6. ábra. A königsbergi hidak E_4 gráfja és a $J_{4,2}$ Johnson-gráf

$\{e_2, e_4, \dots, e_{2n}\}$. A hurkok mindig 2-t adnak hozzá a csúcspont fokszámához, $v_1 = v_{2n+1}$ a v_1 fokszámhoz e_1 és e_{2n} 2-vel járul hozzá, a vonal belső v_{2i+1} csúcspontja ($1 \leq i \leq n-1$) fokszámához az ϵ vonalban minden előfordulás 2-t ad hozzá. A szükségesség világos. Megfordítva, legyen minden fokszám páros, és legyen $s : 2n+1 \rightarrow V \cup E$, $s = [v_1, e_2, v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1}]$ a leghosszabb vonal G -ben. Mivel maximális, s átmegy az összes élen, amely v_{2n+1} -et tartalmazza, de $d(v_{2n+1})$ páros, ezért s zárt vonal. Ha s nem tartalmazza az összes élt, akkor van egy e él, amin s nem megy át. G összefüggő, ezért feltehető, hogy $g(e) = \{u, v_{2i+1}\}$ valamely $1 \leq i \leq n-1$ -re, ahonnan kapjuk, hogy $t = [u, e, v_{2i+1}, e_{2i}, v_{2i+1}, \dots, v_{2n+1}, e_2, v_3, \dots, v_{2i+1}]$ eggyel hosszabb vonal, ellentmondás.

Q.E.D.

Látjuk, hogy a königsbergi séta a kívánt módon nem lehetséges, míg a $J_{4,2}$ gráfban van zárt Euler vonal. Ha a séta kezdő és végpontja különböző kell legyen, akkor a fenti gondolatmenetet kissé átformálva kapjuk, hogy a feltétel a nem zárt Euler vonal létezésére az, hogy két csúcspont páratlan fokszámú legyen, a többi páros.

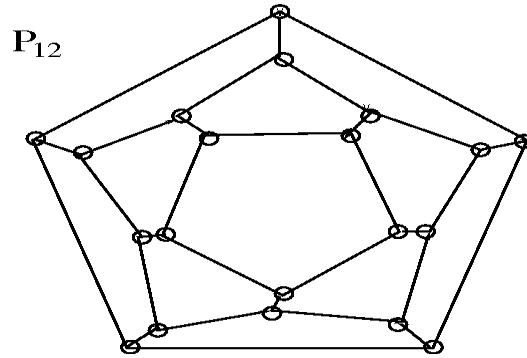
Sir Rowan Hamilton ír matematikus a XIX, szd.-ban alkotott, a következő játékot találta ki, el is készítette fából és forgalmazta. A dodekaéder élgráfját kell bejárni úgy, hogy minden csúcspontot egyszer érintünk, és ugyanoda érkezünk vissza. A $G = (V, E, g)$ gráfban **zárt Hamilton útnak** hívunk egy $s = [v_1, e_2, v_3, \dots, v_{2c-1}, e_{2c}, v_{2c+1}]$ utat, ha $v_1 = v_{2c+1}$ és $|V| = c$.

ORE TÉTEL

Legyen $G = (V, E, g)$ véges egyszerű gráf, $|V| = c$. Ha bármely két nemszomszédos $v, w \in V$ csúcspontra $d(v) + d(w) \geq c$ (*), akkor létezik G -ben zárt Hamilton út.

Bizonyítás.

Hiszen, tegyük fel az ellenkezőjét, és kössünk össze csúcspontokat addig, amíg már tetszőleged két csúcspont összekötése azt jelenti, hogy

