MBLK13E ALGEBRA ÉS SZÁMELMÉLET
(előadás vázlat)
2017-18. 1. félév

1. Komplex számok

1.1. Definíció. *Jelölje $\mathbb{R}$ a valós számok halmazát. Az $\mathbb{R} \times \mathbb{R}$ halmaz elemeit* **komplex számoknak** *nevezzük. A komplex számok halmazát $\mathbb{C}$ fogja jelölni.*

1.2. Definíció. *Legyen $(a, b), (c, d) \in \mathbb{R} \times \mathbb{R}$ két komplex szám. Összegükön és szorzatukon a következő komplex számokat értjük:*

$$(a, b) + (c, d) = (a + c, b + d),$$
$$(a, b) \cdot (c, d) = (ac - bd, ad + bc),$$

Észrevételek.
1. Az imént definiált két művelet mindegyike asszociatív és kommutatív, továbbá a szorzás disztributív az összeadásra.
2. A $(0, 0)$, és az $(1, 0)$ elemek úgy viselkednek az összeadásnál, ill. a szorzásnál, mint a valós számok esetén a 0 és az 1.
3. Egyszerű számolással kaphatók a következők:

$$(a, b) + (-a, -b) = (0, 0)$$
$$(a, b) \cdot (1, 0) = (a, b).$$

4. Az előbbiből adódik, hogy

$$-(a, b) = (-a, -b).$$

1.1. Állítás. *Ha $(a, b) \neq (0, 0)$, akkor megoldható $\mathbb{R} \times \mathbb{R}$-ben az $(a, b) \cdot (x, y) = (1, 0)$ egyenlet.*

Bizonyítás.

$$(a, b) \cdot (x, y) = (ax - by, bx + ay) = (1, 0),$$

amiből az $\mathbb{R}$ fölötti

$$ax - by = 1$$
$$bx + ay = 0$$

lineáris egyenletrendszert kapjuk. Ennek pontosan egy valós megoldása van, mivel determinánsa, $a^2 + b^2 \neq 0$:

$$x = \frac{a}{a^2 + b^2}$$
$$y = \frac{-b}{a^2 + b^2}$$

1.2. Tétel. *A komplex számok $\mathbb{C}$ halmaza az 1.2. Definícióbeli műveletekkel testet alkot.*

1.3. Állítás. *Tekintsük a* $\varphi\colon \mathbb{R} \to \mathbb{R} \times \mathbb{R},\ a \mapsto (a,0)$ *leképezést. E leképezés injektív, továbbá bármely* $a, b \in \mathbb{R}$*-re*

$$(a+b)\varphi = a\varphi + b\varphi$$
$$(ab)\varphi = a\varphi \cdot b\varphi.$$

Megjegyzések.
1. A előbbi állítás lehetővé teszi, hogy a valós számok halmazának bővítéseként tekintsük a komplex számok halmazát.
2. Az $(a,0)$ komplex számot azonosíthatjuk az a valós számmal.
3. Tetszőleges $(a,b) \in \mathbb{C}$-re az

$$(a,b) = (a,0) + (0,b) = (a,0) + (b,0)(0,1),$$

egyenlőséget és az előbbi megjegyzést figyelembe véve az (a,b) komplex szám helyett írhatunk $a+bi$-t, ahol "i" egy olyan szimbólum, amelyre $i^2 = -1$, ugyanis $(0,1)^2 = (-1,0)$.

1.3. Definíció. *Az* $a+bi$ *formális összeget az* (a,b) **komplex szám kanonikus alakjának** *nevezzük. Így azt is írhatjuk, hogy* $\mathbb{C} = \{a+bi\colon a,b \in \mathbb{R},\ i^2 = -1\}$.

A kanonikus alakban írt komplex számokal úgy számolhatunk, mint kéttagú algebrai kifejezésekkel, figyelembe véve, hogy egyrészt az i szimbólum szorzásnál fölcserélhető a valós számokkal, másrészt, hogy $i^2 = -1$.

$$\begin{aligned}
a+bi = c+di \quad &\Longleftrightarrow \quad a=c,\ b=d \\
(a+bi)+(c+di) &= (a+c)+(b+d)i \\
-(a+bi) &= (-a)+(-b)i \\
(a+bi)(c+di) &= (ac-bd)+(ad+bc)i \\
\frac{1}{a+bi} &= \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}i,\ (a^2+b^2 \neq 0)
\end{aligned}$$

1.4. Definíció. *A* $z = a+bi$ *komplex szám* **valós- ill. képzetes része** *az* a*, ill* b *valós szám. Jelölése:* $\mathrm{Re}(z) = a,\ \mathrm{Im}(z) = b$.

Megjegyzés. A komplex számoknál is alkalmazhatjuk azt a — valós számoknál megszokott — módszert, miszerint az $u+(-v)$ helyett $u-v$-t írunk, így $a+(-b)i$ helyett egyszerűen $a-bi$-t írhatunk. De ne feledjük: $\mathrm{Im}(a-bi) = -b$.

1.5. Definíció. *Legyen* $n > 1$ *természetes szám, és* z *egy komplex szám. Azt mondjuk, hogy az* **u komplex szám a z egy n-edik gyöke**, *ha* $u^n = z$.

Meg fogjuk mutatni, hogy egy z komplex számnak bármely n-re létezik n-edik gyöke, mégpedig n számú különböző, föltéve, hogy $z \neq 0$.

Kanonikus alakban általában csak a négyzetgyökök határozhatók meg, például a következő eljárással.

Ha $z = a + bi \neq 0$, akkor olyan $u = x + yi$ komplex számokat kell meghatározni, amelyekre $(x + yi)^2 = a + bi$. Az $x, y \in \mathbb{R}$ valós számok megoldásai az

$$\begin{aligned} x^2 - y^2 &= a \\ 2xy &= b \end{aligned}$$

egyenletrendszernek, amelyet egyszerű megoldani, és a $z \neq 0$ esetben két megoldást kapunk (ezek egymás -1-szeresei).

A valós számok egy egyenes, az ún. számegyenes pontjaiként reprezentálhatók, míg egy $z = a + bi$ komplex számnak a sík (a, b) koordinátájú pontját feleltethetjük meg egy olyan koordináta-rendszerben, amelynek x tengelye a (valós) számegyenes. Ez esetben szokás a síkot **számsíknak**, vagy **Gauss-féle számsíknak** nevezni. A két tengelyre használatos a valós-, ill. képzetes tengely elnevezés.

1.6. Definíció. *A $z = a + bi$ komplex számnak megfelelő (a, b) pont valós tengelyre vett tükörképének megfelelő $a - bi$ komplex számot a z* **konjugáltjának** *nevezzük. Jelölése: $\overline{z} = \overline{a + bi} = a - bi$.*

Megjegyzések.

1. Világos, hogy a $z \mapsto \overline{z}$ megfeleltetés $\mathbb{C}$-nek bijektív leképezését definiálja önmagára, és $\overline{\overline{z}} = z$ minden $z \in \mathbb{C}$-re.
2. E leképezés megőrzi a $\mathbb{C}$ halmazon korábban bevezetett műveleteket, azaz tetszőleges $z_1, z_2 \in \mathbb{C}$ komplex szám és $* \in \{+, \cdot\}$ művelet esetén

$$\begin{aligned} \overline{z_1 * z_2} &= \overline{z_1} * \overline{z_2} \\ \overline{\left(\frac{z_1}{z_2}\right)} &= \frac{\overline{z_1}}{\overline{z_2}}, \quad \text{ha } z_2 \neq 0 \end{aligned}$$

3. A konjugált segítségével egyszerűen elvégezhető s kanonikus alakú komplex számok osztása: tetszőleges $z_1, z_2 \in \mathbb{C}$ komplex számokra, ha $z_2 \neq 0$, akkor

$$\frac{z_1}{z_2} = \frac{z_1 \cdot \overline{z_2}}{z_2 \cdot \overline{z_2}}.$$

Világos, hogy a jobb oldalon a nevezőben valós szám áll.

1.7. Definíció. *Egy $z = a + bi$ komplex szám* **abszolút értéke** *a $|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}$ nemnegatív valós szám.*

Észrevételek.

- Vegyük észre, hogy egyrészt ez a definíció tartalmazza a valós számok ismert abszolút érték fogalmát, másrészt a szorzat, ill. hányados abszolút értéke megegyezik a tényezők abszolút értékének szorzatával, valamint az abszolút értékek hányadosával.

- A komplex szám geometriai interpretációjából látható, hogy valamely z komplex szám abszolút értéke éppen a neki megfelelő pontba mutató helyvektor hosszával egyenlő, továbbá az is, hogy bármely $z \in \mathbb{C}$-re $|z| = |\overline{z}|$.
- Az előbbiből következik az is, hogy a komplex számok abszolút értékére érvényes a háromszög egyenlőtlenség, azaz tetszőleges $z_1, z_2 \in \mathbb{C}$-re
$$|z_1 + z_2| \leq |z_1| + |z_2|.$$

Utóbbi észrevételeinket használva egy újabb, geometriai indíttatású jellemzését adhatjuk a komplex számoknak. Ugyanis a sík pontjait nemcsak derékszögű koordinátákkal, hanem polárkoordinátákkal is jellemezhetjük: a pontba mutató helyvektor hosszával és e helyvektornak az x tengely pozitív felével bezárt szögével.

1.8. Definíció. *A $z = a + bi$ nemzéró komplex szám* **argumentuma** *az az α szög — ívmértékben mérve — amelyet az (a, b) pontba mutató helyvektor zár be az x tengely pozitív felével. Jelölése:* $\arg z$.

Megjegyzések.
1. Az argumentum csak 2π egész számú többszöröseitől eltekintve egyértelmű.
2. A 0 komplex számhoz nem rendelünk argumentumot.
3. Ha a $z = a + bi$ nemzéró komplex számra $|z| = r$ és $\alpha = \arg z$, akkor $a = r\cos\alpha,\ b = r\sin\alpha$.

1.9. Definíció. *A z nemzéró komplex szám* **trigonometrikus alakja**
$$z = r(\cos\varphi + i\sin\varphi),$$
ahol $r = |z|,\ \varphi = \arg z$. Ha $u = s(\cos\psi + i\sin\psi)$, akkor $z = u$ pontosan akkor áll fönn, ha $r = s$ és $\varphi - \psi = 2k\pi$ valamely k egész számra.

Megjegyzés. Az összeadás nehezen végezhető el trigonometrikus alakban (arra rendelkezésre áll a kanonikus alak), de a szorzás és az osztás elvégzése már igen egyszerű feladat a következő állítás alapján.

1.4. Állítás. *Tetszőleges $z, u \in \mathbb{C}$ nemzéró komplex számokra* $\arg(zu) = \arg z + \arg u$, *és* $\arg\dfrac{z}{u} = \arg z - \arg u$.

Legyen $n > 1$ természetes szám. Az előbbi állítás alapján, ha $z, u \in \mathbb{C},\ z = r(\cos\varphi + i\sin\varphi),\ u = s(\cos\psi + i\sin\psi)$ olyan komplex számok, hogy $u^n = z$, akkor $r = s^n$ és $n\psi = \varphi + 2k\pi$ valamilyen $k \in \mathbb{Z}$-re. Ezekből
$$s = \sqrt[n]{r}, \qquad \text{és} \qquad \psi = \frac{\varphi + 2k\pi}{n},\ k \in \mathbb{Z}.$$
Világos, hogy tetszőleges $k \in \mathbb{Z}$-re az
$$u_k = \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right)$$

komplex számok mindegyikére $u_k^n = z$, azaz z n-edik gyöke, de nem mind különbözők. A trigonometrikus függvények periódikussága miatt

$$u_k = u_l \qquad \text{pontosan akkor teljesül, ha} \qquad n|k-l.$$

Ezzel igazoltuk a következő tételt.

1.5. Tétel. *Egy nemzéró komplex számnak pontosan n számú különböző n-edik gyöke van bármely $n > 1$ természetes számra.*

1.10. Definíció. *Azon komplex számokat, amelyek n-edik hatványa valamely $n > 1$ természetes számra* 1,**n-edik egységgyököknek** *nevezzük.*

Az egységgyökök abszolút értéke nyilván 1, így azok az

$$\varepsilon_{n,k} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad n \in \mathbb{N},\ 0 \le k < n$$

komplex számok. Ezek a számsíkon az egységkörön helyezkednek el. Rögzített n-re az $(1,0)$ ponttól indulva egy szabályos n-szög csúcspontjaiban.

Észrevételek.

- Tetszőleges $0 \le k, l < n$-re $\varepsilon_{n,1}^k = \varepsilon_{n,1}^l$ maga után vonja, hogy $k = l$, azaz $\varepsilon_{n,1}$-nek pontosan n számú különböző hatványa van, amelyek kiadják az összes különböző n-edik egységgyököt.
- Ilyen tulajdonságú egységgyök több is van, például $\varepsilon_{n,n-1}$.

1.11. Definíció. *Azt mondjuk, hogy az ε n-edik egységgyök* **primitív n-edik egységgyök**, *ha pontosan n számú különböző egész kitevős hatványa van. Másképpen mondva, egész kitevős hatványaként az összes n-edik egységgyök előáll..*

Iménti észrevételeinkből könnyen adódik a következő tétel.

1.6. Tétel. *Az $\varepsilon_{n,k} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ komplex szám akkor és csak akkor primitív n-edik egységgyök, ha* $\ln.\,\mathrm{k.\,o.}(n,k) = 1$.

