- $8/-2\ldots-1:$

$<$

rülírható értelemben) a logika szabályainak megfelelően belátjuk: az állítás a tételben megfogalmazott esetekben kivétel nélkül mindig igaz.

$>$

rülírható értelemben) a logika szabályainak megfelelően belátjuk: az állítás következik az axiómákból.

- $9/2\ldots4:$

$<$

1.1.1. Az axiomatikus módszer. Tegyük fel, hogy a valóság egy részének modellezésével, egy elmélet problémáinak szabályrendszerével foglalkozunk. Az axiomatikus módszer abban áll, hogy bizonyos feltevésekből, az elmélet axiómáiból valamilyen logika

$>$

1.1.1. Az axiomatikus módszer. Tegyük fel, hogy a valóság egy részének modellezésével foglalkozunk. Az axiomatikus módszer abban áll, hogy bizonyos feltevésekből, az elmélet axiómáiból a logika

- $9/12\ldots16:$

$<$

1.1.2. Logikai jelek, predikátumok, formulák. Egy matematikai elmélet olyan kijelentésekből, állításokból áll, melyek lehetnek igazak, vagy hamisak – úgy értve, hogy a kettő közül pontosan az egyik teljesül. Azokat az állításokat, melyek változókat tartalmaznak, *predikátum*oknak nevezzük. A predikátumok változóinak helyébe alkalmas objektumot helyettesítve, azok igazságértéke eldönthető. Ez az érték szintén igaz (jele: $\uparrow$)

$>$

1.1.2. Logikai jelek, predikátumok, formulák. Egy matematikai elméletben szerepel néhány definiálatlan alapfogalom, az úgynevezett *predikátum*ok, amelyeknek változóiktól függően az értéke igaz (jele: $\uparrow$)

- $10/12\ldots14:$

$<$

$$\begin{aligned}
&\forall x\forall y\Bigg(\big(P(x)\wedge P(y)\wedge\neg x=y\big)\\
&\qquad\Rightarrow\Big(\exists z\big(E(z)\wedge I(x,z)\wedge I(y,z)\big)\\
&\qquad\wedge\forall z\forall w\Big(\big(E(z)\wedge I(x,z)\wedge I(y,z)\wedge E(w)\wedge I(x,w)\wedge I(y,w)\big)\Rightarrow z=w\Big)\Bigg)
\end{aligned}$$

$>$

$$
\begin{aligned}
\forall x \forall y \Big(& \big(P(x) \wedge P(y) \wedge \neg x = y\big) \\
& \Rightarrow \Big(\exists z\big(E(z) \wedge I(x,z) \wedge I(y,z)\big)\Big) \\
& \wedge \forall z \forall w \Big(\big(E(z) \wedge I(x,z) \wedge I(y,z) \wedge E(w) \wedge I(x,w) \wedge I(y,w)\big) \Rightarrow z = w\Big)\Big)
\end{aligned}
$$

- $15/20\ldots22$:

$<$

mazelmélet axiómarendszerének, a Neumann–Bernays–go—delkurtGödel, Kurt (1906–1978)Gödel, rövidítve NBG axiómarendszer, amely ilyen „túl nagy” dolgokat is megenged, de ezeket nem nevezi halmaznak, hanem osztálynak. Lásd részletesebben Kelley

$>$

mazelmélet axiómarendszerének, a Neumann–Bernays–Gödel, rövidítve NBG axiómarendszer, amely ilyen „túl nagy” dolgokat is megenged, de ezeket nem nevezi halmaznak, hanem osztálynak. Lásd részletesebben Kelley

- $23/-4$:

$<$

analóg módon értelmezzük.

$>$

analóg módon értelmezzük. Az itt definiált halmazokat közös néven *intervallum*oknak nevezzük.

- $25/9$:

$<$

(*argumentum*ban) felvett *érték*ének nevezzük és gyakran f_x-el jelöljük. (Vannak, akik

$>$

(*argumentum*ban) felvett *érték*ének nevezzük és gyakran f_x-szel jelöljük. (Vannak, akik

- $31/3\ldots5$:

$<$

Több természetes kérdés merül fel. Az egyik, hogy az axiómák egyértelműen meghatározzák-e $\mathbb{N}$-et? (A válasz igen, egy pontosan meghatározott értelemben.) A másik, hogy létezik-e $\mathbb{N}$? (Erre is igen a válasz.) Egy további, hogy szükség van-e mind az öt

$>$

Több természetes kérdés merül fel. Az első, hogy az axiómák egyértelműen meghatározzák-e $\mathbb{N}$-et? (A válasz igen, egy pontosan meghatározott értelemben.) A második, hogy létezik-e $\mathbb{N}$? (Erre is igen a válasz.) Egy további, hogy szükség van-e mind az öt

- 32/11 :

  $<$

  Bizonyítás. Vegyük észre, hogy ha g és g^* is a tétel feltételeit kielégítő függvény,

  $>$

  * **Bizonyítás.** Vegyük észre, hogy ha g és g^* is a tétel feltételeit kielégítő függvény,

- 36/−18 :

  $<$

észre, hogy ha h-nak h^* az inverze, akkor $g * h$ inverze $h^* * g^*$. Ha egy egységelemes

  $>$

észre, hogy ha h-nak h^* az inverze, akkor $g * h$ inverze $h^* * g^*$. Ha egy semleges elemes

- 36/−9 :

  $<$

(*multiplikatív jelölés*), a semleges elemet *egységelem*nek nevezzük, és e-vel vagy 1-gyel

  $>$

(*multiplikatív jelölés*). Multiplikatív jelölés esetén a semleges elemet *egységelem*nek nevezzük, és e-vel vagy 1-gyel

- 39/−10 :

  $<$

  Bizonyítás. Az egyértelműség bizonyítása $\mathbb{N}$ jólrendezettségén múlik. (Az ilyen

  $>$

  * **Bizonyítás.** Az egyértelműség bizonyítása $\mathbb{N}$ jólrendezettségén múlik. (Az ilyen

- 41/−7 :

  $<$

m-et q-val, azaz írjuk fel $m = m'q + r$ alakban, ahol $m'r \in \mathbb{N}$ és $r < q$. Ha $m' = 0$,

  $>$

m-et q-val, azaz írjuk fel $m = m'q + r$ alakban, ahol $m', r \in \mathbb{N}$ és $r < q$. Ha $m' = 0$,

- 45/9 . . . 10 :

  $<$

  3.1.7. Példák. Bármely X halmazra $\wp(X)$ a $(\triangle, \cap)$ müveletekkel kommutatív egységelemes gyűrű, amely általában nem nullosztómentes.

  $>$

  3.1.7. Példa. Bármely X halmazra $\wp(X)$ a $(\triangle, \cap)$ műveletekkel kommutatív egységelemes gyűrű, amelyben nem nulla elemek „szorzata” lehet nulla.

- 47/12 :

  $<$

$-x+x < -x+0 = -x$. Ezzel beláttuk (1)-et. (2) abból következik, hogy $y-x > y-y = 0$,

  $>$

$-x+x < -x+0 = -x$. Ezzel beláttuk (1)-et. (2) abból következik, hogy $y-x > x-x = 0$,

- $47/-10$:

<

ekvivalenciareláció. Az ekvivalenciosztályok halmazát $\mathbb{Q}$-val fogjuk jelölni, és elemeit

>

ekvivalenciareláció. Az ekvivalenciaosztályok halmazát $\mathbb{Q}$-val fogjuk jelölni, és elemeit

- $56/-1$:

<

koszinusza segítségével. Ez a trigonometrikus alak. A trigonometrikus alaknak (a geo-

>

koszinusza segítségével. A trigonometrikus alaknak (a geo-

- $57/4\ldots7$:

<

Ha $z \in \mathbb{C}$, akkor van olyan t valós szám, amelyre $\mathrm{sgn}(z) = \cos t + i \sin t$. Ha $z = 0$, akkor akármilyen $t \in \mathbb{R}$ választható, egyébként, ha ez az összefüggés fennáll t-re, akkor a $t + 2k\pi$, $k \in \mathbb{Z}$ számokra is, és csak ezekre. Ekkor $z = |z|(\cos t + i \sin t)$, ez a komplex szám *trigonometrikus alak*ja. Ha $0 \neq z \in \mathbb{C}$, akkor legyen a z *argumentum*a, $\arg(z)$ az az

>

Ha $0 \neq z \in \mathbb{C}$, akkor van olyan t valós szám, amelyre $\mathrm{sgn}(z) = \cos t + i \sin t$. Ha ez az összefüggés fennáll t-re, akkor a $t + 2k\pi$, $k \in \mathbb{Z}$ számokra is, és csak ezekre. Ekkor $z = |z|(\cos t + i \sin t)$, ez a komplex szám *trigonometrikus alak*ja. Ha $z = 0$, akkor akármilyen $t \in \mathbb{R}$ választható. Ha $0 \neq z \in \mathbb{C}$, akkor legyen a z *argumentum*a, $\arg(z)$ az az

- $62/-8$:

<

maza ekvivalens $\{1, 2, \ldots, m\}$-el valamely $m < n$ természetes számra.