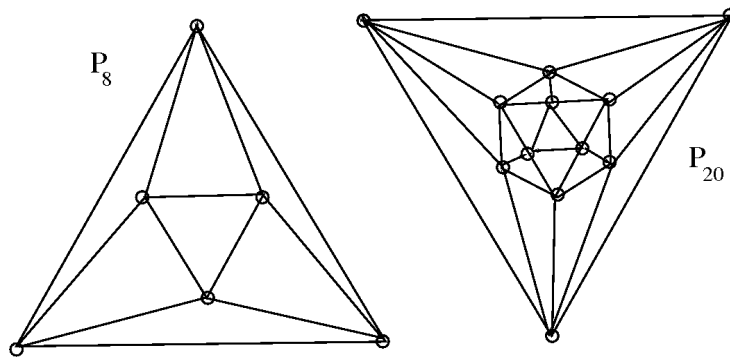
5.7. ábra. A dodekaéder P_{12} élgráfja

zárt Hamilton út létezik. Legyen ez a gráf $H = (V, E', g')$, erre nyilván teljesül (*). H nem lehet K_c teljes gráf, így létezik két nemszomszédos v és w csúcspon, ezeket összekötve éllel már létezne zárt Hamilton út, így H -ban van $h = [v = v_1, e_2, v_3, \dots, v_{2n-1}, e_{2n}, v_{2n+1} = w]$, Hamilton út, innen $E' = \{e_2, e_4, \dots, e_{2n}\}$ n -elemű. Ha v és v_k szomszédosak valamely $3 \leq k \leq 2n - 1$ -re, akkor v_{k-2} és w nemszomszédosak, mivel ellenkező esetben $h' = [v = v_1, e_2, v_3, \dots, v_{k-2}, f, w = v_{2n+1}, e_{2n}, v_{2n-1}, \dots, v_k, f', v_1 = v]$ zárt Hamilton út H -ban, ami ellentmondás. Ezért legalább $d(v)$ csúcspon nemszomszédos w -vel, és $d(w) \leq c - 1 - d(v)$, ami ellentmond (*)-nak.

Q.E.D.

Legyen $G = (V, E, g)$ véges egyszerű gráf, $|V| = c$. Ha bármely $v \in V$ csúcsponra $d(v) \geq \frac{c}{2}$, akkor létezik G -ben zárt Hamilton út.

DIRAC TÉTEL

5.8. ábra. Az oktaéder P_8 és az ikozakaéder P_{20} élgráfja

Található-e zárt Hamilton út a platóni testek élgráfjában? Más feltevésünk is adódhat a platóni testek élgráfjának vizsgálatából, nevezetesen a test csúcspontjai, lapjai ill. élei c , l ill. e számai közötti összefüggéssel kapcsolatosan. Az ikozakaéder esetén $c = 12$, $l = 20$,

$e = 30$, sejtésünk az, hogy $c + l = e + 2$, amelyet egyből ellenőrizhetünk is a többi P_4 , P_6 , P_8 és P_{12} gráfokon, látjuk, hogy ezekre is igaz. Azt mondjuk, hogy a $G = (V, E, g)$ véges egyszerű gráf **síkgráf**, ha V adott sík pontjainak halmaza, E elemei ezeket összekötő görbeszakaszok, tetszőleges $e \in E$ -re $g(e) = \{v, w\}$, ha v és w az e görbeszakasz két végpontja, és e belseje nem tartalmaz más élek pontjait. Az élek a síkot véges sok részre bontják, ezek közül pontosan egy nemkorlátos, ezt **külső lapnak**, a többi síkrészt belső lapnak nevezzük. Jelölje a G síkgráf csúcspontjai, lapjai ill. élei számát c , l ill. e .

EULER
FORMULA

A $G = (V, E, g)$ síkgráfban $c + l = e + 2$.

Bizonyítás.

Hiszen, legyenek az élek gátak, amelyek a belső lapokat választják el, a külső lapban víz van, innen akarjuk elárasztani a belső részt a lehető legkevesebb él elvételével. Egy él elvételével eggyel nő az elárasztott lapok száma, ezért $l - 1$ él elvétele szükséges. Hány gát maradt? Kezdetben mindegyik csúcspontról mindegyik csúcspontra el lehetett jutni a gátakon menve, és ez megmarad, mive egy vizes és egy száraz lap közötti élt veszünk el, és az elvett élt kikerülhetjük az éppen elárasztott lapon körbemenve. Továbbá, bármelyik csúcspontról a másikba pontosan egy út vezet, mivel ellenkező esetben lenne egy zárt út, amely belsejében nem lehet víz. Képzeljük el, hogy mindegyik csúcspontra egy katona áll, egyikük a parancsnok, akinek a fütytelére mindegyik közlegény elindul a parancsnok felé az egyetlen lehetséges úton. A parancsnok újabb fütytelére a közlegények megállnak úgy, hogy egyikük sem érte el még az első csúcspontra. Mindegyikük más-más gáton van, mivel ellenkező esetben lenne a közös gáton két útjuk a parancsnok felé. Üresen nem lehet egyik gát sem, mivel mivel ellenkező esetben lenne zárt út az üres él két végpontjában álló katona útjait összekapcsolva. Vagyis, a megmaradt élek száma $c - 1$.