1.7. Következmény. *Tetszőleges $n > 1$ természetes számra létezik primitív n-edik egységgyök, mégpedig annyi, ahány n-hez relatív prím szám van az $1, 2, \ldots, n$ egészek között (azaz számuk $\varphi(n)$, ahol φ az ún. Euler-függvény).*

1.8. Következmény. *Legyen $n > 1$ természetes szám. Tetszőleges $z \in \mathbb{C}$ komplex szám összes különböző n-edik gyöke felírható $u\varepsilon_1, \ldots, u\varepsilon_n$ alakban, ahol $u^n = z$, és $\varepsilon_1, \ldots, \varepsilon_n$ az összes különböző n-edik egységgyök, illetve $u\varepsilon^k$, $0 \le k < n$ alakban, ahol ε egy primitív n-edik egységgyök.*

1.9. Tétel. *Tetszőleges $n > 1$ természetes számra az összes (különböző) n-edik egységgyök összege* 0.

Megjegyzés. Emlékeztetünk arra, hogy a valós számok halmazán létezik egy olyan rendezés, amelyre nézve az összeadás és a szorzás bizonyos monotonitási tulajdonsággal rendelkezik. Nevezetesen, tetszőleges $a, b, c \in \mathbb{R}$ esetén, egyrészt $a \leq b$ maga után vonja, hogy $a + c \leq b + c$ másrészt, ha $c > 0$, akkor $ac \leq bc$ is következik. Igazolható, hogy ez abból következik, hogy létezik olyan $P \subset \mathbb{R}$ részhalmaz, amely egyrészt zárt az összadásra és a szorzásra, másrészt tetszóleges $d \in \mathbb{R}$ esetén a $d \in P,\ -d \in P$ és a $d = 0$ állítások közül pontosan egy igaz.

A komplex számok halmazának ilyen tulajdonságú részalmaza nincs. Ugyanis, ha a nemüres $A \in \mathbb{C}$ halmaz zárt az összeadásra, akkor mind az $i \in A$, mind a $-i \in A$ állításból $i = 0$ adódna, ami nem igaz. Így a komplex számok halmazán nem definiálható olyan rendezés, amelyre nézve az összeadás és a szorzás — a valós számokra teljesülőhöz hasonló — monotonitási tulajdonságokat mutat.

2. Harmad- és negyedfokú egyenletek.

A komplex számok bevezetésének egyik idítéka az, hogy körükben már minden másodfokú egyenlet megoldható. Később látni fogjuk, hogy ennél lényegesen több is igaz, nevezetesen: a komplex számok teste algebrailag zárt. Ez azt jelenti, hogy tetszőleges fokszámú (persze legalább elsőfokú) komplex együtthatós „algebrai" egyenletnek van komplex gyöke. Erre a kérdéskörre később még visszatérünk. Így a későbbiek teszik teljessé és pontosabban érthetővé a most tárgyalandó speciális eseteket, a harmad- és a negyedfokú egyenletek megoldási eljárását.

Az $ax^3 + bx^2 + cx + d = 0,\ a, b, c, d \in \mathbb{C}$ egyenletből $x = y - \frac{b}{3a}$ helyettesítéssel, majd a kezdő együtthatóval való leosztás után

$$y^3 + py + q = 0$$

alakú harmadfokú egyenlethez juthatunk. Ha ennek megoldásait $y = u + v$ alakban keressük, akkor ezen új határozatlanokra teljesülnie kell az

$$3uv = -p$$
$$u^3 + v^3 = -q$$

egyenletrendszernek. Ugyanis, az $(u + v)^3 = (u^3 + v^3) + 3uv(u + v)$ egyenlőségből

$$(u + v)^3 - 3uv(u + v) - (u^3 + v^3) = 0$$

egynlőség adódik, amit az $y^3 + py + q = 0$ egyenlettel együtthatónként összehasonlítva kapjuk az előbbi egyenletrendszert.

A másodfokú egyenletek gyökei és együtthatói közötti ismert összefüggések (Viète-képletek) alapján u^3, v^3 megoldása a

$$z^2 + qz - \left(\frac{p}{3}\right)^3 = 0$$

másodfokú egyenletnek. Ebből

$$u^3, v^3 = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}.$$

A köbgyökvonások elvégzése után az

$$u, u\varepsilon, u\varepsilon^2, \qquad v, v\varepsilon, v\varepsilon^2$$

számokat kapjuk, ahol e egy harmadik primitív egységgyök. Egyszerűen ellenőrizhető, hogy csak az

$$y_1 = u + v, \qquad y_2 = u\varepsilon + v\varepsilon^2, \qquad y_3 = u\varepsilon^2 + v\varepsilon$$

értékek megoldások. Az

$$y = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

összefüggést **Cardano-képletnek** szokás nevezni, mert az ő 1545-ben megjelent Ars Magna című könyvében szerepelt először (bár nem ő találta meg) valós együtthatókkal.

Példa. Megoldjuk az $x^3 + 9x^2 + 18x + 28 = 0$ egyenletet.

(1) Az $x = y - 3$ helyettesítés után az $y^3 - 9y + 28 = 0$ egyenlethez jutunk.
(2) A Cardano-képlettel számolva:

$$u, v = \sqrt[3]{-14 \pm \sqrt{14^2 - 3^3}} = \sqrt[3]{14 \pm 13},$$

így $u = -1$ és $v = -3$.
(3) Tovább számolva: $y_1 = -4,\ y_2 = -(-\frac{1}{2} + i\frac{\sqrt{3}}{2}) - 3(-\frac{1}{2} - i\frac{\sqrt{3}}{2}) = 2 + \sqrt{3}i,$
$y_3 = -(-\frac{1}{2} - i\frac{\sqrt{3}}{2}) - 3(-\frac{1}{2} + i\frac{\sqrt{3}}{2}) = 2 - \sqrt{3}i.$
(4) Végül: $x_1 = -7,\ x_2 = -1 + \sqrt{3}i,\ x_3 = -1 - \sqrt{3}i.$

Az $x^4 + ax^3 + bx^2 + cx + d = 0,\ a, b, c, d, \in \mathbb{C}$ alakú egyenletek megoldási eljárását először Ferrari találta meg a XVI. században (természetesen valós együtthatókkal), és ezt is Cardano publikálta előbbi könyvében. Ferrari ötletét némileg modernizálva: az egyenlet bal oldalát két másodfokú polinom szorzatára bontjuk. Ezt pedig úgy érhetjük el a legkönnyebben, ha előbb két, legföljebb másodfokú, polinom négyzetének különbségeként írjuk azt.

Jelölje f egyenletünk bal oldalát és legyen $g = x^2 + \frac{a}{2}x + \alpha$, ahol α később meghatározandó komplex szám.

$$f - g^2 = x^4 + ax^3 + bx^2 + cx + d - \left(x^4 + ax^3 \left(\frac{a^2}{4} + 2\alpha\right) x^2 + a\alpha x + \alpha^2\right)$$
$$= \left(b - \frac{a^2}{4} - 2\alpha\right) x^2 + (c - a\alpha)x + (d - \alpha^2)$$

Az $f - g^2$ másodfokú polinom pontosan akkor lesz egy (elsőfokú) polinom négyzete, a két gyöke egybeesik, ami akkor teljesül, ha diszkriminánsa zéró. Ez pedig α-ra egy harmadfokú egyenletet ad, amelyet a Cardano által leírt eljárással oldhatunk meg. Világos, hogy az α-ra kapott bármelyik értéket is használjuk, megkapjuk a kívánt fölbontást.

Példa. Oldjuk meg az $x^4 - 2x^3 + 2x^2 + 4x - 8 = 0$ egyenletek

(1) Jelölje f az egyenlet bal oldalán álló polinomot. Ekkor tetszőleges $\alpha \in \mathbb{C}$-re
(2) $f = (x^2 - x + \alpha)^2 - ((2\alpha - 1)x^2 - (2\alpha - 4)x + (\alpha^2 + 8)),$
(3) A második tag, a másodfokú polinom, pontosan akkor teljes négyzet, ha D diszkriminánsa 0:

$$D = (2\alpha + 4)^2 - 4(2\alpha - 1)(\alpha^2 + 8) = -8\alpha^3 + 8\alpha^2 - 48\alpha + 48 = 0.$$

(4) Megoldandó tehát az

$$\alpha^3 - \alpha^2 + 6\alpha - 6 = 0$$

harmadfokú egyenlet.

(5) Azonnal látszik, hogy $\alpha = 1$ egy megoldás, így az

$$f = (x^2 - x + 1)^2 - (x - 3)^2 = (x^2 - 2)(x^2 - 2y + 4)$$

fölbontást kapjuk.

(6) A gyökök tehát:

$$x_{1,x} = \pm\sqrt{2} \qquad \text{és} \qquad x_{3,4} = 1 \pm \sqrt{3}i.$$

A következő 2.1. Tétel következménye (2.2. Következmény) alapján azonban csak négy — nem föltétlenül különböző — megoldást kapunk.

A harmad- és negyedfokú egyenletek megoldóképlete (megoldási eljárása) megtalálása után több, mint 200 évig kiváló matematikusok hada kereste a négynél magasabbfokú egyenletek megoldóképletét, megoldási eljárását. Alapvetően abból indultak ki, hogy a másodfokú egyenlet megoldása egy elsőfokú-, a harmadfokúé egy másodfokú-, míg a negyedfokú egyenlet megoldása egy harmadfokú egyenlet megoldására vezethető vissza. Azt föltételezték, hogy ez továbbvihető, és általában az n-edfokú egyenlet megoldása egy $n-1$-edfokú egyenlet megoldására, egy ún. *rezolvens egyenlet* megoldására vezethető vissza.

Tették ezt annak ellenére, hogy egészent a XVIII. század legvégéig az sem volt ismert, hogy minden ún. algebrai egyenletnek van megoldása, másképpen mondva minden legalább elsőfokú komplex együtthatós polinomnak (ezt később pontosítjuk) van komplex zéróhelye. Ugyanis csak 1799-ben igazolta (először) Gauss a következő tételt.

2.1. Tétel. *Minden, legalább elsőfokú, komplex együtthatós polinomnak van komplex zéróhelye, azaz az* $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ *komplex együtthatós egyenletnek van gyöke a komplex számok testében.*

2.2. Következmény. *Egy n-edfokú komplex együtthatós polinomnak pontosan n számú — nem föltétlenül különböző — komplex zéróhelye van.*

Megjegyzés. Az előbbi tételt régebben úgy emlegették, mint az **algebra alaptétele**, de ma már a pontosabb elnevezést, a **klasszikus algebra alaptétele**, használják.

Kiegészítés. Először a XIX. század elején az olasz P. Ruffini igazolta, hogy az ötöd- és magasabbfokú egyenletekre nem létezik sem gyökképlet, sem általános megoldási eljárás. Bizonyítása azonban hiányos volt. E tényre az első korrekt bizonyítást a norvég N. H. Abel adta meg 1826-ban. Néhány évvel később a francia E. Galois — elődeitől teljesen eltérő megközelítést és meggondolásokat alkalmazva — megadta annak föltételét, hogy egy polinom zéróhelyei véges sok lépésben,

a testműveleteket és egész kitevős gyökvonásokat alkalmazva, előállíthatók legyenek a polinom együtthatóiból.

3. Bevezetés az absztrakt algebrába 1. Gyűrűk és testek.

E fejezet elején — az olvasó kényelmére — megismétlünk néhány olyan fogalmat, tételt, amelyek már ismertek korábbi kurzusokból.

3.1. Definíció. *Legyen G nemüres halmaz. A $(G,\cdot)$ algebrát* **csoportnak** *nevezzük, ha*

- *a "$\cdot$" művelet asszociatív (másképpen mondva a $(G,\cdot)$ algebra félcsoport), azaz tetszőleges $a,b,c\in G$-re $(a\cdot b)\cdot c=a\cdot(b\cdot c)$;*
- *létezik olyan $e\in G$, hogy bármely $a\in G$-re $e\cdot a=a\cdot e=a$, azaz e egységelem;*
- *minden $a\in G$-hez van olyan $a'\in G$ elem, hogy $a\cdot a'=a'\cdot a=e$, azaz G minden elemének van inverze.*

Azt mondjuk, hogy a $(G,\cdot)$ csoport **Abel-csoport**, *ha a művelete kommutatív.*

Megjegyzés. A "$\cdot$" műveleti jelet általában nem fogjuk kiírni, $a\cdot b$ helyett egyszerűen ab-t írunk.

3.2. Definíció. *Az $(A;+,\cdot)$ algebrát* **gyűrűnek** *nevezzük, ha $(A;+)$ Abel-csoport (a gyűrű additív csoportja), $(A;\cdot)$ félcsoport (a gyűrű multiplikatív félcsoportja), továbbá bármely $a,b,c\in A$-ra*

$$a(b+c)=ab+ac$$
$$(a+b)c=ac+bc,$$

azaz $a\cdot$ művelet **disztributív** *az $+$ műveletre. Ha a gyűrű multiplikatív félcsoportja kommutatív/egységelemes, akkor azt mondjuk, hogy a gyűrű kommutatív/egységelemes.*

Példák.
$(\mathbb{Z};+,\cdot)$, $(\mathbb{Q};+,\cdot)$, $(\mathbb{C};+,\cdot)$, $\mathcal{M}_n(\mathbb{R})=(\mathbb{R}^{n\times n};+,\cdot)$, $(\mathbb{Z}_n;+,\cdot)$, $(n\in\mathbb{N})$, ahol $\mathbb{R}^{n\times n}$ az összes valós elemű $n\times n$ típusú mátrix halmaza;
$(\mathcal{P}(U);\triangle,\cap)$, (ahol $\mathcal{P}(U)$ az U halmaz hatványhalmaza, míg $\triangle$ a szimmetrikus differenciát jelöli), $\mathbb{Z}[i]=\{a+bi\colon a,b\in\mathbb{Z}\}$,
$\mathbb{Z}[\alpha]=\{a+b\alpha\colon a,b\in\mathbb{Z},\ \alpha^3=1,\alpha\neq 1\}$. Az utóbbi két esetben a műveletek a komplex számok szokásos összeadása és szorzása.