>

maza ekvivalens $\{1, 2, \ldots, m\}$-mel valamely $m < n$ természetes számra.

- $62/-5$:

<

$n + 1 \in A$, akkor van olyan $k < n + 1$ természetes szám, amelyre $k \notin A$. Definiáljuk az

>

$n + 1 \in A$, akkor van olyan $0 < k < n + 1$ természetes szám, amelyre $k \notin A$. Definiáljuk az

- $63/14$:

<

Egy halmaz legfeljebb egy n-re ekvivalens a $\{1, 2, \ldots, n\}$ halmazzal, mert ha $\{1, 2, \ldots, m\}$-mel is ekvivalens lenne, akkor $m < n$ vagy $n < m$ miatt $\mathbb{N}^+$ egy kezdőszelete ekvivalens

>

Egy halmaz legfeljebb egy n-re ekvivalens a $\{1, 2, \ldots, n\}$ halmazzal, mert ha ekvivalens lenne $\{1, 2, \ldots, m\}$-mel is, akkor $m < n$ vagy $n < m$ miatt $\mathbb{N}^+$ egy kezdőszelete ekvivalens

- 64/12 :

  $<$

$\{1, 2, \ldots, \natural(X)\}$ egy valódi részhalmaza ekvivalens lenne $\{1, 2, \ldots, \natural(X)\}$-el.

  $>$

$\{1, 2, \ldots, \natural(X)\}$ egy valódi részhalmaza ekvivalens lenne $\{1, 2, \ldots, \natural(X)\}$-nel.

- 67/−7 :

  $<$

  Ha a gyűrű nem egységelemes, akkor is igaz az állítás $r, n \in \mathbb{N}^+$ esetén, ha a szereplő

  $>$

  Ha a gyűrű nem egységelemes, akkor is igaz az állítás $r, n \in \mathbb{N}^+$, $i_1, \ldots, i_r \in \mathbb{N}$ esetén, ha a szereplő

- 71/−13 :

  $<$

valamelyik fennáll (*dichotomitás*). Az is kérdéses, hogy van-e minden X halmazhoz olyan

  $>$

valamelyik fennáll (*dichotomia*). Az is kérdéses, hogy van-e minden X halmazhoz olyan

- 73/−11 . . . − 8 :

  $<$

  A bizonyítás felhasználja a kiválasztási axiómát és az $\mathbb{N}$-re alkalmazott transzfinit rekurziót. Legyen F egy, az X véges részhalmazaihoz a komplementerük egy elemét rendelő (kiválasztási) függvény. Ha $h :]\leftarrow, n[\to X$ egy függvény, legyen $f(h) = F\big(\mathrm{rng}(h)\big)$, és alkalmazzuk a transzfinit rekurzió tételét. Egy $x : \mathbb{N} \to X$ kölcsönösen egyértelmű

  $>$

  A bizonyítás felhasználja a kiválasztási axiómát és az általános rekurzió tételt. Legyen F egy, az X véges részhalmazaihoz a komplementerük egy elemét rendelő (kiválasztási) függvény. Ha $h :]\leftarrow, n[\to X$ egy függvény, legyen $f(h) = F\big(\mathrm{rng}(h)\big)$, és alkalmazzuk az általʻnos rekurzió tételt. Egy $x : \mathbb{N} \to X$ kölcsönösen egyértelmű

- 74/−12 :

  $<$

  Az $f(m, n)$ függvény „működése" az 5.1.ábrán tanulmányozható.

  $>$

  Az $f(m, n)$ függvény „működése" az 5.1. ábrán tanulmányozható.

- 76/9 :

  $<$

  5.3.8. Számosságok. A *számosság*on az ekvivalens halmazok „közös tulajdonsá-

  $>$

  * **5.3.8. Számosságok.** *Számosság*on az ekvivalens halmazok „közös tulajdonsá-

- $78/-5\ldots-3$:

<

azon elemei, amelyeknek van a szorzásra rézve inverzük. Az egységek a szorzásra nézve Abel-csoportot alkotnak, a gyűrű *egységcsoport*ját. Az egységek bármely $a \in R$-nek osztói, mert $1a$-nak osztói. Megfordítva nyilvánvaló: ha egy elem minden $a \in \mathbb{R}$-nek

>

azon elemei, amelyeknek van a szorzásra nézve inverzük. (Így egy egységelemes integritási tartomány pontosan akkor test, ha minden nem nulla eleme egység.) Az egységek a szorzásra nézve Abel-csoportot alkotnak, a gyűrű *egységcsoport*ját. Az egységek bármely $a \in R$-nek osztói, mert $1a$-nak osztói. Megfordítva nyilvánvaló: ha egy elem minden $a \in R$-nek

- $80/-16$:

<

6.1.12. Megjegyzés. Elég r_n, x_n, y_n, r_{n+1}, x_{n+1}, y_{n+1} és n értékét tárolni. Ha

>

6.1.12. Megjegyzés. Elég r_n, x_n, y_n, r_{n+1}, x_{n+1} és y_{n+1} értékét tárolni. Ha

- $84/11\ldots12$:

<

egy rendszerét *maradékrendszer*nek nevezzük. Ha egy maradékrendszer minden maradékosztályból tartalmaz elemet, akkor *teljes maradékrendszer*nek nevezzük. Ha egy mara-

>

egy rendszerét *maradékrendszer*nek nevezzük. Ha egy maradékrendszer minden maradékosztályból tartalmaz elemet, akkor *teljes maradékrendszer*nek nevezzük. Ha egy mara-

- $86/8\ldots13$:

<

6.2.9. Példa. Oldjuk meg a $172x \equiv 6$ kongruenciát, vagy ami ezzel ekvivalens, határozzuk meg a $172x + 62y = 6$ egyenlet egész megoldásait. Mivel $\mathrm{lnko}(172, 62) = 2$ osztója 6-nak, van megoldás. Az egyenlet a $86x + 31y = 3$ egyenlettel ekvivalens. A bővített euklideszi algoritmussal $172\cdot(-9)+62\cdot25 = 2$, ahonnan $x_0 = (-9)\cdot3$, $y_0 = 25\cdot3$, így az egyenlet összes megoldása $x_k = -27+31k$, $y_k = 75-86k$, $k \in \mathbb{Z}$. A kongruencia az $x \equiv 4 \pmod{31}$ kongruenciával ekvivalens, így $x \equiv 4 \pmod{62}$ vagy $x \equiv 35 \pmod{62}$.

>

6.2.9. Példa. Oldjuk meg a $172x \equiv 6 \pmod{62}$ kongruenciát, vagy ami ezzel ekvivalens, határozzuk meg a $172x + 62y = 6$ egyenlet egész megoldásait. Mivel $\mathrm{lnko}(172, 62) = 2$ osztója 6-nak, van megoldás. Az egyenlet a $86x + 31y = 3$ egyenlettel ekvivalens. A bővített euklideszi algoritmussal $172 \cdot (-9) + 62 \cdot 25 = 2$, ahonnan $x_1 = (-9) \cdot 3$, $y_1 = 25 \cdot 3$, így az egyenlet összes megoldása $x = -27 + 31k$, $y = 75 - 86k$, $k \in \mathbb{Z}$. A kongruencia az $x \equiv 4 \pmod{31}$ kongruenciával ekvivalens, így $x \equiv 4 \pmod{62}$ vagy $x \equiv 35 \pmod{62}$.