Q.E.D.

5.4. Síkbaágyazhatóság, síkgráfok színezése

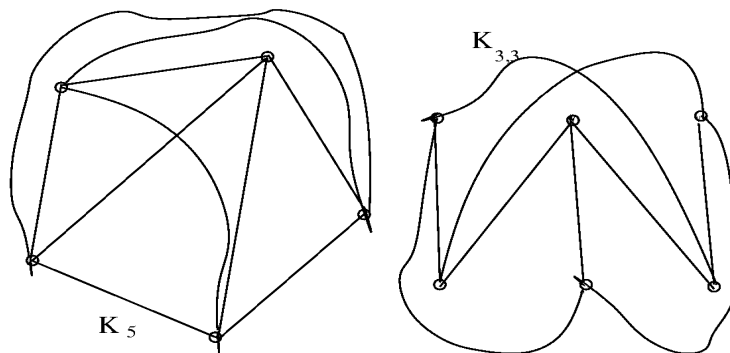
Fogalmak:
izomorf gráfok,
síkbaágyazható
gráf, gráf
színezése,
kromatikus
szám

Látjuk, hogy a K_5 teljes gráfot és a $K_{3,3}$ közműgráfot akárhogyan próbáljuk lerajzolni síkban úgy, hogy élek ne messék egymást, ez az utolsó élen mindig elbukik. Amikor minimális a metszéspontok száma, azaz 1, mint az ábrán, az Euler formula teljesüléséhez még egy csúcspontra kellene hozzávenni, mivel ezzel az élek száma is nő 2, K_5 -nél $c = 5$, $l = 8$, $e = 10$, $K_{3,3}$ -nál $c = 6$, $l = 6$, $e = 9$. Azt mondjuk, hogy $G = (V, E, g)$ és $G' = (V', E', g')$ **izomorf gráfok**, ha létezik izomorfizmusnak hívott $\varphi : V \rightarrow V'$ bijekció, hogy $E' = \{g'^{-1}(\{\varphi(v)\}) | \{v\} \in E\} \cup$

$\{g^{-1}(\{\varphi(v), \varphi(w)\}) \mid \{v, w\} \in E\}$, jelölés $G \cong G'$. Azt mondjuk, hogy $G = (V, E, g)$ **síkbaágyazható gráf**, ha izomorf egy síkgráffal. Mint fentebb láttuk, K_5 és $K_{3,3}$ nem ágyazható síkba.

A $G = (V, E, g)$ véges egyszerű gráf síkbaágyazható pontosan akkor, ha nem tartalmaz K_5 -tel vagy $K_{3,3}$ -mal izomorf részgráfot.

KURATOWSKI
TÉTEL



5.9. ábra. A K_5 teljes gráf és a $K_{3,3}$ közműgráf

Legyen $G = (V, E, g)$ véges gráf, S véges halmaz, amelynek elemeit színeknek nevezzük. Az $k : V \rightarrow S$ leképezést a G **gráf színezése**, ha $k(v) \neq k(w)$ minden szomszédos $v, w \in V$ esetén. Azt a legkisebb $\chi(G) \in \mathbb{N}$ számot, amelyre létezik G -nek $k : V \rightarrow S$, $|S| = \chi(G)$ színezése, a G **gráf kromatikus számának** nevezzük, és azt mondjuk, hogy G **$\chi(G)$ -színezhető**. Nevezetes a térképszínezési probléma. A térkép országai legyenek a gráf csúcspontjai, az egymással határos országoknak megfelelő csúcspontokat kösse össze él. A kapott gráf síkbaágyazható.

$G = (V, E, g)$ síkbaágyazható gráfra $\chi(G) \leq 4$.

A bizonyítás igen bonyolult, jelentős része számítógéppel történt, véges, de nagyon sok esetet áttekintve.