Megjegyzés. Az előbbiek közül az $\mathcal{M}_n(\mathbb{R})$, $\mathbb{Z}[i]$, $\mathbb{Z}[\alpha]$ gyűrűkre mint az $\mathbb{R}$ fölötti $n\times n$-es teljes mátrixgyűrű, a másik kettőre pedig mint a Gauss-, ill. Euler-egészek gyűrűje fogunk hivatkozni. A Gauss-egészekkel később részletesebben is foglakozunk.

3.1. Tétel. *Tetszőleges $(A;+,\cdot)$ gyűrű esetén a 0 (az additív csoport egységeleme) a szorzásra nézve zéruselem, továbbá tetszőleges $a,b\in A$-ra $(-a)\cdot b=a\cdot(-b)=-(a\cdot b)$.*

Jelölés. Tetszőleges gyűrűben 0 jelöli majd az additív egységelemet, $-a$ az a elem additív inverzét, továbbá 1 a multiplikatív egységelemet (ha van).
Bizonyítás. Legyenek $a, b \in A$ tetszőleges elemek.

$$0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a \qquad \Rightarrow \quad 0 = 0 \cdot a.$$
$$a \cdot (-b) + a \cdot b = a \cdot (-b+b) = a \cdot 0 = 0$$

Az utóbbihoz hasonlóan mutatható meg, hogy $(-a) \cdot b$ is additív inverze $a \cdot b$-nek, de az inverz asszociatív művelet esetén egyértelmű (ezt később igazolni is fogjuk).
Megjegyzés. Használni fogjuk az $a - b = a + (-b)$ írásmódot.

3.3. Definíció. *Legyen R gyűrű. Azt mondjuk, hogy a nemzéró $a \in R$ elem* **baloldali zérusosztó***, ha van olyan nemzéró $b \in R$ elem, amelyre $ab = 0$. Ezen $b \in R$ elemet* **jobboldali zérusosztónak** *nevezzük. Azt mondjuk, hogy az R gyűrű* **zérusosztómentes gyűrű***, ha nem tartalmaz sem baloldali-, sem jobboldali zérusosztót, azaz bármely $a, b \in R \setminus \{0\}$ elemekre $ab \neq 0$. Ha röviden csak zérusosztót mondunk, az bármely oldali zérusosztót jelenthet.*

Példák.
(1) A $\mathbb{Z}_6$ maradékosztálygyűrűben $\overline{2}, \overline{3}$ zérusosztók.
(2) A teljes mátrixgyűrűk sem zérusosztómentesek. Hasznos gyakorló feladat a zérusosztó keresés pl. az $\mathcal{M}_2(\mathbb{R})$ gyűrűben.

3.4. Definíció. *A legalább kételemű, egységelemes, kommutatív, zérusosztómentes gyűrűt* **integritástartománynak** *nevezzük.*

Megjegyzések.
(1) A „legalább kételemű" megkötés az egyetlen zéróelemből álló gyűrűt zárja ki az integritástartományok köréből.
(2) Amennyiben nem okoz félreértést, a gyűrűk, és a további algebrák esetén a műveleti jelek föltüntetésétől eltekintünk, azokat tartó(alap)halmazuk jelével adjuk meg,

3.5. Definíció. *Legyen R integritástartomány és $a, b \in R$. Azt mondjuk, hogy a* **osztója** *b-nek (b* **osztható** *a-val) — jelölése $a|b$ —, ha van olyan $c \in R$, hogy $ac = b$. Az egységelem osztóit* **egységeknek** *nevezzük. Az egységek a gyűrű invertálható elemei. Ha $a|1$ akkor azon $c \in R$ elemet, amelyre $ac = 1$ a* **inverzének** *nevezzük, és használjuk a $c = a^{-1}$ jelölést.*

3.2. Állítás. *Az integritástartományokban az előbb bevezetett oszthatóság rendelkezik mindazon tulajdonságokkal, amelyekkel az egész számok gyűrűjében megismert oszthatóság bír, kivéve, hogy most bármely a, b elemre*

$$a|b \text{ és } b|a \;\Rightarrow\; ac = b \text{ valamely } c|1 \text{ -re.}$$

Bizonyítás. Csak az egész számokétól (látszólag) eltérő tulajdonságot részletezzük. Legyen R integritástartomány és $a, b \in R$. Ha $a|b$ és $b|a$, akkor $ac = b$ és $bd = a$ valamely $c, d \in R$ elemekre. A két egyenlőségből $cd = 1$ adódik, azaz c, d invertálható elemek, egységek.

Vegyük észre, hogy ha $R = \mathbb{Z}$, akkor a $cd = 1$ egyenlőségből $c = d = 1$, vagy $c = d = -1$ következik, azaz $|a| = |b|$ ebben az esetben.

3.3. Tétel. *Tetszőleges R integritástartomány invertálható elemeinek R^* halmaza (Abel)csoportot alkot a szorzással.*

Bizonyítás. Ismét fölhasználva az inverz egyértelműségét, csak azt kell igazolni, hogy invertálható elemek szorzata is invertálható. Ez nem kommutatív művelet esetén is igaz: tetszőleges $a, b \in R$ invertálható elemekre

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1,$$

azaz ab is invertálható, mert a $(b^{-1}a^{-1})(ab) = 1$ egyenlőség ugyanígy kapható.

3.6. Definíció. *Az R integritástartomány egységeinek R^* multiplikatív csoportját R* **egységcsoportjának** *nevezzük.*

3.4. Tétel. *Integritástartományban bármely nemzéró elemmel lehet egyszerűsíteni, azaz ha c az R integritástartomány egy nemzéró eleme, akkor tetszőleges $a, b \in R$ elemekre*

$$ac = bc \qquad \Rightarrow \qquad a = b.$$

Bizonyítás. Legyen R integritástartomány, $a, b, c \in R$, $c \neq 0$. Ha $ac = bc$, akkor $0 = ac - bc = (a - b)c$, amiből a zérusosztómentesség miatt $a - b = 0$, azaz $a = b$ következik.

3.7. Definíció. *Legyen R integritástartomány. Azt mondjuk, hogy az $a, b \in R$ elemek* **asszociáltak**, *jelölése: $a \sim b$, ha $a|b$ és $b|a$.*

3.5. Állítás. *Legyen R integritástartomány. Az $a, b \in R$ elemek pontosan akkor asszociáltak, ha valamely c egységre $ac = b$.*

3.6. Állítás. *Az egész számok gyűrűjében két egység van: ± 1, míg a Gauss-egészek gyűrűjének egységei a negyedik egységgyökök: $\pm 1, \pm i$.*

3.7. Állítás. *Tetszőleges $n > 1$ természetes számra a $\mathbb{Z}_n$ maradékosztálygyűrű egységei azon $\overline{a}$ maradékosztályok, amelyekre* $\ln. \text{k. o.}(a, n) = 1$.

Bizonyítás. Állításunk abból a tényből következik, hogy ha egy maradékosztály valamely eleme relatív prím a modulushoz, akkor az adott osztály minden eleme relatív prím a modulushoz. Legyen $\ln. \text{k. o.}(a, n) = 1$ és $b \in \overline{a}$. Mivel $b = a + kn$ valamely $k \in \mathbb{Z}$-re,

$$\ln. \text{k. o.}(b, n) = \ln. \text{k. o.}(a + kn) = \ln. \text{k. o.}(a, n) = 1,$$

a legnagyobb közös osztónak az elemi számelméletben megismert tulajdonságai alapján

Megjegyzés. Az egységek az invertálható elemek, így e fogalom tetszőleges egységelemes gyűrűben is bevezethető. Például, az $\mathcal{M}_n(\mathbb{R})$ mátrixgyűrű egységei a nemzéró determinánsú mátrixok.

3.8. Definíció. *Legyen R integritástartomány, $a, b \in R$. Azt mondjuk, hogy $c \in R$ az a, b elemek egy* **legnagyobb közös osztója**, *ha $c|a$ és $c|b$, továbbá valahányszor egy $d \in R$-re $d|a$ és $d|b$, mindannyiszor $d|c$. Másképpen mondva: a legnagyobb közös osztó egy olyan közös osztó, amelynek mindegyik közös osztó osztója. Jelölése: $c \sim \text{ln. k. o.}(a, b)$.*

3.9. Definíció. *Legyen R integritástartomány, $a, b \in R$. Azt mondjuk, hogy $d \in R$ az a, b elemek egy* **legkisebb közös többszöröse**, *ha $a|d$ és $b|d$, továbbá valahányszor egy $c \in R$-re $a|c$ és $b|c$, mindannyiszor $d|c$. Másképpen mondva: a legkisebb közös többszörös olyan közös többszörös, amely mindegyik közös többszörösnek osztója. Jelölése: $d \sim \text{lk. k. t.}(a, b)$.*

Az oszthatóság tulajdonságaiból azonnal adódik a következő állítás.

3.8. Állítás. *Integritástartományban a legnagyobb közös osztó, ill. a legkisebb közös többszörös — ha léteznek — csak asszociáltság erejéig meghatározottak.*

Megjegyzés. Az általában nem igaz, hogy egy integritástartomány bármely két elemének létezik legnagyobb közös osztója a $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \colon a, b \in \mathbb{Z}\}$ integritástartományban a 9, $3(2 + i\sqrt{5})$ elempár ilyen. (Igazolja!)

3.10. Definíció. *Legyen R integritástartomány. Azt mondjuk, hogy az $a, b \in R$ elemek* **relatív prímek**, *ha $\text{ln. k. o.}(a, b) \sim 1$.*

3.11. Definíció. *Az $(A; +, \cdot)$ legalább kételemű gyűrűt* **testnek** *nevezzük, ha az $(A \setminus \{0\}; \cdot)$ algebra Abel-csoport, amelyet a test multiplikatív csoportjának nevezünk.*

Megjegyzések.
1. Az előbbi példák közül $(\mathbb{Z}; +, \cdot)$, $\mathbb{Z}[i]$ integritástartományok. Az összes páros számok halmaza a szokásos műveletekkel kommutatív zérusosztó mentes gyűrű, DE nem integritástartomány, mert nincs egységeleme.
2. Az előbbi példák közül $(\mathbb{Q}; +, \cdot)$, $(\mathbb{C}; +, \cdot)$, $\mathbb{Q}(\alpha) = \{a + b\alpha \colon a, b \in \mathbb{Q},\ \alpha^3 = 1, \alpha \neq 1\}$, továbbá tetszőleges p prímre $(\mathbb{Z}_p; +, \cdot)$ testek.
3. Vegyük észre, hogy a testek integritástartományok.

3.9. Tétel. *Legyen F test, $n > 1$ egész. Az F-fölötti $n \times n$-es mátrixok $\mathcal{M}_n(F)$ gyűrűje egységelemes, de se nem kommutatív, se nem zérusosztómentes. E gyűrű egységei (mint speciális esetben már említettük) a nemzéró determinánsú mátrixok.*

Megjegyzés. Korábban említettük, hogy integritástartományokban, sőt egységelemes gyűrűkben is, az invertálható elemek csoportot alkotnak. Az $\mathcal{M}_n(F)$ test fölötti teljes mátrixgyűrűk esetént az ilyen

csoportokat **általános lineáris csoportnak** nevezzük, és használjuk rájuk a $\mathrm{GL}_n(F)$ jelölést.

3.10. Tétel. *Tetszőleges $m \geq 2$ egészre a modulo m maradékosztályok $\mathbb{Z}_m$ halmaza az ismert összeadással és szorzással egységelemes kommutatív gyűrűt alkot. Ezen gyűrű egységei éppen a redukált maradékosztályok (halmazukat $\mathbb{Z}_m^*$ jelöli). Ha m prím, akkor $\mathbb{Z}_m$ test, míg ha m öszetett szám, akkor a $\mathbb{Z}_m$ gyűrű tartalmaz zérusosztót, így nem integritástartomány.*

Bizonyítás. Az előzmények alapján csak az szorul igazolásra, hogy tetszőleges p prímre a $\mathbb{Z}_p$ gyűrűk testek. Ez pedig abból következik, hogy tetszőleges $1 \leq a < p$-re az $ax \equiv 1 \pmod{p}$ kongruencia megoldható, tehát a gyűrű minden nemzéró elemének van multiplikatív inverze.