- $91/-14\ldots-11$:

  $<$

összegzési függvénye, multiplikatív. Továbbá, ha $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ az n prímtényezős felbontása, akkor

  $>$

összegzési függvénye, multiplikatív. Továbbá, ha $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ az n kanonikus alakja, akkor

- $94/-14$:

  $<$

felhasználásával

  $>$

felhasználásával, mivel P_{n-2}, P_{n-3}, Q_{n-2}, Q_{n-3} csak a $q_1, \ldots, q_{n-2}$ függvényei,

- $97/-9\ldots-1$:

  $<$

és egy $G = (E, V)$ gráfról beszélni. Egyébként a csúcsok és élek közötti illeszkedés egy reláció V és E között, amelyet *illeszkedési reláció*nak nevezünk.

Két különböző élt *szomszédos*nak nevezünk, ha van olyan csúcs, amely mindkettőre illeszkedik. Két különböző csúcsot *szomszédos*nak nevezünk, ha van olyan él, amelyre mindkettő illeszkedik.

Ha egy él csak egy csúcsra illeszkedik, akkor *hurokél*nek nevezzük. Ha az $e_1 \neq e_2$ élekre ugyanazok a csúcsok illeszkednek, akkor *párhuzamos élek*ről vagy *többszörös élek*ről beszélünk. Ha egy gráf nem tartalmaz sem hurokélt, sem párhuzamos éleket, akkor *egyszerű gráf*nak nevezzük. Az 8.1. ábrán például e_1, e_2 párhuzamos élek, e_5 hurokél.

  $>$

és egy $G = (E, V)$ gráfról beszélni. Egyébként az élek és csúcsok közötti illeszkedés egy reláció E és V között, amelyet *illeszkedési reláció*nak nevezünk.

Két különböző élt *szomszédos*nak nevezünk, ha van olyan csúcs, amelyre mindkettő illeszkedik. Két különböző csúcsot *szomszédos*nak nevezünk, ha van olyan él, amely mindkettőre illeszkedik.

Ha egy él csak egy csúcsra illeszkedik, akkor *hurokél*nek nevezzük. Ha az $e_1 \neq e_2$ élek ugyanazokra a csúcsokra illeszkednek, akkor *párhuzamos élek*ről vagy *többszörös élek*ről beszélünk. Ha egy gráf nem tartalmaz sem hurokélt, sem párhuzamos éleket, akkor *egyszerű gráf*nak nevezzük. Az 7.1. ábrán például e_1, e_2 párhuzamos élek, e_5 hurokél.

- $98/5$:

  $<$

  Ha egy csúcs csak véges sok élre illeszkedik, akkor a csúcs *fokszám*án a rá illeszkedő

  $>$

  Ha egy csúcsra csak véges sok él illeszkedik, akkor a csúcs *fokszám*án a rá illeszkedő

- $99/-2\ldots-1$:

  $<$

vezésétől eltekintve azonosak, azaz izomorfak.) A 8.3. ábrán szaggatott vonal mutatja a komplementer gráfot, $(v_1, v_2, v_4, e_1, e_4, e_6)$ telített, $(v_1, v_2, v_4, e_1, e_6)$ nem telített részgráf.

  $>$

vezésétől eltekintve azonosak, azaz izomorfak.) A 7.3. ábrán szaggatott vonal mutatja a komplementer gráfot, $(\{e_1, e_4, e_6\}, \{v_1, v_2, v_4\})$ telített, $(\{e_1, e_6\}, \{v_1, v_2, v_4\})$ nem telített részgráf.

- $100/-7\ldots-6$:

  $<$

*háromszög*nek, *négyszög*nek, ... nevezzük. A 8.4. ábrán $v_1, \ldots, v_9$ séta, de nem út és nem vonal, $v_1, \ldots, v_8$ vonal, de nem út, $v_1, \ldots, v_3$ út is vonal is, $v_3, \ldots, v_7, e_7, v_3$ kör.

  $>$

*háromszög*nek, *négyszög*nek, ... nevezzük. A 7.4. ábrán

$$v_1, e_1, v_2, e_2, v_3, e_8, v_8, e_9, v_9, e_9, v_8$$

séta, de nem út és nem vonal;

$$v_1, e_1, v_2, e_2, v_3, e_3, v_4, e_4, v_5, e_5, v_6, e_6, v_7, e_7, v_3, e_8, v_8$$

vonal, de nem út;

$$v_1, e_1, v_2, e_2, v_3$$

út is, vonal is;

$$v_3, e_3, v_4, e_4, v_5, e_5, v_6, e_6, v_7, e_7, v_3$$

kör.

- $102/-2\ldots-1$:

  $<$

gráfnak létezhet feszítőfája.) Az 8.5. ábrán két izomorf, de nem identikus gráf látható, $v_1, e_1, v_2, e_2, v_3, e_3$ feszítőfa a bal oldali gráfban.

  $>$

gráfnak létezhet feszítőfája.) A 7.5. ábrán két izomorf, de nem identikus gráf látható, az e_4 törlésével kapott részgráf feszítőfa a bal oldali gráfban.

- $104/11$:

  $<$

elvágó halmaz, akkor *vágás*nak nevezzük. Az 8.1. ábrán például e_4, e_1, e_2 vágás.

  $>$

elvágó halmaz, akkor *vágás*nak nevezzük. A 7.1. ábrán például $\{e_4\}$ illetve $\{e_1, e_2\}$ vágás.

- 106/6 . . . 7 :

$<$

merünk lényegesen jobb algoritmust Hamilton-kör keresésére. A 7.8 ábrán láthatunk egy Hamilton-vonalat, amelyben nem Euler-vonal.

$>$

merünk lényegesen jobb algoritmust Hamilton-kör keresésére. A 7.8. ábrán egy olyan gráfot láthatunk, amelyben van Euler-vonal, de nincs Hamilton-kör.

- 106/8 . . . 13 :

$<$

7.1.24. Súlyozott gráfok. Gyakorlati alkalmazásokban gyakran adott egy $G = (\varphi, E, V)$ gráf és egy $w : E \to \mathbb{R}$ függvény; a w-t *súlyozás*nak, a (φ, E, V, w) négyest pedig *súlyozott gráf*nak nevezzük. (Vannak alkalmazások amelyekben másként adunk további információkat a gráfhoz, például az adott csúcsra illeszkedő éleket rendezzük vagy megszámozzuk, a csúcsokat súlyozzuk, a csúcsokhoz színeket rendelünk, stb.) Egy súlyozott gráfban egy $E' \subset E$ véges részhalmaz *súly*a $\sum_{e \in E'} w(e)$. Nagyon sok gráfalgoritmus

$>$

7.1.24. Címkézett és súlyozott gráfok. Gyakorlati alkalmazásokban gyakran további adatokat rendelünk a gráf éleihez, illetve csúcsaihoz. Ha adott egy $G = (\varphi, E, V)$ gráf, a C_e és C_v halmazok, az *élcímké*k illetve *csúcscímké*k halmaza, valamint a $c_e : E \to C_e$ és $c_v : V \to C_v$ leképezések, az *élcímkézés* illetve *csúcscímkézés*, akkor a $(\varphi, E, V, c_e, C_e, c_v, C_v)$ hetest *címkézett gráf*nak nevezzük. Ha csak élcímkék és élcímkézés adott, akkor *élcímkézett gráf*ról, ha pedig csak csúcscímkék és csúcscímkézés adott, akkor *csúcscímkézett gráf*ról beszélünk. Gyakran *színezett gráf*ról beszélünk címkézett gráf helyett. A címkéket felhasználhatjuk például arra, hogy az adott csúcsra illeszkedő éleket megszámozzuk, rendezzük, stb. Igen gyakori, hogy $C_e = \mathbb{R}$ illetve $C_v = \mathbb{R}$, ekkor *élsúlyozás*ról és *élsúlyozott gráf*ról illetve *csúcssúlyozás*ról és *csúcssúlyozott gráf*ról beszélünk, és a jelölésből C_e-t illetve C_v-t elhagyjuk. Egy (φ, E, V, w) élsúlyozott gráfban egy $E' \subset E$ véges részhalmaz *súly*a $\sum_{e \in E'} w(e)$. Hasonlóan egy (φ, E, V, w) csúcssúlyozott gráfban egy $V' \subset V$ véges részhalmaz *súly*a $\sum_{v \in V'} w(v)$. Nagyon sok gráfalgoritmus

- 107/6 :

$<$

A 7.9. ábra mutatja, hogy nem tudunk mindig minimális súlyú élet választani, kü-

$>$

A 7.9. ábra mutatja, hogy nem tudunk mindig minimális súlyú élt választani, kü-

- 107/−6 . . . − 3 :

$<$

7.1.27. Megjegyzés. A gráfelmélet több mint 100 évig megoldatlan problémája volt a *négyszínsejtés*, mely szerint bármely síkba rajzolható egyszerű gráf csúcsaihoz hozzárendelhetünk négy színt úgy, hogy a szomszédos csúcsokhoz rendelt színek különbözőek. 1976-ban Appel és Haken amerikai matematikusok bizonyították be a sejtést.