NÉGYSZÍNTÉTEL

$G = (V, E, g)$ síkbaágyazható gráfban a minimális fokszám legfeljebb 5.

FOKSZÁM
MINIMUM

Hiszen, tegyük fel, hogy G minden csúcspontjának fokszáma legalább

Bizonyítás.

6. Egy összefüggő síkgráf, amelyben az élek száma maximális, nyilván trianguláció, ahol is $e = 3c - 6$. Mivel $\sum_{v \in V} d(v) = 2e$ G -ben, egyrészt $2e \leq 6c - 12$, másrészt $2e = \sum_{v \in V} d(v) \geq 6c$, ellentmondás.

Q.E.D.

$G = (V, E, g)$ síkbaágyazható gráfra $\chi(G) \leq 5$.

ÖTSZÍNTÉTEL

Hiszen, ha $|V| = 5$, az állítás világos. Legyen $V = c \geq 6$, alkalmazunk indukciót c -re. Feltehetjük, hogy G egyszerű, összefüggő. Az előző állítás miatt van egy v csúcspontja, hogy $d(v) \leq 5$. Ha $d(v) \leq 4$, akkor G' legyen a v és a v -t tartalmazó élek elhagyásával keletkezett gráf.

Bizonyítás.

Ez indukció szerint 5-színezhető. Visszahelyezve v -t kiszínezhetjük szomszédjai színeitől különböző ötödik színnel. Most legyen $d(v) = 5$, v mind az öt szomszédja nem alkothat G K_5 -tel izomorf részgráfját Kuratowski tétele miatt, ezért van nemszomszédos $w, z \in V$ csúcspont. Húzzuk össze w -t és z -t egyetlen ponttá, a kapott G' gráf síkgráf marad, indukció szerint kiszínezhető 5 színnel. Ezt a színezést korrigáljuk úgy, hogy v három másik szomszédja lefoglal 3 színt G' színezésénél, a negyedik színt kaphatja w és z , míg az ötödik szín lehet v színe.

Q.E.D.

GRÖTZSCH
TÉTEL

$G = (V, E, g)$ síkbaágyazható gráfra, amely nem tartalmaz háromszöget, $\chi(G) \leq 3$

ALGORITMUS:
HEURISZTIKUS
SZÍNEZÉS

Bemenet: A gráf $n \times n$ -es szimmetrikus matrix előállítás; Határozzuk meg a fokszámkokat.

Válasszunk ki egy legkisebb fokszámu v_0 pontot;
színe legyen 1;

Amíg nincs kiszínezve az összes csináljuk;

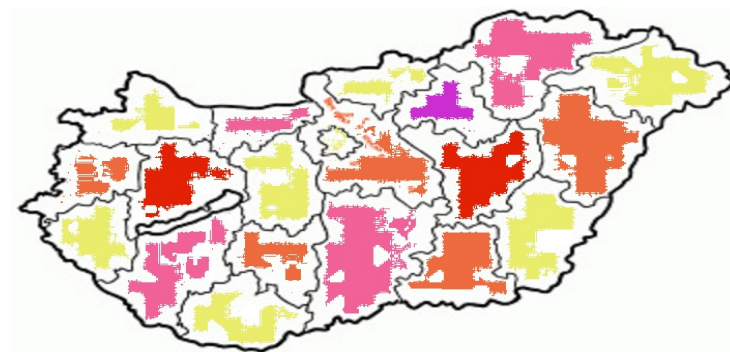
Amíg v_0 szomszédai közül nincs mindegyik
kiszínezve csináljuk;

v_0 nem színes szomszédai közül
a legkisebb fokszámu v_1 ;

v_1 színe legyen az a legkisebb $0 < k \leq n$, amilyen
színű szomszédja nincsen v_1 -nek;

v_0 legyen egy legkisebb fokszámu színtelen pont;

Kimenet: A csúcspontok színei.



5.10. ábra. Megyetérkép heurisztikus színezése öt színnel, a v_0 választások Budapest, Szabolcs, Békés, Nógrád, Baranya, Zala, Győr, Fejér voltak.