3.12. Definíció. *A $\mathbb{Z}_m$ gyűrűt* **modulo m maradékosztálygyűrűnek**, *míg ha p prímszám, akkor a $\mathbb{Z}_p$ testet* **maradékosztály-testnek** *nevezzük.*

3.11. Állítás. *A Gauss-egészek $\mathbb{Z}[i] = \{a + bi \colon a, b \in \mathbb{Z},\ i^2 = -1\}$ halmaza a komplex számok ismert összeadásával és szorzásával integritástartomány, amelynek egységei a negyedik egységgyökök: $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.*

4. A klasszikus számelmélet néhány kérdése,

Kezdetként emlékeztetünk néhány olyan — más kurzusban már megismert — fogalomra és tételre, amelyek alapvető fontosságúak lesznek az elkövetkezőkben. A fejezet egyes tételei megfogalmazásában és/vagy bizonyításában föl fogunk használni — az előző fejezetben ismertetett — gyűrűelméleti fogalmakat, összefüggéseket.

4.1. Kongruenciák, néhány klasszikus kongruenciatétel.

4.1. Definíció. *Legyen* $a, b, m \in \mathbb{Z},\ m > 1$. *Azt mondjuk, hogy* a **kongruens** b**-vel modulo** m, *ha* $m|a-b$. *Ezen relációt* **modulo m kongruencia relációnak** *nevezzük. Jelölése:* $a \equiv b \pmod{m}$.

4.1. Állítás. *Az imént definiált modulo m kongruencia reláció ekvivalenciareláció az egész számok* $\mathbb{Z}$ *halmazán.*

4.2. Tétel. *Legyenek* a_1, a_2, b_1, b_2, m *tetszőleges egészek, és* $m > 1$, *továbbá* $a_i \equiv b_i \pmod{m},\ i = 1, 2$. *Ekkor*

$$a_1 + a_2 \equiv b_1 + b_2 \pmod{m}, \qquad \text{és} \qquad a_1 a_2 \equiv b_1 b_2 \pmod{m}.$$

4.3. Tétel. *Legyenek* $a, b, c, m \in \mathbb{Z},\ m > 1$. *Ekkor* $ca \equiv cb \pmod{m}$ *maga után vonja, hogy* $a \equiv b \pmod{\frac{m}{\text{ln.k.o.}(m,c)}}$.

4.4. Állítás. *Legyen* $a, b, m \in \mathbb{Z},\ m > 1$. *Pontosan akkor létezik olyan* $c \in \mathbb{Z}$, *hogy* $ac \equiv b \pmod{m}$, *másképpen mondva pontosan akkor oldható meg az* $ax \equiv b \pmod{m}$ *ún. lineáris kongruencia, ha* $\text{ln. k. o.}(a, m)|b$. *E lineáris kongruenciának modulo m kongruenciától eltekintve* $\text{ln. k. o.}(a, m)$ *számú modulo m inkongruens megoldása van.*

4.5. Állítás. *Legyen* $a, b, c \in \mathbb{Z}$. *Az* $ax + by = c$ *diophantoszi egyenletnek ponosan akkor van egész megoldása, ha* $\text{ln. k. o.}(a, b)|c$. *Ha* x_0, y_0 *megoldások, akkor egyenletünk összes megoldása*

$$x_0 + \frac{b}{\text{ln. k. o.}(a,b)}t, \qquad y_0 - \frac{a}{\text{ln. k. o.}(a,b)}t, \qquad t \in \mathbb{Z}.$$

4.2. Definíció. *Az* $\mathbb{N} \to \mathbb{C}$ *leképezéseket* **számelméleti függvényeknek** *nevezzük.*

Megjegyzés. E kurzusban csak olyan számelméleti függvényekkel foglalkozunk, amelyek értékkészlete az egész számok halmazának egy részhalmaza.

Példák.

(1) $\sigma(n) = n$ pozitív osztói száma,
(2) $\tau(n) = n$ pozitív osztói összege.

4.3. Definíció. *Jelölje* $\varphi(n)$ *tetszőleges* $n \in \mathbb{N}$*-re az n-nél nem nagyobb n-hez relatív prím természetes számok számát. E (számelméleti) függvényt* **Euler-féle** φ **függvénynek** *nevezzük.*

4.6. Állítás. *Legyen $m > 1$ egész. A $\mathbb{Z}_m$ maradékosztálygyűrű egységeinek (invertálható elemeinek) száma éppen $\varphi(m)$.*

4.4. Definíció. *Azt mondjuk, hogy az f számelméleti függvény* **gyengén multiplikatív**, *ha tetszőleges $a, b \in \mathbb{N}$-re $f(ab) = f(a)f(b)$, valahányszor* $\ln.\,k.\,o.(a, b) = 1$.

4.7. Tétel. *Az Euler-féle φ függvény gyengén multiplikatív.*

Megjegyzés. E tételnek egy elemi bizonyítása olvasható Megyesi, Bevezetés a számelméletbe c. Polygon jegyzetében.

Fölhasználva az Euler-függvény gyengén multiplikatív voltát egyszerűen kiszámíthatjuk e függvény értékeit. Ugyanis, ha $a = p_1^{m_1} \dots p_k^{m_k}$, ahol a p_i-k különböző prímek, akkor

$$\begin{aligned}\varphi(a) &= \varphi(p_1^{m_1}) \dots \varphi(p_k^{m_k}) \\ &= \prod_{i=1}^{k} (p_i^{m_i} - p_i^{m_i - 1}) \\ &= a \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).\end{aligned}$$

4.5. Definíció. *Legyen $m > 1$ egész. Azt mondjuk, hogy az $a_1, \dots, a_m$ egészek* **modulo m teljes maradékrendszert** *alkotnak, ha páronként inkongruensek modulo m. Az $a_1, \dots, a_{\varphi(m)}$ egészek* **modulo m redukált maradékrendszert** *alkotnak, ha páronként inkongruensek modulo m, és mindegyikük relatív prím m-hez.*

4.8. Tétel. *Legyen $m > 1$ egész. Ha $a_1, \dots, a_m$ teljes maradékrendszer modulo m, akkor*
(1) $a_1 + b, \dots, a_m + b$ is teljes maradékrendszer modulo m tetszőleges $b \in \mathbb{Z}$-re,
(2) $ca_1, \dots, ca_m$ szintén teljes maradékrendszer modulo m minden olyan c egészre, amelyre $\ln.\,k.\,o.(c, m) = 1$.

4.9. Tétel. *Legyen $m > 1$ egész, és $r_1, \dots, r_{\varphi(m)}$ egy redukált maradékrendszer modulo m. Ha az a egész relatív prím m-hez, akkor $ar_1, \dots, ar_{\varphi(m)}$ szintén egy redukált maradékrendszer modulo m.*

Megjegyzés. E két utóbbi tétel önálló bizonyítását melegen ajánljuk.

4.10. Tétel. *(Euler-Fermat) Legyen $a, m \in \mathbb{Z}$, $m > 1$. Ha* $\ln.\,k.\,o.(a, m) = 1$, *akkor*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Bizonyítás. Legyen $r_1, \dots, r_{\varphi(m)}$ egy redukált maradékrendszer modulo m, és $a \in \mathbb{Z}$ olyan, hogy $\ln.\,k.\,o.(a, m) = 1$. Az előző tétel szerint $ar_1, \dots, ar_{\varphi(m)}$ szintén egy redukált maradékrendszer modulo m, így

tetszőleges $1 \leq i \leq \varphi(m)$-hez van olyan $1 \leq j \leq \varphi(m)$, hogy $r_i \equiv ar_j \pmod{m}$. Ez maga után vonja, hogy

$$r_1 \cdot \ldots \cdot r_{\varphi(m)} \equiv ar_1 \cdot \ldots \cdot ar_{\varphi(m)} \pmod{m}.$$

Ezt rendezve kapjuk, hogy

$$r_1 \cdot \ldots \cdot r_{\varphi(m)} \equiv a^{\varphi(m)} r_1 \cdot \ldots \cdot r_{\varphi(m)} \pmod{m}.$$

Lévén, hogy a bal oldalon álló szorzat relatív prím a modulushoz, azzal lehet egyszerűsíteni, és kapjuk is a bizonyítandó kongruenciát:

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

4.11. Következmény. *(Fermat) Legyen p prímszám. Ha az $a \in \mathbb{Z}$ nem osztható p-vel. akkor*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Megjegyzés. Ez utóbbi következményre úgy is szokás hivatkozni, mint a „kis Fermat tétel".

4.12. Következmény. *Legyen p prímszám. Tetszőleges $a \in \mathbb{Z}$-re*

$$a^p \equiv a \pmod{p}.$$

4.13. Tétel. (Wilson tétele) *Ha p prímszám, akkor* $(p-1)! \equiv -1 \pmod{p}$.

Bizonyítás. Ha $p = 2, 3$, akkor az állítás nyilvánvaló, így föltehető, hogy $p > 3$. Az $\{1, 2, \ldots, p-1\}$ számok redukált maradékrendszert alkotnak modulo p, így bármely $i \in \{1, 2, \ldots, p-1\}$ esetén pontosan egy olyan $1 \leq j \leq p-1$ van, amelyre $ij \equiv 1 \pmod{p}$. Ez alapján az $\{1, 2, \ldots, p-1\}$ halmazbeli számok párokba rendezhetők. Kérdés, hogy minden egyes párban különböző számon vanak. Ha valamely i párja önmaga, akkor teljesül rá az $i^2 \equiv 1 \pmod{p}$ kongruencia, azaz $p|i^2-1$, azaz $p|(i-1)(i+1)$. Mivel p prímszám, ez csak akkor teljesül, ha $i \in \{1, p-1\}$. Kaptuk hogy a $2, 3, \ldots, p-2$ számok mindegyike különbözik párjától. Ez azt jelenti, hogy $(p-2)! \equiv 1 \pmod{p}$, amiből — mindkét oldalt $p-1$-gyel szorozva — a bizonyítandó állítást kapjuk.

Igaz e tétel megfordítása is.

4.14. Tétel. *Ha valamely $m > 1$ egészre* $(m-1)! + 1 \equiv 0 \pmod{m}$, *akkor m prímszám.*

Bizonyítás. Ha az m összetett szám nem egy prímszám négyzete, akkor léteznek olyan $1 < k < l < m$ egészek, hogy $m = kl$. Ekkor $(m-1)! \equiv 0 \pmod{m}$, ami ellentmond a tétel föltételének.

Marad az $m = p^2$ eset, ahol p prímszám. A $p = 2$ eset egyszerű számolással elintézhető, így föltehető, hogy $p \geq 3$. Ekkor azonban az $(m-1)!$ szozatban szerepelnek a p és $2p$ tényezők, így $p^2|(m-1)!$, ami a bizonyítást teljessé teszi.

Megjegyzés. A Wilson tétel elvileg prímtesztnek is alkalmas, de tekintettel arra, hogy a faktoriálisok igen gyorsan nőnek, csak kis számokra hatékony.

4.2. Hatványozás modulo m.

4.6. Definíció. *Legyen* $a, m \in \mathbb{Z},\ m > 1,\ \text{ln. k. o.}(a, m) = 1$. *Azt mondjuk, hogy az* a *egész szám* **multiplikatív rendje modulo** m $k \in \mathbb{N}$, *ha* k *a legkisebb olyan pozitív (egész) kitevő, amelyre* $a^k \equiv 1 \pmod{m}$. *Jelölése:* $\mathrm{o}_m(a) = k$.

4.15. Tétel. *Legyen* $a, m \in \mathbb{Z},\ m > 1,\ \text{ln. k. o.}(a, m) = 1$, *továbbá* $\mathrm{o}_m(a) = k$. *Ha valamely* $n \in \mathbb{N}$*-re* $a^n \equiv 1 \pmod{m}$, *akkor* $k|n$.

Bizonyítás. Végezzünk euklideszi (maradékos) osztást n és k-n: $n = kq + r,\ 0 \le r < k$. Ekkor

$$a^n = a^{kq+r} = (a^k)^q \cdot a^r \equiv 1 \cdot a^r \equiv 1 \pmod{m},$$

amiből $r = 0$ következik.

4.16. Állítás. *Legyen* $a, m \in \mathbb{Z},\ m > 1$, *és* $k_1, k_2 \in \mathbb{N}$. *Ekkor*

$$a^{k_1} \equiv a^{k_2} \pmod{m} \quad \Leftrightarrow \quad k_1 \equiv k_2 \pmod{\mathrm{o}_m(a)}.$$

Bizonyítás. Föltehető, hogy $k_2 < k_1$, és így

$$a^{k_1-k_2} \equiv 0 \pmod{m} \qquad \Leftrightarrow \qquad \mathrm{o}_m(a)|k_1 - k_2.$$

4.7. Definíció. *Legyen* m *egynél nagyobb egész szám. Azt mondjuk, hogy a* $g \in \mathbb{Z}$ **primitív gyök modulo** m, *ha a* $g, g^2, \ldots, g^{\varphi(m)}$ *egészek redukált maradékrendszert alkotnak modulo* m.

A definíció alapján egyszerűen igazolható a következő tétel, amelynek állítása a primitív gyök egy alternatív definíciója is lehet.

4.17. Tétel. *Legyen* $m > 1$ *egész. A* $g \in \mathbb{Z}$ *egész pontosan akkor primitív gyök modulo* m, *ha* $\mathrm{o}_m(g) = \varphi(g)$.

Nem minden $m > 1$ egészhez létezik primitív gyök modulo m. Nevezetesen, igazolható a következő tétel (nem bizonyítjuk).