$>$

7.1.27. Megjegyzés. A gráfelmélet több mint 100 évig megoldatlan problémája volt a *négyszínsejtés*, mely szerint bármely térkép kiszínezhető négy színnel úgy, hogy a szomszédos országok különböző színűek. Ez egy gráfszínezési probléma: kössük össze a szomszédos országok fővárosait éllel. 1976-ban Appel és Haken amerikai matematikusok bizonyították be a sejtést.

- $108/-13$:

<

hiszen minden újabb él mindkét összeget eggyel növeli.

>

hiszen minden újabb él mindhárom összeget eggyel növeli.

- $108/-10$:

<

dikkal. Ekkor (ψ, E, V) irányított gráf. Így relációk irányított gráfokkal szemléltethetők.

>

dikkal. Ekkor (ψ, E, V) irányított gráf. Így relációk irányított gráfokkal szemléltethetők. Ezt már használtuk is a relációknál.

- $109/-9\ldots-5$:

<

csúcsból irányított út.)

>

csúcsból irányított út.) Irányított fában a gyökértől nyilván csak egy út vezet minden csúcshoz. Ebből következik, hogy minden, a gyökértől különböző csúcs befoka egy. Azok a csúcsok, amelyekhez n hosszú út vezet a gyökértől, alkotják az n-edik *szint*et. A csúcsok szintjeinek maximumát (amely véges irányított fa esetén nyilván létezik) a fa *magasság*ának nevezzük. Ha van olyan él, amelynek v a kezdőpontja, v' pedig a végpontja, akkor az mondjuk, hogy v' a v *gyermeke*, illetve hogy v a v' *szülője*. Ha két csúcsnak ugyanaz a szülője, akkor *testvérek*nek nevezzük őket. Bármely v csúcsra tekinthetjük azon csúcsok halmazát, amelyekhez vezet irányított út v-ből. Ezek a csúcsok meghatároznak egy feszített irányított részgráfot, amely nyilván irányított fa, és v a gyökere; ezt a v-ben gyökerező *irányított részfá*nak nevezzük. Irányított fának azokat a csúcsait, amelyek kifoka nulla, *levél*nek nevezzük.

- $109/-4$:

<

◦ **7.2.8. Gráfok rajzolhatósága.** Legyen $X \subset \mathbb{R}^n$. Egy X-beli *egyszerű görbe* egy,

>

◦* **7.2.8. Gráfok rajzolhatósága.** Legyen $X \subset \mathbb{R}^n$. Egy X-beli *egyszerű görbe* egy,

- $110/18$:

<

◦ **7.2.9. Állítás.** *Tetszőleges véges egyszerű gráf* $\mathbb{R}^3$*-ba rajzolható.*

$>$

∘* **7.2.9. Állítás.** *Tetszőleges véges egyszerű gráf* $\mathbb{R}^3$*-ba rajzolható.*

- $110/-14$:

$<$

∘ **7.2.10. Segédtétel.** *Legyen* $X \subset \mathbb{R}^3$ *egy gömbfelület és* (f, g) a $G = (\psi, E, V)$

$>$

∘* **7.2.10. Segédtétel.** *Legyen* $X \subset \mathbb{R}^3$ *egy gömbfelület és* (f, g) a $G = (\psi, E, V)$

- $111/6$:

$<$

∘ **7.2.11. Tétel.** *Egy* $G = (\psi, E, V)$ *egyszerű véges gráf pontosan akkor rajzolható*

$>$

∘* **7.2.11. Tétel.** *Egy* $G = (\psi, E, V)$ *egyszerű véges gráf pontosan akkor rajzolható*

- $111/14$:

$<$

∘ **7.2.12. Tartományok.** Az $\mathbb{R}^n$ egy X nyílt részhalmazát *tartomány*nak nevezzük,

$>$

∘* **7.2.12. Tartományok.** Az $\mathbb{R}^n$ egy X nyílt részhalmazát *tartomány*nak nevezzük,

- $111/17 \ldots 19$:

$<$

∘ **7.2.13. Euler tétele.** Legyen (f, g) a $G = (\psi, E, V)$ egyszerű véges összefüggő gráf egy síkba rajzolása. Ekkor a $G' = \cup_{e \in E} \operatorname{rng}(g_e)$ halmaz komplementere $2 + \natural(E) - \natural(V)$ páronként diszjunkt tartomány egyesítése.

$>$

∘* **7.2.13. Euler tétele.** *Legyen* (f, g) a $G = (\psi, E, V)$ *egyszerű véges összefüggő gráf egy síkba rajzolása. Ekkor a* $G' = \cup_{e \in E} \operatorname{rng}(g_e)$ *halmaz komplementere* $2 + \natural(E) - \natural(V)$ *páronként diszjunkt tartomány egyesítése.*

- $111/-17$:

$<$

∘ **7.2.14. Megjegyzés.** Az előző „bizonyítás” kihagyott részeinek pontos igazolása

$>$

∘* **7.2.14. Megjegyzés.** Az előző „bizonyítás” kihagyott részeinek pontos igazolása

- $111/-7$:

$<$

7.2.15. Gráfok topologikus ekvivalenciája. A G és G' véges gráfokat *topologi-*

$>$

* **7.2.15. Gráfok topologikus ekvivalenciája.** A G és G' véges gráfokat *topologi-*

- 111/-3 :

  $<$

  7.2.16. Kuratowski tétele. *Egy egyszerű véges gráf akkor és csak akkor síkba*

  $>$

  * **7.2.16. Kuratowski tétele.** *Egy egyszerű véges gráf akkor és csak akkor síkba*

- 112/$1\ldots3$:

  $<$

  A bizonyítás nehéz, itt nem tárgyaljuk. $\square$

  A 7.11. ábrán látható Petersen gráf nem síkba rajzolható, mivel tartalmaz a $K_{3,3}$-mal topologikusan izomorf részgráfot.

  $>$

  A bizonyítás nehéz, itt nem tárgyaljuk. $\square$

  A 7.11. ábrán látható Petersen-gráf nem síkba rajzolható, mivel tartalmaz a $K_{3,3}$-mal topologikusan izomorf részgráfot. (Töröljünk egy csúcsot.)

- 112/$-3\ldots-2$:

  $<$

  Megjegyezük, hogy bár több más módon is rendelhetünk gráfokhoz mátrixokat és a mátrixok felhasználhatók gráf számítógépes ábrázolására, bár erre a célra más adatszer-

  $>$

  Megjegyezzük, hogy bár több más módon is rendelhetünk gráfokhoz mátrixokat és a mátrixok felhasználhatók gráf számítógépes ábrázolására, erre a célra más adatszer-

- 113/$4\ldots7$:

  $<$

  mazára, amelyeken a szorzás és az összeadás tulajdonságait vizsgáltuk. A számhamazoknál megfigyelt fogalmak jelentős része értelmezhető olyan halmazokon is, amelyek elemei nem számok. Ennek a fejezetnek a fő feladata az, hogy az eddigiekben már értelmezett, a műveletekkel kapcsolatos fogalmakat a halmazok minél általánosabb körére kiterjesszük,

  $>$

  mazára, amelyeken a szorzás és az összeadás tulajdonságait vizsgáltuk. A számoknál megismert fogalmak jelentős része értelmezhető olyan halmazokon is, amelyek elemei nem számok. Ennek a fejezetnek a fő feladata az, hogy az eddigiekben már értelmezett, a műveletekkel kapcsolatos fogalmakat minél általánosabb körre terjesszük ki,

- 113/$-10\ldots-7$:

  $<$

  a függvényterek. Csoportok leírásánál additív vagy multiplikatív írásmódot használunk, de figyelmeztetünk, hogy ez nem feltétlenül jelenti, hogy a művelet az összeadás vagy a szorzás.

  8.1.2. Homomorfizmusok. Két csoport vizsgálatánál fontos szerepet játszanak a

  $>$

  a függvényterek.