Irodalomjegyzék

- [1] Boga Norbert, *Gráfelmélet*. elektronikus jegyzet, www.math.u-szeged.hu/~nboga, SZE, hozzáférés 2018.08.11.
- [2] Diestel, Reinhard, *Graph theory*. Springer, Heidelberg, New York, 1997
- [3] Fuchs László, *Algebra*. Tankönyvkiadó, Budapest, 1981. egyetemi jegyzet
- [4] Halmos Pál, *Lectures on Boolean Algebra*. Van Nostrand, Princeton, 1963.
- [5] Kurdics János. *Algebra alapjai*. Bessenyei Könyvkiadó, Nyíregyháza, 2006. főiskolai jegyzet
- [6] Kurdics János, *Diszkrét matematika*. Bessenyei Könyvkiadó, Nyíregyháza, 2006. főiskolai jegyzet
- [7] Kurdics János, *Algebra I*. Bessenyei Könyvkiadó, Nyíregyháza, 2007. főiskolai jegyzet
- [8] Kurdics János, *Algebra II*. Bessenyei Könyvkiadó, Nyíregyháza, 2007. főiskolai jegyzet
- [9] Maxima, Maxima, a computer algebra system. version 5.27.0, 2012.
- [10] Rosen, Kenneth H. et. al. *Handbook of discrete and combinatorial mathematics*. CRC Press, Boca Raton, 1999.
- [11] Szendrei János, *Algebra and number theory*. Tankönyvkiadó, Budapest, 1978. főiskolai jegyzet.

- [12] Tripathi, Amitabha; Venugopalan, Sushmita és West, Douglas B., *A short constructive proof of the Erdős–Gallai characterization of graphic lists*. Discrete Math. 310, 2010, 843–844.
- [13] Turjányi Sándor, *Bevezetés a kombinatorikába és a gráfelméletbe*. elektronikus jegyzet, www.gyires.inf.unideb.hu, DE, hozzáférés 2018.08.11.
- [14] van der Waerden, Bartel Leendert, *Algebra I, II*. Springer Verlag, New York, Berlin, Heidelberg, 2003.

Definíció index

- G -kongruens, 26
- összeadás, N , 11
- üres gráf, 54
- ábécé, 10
- él csúcspontjai, 50
- él kezdő (vég-) pontja, 50
- él súlya, 50
- összekötött, 53
- átrendezés, 26
- út, 53

- abszorbtív, 6
- additív struktúra, 6
- algebrai elem, 48
- algebrai struktúra,
 - m -műveletes, 4
- algebrai testbővítés, 48
- algebrailag zárt test, 48
- and művelet, 20
- antiszimmetrikus reláció, 2
- asszociált, 29
- asszociatív, 5

- bijektív, 3
- binomiális együttható, 23
- Boole-algebra, 17
- Boole-gyűrű, 21
- Boole-művelet, 20

- ciklikus csoport, 27
- ciklus, 8

- ciklus hossza, 8
- ciklusindex, 27
- csoport, 6
- csoportelem rendje, 8

- Descartes-szorzat, 2
- diofantoszi egyenlet, 34
- diofantoszi egyenlet, elsőfokú
 - kétismeretlenes, 34
- diszjunkció, 16
- diszjunkt ciklusok, 8
- diszjunkt halmazok, 1
- diszjunktív normál forma
 - (d.n.f.), 20
- disztributív, 6

- egész szám osztója, 29
- egész számok gyűrűje, 12
- egyhatározatlanú polinom, 40
- egyhatározatlanú
 - polinomgyűrű, 41
- egyismeretlenes elsőfokú
 - kongruencia egyenlet, 36
- egységelem, 6
- egységelem, hálóa, 17
- egységelemes gyűrű, 6
- egysoros alak típusa, 27
- egyszerű gráf, 50
- ekvivalencia művelet, 20