4.18. Tétel. *Valamely* $m \in \mathbb{Z}$*-hez pontosan akkor létezik primitív gyök modulo* m, *ha* $m = 2, 4, p^m, 2p^m$, *ahol* p *páratlan prím,* m *pedig természetes szám.*

4.8. Definíció. *Tegyük föl, hogy* g *primitív gyök az* m *modulushoz. Az* $\alpha \in \mathbb{Z}$ **indexén** *(az* m *modulusra és a* g *primitív gyökre nézve) olyan* i *kitevőt értünk, amelyre* $g^i \equiv a \pmod{a}$,

Jelölés. A modulust az egyszerűség kedvéért általában nem írjuk ki (ez a legtöbb esetben világos a szövegkörnyezetből), így az $\mathrm{ind}_g\, a$ jelölést alkalmazzuk.

Megjegyzések.
(1) Világos, hogy ha $\ln.\,\mathrm{k.\,o.}(a,m) \neq 1$, akkor $\mathrm{ind}_g\, a$ nem értelmezett, ugyanis g^i mindig relatív prím m-hez. Ha viszont $\ln.\,\mathrm{k.\,o.}(a,m) = 1$, akkor a primitív gyök definíciójából következően a kongruens g valamely hatványával, így az indexe értelmezett.
(2) Vegyük észre, hogy az index nem más, mint a logaritmus mod m analogonja (ezért szokás „diszkrét logaritmusnak" is nevezni). Nem meglepő tehát, hogy hasonló tulajdonságokkal rendelkezik.

4.19. Tétel. *Legyen g primitív gyök modulo m, $a, b \in \mathbb{N}$, $\ln.\,\mathrm{k.\,o.}(a,m) = \ln.\,\mathrm{k.\,o.}(b,m) = 1$, továbbá k tetszőleges egész szám. Ekkor érvényesek a következő azonosságok.*

(1) $\mathrm{ind}_g\, 1 \equiv 0 \pmod{\varphi(m)}$,
(2) $\mathrm{ind}_g\,(ab) \equiv \mathrm{ind}_g\, a + \mathrm{ind}_g\, b \pmod{\varphi(m)}$,
(3) $\mathrm{ind}_g\, a^k \equiv k \cdot \mathrm{ind}_g\, a \pmod{\varphi(m)}$,
(4) $\mathrm{ind}_g\,(ab^{-1}) \equiv \mathrm{ind}_g\, a - \mathrm{ind}_g\, b \pmod{\varphi(m)}$.

A következőkben a modulo m gyökvonással foglalkozunk. Részletezni azonban csak a négyzetgyökvonás kérdést tárgyaljuk.

4.9. Definíció. *Azt mondjuk, hogy az a egész szám* **n-edik hatványmaradék** *modulo m, ha az $x^n \equiv a \pmod{m}$ kongruenciának van megoldása.*

4.20. Tétel. *Legyen g primitív gyök modulo m, és legyen $\ln.\,\mathrm{k.\,o.}(m,a) = 1$. a pontosan akkor n-edik hatványmaradék, ha $\ln.\,\mathrm{k.\,o.}(n,\varphi(m)) \mid \mathrm{ind}_g\, a$.*

4.10. Definíció. *Azt mondjuk, hogy az a egész szám* **négyzetes maradék modulo m,** *ha az $x^2 \equiv a \pmod{m}$ kongruencia megoldható. Ellenkező esetben azt mondjuk, hogy a* **négyzetes nemmaradék** *modulo m.*

4.21. Tétel. *Legyen p páratlan prímszám, g pedig primitív gyök modulo p. Ekkor valamely $a \in \mathbb{Z}$ pontosan akkor négyzetes maradék modulo p, ha $p|a$, vagy $\mathrm{ind}_g\, a$ páros.*

4.11. Definíció. *Tetszőlges p páratlan prímszám, és $a \in \mathbb{Z}$ p-vel nem osztható egész szám esetén bevezetjük az $\left(\frac{a}{p}\right)$* **Legendre szimbólumot***:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ négyzetes maradék modulo } p; \\ -1, & \text{ha } a \text{ négyzetes nemmaradék modulo } p. \end{cases}$$

4.22. Tétel. (Euler-kritérium) *Ha p páratlan prímszám, és $p \nmid a$, akkor*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

4.23. Tétel. *Legyen $a, b \in \mathbb{Z}$ és p páratlan prímszám. Ha $p \nmid a, b$, akkor*

(1) $a \equiv b \pmod{p} \quad \Longrightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,

(3) $\left(\frac{a^2}{p}\right) = 1$.

4.24. Tétel. *Tetszőleges p páratlan prímszám esetén*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & ha\ p \equiv 1 \pmod 4, \\ -1, & ha\ p \equiv 3 \pmod 4. \end{cases}$$

4.25. Tétel. (négyzetes reciprocitás tétel) *Tetszőleges p, q különböző páratlan prímekre*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

4.26. Tétel. *Tetszőleges p páratlan prímre*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{2}} = \begin{cases} 1, & ha\ p \equiv 1, 7 \pmod 8, \\ -1, & ha\ p \equiv 3, 5 \pmod 8. \end{cases}$$

Az előbbi 4.18. - 4.25. Tételek bizonyítása megtalálható pl. a Megyesi, Bevezetés a számelméletbe c. Polygon jegyzetben.

5. Néhány nevezetes — részben megoldatlan — számelméleti probléma

5.1. Mersenne-prímek, tökéletes számok

5.1. Definíció. *Egy $n \in \mathbb{N}$ szám* **tökéletes szám**, *ha megegyezik nála kisebb pozitív osztói összegével.*

5.1. Tétel. (Euklidesz, Elemek, IX. 36. Tétel) *(mai megfogalmazás) A $P_n = 2^{n-1}(2^n - 1)$ alakú számok mindannyiszor tökéletes számok, valahányszor $2^n - 1$ prímszám.*

5.2. Tétel. (Euler) *Minden páros tökéletes szám $P_n = 2^{n-1}(2^n - 1)$ alakú, ahol $2^n - 1$ prímszám.*

Az első négy tökéletes szám — a $6,\ 28,\ 496,\ 8128$ — már az ókorban ismert volt.

5.2. Definíció. (Mersenne 1644) *Az $M_k = 2^k - 1$ alakú számokat Mersenne-számoknak, közülük a prímeket* **Mersenne-prímeknek** *nevezzük.*

Megjegyzés. Világos, hogy M_k csak akkor lehet prím, ha k prím.

5.3. Állítás. (Mersenne 1644) *M_p prím, ha*

$$p = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127,\ 257,$$

de minden további $p \leq 257$ prímre összetett szám.

A XIX. században kiderült, hogy Mersenne listája öt hibát tartalmaz: $p = 61,\ 89,\ 107$-re M_p prím (ezek hiányozna a listáról), míg M_{67} és M_{257} összetett szám.

Természetes kérdés, hogy van-e végtelen sok Mersenne-prím. A válasz nem ismert. Azt sejtik, hogy végtelen sok van. Jelenleg explicite 49 ilyen szám ismert. A legnagyobbat, a 49-ediket 2016-ban tették közzé. A 10 legnagyobb ismert Mersenne-prím a következő

	a prím	jegyek száma	évszám	megj.
1.	$2^{74.207.281} - 1$	22.338.618	2016	49.? Mersenne
2.	$2^{57.885.161} - 1$	17.425.170	2013	48.? Mersenne
3.	$2^{43,112.609} - 1$	12.978.189	2008	47.? Mersenne
4.	$2^{42.643.801} - 1$	12.837.064	2009	46.? Mersenne
5.	$2^{37.156.667} - 1$	11.185.272	2008	45.? Mersenne
6.	$2^{32.582.657} - 1$	9.808.358	2006	44. Mersenne
7.	$2^{30.402.457} - 1$	9.152.052	2005	43. Mersenne
8.	$2^{25.964.591} - 1$	7.816.230	2005	42. Mersenne
9.	$2^{24.036.583} - 1$	7.235.733	2004	41. Mersenne
10.	$2^{20.996.011} - 1$	6.320.430	2003	40. Mersenne

A sorszámot követő kérdőjelek arra utalnak, hogy nem bizonyított hogy közöttük nincs, eddig még nem ismert, Mersenne-prím.

Megjegyzések.

(1) A fönti 10 Mersenne-prím egyben a jelenleg ismert 10 legnagyobb prímszám. Csak a 12. legnagyobb prímszám nem Mersenne-szám, ez a $19.249 \cdot 2^{13.018.586} + 1$, amelynek 3.918.990 decimális jegye van.

(2) Az a mai napig sem ismert, hogy létezik-e egyáltalán páratlan tökéletes szám.

(3) A legnagyobb olyan Mersenne prím, amelyet „kézi erővel" számoltak ki a $2^{127} - 1$. Ezt 1876-ban találta Lucas. Decimális jegyei száma 39.

(4) Utoljára 1914-ben találtak nem számítógép segítségével Mersenne prímet, ez a $2^{107} - 1$ volt.

(5) Az első számítógéppel talált Mersenne prím R. Robinson nevéhez fűződik 1952-ből, ez a 157 decimális jegyű $2^{512} - 1$.

A páros tökéletes számok keresése elvileg egyszerű a következő tétel alapján.

5.4. Tétel. (Lucas-Lehmer teszt) *Legyen p prím, és alkossuk meg az $a_1 = 4$ és $a_{k+1} \equiv a_k^2 - 2 \pmod{M_p}$ $(k \geq 1)$ sozozatot. M_p pontosan akkor prím, ha $a_{p-1} \equiv 0 \pmod{M_p}$.*

Megjegyzés. Vegyük észre, hogy az előbbi sorozat nagyon gyorsan nő, így hamar oda jutunk, hogy a számolásainkat olyan számokkal kellene végezni, amelynek jegyei száma milliós, sőt olykor tízmilliós nagyságrendű

5.2. Ikerprímek

Az $\{3, 5\}$, $\{5, 7\}$, $\{11, 13\}$, $\{17, 19\}$, $\{29, 31\}, \ldots$ párok (egymást követő páratlan számok) mindkét tagja prímszám. Előfordul-e végtelen sokszor, hogy két egymást követő páratlan szám mindegyike prímszám? Másképpen mondva, létezik-e végtelen sok ikerprím. A kérdés nyitott, megválaszolása nagyon nehéznek tűnik. Egy egyszerűbbnek látszó kérdés az, hogy van-e végtelen sok olyan prímszám pár, amelyek különbsége elegendően kicsi, azaz egy adott korlátnál kisebb. Ha találunk egy ilyen korlátot, akkor „már csak" azt kell csökkenteni egészen 2-ig.

2013. elején jelentette be a Nature-ben Jilang Csang azon eredményét, miszerint végtelen sok olyan prímszám pár létezik, amelyek különbsége kisebb 70 milliónál. Ez az első igazolt korlát, de meglehetősen nagy. Minden esetre ez az első eredmény az ikerprím-probléma megoldása felé vezető úton. Várható, hogy a 70 milliós korlátot rövidesen jelentősen csökkenteni tudják, de a 2 elérése, azaz annak igazolása, hogy végtelen sok ikerprím létezik, még mindig messze van.

Itt is vannak empírikus eredmények, állandóan keresik az egyre nagyobb ikerprímeket. A 2009-es rekorder pár a 100.355 decimális jegyű

$$65.516.468.355 \cdot 2^{333333} \pm 1$$

volt. A jelenlegi csúcstartó a 2016. szeptemberében talált 388.342 jegyű

$$2.996.683.034.895 \cdot 2^{1.290.000} \pm 1,$$

míg a 2017. júliusában talált — tehát a „legfrissebb" — ikerprím pár a „mindössze" 66.907 jegyű $12.770.275.971 \cdot 2^{222.225} \pm 1$.

Néhány elméleti eredményt is említünk.

(1) Az n és $n+2$ egészek prímszám volta független események.

(2) 1948-ban Clement igazolta, hogy n és $n+2$ pontosan akkor pímek, ha

$$4((n-1)!+1) \equiv -n \pmod{n(n+2)}.$$

(3) Tudjuk (Euler bizonyította), hogy a prímszámok reciprokaiból álló sor divergens. Annak ellenére, hogy nem ismert az ikerprím párok száma (végtelen sokan vannak-e) tudjuk, hogy az alábbi párok összege véges, azaz létezik olyan B valós szám, amely az

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\ldots,$$

összeg határértéke. Ez azt is jelenti, hogy e sor, az ikerprímek reciprokai által ílymódon alkotta sor, konvergens. Ezt Brun igazolta 1918-ban, természetesen föltételezte, hogy végtelen sok ilyen pár létezik. A B konstansra a jelenleg ismert legjobb becslést 2002-ben adta Sebah, föltételezve Hardy és Littlewood azon sejtését, miszerint $\pi(x+y)-\pi(y) \leq \pi(x)$, valahányszor $x, y \geq 2$. ($\pi(x)$ az $x \in \mathbb{R}$-nél nem nagyobb prímszámok száma.) Eredménye:

$$B \approx 1,902160583104.$$

(4) Végtelen sok olyan p prímszám létezik, amelyre $p+2$ prímszám, vagy két prímszám szorzata. Innen már csak egyetlen „kis" lépés az ikerprím-probléma megoldása.

5.3. Fermat-prímek.

Az előbb említett Mersenne-prímek mellett egy másik típusú prímeknek is fontos — talán még fontosabb — alkalmazásai vannak. Fermat a 2^k+1 alakú számokat vizsgálva az vette észre, hogy egyrészt ha egy ilyen alakú szám prím, akkor $k = 2^n$, másrészt az $F_n = 2^{2^n}+1$ alakú számok $n = 0, 1, 2, 3, 4$-re prímek. Azt sejtette, hogy ezek mindig prímek. Ezt a sejtést Euler cáfolta meg azzal, hogy $641|F_5$.