8.1.2. Homomorfizmusok. Csoportok vizsgálatánál fontos szerepet játszanak a

- 115/−14 :

<

8.1.6. Tétel. *Ha G egy félcsoport, akkor az alábbi feltételek ekvivalensek:*

>

* **8.1.6. Tétel.** *Ha G egy félcsoport, akkor az alábbi feltételek ekvivalensek:*

- 116/7 :

<

megoldható, megoldását jelölje e. Megmutatjuk, hogy e jobb oldali egységelem. Legyen

>

megoldható, megoldását jelölje e. Legyen

- 116/17 . . . 23 :

<

Bizonyítás. A (3)-beli egyértelműségből következik. □

8.1.8. Megjegyzés. Az $\{\alpha, \beta, \gamma\}$ halmazon a

$\cdot$	α	β	γ
α	β	α	γ
β	α	γ	β
γ	γ	β	α

táblázattal megadott művelet invertálható, mégsem kapunk csoportot, mert a művelet

>

Bizonyítás. A (3)-beli egyértelműségből következik (vagy c inverzével szorozva). □

* **8.1.8. Megjegyzés.** Az $\{\alpha, \beta, \gamma\}$ halmazon a

$\cdot$	α	β	γ
α	β	α	γ
β	α	γ	β
γ	γ	β	α

táblázattal megadott műveletnél az $ax = b$ és $ya = b$ egyenletek egyértelműen megoldhatók, mégsem kapunk csoportot, mert a művelet

- 117/11 :

<

a számoláshoz pedig elég tudni, hogy $\varepsilon^n = \tau^2 = e$, és $\varepsilon\tau = \tau\varepsilon^{-1}$. A diédercsoport név

>

a számoláshoz pedig elég tudni, hogy $\varepsilon^n = \tau^2 = e$ és $\varepsilon\tau = \tau\varepsilon^{-1}$. A diédercsoport név

• 119/$-11 \ldots -9$:

<

H, ahonnan d definíciója miatt $r = 0$, és így $g^m = (g^d)^q$. $\square$

Eddigi tanulmányaink során is találkoztunk már olyan feladattal, hogy egy halmaz elemeit egy műveleti tulajdonság szerint osztályokba soroltuk, és a továbbiakban ezeket

>

H, ahonnan d definíciója miatt $r = 0$, és így $g^m = (g^d)^q$. $\square$

8.1.23. Tétel. *Legyen G egy n rendű véges ciklikus csoport, g pedig egy generátoreleme G-nek. Ha $a \in \mathbb{Z}$ és $d = \operatorname{lnko}(a, n)$, akkor g^a a $H = \{g^d, g^{2d}, \ldots, g^{md} = e\}$ ciklikus részcsoportot generálja, ahol $n = md$. A G minden részcsoportja előáll így valamely $d|n$-re. A G-nek $\varphi(n)$ generátora van.*

Bizonyítás. Az előző tétel bizonyítása szerint minden H részcsoport g^d hatványaiból áll, ahol d a legkisebb pozitív kitevő, amelyre $g^d \in H$. Mivel g^a a g^d hatványa, így az általa generált részcsoport része H-nak. Mivel alkalmas $x, y \in \mathbb{Z}$-re $d = ax + ny$, azt kapjuk, hogy $g^d = g^{ax+ny} = g^{ax}g^{ny} = g^{ax}e^y = g^{ax}$, így g^a generálja H-t. Az utolsó állítás abból következik, hogy $\varphi(n)$ darab olyan $0 \le a < n$ természetes szám van, amelyre a és n relatív prímek. $\square$

Eddigi tanulmányaink során is előfordult már, hogy egy halmaz elemeit osztályokba soroltuk, és a továbbiakban ezeket

• 119/$-3 \ldots -2$:

<

portja. Ve

zessük be az $a \sim b$, ha $ab^{-1} \in H$ relációt. Ez nyilván ekvivalenciareláció. Vizsgáljuk

>

portja. Vezessük be az $a \sim b$, ha $ab^{-1} \in H$ relációt. Ez nyilván ekvivalenciareláció. Vizsgáljuk

• 120/-2 :

<

8.1.27. Tétel. *Egy nem egyelemű csoport pontosan akkor prímszámrendű, ha*

>

* **8.1.27. Tétel.** *Egy nem egyelemű csoport pontosan akkor prímszámrendű, ha*

• 121/-8 :

<

8.1.32. Belső automorfizmusok. Ha G csoport és $a \in G$ rögzített, akkor a

>

* **8.1.32. Belső automorfizmusok.** Ha G csoport és $a \in G$ rögzített, akkor a

- $122/{-11} \ldots -10$:

  $<$

arra, hogy ezekben vizsgáljuk az eredeti struktúra bizonyos tulajdonságait. Például a számítógéppel végrehajtott algoritmusok felgyorsítása is ezen a módszeren alapul.

  $>$

arra, hogy ezekben vizsgáljuk az eredeti struktúra bizonyos tulajdonságait. Bizonyos algoritmusok felgyorsítása is ezen a módszeren alapul.

- $123/{-8} \ldots -7$:

  $<$

a páros vagy páratlan szót adja, így $\ker\varphi = 2\mathbb{Z}$. ν a kanonikus leképezés G és $G/\ker\varphi$ között.

  $>$

a páros vagy páratlan szót adja, így $\ker\varphi = 2\mathbb{Z}$. A kanonikus leképezés G és $G/\ker\varphi$ között ν.

- $124/10$:

  $<$

  8.1.40. Véges Abel-csoportok alaptétele. *Egy véges Abel-csoport prímhat-*

  $>$

  * **8.1.40. Véges Abel-csoportok alaptétele.** *Egy véges Abel-csoport prímhat-*

- $126/{-14}$:

  $<$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1,2,4,3) = (1,3)(1,2)(3,4)$$

  $>$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1,2,3,4) = (1,3)(1,2)(3,4)$$

- $126/{-10}$:

  $<$

  8.1.46. Definíció. Egy G csoport egy *normállánc*án részcsoportoknak egy olyan

  $>$

  * **8.1.46. Definíció.** Egy G csoport egy *normállánc*án részcsoportoknak egy olyan

- $127/7$:

  $<$

permutációk egy részcsoportot alkotnak, amelyet A_n-nel jelölünkm, és n-edfokú *alternáló*

  $>$

permutációk egy részcsoportot alkotnak, amelyet A_n-nel jelölünk, és n-edfokú *alternáló*

- $127/12\dots13$:

$<$

nem felodható, ha $n \geq 5$.

8.1.47. Példa. Megmutatható, hogy S_4-ben

$>$

nem feloldható, ha $n \geq 5$.

* **8.1.47. Példa.** Megmutatható, hogy S_4-ben

- $127/18$:

$<$

mint tudjuk, egy alaphalmazból és rajta értelmezett két binér műveleteből állnak. A

$>$

mint tudjuk, egy alaphalmazból és rajta értelmezett két binér műveletből állnak. A

- $127/-15$:

$<$

gyűrűkre az egész számok gyűrűje és $\mathbb{Z}_m$, ferdetestre a kvarterniók, testre pedig a racio-

$>$

gyűrűkre az egész számok gyűrűje és $\mathbb{Z}_m$, ferdetestre a kvaterniók, testre pedig a racio-

- $127/-12\dots-11$:

$<$

8.2.2. Megjegyzés. Egy egységelemes integritási tartomány nyilván pontosan akkor test, ha minden nem nulla eleme egység. Egy véges integritási tartomány test, mert egy rögzített nem nulla elemmel szorozva a nem nulla elemeket, mindegyiket megkapjuk, így a nem nulla elemek körében az $ax = b$ egyenlet megoldható.

$>$

* **8.2.2. Megjegyzés.** Egy véges integritási tartomány test, mert egy rögzített nem nulla elemmel szorozva a nem nulla elemeket jobbról vagy balról, mindegyiket megkapjuk, így a nem nulla elemek körében az $ax = b$ és $ya = b$ egyenletek megoldhatók

- $128/1\dots5$:

$<$

8.2.4. Gyűrű karakterisztikája. Úgy a gyűrűknél, mint a testeknél is fontos jellemző az elemek additív rendje, amely bizonyos feltételek teljesülése esetén minden nem nulla elemnél megegyezik.