- ekvivalenciareláció, 2
- előszakasz, 38
- elem képe, relációnál, 2
- elem képe, 3
- elem n -esek egyenlőek, 2
- elempár (n -es) első, második,...
tagja, 2
- elempár egyenlő, 2
- ellentett, 6
- epimorfizmus, 48
- erdő, 55
- Euler vonal, 58
- Euler-féle φ , 26
- függvény, 3
- függvények egyenlőek, 3
- félcsoport, 6
- félháló, 6
- főpolinom, 40
- függvényteljes, 20
- fagráf, 55
- faktorhalmaz, 3
- ferdetest, 6
- fokszám, gráfban, 50
- Galois-test, 48
- Gauss-féle számsík, 47
- gráf, 50
- gráf összefüggőségi komponens,
54
- gráf élei, 50
- gráf csúcspontja, 50
- gráf összefüggő, 54
- gráf színezése, 61
- gyűrű, 6
- háló, 16
- háló, disztributív, 16
- hálószerűen rendezett, 16
- hányados, 30
- hányadostest, 13
- halmaz, 1
- halmaz eleme, 1
- halmazrendszer metszete, 2
- halmazrendszer uniója, 2
- halmaztest, 18
- határozatlan, 40
- hatványhalmaz, 1
- helyiérték, 38
- homomorfizmus, 48
- hurokél, 50
- idempotens, 5
- identikus leképezés, 3
- implikáció művelet, 20
- incidencia leképezés, 50
- injektív, 3
- integritástartomány, 10
- invertálható, 5
- invertálható függvény, 4
- inverzv, 5
- irányított gráf, 50
- irreducibilis elem, 33
- irreducibilis polinom, 43, 44
- ismétlődő szakasz, 38
- izomorf gráfok, 61
- izomorf gyűrűk, 48
- izomorfizmus, 48
- közműgráf, 54
- különbség, 1
- képzetes egység, 45
- képzetes rész, 45
- körgráf, 54
- karakterisztika, 21
- karakterisztikus függvény, 23
- klón, 20
- kombináció, ismétlés nélküli,
23
- kombináció, ismétléses, 24
- kommutatív, 5

- kommutatív (Abel) csoport, 6
- kommutatív félcsoport, 6
- kommutatív gyűrű, 6
- komplementer, 1
- komplementum, 17
- komplex egységgyökök, 47
- komplex gyökvonás, 47
- komplex szám argumentuma, 47
- komplex szám, algebrai alak, 46
- komplex számok teste, 46
- komplex szám abszolútértéke, 45
- kompozíciósorozat, 4
- kongruencia modulo m , 35
- konjugált, 9, 45
- konjugáltsági osztály, 9
- konjunkció, 16
- konjunktív normálforma (k.n.f.), 20
- konkatenáció, 10
- konvergens, 14
- konvolúciósorozás, 41
- kromatikus szám, 61
- l.k.k.t., 32
- legnagyobb közös osztó, 31
- lineáris vagy teljes rendezés, 2
- lista i. tagja, 22
- lista, k hosszú, 22
- művelet, n -változós (n -ér), 4
- művelet, egyváltozós (unér), 4
- művelet, kétváltozós (binér), 4
- maradék, 30
- maradékosztály, 36
- maradékosztálygyűrű, 36
- maximálisan körmentes gráf, 55
- maximum, 16
- maxterm, 20
- megszámlálható, 10
- megszámlálhatatlan, 10
- metszet, 1
- minimálisan összefüggő gráf, 55
- minimum, 16
- mintázat leltár, 28
- minterm, 20
- modulus, 35
- monoid, 6
- monomorfizmus, 48
- multihalmaz, 24
- multiplikatív struktúra, 6
- nand művelet, 20
- negáció művelet, 20
- negatív egész számok, 12
- neutrális elem, 5
- nor művelet, 20
- norma, 45
- nulla, 6
- nullsorozat, 14
- or művelet, 20
- osztályozás, 2
- osztó, 30
- osztandó, 30
- pálya, permutációé, 8
- Peano-axiómák, 10
- permutáció, ismétlés nélküli, 7
- permutáció típuselőállítása, 27
- permutáció, ismétlés nélküli, 22
- permutáció, ismétléses, 23
- polinom asszociáltja, 41
- polinom fokszáma, 40
- polinom helyettesítési értéke, 40
- polinom oszthatósága, 41
- polinomokra l.n.k.o., l.k.k.t., 43
- polinomokra, euklideszi algoritmus, 42