Ezen, ún. Fermat-számok (Fermat-prímek) vizsgálata akkor került a matematikusok fókuszába, amikor Gauss igazolta a következő tételt.

5.5. Tétel. *A szabályos n-szög pontosan akkor szerkeszthető meg körzővel és egyélű vonalzóval (véges sok lépésben), ha*

$$n = 2^t p_1 p_2 \dots p_k$$

alakú, ahol $p_1, p_2, \dots, p_k$ különböző Fermat-prímek, $t \in \mathbb{N}_0$, de $k = 0$ esetén $t > 1$.

Sajnos jelenleg csak 5 Fermat-prím ismert (amelyeket már Fermat is ismert), ezek a következők:

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65.537$$

Ma (2003. óta) azt tudjuk, hogy, ha $5 \leq n \leq 32$, akkor F_n összetett szám, és ugyanezt tudjuk néhány további n-re is. A rekorder explicite vizsgált Fermat-szám az $F_{23.471}$, amelynek több mint $10^{7.000}$ decimális jegye van, és osztható $5 \cdot 2^{23.473} + 1$-gyel.
Néhány egyszerű állítás a Fermat-számokkal kapcsolatban.

5.6. Állítás. *A különböző Fermat-számok relatív prímek.*

5.7. Következmény. *Végtelen sok prímszám van.*

5.4. Hatványösszegekre bontás

Már az ókorban ismert volt, hogy bizonyos négyetszámok fölbonthatók két négyzetszám összegére. Másképpen mondva megoldható a pozitív egész számok körében az $x^2 + y^2 = z^2$ egyenlet. P. Fermat a XVII. század közepén bizonyítani vélte, hogy egyetlen másodiknál magasabb kitevőjű hatvány sem bontható föl két ugyanolyan kitevőjű hatvány összegére, azaz $n > 2$ esetén nincs pozitív egész megoldása az $x^n + y^n = z^n$ egyenletnek. Ezen állítást kezdetben a „nagy Fermat-tétel"-ként említették, de később — mivel mintegy három évszázadon át hiába próbálták rekonstruálni a bizonyítást — inkább **Fermat-sejtésnek** nevezték.

5.3. Definíció. *Legyen $a, b \in \mathbb{Z}$, α pedig harmadik primitív egységgyök. Az $a + b\alpha$ alakú komplex számokat* **Euler-egészeknek** *nevezzük.*

5.8. Tétel. *Az Euler-egészek olyan integritástartományt alkotnak, amelyben érvényes a számelmélet alaptételének általánosítása.*

5.9. Tétel. (Euler) *Az $x^3 + y^3 = z^3$ egyenletnek nincs nemzéró megoldása az Euler egészek gyűrűjében.*

5.10. Következmény. *Az $x^3 + y^3 = z^3$ egyenletnek nincs megoldása a természetes számok halmazában. Másképpen mondva, egyetlen köbszám sem bontható föl két köbszám összegére.*

5.11. Tétel. (Fermat) *Az $x^4 + y^4 = z^4$ egyenletnek nincs megoldása a természetes számok halmazában, azaz egyetlen negyedik hatvány sem bontható föl két negyedik hatvány összegére.*

5.12. Tétel. (Andrew Wiles 1993) *Ha $n > 2$, akkor az $x^n + y^n = z^n$ egyenletnek nincs megoldása a természetes számok körében, azaz $n > 2$ esetén egyetlen n-edik hatvány sem bontható föl két n-edik hatvány összegére.*

Több összeadandó esete.

5.13. Tétel. (Gauss) *Egy $n \in \mathbb{N}$ természetes szám akkor és csak akkor bontható föl legföljebb három négyzetszám összegére, ha $n \neq 4^k(8t+7)$.*

5.14. Tétel. (Lagrange) *Minden természetes szám fölbontható legföljebb négy négyzetszám összegére.*

Megjegyzés. Az előbbi két tételben a „legföljebb" kitétel arra utal, hogy az általánosság kedvéért a fölbontásokban valamely tag zéró is lehet.

Edward Waring 1770-ben megjelent *Meditationes Algebraicae* c. könyvében — többek közt — azt állította, hogy

(1) bármely természetes szám előáll legföljebb 9 köbszám összegeként,
(2) bármely természetes szám előáll legföljebb 19 negyedik hatvány összegeként,
(3) sőt, hasonló állítások kaphatók a negyediknél magasabb hatványokra is.

Utolsó állítása lényegében azt kérdezi: Létezik-e olyan $g\colon \mathbb{N} \to \mathbb{N}$ függvény, hogy minden természetes szám előáll legföljebb $g(k)$ számú k-adik hatvány összegeként, ahol $g(k)$ csak k-tól függ (azaz független a reprezentálandó számoktól)? Ha 0 összeadandókat is megengedünk (ahogy eddig is tettük), akkor a „legföljebb" kitétel elhagyható.

Ma már világos, hogy Waring e 3 állítását nem tudta igazolni. Ezzel a kérdéssorral – az ún. Waring-problémakörrel — kapcsolatban a következőket tudjuk/állíthatjuk.

- Lagrange iménti tétele szerint $g(2) = 4$.
- Liouville becslése 1859-ből: $g(4) \leq 53$.
- David Hilbert 1909-ben igazolta, hogy e g függvény létezik, de bizonyítása egy ún. „tiszta egzisztenicia bizonyítás", azaz csak a függvény létezését mutatta meg. Eljárása alapján egyetlen $k \in \mathbb{N}$-re sem határozható meg a $g(k)$ érték.
- Dickson tétele XX. század elejéről: $g(3) = 9$, és csupán két olyan szám van amelyik köbök összegeként való előállításához ténylegesen 9 köbszám kell. Nevezetesen

$$23 = 2^3 + 2^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3$$
$$238 = 4^3 + 4^3 + 3^3 + 3^3 + 3^3 + 3^3 + 1^3 + 1^3 + 1^3,$$

  és így minden $n > 238$ egész előállítható legföljebb 8 köbszám összegeként.

- Linnik 1942-es eredménye szerint: csak véges sok olyan természetes szám van, amelyik a köbök osszegeként való előállításban ténylegesen igényli a 8 összedandót, ezért valahonnan kezdve minden természetes szám előáll legföljebb 7 köbszám összegeként. Sőt, csak véges sok olyan van, amelyek nem állnak elő legföljebb 6 köbszám összegeként.
- A $k = 4, 5$ esetek igen nehéznek tűnnek. Hosszú ideig csak azt lehetett tudni, hogy

  $$19 \leq g(4) \leq 35 \qquad \text{és} \qquad 37 \leq g(5) \leq 54.$$

  Utóbb (1964) igazolták, hogy $g(5) = 37$, és a $g(4)$-re vonatkozó fölső korlátot sikerült radidálisan csökkenteni: $g(4) \leq 20$. Később: ha $n < 10^{140}$, vagy $n > 10^{367}$, akkor 19 összeadandó is elég. Ezzel elvileg megoldódott a kérdés, mert „csak" véges sok konkrét esetet kell még megvizsgálni. Ezt 1986-ra befejezték, kiderült, hogy $g(4) = 19$.
- A $k > 5$ eset azonban lényegében még teljesen nyitott, csak annyit tudunk, hogy a

  $$g(k) = \left[\left(\frac{3}{2}\right)^k\right] + 2^k - 2$$

  egyenlőség véges sok k kivételével mindig fönnáll. Elég sokan vallják azonban azt a nézetet, hogy az előbbi formula minden $k > 1$-re korrekt.

Egy más irányú vizsgálat kiindulópontja volt az a fölismerés, hogy $k \geq 3$ minden elegendően nagy egész $g(k)$-nál kevesebb k-adik hatvány összegeként állt elő. Ez vezetett a következő függvény bevezetéséhez.

5.4. Definíció. *Jelölje $G(k)$ azt a legkisebb $r \in \mathbb{N}$ természetes számot, amelyre minden elegendően nagy egész előáll legföljebb r számú k-adik hatvány összegeként.*

Megjegyzés. Nyilvánvaló, hogy $G(k) \leq g(k)$.

Sajnos mindössze 2 konkrét $G(k)$ érték ismeretes: $G(2) = 4$ és $G(4) = 16$. Linnik köbös eredménye azt mutatja, hogy $G(3) \leq 7$, de már Jacobi sejtette 1851-ben, hogy $G(3) \leq 5$. Azt csak a XX. század vége felé igazolták, hogy $G(5) \leq 21$ és $G(6) \leq 31$.

5.5. Analitikus jelegű kérdések.

A prímszámok eloszlása a természetes számok között szintén egy régóta vizsgált kérdés. Itt alapvető a következő — korábban már említett — függvény.

5.5. Definíció. *Tetszőleges $a \in \mathbb{R}$-re jelölje $\pi(a)$ az a-nál nem nagyobb prímszámok számát.*

5.15. Tétel. (nagy prímszámtétel)

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 1.$$

Megjegyzés. Ezen eredményt először Gauss sejtette meg a XIX. század elején, de csak 1896-ban igazolta Hadamard és de la Valée Poussin.

Közbülső eredményként 1850-ben Csebisev igazolta a következő tételt.

5.16. Tétel. (Csebisev) *Léteznek olyan $a < 1 < b$ konstansok, hogy*

$$a\frac{x}{\log x} < \pi(x) < b\frac{x}{\log x}$$

teljesül minden elegendően nagy $x \in \mathbb{R}$ számra.

Megjegyzés. Világos, hogy Csebisev tétele könnyen adódik a nagy prímszámtételből.

Euler sejtette, hogy „vannak olyan számok, amelyek meghaladják az algebrai módszerek erejét". Véleménye szerint ilyenek e és π, de a trigonometrikus, az exponenciális és a logaritmus függvények értékei is sok helyen. E (valós) számokat *transzcendens számoknak* nevezte.

5.6. Definíció. *Azt mondjuk, hogy az $\alpha \in \mathbb{C}$ komplex szám* **algebrai szám**, *ha van olyan nemkonstans $f \in \mathbb{Q}[x]$ polinom, hogy $f(\alpha) = 0$. A nem algebrai komplex számokat* **transzcendens számoknak** *nevezzük.*

Az első transzcendens számot 1844-ben adta meg Liouville.

5.17. Tétel. *Az*

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} = 0,110001000000000000000001\ldots$$

szám transzcendens.

Megjegyzés. Egyszerű halmazelméleti eszközökkel ugyan belátható, hogy kontinuum sok transzcendens valós szám van, azaz „majdnem minden" komplex/valós szám transzcendens, de ez egy ún. tiszta egzisztencia bizonyítás, ami semmit sem mond e számok mibenlétéről.

5.18. Tétel. (Hermite 1876 és Lindemann 1882) *Az e és a π transzcendens számok.*

David Hilbert a 2. Matematikai Világkongresszuson (1900. Párizs) tette föl a következő kérdést.
Legyen $\alpha \neq 0, \pm 1$ algebrai szám és β irracionális algebrai szám. Igazolandó, hogy ekkor az α^β alakú számok, például $2^{\sqrt{2}}$, $e^\pi = i^{-2i}$ mindig transzcendens szám, vagy legalább irracionális.

5.19. Tétel. (Gelfond-Schneider tétel 1934) *Ha α, β algebrai számok, $\alpha \neq 0, \pm 1$ és β irracionális, akkor α^β transzcendens szám.*

Megjegyzés. A mai napig sem ismert, hogy $e + \pi$ algebrai, vagy transzcendens, míg $e + i\pi$ nyilvánvalóan transzcendens.

6. Nyilvános kódú titkosírások.

Titkos üzenetváltáshoz gyakran alkalmazzák a digitalizálást, azaz a folyó szöveget (nemnegatív egészekből álló) számsorozatokkal helyettesítik. Az elv egyszerű, hiszen ha az $A = \{0, 1, \ldots, N\}$ halmazbeli számokat használjuk, akkor a „kódolás" nem más, mint egy $\varphi \in S_N$ permutáció. A kódolt szöveg visszafejtéséhez (dekódolásához) pedig ismerni kell ezen permutáció (bijektív leképezés) inverzét. φ ismeretében csak látszólag egyszerű inverzének meghatározása. Ha N elég nagy, akkor ez komoly próbatétel. Gondoljuk végig, hogy tudnánke hatékonyan használni a magyar-angol szótárunkat egy angol szöveg magyarra fordításában.

Egy olyan digitális alapú sokszereplős titkos üzenetváltás elveit tette közzé 1977-ben R. Rivest, A. Shamir és L. Adleman, amely alkalmazásakor a titkos levelezés minden egyes résztvevője nyilvánosságra hozza, hogy a neki szánt (digitalizált) üzenetet hogyan kell kódolni. A kódolt üzenet nyilvánosan küldhető el, de csak a címzett képes azt dekódolni, azaz visszafejteni. A rendszert megalkotóiról **RSA** rendszernek nevezték el.

A rendszer működése.

(1) A titkos levelezés minden egyes résztvevője válasz magának egy p, q $p \neq q$ prímszám párt. Ezek nagysága olyan legyen, hogy az $n = pq$ szorzat, az ún. **kódoló modulus**, faktorizálása meghaladja a számítógépek lehetőségeit. Ez jelenleg azt igényli, hogy a prímek legalább 200 (decimális) jegyűek legyenek.