8.2.5. Tétel. *Egy nullosztómentes R gyűrűben a nemnulla elemek additív rendje megegyezik, ami vagy végtelen, vagy prímszám.*

$>$

Úgy a gyűrűknél, mint a testeknél is fontos jellemző az elemek additív rendje, amely bizonyos feltételek teljesülése esetén minden nem nulla elemnél megegyezik.

8.2.4. Tétel. *Egy nullosztómentes R gyűrűben a nem nulla elemek additív rendje megegyezik, és vagy végtelen, vagy prímszám.*

- 129/1 . . . 3 :

<

Ha ez a közös n érték véges, akkor azt mondjuk, hogy a *gyűrű karakterisztikája* n, ha pedig végtelen, akkor azt mondjuk, hogy a *gyűrű karakterisztikája* nulla. Jelölése: $\mathrm{char}(R)$.

>

8.2.5. Gyűrű karakterisztikája. Az előző tétel szerint nullosztómentes gyűrűben a nem nulla elemek additív rendje megegyezik. Ha ez a közös érték végtelen, akkor azt mondjuk, hogy a *gyűrű karakterisztikája* nulla, ha pedig egy véges n érték, akkor azt mondjuk, hogy a *gyűrű karakterisztikája* n. Jelölése: $\mathrm{char}(R)$.

- 129/−9 :

<

gyűrű /nek nevezünk. Boole-gyűrűben minden a elemre $2a = 0$, hiszen $a+a = (a+a)^2 =$

>

*gyűrű*nek nevezünk. Boole-gyűrűben minden a elemre $2a = 0$, hiszen $a + a = (a + a)^2 =$

- 130/−18 :

<

8.2.12. Példa. (1) Az egész számok gyűrűjében egy m egész szám többszörösei

>

8.2.12. Példák. (1) Az egész számok gyűrűjében egy m egész szám többszörösei

- 131/−13 :

<

8.2.18. Példa. Ha $R = \mathbb{Z}$ és $I = m\mathbb{Z}$ akkor $R/I = \mathbb{Z}_m$.

>

8.2.18. Példa. Ha $R = \mathbb{Z}$ és $I = m\mathbb{Z}$, akkor $R/I = \mathbb{Z}_m$.

- 131/−9 . . . − 6 :

<

$$(I + a)(I + b) = (8\mathbb{Z} + 4)(8\mathbb{Z} + 4) = 64\mathbb{Z}^2 + 32\mathbb{Z} + 32\mathbb{Z} + 16 = 64\mathbb{Z} + 32\mathbb{Z} + 16 \subset 16\mathbb{Z} \neq I$$

ami csupa 16-tal osztható számot tartalmaz, viszont 8ℤ+16 csupa 8-cal oszthatót, tehát kapjuk, hogy

$$(8\mathbb{Z} + 4)(8\mathbb{Z} + 4) \subset 16\mathbb{Z} \neq 8\mathbb{Z} + 16.$$

>

$$(I + a)(I + b) = (8\mathbb{Z} + 4)(8\mathbb{Z} + 4) = 64\mathbb{Z}^2 + 32\mathbb{Z} + 32\mathbb{Z} + 16 = 64\mathbb{Z} + 32\mathbb{Z} + 16 \subset 16\mathbb{Z}$$

ami csupa 16-tal osztható számot tartalmaz, viszont $8\mathbb{Z}+16$ nem, tehát kapjuk, hogy

$$(8\mathbb{Z}+4)(8\mathbb{Z}+4) \subset 16\mathbb{Z} \subsetneq 8\mathbb{Z}+16.$$

- 135/4 :

$<$

speciálisan $a = r_0$ és $b = r_1$ többszörösei d-nek.

$>$

speciálisan $a = r_0$ és $b = r_1$ többszörösei d-nek. $\square$

- 136/4 :

$<$

generátorára $b|a$, de b nem egység és nem is asszociáltja a-nak, ami lehetetlen.

$>$

generátorára $b|a$, de b nem egység és nem is asszociáltja a-nak, ami lehetetlen. $\square$

- 136/−13 :

$<$

8.2.42. Tétel. *Egy kommutatív egységelemes egyszerű gyűrű akkor és csak akkor*

$>$

* **8.2.42. Tétel.** *Egy kommutatív egységelemes egyszerű gyűrű akkor és csak akkor*

- 136/−7 :

$<$

8.2.43. Hányadostest. Legyen R integritási tartomány. Az $R \times R \setminus \{0\}$ halmazon

$>$

8.2.43. Hányadostest. Legyen R integritási tartomány. Az $R \times \big(R \setminus \{0\}\big)$ halmazon

- 137/1 . . . 7 :

$<$

8.2.44. Algebrai struktúrák. Tulajdonképpen nem csak egy vagy két műveletet definiálhatunk egy halmazon, hanem tetszőlegesen sokat, vagy akár 0-t is. Így bevezethetünk egy új fogalmat. Az algebrai struktúrákat $(H;\Omega)$ párral jelöljük, ahol H tetszőleges halmaz (alaphalmaz), és Ω H-n értelmezett műveletek halmaza. Amennyiben nem okoz félreértést, $(H;\Omega)$-t jelölhetjük egyszerűen H-val. Ha Ω az n_0 nullaváltozós, n_1 egyváltozós és rendre n_i i-változós műveletekből áll, akkor azt mondjuk, hogy az $(n_0, n_1, \dots, n_i, \dots)$ sorozat a H struktúra típusa.

$>$

* **8.2.44. Algebrai struktúrák.** Tulajdonképpen nem csak egy vagy két műveletet definiálhatunk egy halmazon, hanem tetszőlegesen sokat is. Így bevezethetünk egy új fogalmat. Az algebrai struktúrákat $(H;\Omega)$ párral jelöljük, ahol H tetszőleges halmaz (alaphalmaz), és Ω legyen H-n értelmezett (nem feltétlenül ugyanannyi változós) műveletek halmaza. Amennyiben nem okoz félreértést, $(H;\Omega)$-t jelölhetjük egyszerűen H-val. Számos tétel ilyen általánosságban is bebizonyítható.

- 138/12 . . . 15 :

<

szokás írni. Speciálisan $x = (0, e, 0, 0, \ldots)$, és indukcióval kapjuk, hogy ha $n \in \mathbb{N}$, akkor x^n olyan sorozat, amelyben az n indexű tag az e egységelem, az összes többi tag pedig nulla. Ha egy polinom főegyütthatója R egységeleme, akkor *főpolinom*nak (vagy *normált polinom*nak) nevezzük.

>

szokás írni. Ha egy polinom főegyütthatója R egységeleme, akkor *főpolinom*nak (vagy *normált polinom*nak) nevezzük.

- 139/17 . . . 22 :

<

8.3.5. Következmény. *Ha R test, akkor a $0 \neq f \mapsto \deg f$ leképezéssel $R[x]$ euklideszi gyűrű.*

Bizonyítás. Testben minden nem nulla elem egység, így minden nem nulla g-re alkalmazható az előző tétel, továbbá ha f, g nem nulla polinomok, akkor $\deg fg = \deg f + \deg g \geq \max\{\deg f, \deg g\}$. □

8.3.6. Következmény: gyöktényező leválasztása. *Ha $f \neq 0$ és c az f gyöke,*

>

8.3.5. Következmény: gyöktényező leválasztása. *Ha $f \neq 0$ és c az f gyöke,*

- 139/−1 :

<

Bizonyítás. Egyébként a különbségpolinomnak végtelen sok gyöke lenne. □

>

Bizonyítás. Egyébként a különbségpolinomnak végtelen sok gyöke lenne. □

8.3.9. Következmény. *Ha R test, akkor a $0 \neq f \mapsto \deg f$ leképezéssel $R[x]$ euklideszi gyűrű.*

Bizonyítás. Testben minden nem nulla elem egység, így minden nem nulla g-re alkalmazható az előző tétel, továbbá ha f, g nem nulla polinomok, akkor $\deg fg = \deg f + \deg g \geq \max\{\deg f, \deg g\}$. □

- 140/8 . . . 23 :

<

8.3.11. Megjegyzés: Horner-elrendezés. Az

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} \ldots a_1 x + a_0$$

polinom

$$f(x) = ((\ldots((a_n x + a_{n-1})x + a_{n-2})x + \cdots + a_1)x + a_0$$

alakú felírása adja az ötletet, hogy f egy helyettesítési értékét kiszámoljuk csupán $n - 1$ szorzással és ugyanannyi összeadással. A maradékos osztás tételét alkalmazva az f és a

$g = x - c$ polinomra azt kapjuk, hogy $f = (x - c)q + r$, ahol r konstans, értéke $f(c)$, tehát

$$f = (x - c)q + f(c).$$

	a_n	a_{n-1}	a_{n-2}	$\dots$	a_0	
c		a_n	b_{n-2}	$\dots$	b_0	$f(c)$

8.5. ábra

A táblázat (8.5. ábra) első sora f együtthatóit, míg a második sor q együtthatóit tartalmazza. A második sor első eleme kimarad, a második elem f főegyütthatója. Egyébként egy kiszámolt elemből a következőt úgy kapjuk, hogy c-vel szorozzuk, és hozzáadjuk a felette lévő számot.