- polinomokra, osztandó, osztó,
 hányados, maradék, 42
 pozitív, 10
 prímelem, 33
 prímpolinom, 43, 44
 prímszám, 33
 prímtest, 48
 primitív n -edik egységgyökök,
 47
 puffer művelet, 20

 részgráf, 54
 részhalmaz, 1
 résztest, 48
 racionális számtest, 13
 recipro, 6
 redukált alak, 10, 13
 redukált maradékosztály, 37
 reflexív reláció, 2
 reláció értékkészlete, 2
 reláció értelmezési tartománya,
 2
 reláció inverze, 2
 reláció képhalmaza, 2
 relatív prímek, 32
 rend, 10
 rendezés $\mathbb{R}$ -é, 15
 rendezési reláció, 2
 rendezés, N -en, 12
 rendezett elempár, elem n -es, 2

 síkbaágyazható gráf, 61
 séta, 53
 súlyozott gráf, 50
 séta kezdőpontja, 53
 séta végpontja, 53
 sorozat, 14
 sorozat határértéke, 14
 szürjektív, 3
 számrendszer alapja, 38
 színezés v. mintázat, 26
 számosság, 4
 szabad csoport, 10
 szabad félcsoport, 10
 szimmetrikus csoport, 7
 szimmetrikus különbség, 1
 szimmetrikus reláció, 2
 szomszédos csúcspontok, 50
 szorzás, N -en, 11

 törzsszám, 33
 teljes gráf, 54
 természetes számok halmaza,
 10
 test, 6
 testbővítés, 48
 tizedes tört, tiszta szakaszos ,
 38
 tizedes tört, véges, 38
 tizedes tört, vegyes szakaszos,
 38
 transzcendens elem, 48
 transzpozíció, 7, 8
 tranzitív reláció, 2
 trigonometrikus alak, 47

 unió, 1
 univerzum, 1

 véges gráf, 50
 véges halmaz, 4
 végtelen halmaz, 4
 valós rész, 45
 valós szám tizedes tört alakja,
 40
 valós számok teste, 15
 variáció, ismétlés nélkül, 22
 variáció, ismétléses, 23
 vonal, 53

 xor művelet, 20

zárt intervallum, 15

zéruselem, 5

zéruselem, hálóa, 17

zérusosztó, 5

zárt Hamilton út, 58

zárt séta, 53

Tétel index

- $C_n^{k,i}$ értéke, 25
- C_n^k értéke, 23
- P_n értéke, 22
- $P_n^{k_1, k_2, \dots, k_r}$ értéke, 23
- V_n^k értéke, 22
- $V_n^{k,i}$ értéke, 23
- $\mathbb{R}$ rendezése, 16
- $\mathbb{N}$ rendezése, 12
- $\mathbb{Q}$ rendezése, $\mathbb{Q}$ rendezése, 13
- $\mathbb{Z}$ rendezése, $\mathbb{Z}$ rendezése, 12
- φ kiszámítása, 26
- $x_1 + x_2 + \dots + x_n = k$
megoldásai, 25
- Összefüggőségi reláció, 53
- Ötszintétel, 62
- Átrendezések száma, 26

- A G -kongruenciáról, 27
- A természetes számok
struktúrája, 11
- A valós számok struktúrája, 14
- Abszolút érték tulajdonságai,
46
- Algoritmus, kongruencia
egyenlet, 36
- Algoritmus: elsőfokú
kétismeretlenes d. e.
megoldása, 35
- Algoritmus: euklideszi, 30
- Algoritmus: euklideszi,
polinomokra, 42
- Algoritmus: Heurisztikus
színezés, 63
- Algoritmus: Kruskal, 57
- Algoritmus: maradékos osztás,
30
- Algoritmus: polinom osztása
polinommal, 42
- Asszociativitás következményei,
7
- Az egészek struktúrája, 12

- Binomiális együtthatók
tulajdonságai, 23
- Boole algebra és gyűrű, 21
- Burnside-lemma, 27

- De Morgan, 18
- Dirac tétel, 60
- Disztributivitás
következményei, 10

- Egysoros alak, 8
- Ekvivalencia reláció és
osztályozás, 3
- Elsőfokú kétismeretlenes d. e.
megoldása, 35
- Eratoszthenészi szita, 34
- Euler fokszám-tétele, 51
- Euler formula, 61
- Euler-Fermat, 37