(2) Ezek után mindenki véletlenszerűen választ magának egy $k \in \mathbb{N}$ **kódoló kitevőt** úgy, hogy $\ln.\,\mathrm{k.\,o.}(k, \varphi(n)) = 1$. Ezt gyakran úgy érik el, hogy a k-t a $\varphi(n) + 1$ valamelyik prímosztójának választják. A (n, k) párját mindenki nyilvánosságra hozza. A saját p, q prímpárját azonban szigorúan titokban kell tartania minden egyes résztvevőnek.

(3) Az ábécé betűi, az írásjelek (a szóköz is), valamint a számjegyek mindegyike egy-egy kétjegyű számmal jelölhető nyilvánosan egyeztetett módon. Ezt alkalmazva a titkosítani kívánt szöveg egy nagy M természetes számként jelenik meg. Ez a szám általában igen nagy, ezért fölbontják adott egyenlő hosszúságú $M_1, M_2, \ldots, M_m$ számokra. A közös hossz nyilvános.

(4) A kódolás menete a következő. A továbbiakban legyen $M \in \{M_1, \ldots, M_m\}$. M kódolt változata legyen

$$M^k \equiv r \pmod{n},$$

ahol r a legkisebb nemnegatív maradéka az M^k-nak modulo n. Ha M legföljebb 200 jegyű, akkor ez egyszerűen meghatározható a mai számítógépekkel. Ezen r küldendő el (nyilvánosan).

(5) A címzett először az ő j **titkos dekódoló kitevőjét** határozza meg:

$$kj \equiv 1 \pmod{\varphi(n)}.$$

A k-ra kirótt föltétel miatt e kongruenciának pontosan egy megoldása van. Emlékeztetünk: a $\varphi(n) = (p-1)(q-1)$ értéket csak a címzett tudja meghatározni, mert más nem ismeri a p, q prímpárt.

(6) A címzett az r kódolt üzenetből a következőképp kapja meg az eredeti M üzenetet. Mivel $kj = 1 + \varphi(n)t$ valamely $t \in \mathbb{Z}$-re,

$$r^j \equiv (M^k)^j \equiv M^{1+\varphi(n)t} \equiv M(M^{\varphi(n)})^t \equiv M \cdot 1^t \equiv M \pmod{n},$$

valahányszor $\ln. \text{k. o.}(M, n) = 1$. (Ez utóbbi nem perdöntő, mert csak a Fermat-tétel helyett az Euler-Fermat tételt kell alkalmazni.)

Megjegyzés. A javasolt nagyságú prímek kiválasztása, sőt a kb. 250 jegyűeké is, nem nehéz probléma. Az 500 körüli decimális jegyű számok faktorizálása azonban ma még lehetetlen vállalkozásnak tekinthető.

6.1. Prímtesztek.

6.1. Állítás. *Egy $n > 1$ egész pontosan akkor összetett szám, ha valamely $p \leq \sqrt{n}$ prímszámra $p|n$.*

Mivel számos oszthatósági szabályt ismerünk, sőt Fermat tétele alapján bármely prímre alkotható ilyen e tesztelési módszer egyszerűnek látszik. Sajnos az így nyert teszt csak viszonylag kis számokra hatékony.

Ha azonban n kb. 100 jegyű, azaz $n \approx 10^{100}$ (ennél jóval nagyobb nagyságrendű prímeket gyakran alkalmaznak a kriptográfiában), akkor mintegy $8 \cdot 10^{47}$ prímet kellene megvizsgálnunk. Ez azonban gyakorlatilag lehetetlen, hiszen egy olyan számítógépnek is, amely másodpercenként 10^{26} számú műveletet végez el (az elektron 10^{-26} másodperc alatt ugrik az egyik pályáról egy másikra!), akkor ez a feladat nagyságrendileg 10^{10} évig tartana (e szám a Naprendszer életkora közelítőleg).

Léteznek „gyors prímtesztek", ezek azonban nem osztókat keresnek, hanem olyan gyorsan ellenőrizhető tulajdonságokat vizsgálnak, amelyekkel a prímszámok rendelkeznek, de az összetettek gyakorlatilag nem. Ez utóbbi kitétel azt jelenti, hogy csak ritka kivételek vannak, tehát a tévedés esélye kicsi.

6.2. Tétel. (Solovay-Strassen prímteszt)
(A) *Legyen $n > 1$ páratlan egész, és tekintsük az*

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n} \tag{1}$$

kongruenciát, ahol $\left(\frac{a}{n}\right)$ Jacobi-szimbólum.
Ha n prím, akkor (1) minden $a \not\equiv 0 \pmod{n}$ esetén teljesül.

Ha n összetett, akkor (1) *egy modulo n teljes maradékrendszer elemeinek kevesebb, mint felére teljesül.*
(B) *Az* (A) *kritérium alapján a következőképp dönthető el egy nagy páratlan n-ről, hogy prím-e vagy összetett. Válasszunk (mondjuk) 1000 véletlen $a \not\equiv 0 \pmod{n}$ számot, és mindegyikre vizsgáljuk meg, hogy a* (1) *föltétel teljesül-e. Ha legalább egy esetben nem teljesül, akkor az n biztosan összetett. Ha mind az 1000 esetben teljesül, akkor 2^{-1000}-nél kisebb annak a valószínűsége, hogy n összetett.*

Megjegyzés. A (B) pontban említett valószínűség olyan kicsi, hogy a teszt gyakorlatilag biztosnak tekinthető.

6.3. Tétel. (Miller-Lenstra-Rabin prímteszt) *Legyen $n > 1$ páratlan egész, $n - 1 = 2^k r$, ahol r páratlan. Az*

$$a^r,\ a^{2r},\ a^{4r}, \ldots, a^{2^{k-2}r} = a^{\frac{n-1}{4}},\ a^{2^{k-1}r} = a^{\frac{n-1}{2}} \tag{2}$$

számokat „jó sorozatnak” nevezzük, ha ezek modulo n vett legkisebb abszolút értékű maradékai között előfordul a -1, vagy pedig a^r maradéka 1.
Ha n prím, akkor (2) *minden $a \not\equiv 0 \pmod{n}$ esetén jó sorozat.*
Ha n összetett akkor (2) *egy modulo n teljes maradékrendszer elemeinek kevesebb, mint felére alkot jó sorozatot.*

7. Test fölötti egyhatározatlanos polinomok.

A továbbiakban R mindig egy tetszőleges integritástartományt, míg F egy tetszőleges testet jelöl.

7.1. Definíció. *R fölötti* **polinomnak** *nevezzük az olyan, R-beli elemekből képezett, $(a_0, a_1, \ldots)$ végtelen sorozatot, amelynek csak véges sok nemzéró tagja van. Az összes R fölötti polinomok halmazát $R[x]$ fogja jelölni.*

7.2. Definíció. *Legyen $f = (a_0, a_1, \ldots) \in R[x]$ tetszőleges polinom, és $n \in \mathbb{N}$. Az f* **polinom n edik tagja** *e sorozat n indexű tagja: $(f)_n = a_n$.*

7.3. Definíció. *Az $f \in R[x]$* **polinom fokszáma** *a legnagyobb olyan $n \in \mathbb{N}_0$, amelyre $a_n \neq 0$. Ha ilyen n nincs, azaz $f = (0, 0, \ldots)$, akkor f fokszáma $-\infty$. Az f polinom fokszámát $\deg f$ fogja jelölni. Ha $\deg f = 1, -\infty$, akkor azt mondjuk, hogy f* **konstans polinom**. *Ha $\deg f = n \geq 0$, akkor az a_n elemet f* **főegyütthatójának** *nevezzük, az 1 főegyütthatójú polinomokat pedig* **főpolinomoknak**.

7.4. Definíció. *Az $f, g \in R[x]$* **polinomok összege ill. szorzata** *a következő két polinom:*

$$(f + g)_n = (f)_n + (g)_n$$

$$(f \cdot g)_n = \sum_{i=0}^{n} (f)_i (g)_{n-i}$$

7.1. Állítás. *Tetszőleges $f, g \in R[x]$ polinomokra*

$$\deg(f + g) \leq \max\{\deg f, \deg g\} \text{ és } \deg(f \cdot g) = \deg f + \deg g.$$

7.2. Tétel. *A 7.4. Definícióbeli műveletekkel $R[x]$ integritástartomány.*

7.5. Definíció. *A $R[x]$ gyűrűt az R* **fölötti egyhatározatlanos polinomgyűrűnek** *nevezzük. használni fogjuk a rövidebb: R fölötti polinomgyűrű elnevezést is.*

7.3. Állítás. *Minden $a, b \in R$ esetén*

$$(a, 0, 0, \ldots) + (b, 0, 0, \ldots) = (a + b, 0, 0, \ldots)$$

$$(a, 0, 0, \ldots) \cdot (b, 0, 0, \ldots) = (a \cdot b, 0, 0, \ldots)$$

Jelölés. Az elkövetkezőkben az $(a, 0, 0, \ldots)$ polinom helyett egyszerűen a-t írunk, és nem különböztetjük meg az a gyűrűelemtől, azaz úgy tekintjük, hogy $R \subseteq R[x]$. A $(0, 1, 0, 0, \ldots)$ polinomot pedig x jelöli a jövőben.

7.4. Tétel. *Minden polinom előáll $\sum_{i=0}^{n} a_n x^n$ $(a_n \neq 0)$ alakban, és ez az előállítás egyértelmű. Ha $f = (a_0, a_1, \ldots)$ egy n-edfokú polinom, akkor*

$$f = (a_0, a_1, \ldots, a_n, 0, \ldots) = a_0 + a_1 x + \ldots + a_n x^n.$$

Jelölés. A polinomokat az elkövetkezőkben $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, vagy $\sum_{i=0}^{n} a_i x^i$ alakban írjuk, és hallgatólagosan mindig föltesszük, hogy $a_n \neq 0$, valamint azt, hogy e polinom n-edfokú, azaz $a_{n+1} = a_{n+2} = \ldots = 0$. Az x szimbólum neve **határozatlan** (és nyilván $x \notin R$). A határozatlant természetesen más betű is jelölheti, leggyakrabban y, vagy pl. z. Ez esetekben a polinomgyűrűt $R[y]$, $R[z], \ldots$ jelöli.

Jelölés. A továbbiakban, mint már említettük, F mindig egy testet jelöl, és $F^* = F \setminus \{0\}$.

7.5. Állítás. *Legyen F test. Az $F[x]$ polinomgyűrű egységei épp a nemzéró konstans polinomok.*

7.1. A polinomok számelmélete.

E részben test fölötti egyhatározatlanos polinomokkal foglalkozunk, bár több eredmény/összefüggés integritástartományok fölötti polinomokra is érvényes.

7.6. Definíció. *Legyenek $f, g \in F[x]$. Azt mondjuk, hogy az f polinom* **osztója** *a g polinomnak, ha létezik olyan $h \in F[x]$ polinom, hogy $g = fh$. Jelölése: $f|g$.*

7.7. Definíció. *Azt mondjuk, hogy az $f, g \in R[x]$ polinomok* **asszociáltak**, *ha $f|g$ és $g|f$.*

7.6. Tétel. *Legyen F test. Az asszociáltság ekvivalenciareláció $F[x]$-en. A nulla osztályt kivéve minden asszociáltsági osztály tartalmaz főpolinomot, mégpedig pontosan egyet.*

7.7. Tétel. *Bármely $F[x]$ polinomgyűrűben az oszthatóság reflexív és tranzitív reláció, továbbá tetszőleges $f, g \in F[x]$ polinomokra*

(1) $f \sim g \;\Leftrightarrow\; \exists c \in F^* \colon g = cf$, (2) $(f|g \text{ és } g \neq 0) \;\Rightarrow \deg f \leq \deg g$.

7.8. Tétel. *Legyen F test. tetszőleges $f, g, h \in F[x]$ polinomokra*

(1) $f|f$;
(2) $(f|g \text{ és } g|h) \;\Rightarrow\; f|h$;
(3) $(f|g \text{ és } g|f) \;\Leftrightarrow\; \exists c \in F^* \colon g = cf$;
(4) $1|f$;
(5) $f|0$;
(6) $f|1 \;\Leftrightarrow\; f \in F^*$;
(7) $0|f \;\Leftrightarrow\; f = 0$;
(8) $(f|g \text{ és } f|h) \;\Rightarrow\; f|g \pm h$;
(9) $f|g \;\Rightarrow\; f|gh$;
(10) $f|g \;\Leftrightarrow\; fh|gh$, *ha* $h \neq 0$;
(11) $f|g \;\Rightarrow\; \deg f \leq \deg g$, *ha* $g \neq 0$.

7.9. Tétel. (a maradékos osztás tétele) *Legyenek $f, g \in F[x]$, és $g \neq 0$ polinomok. Léteznek olyan egyértelműen meghatározott $q, r \in F[x]$ polinomok, hogy $f = gq + r$, ahol $r = 0$, vagy $\deg r < \deg g$.*

Bizonyítás. Legyen $f = a_n x^n + \ldots + a_0$, $g = b_m x^m + \ldots + b_0$, $a_n b_m \neq 0$. A

$$q_1 = f - a_n b_m^{-1} x^{n-m} g$$

polinom fokszáma kisebb n-nél. Ha $\deg q_1 \geq m$, akkor ismételjük meg ezt az eljárást most az f helyett a q_1 polinomra, kapjuk a q_2 polinomot. Ezt addig ismételjük, amíg olyan q_i polinomhoz nem jutunk, amelyre $\deg q_i < m$. Ekkor a $q_1 + \ldots + q_i = q$ polinom, valamint az $r = f - qg$ polinom eleget tesz a tétel föltételeinek, csak az unicitást kell még igazolni.