>

8.3.11. Megjegyzés: Horner-elrendezés. A maradékos osztás tételét alkalmazva az f és a $g = x - c$ polinomra azt kapjuk, hogy $f = (x - c)q + r$, ahol r konstans, értéke $f(c)$. Így $n - 1$ szorzással és ugyanannyi összeadással megkaphatjuk $f(c)$-t.

- 142/13 :

<

* **Példák.** (1) Tekintsük az $\mathbb{R}[x]$ polinomgyűrűben az $(x^2 + 1)$ főideált. Minden

>

* **8.3.19. Példák.** (1) Tekintsük az $\mathbb{R}[x]$ polinomgyűrűben az $(x^2 + 1)$ főideált. Minden

- 142/−4 :

<

$\mathbb{Z}_p^n$-ben minden elem additív rendje legfeljebb p).

>

$\mathbb{Z}_p^n$-ben minden elem additív rendje legfeljebb p).

8.3.21. Tétel. *Véges test nem nulla elemeinek multiplikatív csoportja ciklikus.*

* **Bizonyítás.** Egy n rendű G ciklikus csoportban minden $d|n$ esetén pontosan egy d rendű részcsoport van. Ez ciklikus és $\varphi(d)$ generátora van. Mivel G minden eleme generál egy részcsoportot, $\sum_{d|n} \varphi(d) = n$.

Legyen most a nem nulla elemek multiplikatív csoportja G és legyen a G rendje n. Ha $d|n$ és van olyan $g \in G$, amelynek rendje d, akkor ez egy $H = \{1, g, g^2, \dots, g^{d-1}\}$ ciklikus részcsoportot generál. Mivel testben az $x^d = 1$ egyenletnek legfeljebb d megoldása van, azok mind a H részcsoportban vannak. Speciálisan, minden d rendű eleme G-nek generátora H-nak, és $\varphi(d)$ ilyen van. Így d rendű eleme G-nek 0 vagy $\varphi(d)$ darab van. Ha valamely $d|n$-re nulla lenne, az ellentmondana annak, hogy $\sum_{d|n}\varphi(d) = n$. Így van n rendű elem is, tehát G ciklikus. $\square$

- 143/13 :

  $<$

is gyök. A $g_c = (x-c)(x-\overline{c}) = x^2 - 2\Re cx + |c|^2$ valós együtthatós polinommal $\mathbb{R}$ felett

  $>$

is gyök. A $g_c = (x-c)(x-\overline{c}) = x^2 - 2\Re(c)x + |c|^2$ valós együtthatós polinommal $\mathbb{R}$ felett

- 143/−3 :

  $<$

  8.3.22. Primitív polinomok. Legyen R egy Gauss-gyűrű. Ekkor $R[x]$ egy po-

  $>$

  * **8.3.22. Primitív polinomok.** Legyen R egy Gauss-gyűrű. Ekkor $R[x]$ egy po-

- 147/−18 :

  $<$

elemet R-ben, bármely $d_j|f(c_j)$, $j = 0, 1, \ldots, n$ értékhez Lagrange-interpolációval meg-

  $>$

elemet R-ben, bármely $d_j|f(c_j)$, $j = 0, 1, \ldots, n$ értékekhez Lagrange-interpolációval meg-

- 150/1 . . . 151/14 :

  $<$

8.3.36. Többhatározatlanú polinomok. Legyen R gyűrű, $n \in \mathbb{N}$. Az R feletti n-határozatlanú *polinom*ok gyűrűjét n szerinti indukcióval definiáljuk: ha $n = 0$, legyen $R[x_1, x_2, \ldots, x_n] = R$, az egyhatározatlanú polinomok gyűrűjét már definiáltuk, ha pedig $n > 1$, akkor legyen $R[x_1, x_2, \ldots, x_n] = R[x_1, x_2, \ldots, x_{n-1}][x_n]$. Nyilván $x_1, x_2, \ldots, x_n$ helyett bármilyen más betűk is szerepelhetnek. Néha egy $f \in R[x_1, x_2, \ldots, x_n]$ polinomra inkább az $f(x_1, x_2, \ldots, x_n)$ jelölést fogjuk használni.

Könnyen látható, hogy az n-határozatlanú polinomok

$$\sum_{i_1, i_2, \ldots, i_n} f_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

alakú véges összegek, ahol $x_1, x_2, \ldots, x_n$ a „*határozatlan*ok” és $f_{i_1, i_2, \ldots, i_n} \in R$, az összeadás és szorzás pedig tagonként történik. A felírás tömörebbé tehető az alábbi módon: Az $\mathbb{N}^n$ elemeit *multiindex*eknek fogjuk nevezni. Multiindexek összegét koordinátánként definiáljuk. Ha $i = (i_1, i_2, \ldots, i_n)$, akkor legyen $x^i = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. Ezzel a jelöléssel az f polinom $\sum_i f_i x^i$ véges összegként írható. (Tulajdonképpen f egy olyan $\mathbb{N}^n$-et R-be képező függvénnyel azonosítható, amely véges sok helyen vesz fel nem nulla értéket.)

Az $a \in R$ elemhez hozzárendelve azt az f polinomot, amelyre $f_{0,0,\ldots,0} = a$ és $f_{i_1, i_2, \ldots, i_n} = 0$ egyébként, az R egy olyan leképezését kapjuk a polinomok gyűrűjébe, amely nyilván monomorfizmus, értékkészletének elemei a *konstans polinom*ok, ezeket R elemeivel azonosíthatjuk.

Az n-határozatlanú polinomok jelölésére a hagyományos

$$f = \sum_{i_1+\cdots+i_n \leq m} f_i x^i = \sum_{i_1+i_2+\cdots+i_n \leq m} f_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

felírást fogjuk használni. Gyakran az x_j^0 alakú tényezőket nem írjuk ki, x_j^1 helyett pedig x_j-t írunk. Az f_i-k az *együtthatók*, $i = (i_1, i_2, \ldots, i_n)$ az $f_i x^i$ tag *multifok*a, $i_1 + \cdots + i_n$ pedig a *fok*a. Az (egyetlen) nulladfokú tag együtthatója a polinom *konstans tag*ja. Mivel az $f = \sum_{i_1+\cdots+i_n \leq m} f_i x^i$ felírásból a nulla együtthatójú tagokat szokás elhagyni illetve a felíráshoz további nulla együtthatójú tagok adhatók hozzá, a felírás nem egyértelmű. Egyértelművé válik azonban, ha kikötjük, hogy m minimális legyen, és minden m-nél nem magasabb fokú tag szerepeljen. Ez a minimális m a polinom *fok*a, jelölése $\deg f$. (Egy másik lehetőség a felírás egyértelművé tételére, hogy minden nulla együtthatójú tagot elhagyunk.)

A nulla polinom egyértelmű felírása az üres összeg, és fokát -1-nek definiáljuk. (Vannak, akik a nulla polinom fokát a $-\infty$ szimbólumnak definiálják vagy nem definiálják.) A konstans polinomok a legfeljebb nulladfokú polinomok. A legfeljebb elsőfokú polinomok a *lineáris polinom*ok. Azokat a polinomokat, amelyek $f_i x^i$ alakba írhatók, *monom*oknak nevezzük. Ha egy polinom minden (nem nulla) tagjának ugyanaz a k a foka, akkor k-adfokú *homogén polinom*nak nevezzük.