- Függvény invertálhatósága, 4
- függvényteljesség, 21
- Fák jellemzése, 56
- Fagráfok élei, csúcsai, 55
- Feszítőfa létezése, 57
- Fokszám minimum, 62
- Gallai-Erdős, 51
- Grötsch tétel, 63
- Gráfok fokszám realizációja, 51
- Hányadostest, 13
- Halmaztestekről , 18
- Königsbergi hidak, 58
- Kézfogás, 54
- Kibővített euklideszi algoritmus, 31
- Klasszikus algebra alaptétele, 48
- Komplex egységgyökök, 47
- Komplex számok struktúrája, 45
- Komponens részgráf, 54
- Kompozíció szorzás zárójelezése, 4
- Kongruencia egyenlet megoldása, 36
- Kongruencia tulajdonságai, 35
- Konjugálás tulajdonságai, 46
- Kuratowski tétel, 62
- L.k.k.t, l.n.k.o. háló, 33
- L.k.k.t. tulajdonságai, 32
- l.n.k.o. létezése, 31
- L.n.k.o. tulajdonságai, 32
- Maradékös osztás, 30
- Maradékösztálygyűrű, 36
- Négyszíntétel, 62
- Ore tétel, 59
- Oszthatósági szabályok, 38
- Oszthatósági tulajdonságok, 29
- Pólya-Redfeld tétele, 28
- Permutáció rendje, 9
- Permutáció konjugáltja, 9
- Polinom osztása polinommal, 41
- Polinomelmélet alaptétele, 44
- Polinomgyűrű, 40
- Polinomiális tétel, 24
- Polinomokra kibővített euklideszi algoritmus, 43
- Polinomokra l.k.k.t. létezése, 44
- Polinomokra l.n.k.o. létezése, 43
- Prímszám és a törzsszám, 33
- Prímszámok száma, 34
- Prímtestek, 48
- Racionális számok szakaszos tizedes tört alakja, 40
- Redukált alak, 13
- Rendezés és háló, 17
- Stone-tétel, 19
- Számelmélet alaptétele, 33
- Számrendszerek, 37
- Színezési Burnside lemma, 28
- Szita formula, 25
- Tiszta szakaszból közönséges, 39
- Trigonometrikus alak, műveletek, 47
- Véges testek, 48
- Véges Boole-algebrák, 19
- Valós szám tizedes tört alakja, 40
- Vegyes szakaszból közönséges, 39

Tartalomjegyzék

1. Halmazok, struktúrák	1
1.1. Alapfogalmak	1
1.1.1. Halmazok.	1
1.1.2. Relációk, függvények	2
1.1.3. Műveletek.	4
1.1.4. A természetes számoktól a valós számokig . . .	10
1.2. Hálók, Boole algebrák	16
1.2.1. Hálóelméleti lapfogalmak	16
1.2.2. Boole műveletek	20
2. Kombinatorika	22
2.1. Alapesetek	22
2.1.1. Rendezett kiválasztás, ismétlés nélkül	22
2.1.2. Rendezett kiválasztás, ismétléses	23
2.1.3. Rendezetlen kiválasztás, ismétlés nélküli	23
2.1.4. Rendezetlen kiválasztás, ismétléssel	24
2.1.5. Szita formula	25
2.2. Alkalmazások	26
2.2.1. Euler-féle φ -függvény	26
2.2.2. Átrendezések	26
2.2.3. Színezések	26
3. Elemi számelmélet...	29
3.1. Oszthatóság az egész számok körében	29
3.1.1. Oszthatósági alapfogalmak	29
3.1.2. Egyértelmű prímfaktorizáció	33
3.2. Diofantoszi egyenlet, kongruencia	34
3.3. Számrendszerek, tizedes törtek	37
3.4. A polinomgyűrű	40

TARTALOMJEGYZÉK	75
4. Testelmélet	45
4.1. Komplex számok	45
4.2. Galois testek	48
5. Gráfelmélet	50
5.1. Alapfogalmak	50
5.2. Fák és erdők	55
5.3. Euler vonal, Hamilton út, Euler formula	58
5.4. Síkbaágyazhatóság, síkgráfok színezése	61
Definíció index	65
Tétel index	70
Tartalomjegyzék	73

**A szerző okleveles
matematikus, 1989-
ben végzett a KLTE-n.**



**1997-ben PhD
fokozatot szerzett,
1999-től a NYE (ill.
jogelődje) főiskolai
tanára.**