Ha $f = \sum_i f_i x^i$ és $g = \sum_i g_i x^i$ polinomok, akkor összegük a $\sum_i (f_i + g_i) x^i$ polinom, szorzatuk pedig az a $h = fg$ polinom, amelyre $h_k = \sum_{i,j \in \mathbb{N}^n, i+j=k} f_i g_j$, ha $k \in \mathbb{N}^n$, vagy a szokásosabb módon, kiírva a multiindexek koordinátáit

$$h_{k_1,k_2,\ldots,k_n} = \sum_{i_1+j_1=k_1,\ldots,i_n+j_n=k_n} f_{i_1,i_2,\ldots,i_n} g_{j_1,j_2,\ldots,j_n}$$

(Vegyük észre, hogy ha f legfeljebb m-edfokú, g legfeljebb l-edfokú, akkor h legfeljebb $m + l$-edfokú.)

Ha R egységelemes az e egységelemmel, akkor $R[x_1, \ldots, x_n]$ is egységelemes, benne az $f_{0,0,\ldots,0} = e$ és egyébként $f_{i_1,i_2,\ldots,i_n} = 0$ összefüggéssel definiált polinom egységelem. Az $f_i x^i$ tag helyett $f_i = e$ esetén x^i-t szokás írni. Speciálisan, x_j az az f polinom, amelyre $f_{i_1,i_2,\ldots,i_n} = e$, ha $i_j = 1$ és az összes többi i_k nulla, minden más $i_1, i_2, \ldots, i_n$ indexsorozatra pedig $f_{i_1,i_2,\ldots,i_n} = 0$, továbbá indukcióval kapjuk, hogy ha $i = (i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$, akkor $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ az az f polinom, amelyre $f_{i_1,i_2,\ldots,i_n} = e$, minden más együtthatója nulla.

Ha az R gyűrű nullosztómentes, akkor az $R[x_1, x_2, \ldots, x_n]$ gyűrű is nullosztómentes, és két nem nulla polinom szorzatának a foka a fokok összege.

Számítógépen vagy az m fokszámot és az együtthatók $f_{i_1,i_2,\ldots,i_n}$, $i_j \leq m$, ha $j = 1, 2, \ldots, n$ tömbjét tároljuk, vagy a nem nulla együtthatókra az (i, f_i) párok egy láncolt listáját.

$>$

8.3.36. Többhatározatlanú polinomok. Legyen R gyűrű, $n \in \mathbb{N}$. Az R feletti n-határozatlanú *polinom*ok gyűrűjét n szerinti indukcióval definiáljuk: ha $n = 0$, legyen $R[x_1, x_2, \dots, x_n] = R$, az egyhatározatlanú polinomok gyűrűjét már definiáltuk, ha pedig $n > 1$, akkor legyen $R[x_1, x_2, \dots, x_n] = R[x_1, x_2, \dots, x_{n-1}][x_n]$. Nyilván $x_1, x_2, \dots, x_n$ helyett bármilyen más betűk is szerepelhetnek. Néha egy $f \in R[x_1, x_2, \dots, x_n]$ polinomra inkább az $f(x_1, x_2, \dots, x_n)$ jelölést fogjuk használni.

Könnyen látható, hogy az n-határozatlanú polinomok

$$\sum_{i_1, i_2, \dots, i_n} f_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

alakú véges összegek, ahol $x_1, x_2, \dots, x_n$ a „*határozatlan*ok” és $f_{i_1, i_2, \dots, i_n} \in R$. Az $a \in R$ elemhez hozzárendelve azt az f polinomot, amelyre $f_{0,0,\dots,0} = a$ és $f_{i_1, i_2, \dots, i_n} = 0$ egyébként, az R egy olyan leképezését kapjuk a polinomok gyűrűjébe, amely nyilván monomorfizmus, értékkészletének elemei a *konstans polinom*ok, ezeket R elemeivel azonosíthatjuk. Az

$$f_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

tagot *monom*nak nevezzük, $f_{i_1, i_2, \dots, i_n}$ az *együttható*ja, $(i_1, i_2, \dots, i_n)$ a *multifok*a, $i_1 + \cdots + i_n$ pedig a *fok*a. Az n-határozatlanú polinomok jelölésére a hagyományos

$$f = \sum_{i_1 + i_2 + \cdots + i_n \le m} f_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \tag{1}$$

felírást fogjuk használni. Gyakran az x_j^0 alakú tényezőket nem írjuk ki, x_j^1 helyett pedig x_j-t írunk. Az (egyetlen) nulladfokú tag együtthatója a polinom *konstans tag*ja. Mivel az (1) felírásból a nulla együtthatójú tagokat szokás elhagyni illetve a felíráshoz további nulla együtthatójú tagok adhatók hozzá, a felírás nem egyértelmű. Egyértelművé válik azonban, ha kikötjük, hogy m minimális legyen, és minden m-nél nem magasabb fokú tag szerepeljen. Ez a minimális m a polinom *fok*a, jelölése $\deg(f)$. (Egy másik lehetőség a felírás egyértelművé tételére, hogy minden nulla együtthatójú tagot elhagyunk.) A nulla polinom egyértelmű felírása az üres összeg, és fokát -1-nek definiáljuk. (Vannak, akik a nulla polinom fokát a $-\infty$ szimbólumnak definiálják vagy nem definiálják.) A konstans polinomok a legfeljebb nulladfokú polinomok. A legfeljebb elsőfokú polinomok a *lineáris polinom*ok. Ha egy polinom minden (nem nulla) tagjának ugyanaz a k a foka, akkor k-adfokú *homogén polinom*nak nevezzük.

A definícióból adódik, hogy az összeadás és szorzás tagonként történik: ha

$$g = \sum_{i_1 + i_2 + \cdots + i_n \le m} g_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

egy másik polinom, akkor összegük az

$$f + g = \sum_{i_1 + i_2 + \cdots + i_n \le m} (f_{i_1, i_2, \dots, i_n} + g_{i_1, i_2, \dots, i_n}) x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

polinom, szorzatuk pedig az a $h = fg$ polinom, amelyre

$$h_{k_1,k_2,\ldots,k_n} = \sum_{i_1+j_1=k_1,\ldots,i_n+j_n=k_n} f_{i_1,i_2,\ldots,i_n} g_{j_1,j_2,\ldots,j_n}$$

(Vegyük észre, hogy ha f legfeljebb m-edfokú, g legfeljebb l-edfokú, akkor h legfeljebb $m + l$-edfokú.) Ha az R gyűrű nullosztómentes, akkor az $R[x_1, x_2, \ldots, x_n]$ gyűrű is nullosztómentes, és két nem nulla polinom szorzatának a foka a fokok összege.

Ha R egységelemes az e egységelemmel, akkor $R[x_1, \ldots, x_n]$ is egységelemes, benne az $f_{0,0,\ldots,0} = e$ és egyébként $f_{i_1,i_2,\ldots,i_n} = 0$ összefüggéssel definiált polinom egységelem. Az

$$f_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

tag szokásos írásmódja $f_{i_1,i_2,\ldots,i_n} = e$ esetén

$$x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}.$$

Számítógépen vagy az m fokszámot és az együtthatók

$$f_{i_1,i_2,\ldots,i_n},\ i_j \leq m, \text{ ha } j = 1, 2, \ldots, n$$

tömbjét tároljuk, vagy a nem nulla együtthatókra az

$$\big((i_1, i_2, \ldots, i_n), f_{i_1,i_2,\ldots,i_n}\big)$$

párok egy láncolt listáját.

* **8.3.37. Multiindexek.** Többhatározatlanú polinomok felírása tömörebbé tehető az alábbi módon: Az $\mathbb{N}^n$ elemeit *multiindex*eknek fogjuk nevezni. Multiindexek összegét koordinátánként definiáljuk. Ha $i = (i_1, i_2, \ldots, i_n)$, akkor legyen $|i| = i_1 + i_2 + \cdots + i_n$ és $x^i = x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. Ezzel a jelöléssel az f polinom $\sum_{|i| \leq m} f_i x^i$ véges összegként írható. (Tulajdonképpen f egy olyan $\mathbb{N}^n$-et R-be képező függvénnyel azonosítható, amely véges sok helyen vesz fel nem nulla értéket.) Az $f_i x^i$ monom multifoka i, foka $|i|$.

Ha $f = \sum_i f_i x^i$ és $g = \sum_i g_i x^i$ polinomok, akkor összegük a $\sum_i (f_i + g_i) x^i$ polinom, szorzatuk pedig az a $h = fg$ polinom, amelyre $h_k = \sum_{i,j \in \mathbb{N}^n, i+j=k} f_i g_j$, ha $k \in \mathbb{N}^n$.