Ha $f = qg + r = q'g + r'$, ahol $\deg r, \deg r' < m$, akkor a a két egyenlőségből

$$(q - q')g + (r - r') = 0,$$

amiből $g | r - r'$. Ez pedig csak úgy lehetséges, ha $r - r' = 0$.

7.8. Definíció. *Legyenek $f, g, h, k \in F[x]$ polinomok. Azt mondjuk, hogy h az f, g polinomok egy* **legnagyobb közös osztója***, ha*

$$h | f \text{ és } h | g$$
$$\forall h' \in F[x]\text{-re } h' | f \text{ és } h' | g \;\Rightarrow\; h' | h.$$

Továbbá, azt mondjuk, hogy a $k \in F[x]$ polinom az f és g polinomok egy **legkisebb közös többszöröse***, ha*

$$f | k \text{ és } g | k,$$
$$\forall k' \in F[x] \colon f | k',\ g | k' \Rightarrow k | k'.$$

Jelölés. Az f, g polinomok legnagyobb közös osztóját, ill. legkisebb közös többszörösét $\ln.\,\mathrm{k.\,o.}(f, g)$, ill. $\mathrm{lk.\,k.\,t.}(f, g)$ fogja jelölni.
Megjegyzés. Vegyük észre, hogy a legnagyobb közös osztó olyan közös osztó, amelynek mindegyik összes közös osztó osztója. Hasonlóan, a legkisebb közös többszörös egy olyan közös többszörös, amely az összes közös többszörösnek osztója.

7.10. Állítás. *A legnagyobb közös osztó, ill. a legkisebb közö többszörös — föltéve, hogy léteznek — csak asszociáltság erejéig meghatározottak.*

7.11. Tétel. *Bármely két $f, g \in F[x]$ nemzéró polinomnak létezik legnagyobb közös osztója és legkisebb közös többszöröse. Ezek asszociáltság erejéig egyértelműen meghatározottak. A legnagyobb közös osztó előállítható az f és a g polinomok lineáris kombinációjaként, azaz léteznek olyan F fölötti u, v polinomok, hogy* $\ln.\,\mathrm{k.\,o.}(f, g) = fu + gv$.

Bizonyítás. Legyen $\deg f \geq \deg g$, és végezzünk maradékos osztásokat a következőképp.

$$\begin{aligned} f &= gq_1 + r_1 \\ g &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \end{aligned}$$

Tudjuk, hogy

$$\deg g > \deg r_1 > \deg r_2 > \deg r_3 > \ldots \geq 0,$$

ezért az osztás sorozatunk véges, azaz van egy utolsó nemzéró maradék. Erről egyszerű számolással megkapható, hogy az éppen egy legnagyobb közös osztó.

A legkisebb közös többszörös létezésének igazolása ezek után egy rutin feladat, aminek végiggondolását melegen ajánljuk, míg a legnagyobb közös osztó lineáris kombinációként való előállítása az osztássorozatból kapható, a végétől az elejére haladó behelyettesítésekkel. Ezt az eljárást később megmutatjuk.

Megjegyzés. A tétel bizonyításában szereplő osztás-sorozatot — hasonlóan mint az elemi számelméletbeli analóg eljárást — **Euklideszi-algoritmusnak** nevezzük.

7.9. Definíció. *Azt mondjuk, hogy az f, g polinomok* **relatív prímek**, *ha* $\text{ln. k. o.}(f, g) \sim 1$.

7.12. Tétel. *Tetszőleges $f, g, h \in F[x]$ polinomok esetén,*

(1) *ha $fg \neq 0$, akkor*

$$\text{ln. k. o.}\left(\frac{f}{\text{ln. k. o.}(f,g)}, \frac{g}{\text{ln. k. o.}(f,g)}\right) \sim 1,$$

azaz a két hányados relatív prím;

(2) *ha f és g relatív prím, akkor*

$$f|gh \quad \Leftrightarrow \quad f|h;$$

(3) *ha $\text{ln. k. o.}(f, g) \neq 0$, akkor*

$$f|gh \quad \Leftrightarrow \quad \frac{f}{\text{ln. k. o.}(f,g)}|h.$$

7.13. Tétel. *Tetszőleges $f, g, h \in F[x]$ polinomok esetén,*

(1) *ha $fg \neq 0$, akkor*

$$\text{ln. k. o.}\left(\frac{f}{\text{ln. k. o.}(f,g)}, \frac{g}{\text{ln. k. o.}(f,g)}\right) \sim 1,$$

azaz a két hányados relatív prím;

(2) *ha f és g relatív prím, akkor*

$$f|gh \quad \Leftrightarrow \quad f|h;$$

(3) *ha* $\ln.\,\mathrm{k.\,o.}(f,g) \neq 0$, *akkor*

$$f|gh \quad \Leftrightarrow \quad \frac{f}{\ln.\,\mathrm{k.\,o.}(f,g)}|h.$$

7.14. Tétel. *Legyenek* $f,g,h \in F[x]$ *nemzéró polinomok. Pontosan akkor léteznek olyan* F *fölötti* u,v *polinomok, hogy* $fu+gv=h$, *másképpen mondva, megoldható* $F[x]$*-ben* u,v*-re az előbbi egyenlet, ha* $\ln.\,\mathrm{k.\,o.}(f,g)|h$. *Ha* (u_0,v_0) *egy megoldás, akkor tetszőleges* $t \in F[x]$*-re*

$$u = u_0 + \frac{g}{\ln.\,\mathrm{k.\,o.}(f,g)}t, \qquad v = v_0 - \frac{f}{\ln.\,\mathrm{k.\,o.}(f,g)}t$$

is megoldás, és minden megoldás ilyen alakban írható.

Bizonyítás. Tegyük föl, hogy egyrészt $\ln.\,\mathrm{k.\,o.}(f,g)|h$, másrészt $\deg f \geq \deg g$, és végezzünk Euklideszi algoritmust az f,g polinomokon

$$\begin{aligned} f &= gq_1 + r_1 \\ g &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} \\ r_{n-2} &= r_{n-1}q_n + r_n \end{aligned}$$

ahol r_n az utolsó nemzéró maradék, s így $r_n = \ln.\,\mathrm{k.\,o.}(f,g)$.

Az utolsó egyenlőségből: $r_{n-1}q_n = r_{n-2} - r_n$. Az utolsó előtti egyenlőséget szorozzuk meg q_n-nel és az előbbi egyenlőség fölhasználásával az

$$r_{n-3} = r_{n-2}q_{n-1} + r_{n-2} - r_n = r_{n-2}(q_{n-1}+1) - r_n$$

egyenlőséget kapjuk, azaz „megszabadultunk" r_{n-1}-től. Az eljárást folytatva megszabadulunk az összes r_k-tól, kivéve az r_n-et. Így megkapjuk az

$$fu' + gv' = r_n = \ln.\,\mathrm{k.\,o.}(f,g)$$

egyenlőséget. Ezt megszorozva a $h/\ln.\,\mathrm{k.\,o.}(f,g)$ polinommal kapjuk az u,v megoldásokat.

Ha egyenletünknek van megoldása, akkor triviálisan teljesül, hogy $\ln.\,\mathrm{k.\,o.}(f,g)|h$. Mivel a tétel további állításai ezek után nyilvánvalók, a bizonyítást befejeztük.

7.2. Polinomgyűrűk faktorgyűrűi.

7.10. Definíció. *Legyenek* $f,g,m \in F[x]$ *tetszőleges polinomok. Azt mondjuk, hogy* **f kongruens g-vel modulo m**, *jelölése* $f \equiv g \pmod{m}$, *ha* $m|f-g$

7.15. Állítás. *Az imént bevezetett mod m konruenciareláció ekvivalenciareláció* $F[x]$*-en. Két polinom pontosan akkor kongruens modulo m, ha m-mel osztva ugyazazt a maradékot adja.*

Megjegyzés. Az előbbi lemma és a következő tétel önálló bizonyítása jó gyakorló feladat, elvégzését melegen ajánljuk.

7.16. Tétel. *Tetszőleges F test és $f, g, f_1, g_1, f_2, g_2, m \in F[x]$ polinomok esetén*

(1) $f_i \equiv g_i \pmod{m}$, $i \in \{1, 2\}$ *maga után vonja, hogy*

$$f_1 \pm f_2 \equiv g_1 \pm g_2 \pmod{m}$$
$$f_1 \cdot f_2 \equiv g_1 \cdot g_2 \pmod{m}.$$

(2) *Ha* $h \neq 0$, *akkor* $hf \equiv gh \pmod{m} \Leftrightarrow f \equiv g \pmod{\frac{m}{\text{ln.k.o.}(m,h)}}$.

(3) *Ha* $\text{ln. k. o.}(m, h) \sim 1$, *akkor* $hf \equiv hg \pmod{m} \Leftrightarrow f \equiv g \pmod{m}$.

7.17. Tétel. *Tetszőleges $f, g, m \in F[x]$ polinomok esetén az $fu \equiv g \pmod{m}$ lineáris kongruencia pontosan akkor oldható meg, ha $\text{ln. k. o.}(f, m) | g$. Ha ez teljesül, akkor a modulo m inkongruens megoldások száma $\text{ln. k. o.}(f, m)$.*

Bizonyítás. A tétel állítása azonnal adódik abból az észrevételből hogy az $fu \equiv g \pmod{m}$ lineáris kongruencia pontosan akkor oldható meg, ha megoldható az $fu+mv = g$ egyenlet az $F[x]$ polinomgyűrűben.

7.11. Definíció. *A mod m kongruenciához tartozó ekvivalenciaosztályokat* **modulo m maradékosztályoknak** *nevezzük. Az $f \in F[x]$ polinomot tartalmazó modulo m maradékosztályt $\overline{f}$ jelöli, míg a maradékosztályok halmazát (másképpen mondva, a modulo m kongruenciához tartozó faktorhalmazt, pedig $F[x]/(m)$. Tehát $F[x]/(m) = \{\overline{f} : f \in F[x]\}$.*

7.12. Definíció. *Az $F[x]/(m)$ faktorhalmazon bevezetünk két műveletet: összeadást és szorzást: tetszőleges $f, g \in F[x]$-re legyen*

$$\overline{f} + \overline{g} = \overline{f + g}, \quad -\overline{f} = \overline{-f}, \quad \overline{f} \cdot \overline{g} = \overline{f \cdot g}.$$

7.18. Állítás. *Az előbbi műveletel jóldefiniáltak, azaz az eredmény nem függ attól, hogy az adott maradékosztály mely elemét választottuk reprezentánsnak, és e műveletekkel az $F[x]/(m)$ faktorhalmaz egységelemes kommutatív gyűrűt alkot.*

Bizonyítás. Az állítás lényegében ugyanúgy igazolható, mint a már ismert számelméleti tétel.

7.13. Definíció. *Az előbbi gyűrűt* **modulo m maradékosztály-gyűrűnek** *nevezzük.*

7.19. Állítás. *Tekintsük az $F[x]/(m)$ maradékosztálygyűrűt. Ha valamely $f \in F[x]$ polinomra $\text{ln. k. o.}(f, m) \sim 1$, akkor bármely $g \in \overline{f}$ polinomra $\text{ln. k. o.}(g, m) \sim 1$.*

Megjegyzés. Az előbbi állítás ugy is fogalmazható, hogy egy maradékosztálynak vagy minden eleme relatív prím a modulushor, vagy egyetlen eleme sem ilyen. Ezért beszélhetünk **relatív prím maradékosztályokról** is.

7.20. Tétel. *Az* $\overline{f} \in F[x]/(m)$ *maradékosztálynak pontosan akkor van multiplikatív inverze (pontosan akkor invertálható elem, azaz egység), ha* $\ln.\,k.\,o.(f, m) \sim 1$. *A multiplikatív inverz, ha létezik, egyértelműen meghatározott.*

Megjegyzés. Vegyük észre, hogy e tételünk pontos analogonja a korábbi elemi számelméleti tételnek, miszerint egy maradékosztálygyűrű invertálható elemei éppen a relatív prím maradékosztályok.

Gondolkozzunk tovább az előbbi analógia mentén. Ha $m \in \mathbb{Z},\ m > 1$, akkor egy $\overline{a} \in \mathbb{Z}_m$ maradékosztály elemei $a + km$ alakú egészek, ahol $k \in \mathbb{Z}$ (nyilván föltehető, hogy $0 \leq a < m$). Ha most (m) jelöli az m összes egész többszörösét, azaz $(m) = \{km\colon k \in \mathbb{Z}\}$, akkor az $\overline{a} = a + (m) = \{a + km\colon k \in \mathbb{Z}\}$ írásmód is használható.

Most vigyük át eljárásunkat test fölötti polinomgyűrűk faktorgyűrűire. Ezt minden további nélkül megtehetjük, hiszen az iménti számelméleti meggondolásaink mélyén a maradékos osztás rejlett, és az most is rendelkezésünkre áll majd. Legyen F test és $m \in F[x]$ nemkonstans polinom. Az $F[x]/(m)$ maradékosztálygyűrű egy $\overline{f}$ eleme

$$\overline{f} = \{f + gm\colon g \in F[x]\} = f + (m)$$

alakban írható, ahol $(m) = \{gm\colon g \in F[x]\}$. Világos, hogy csak azokat az $\overline{f}$ osztályokat kell tekintenünk, amelyekre $\deg f < \deg m$, hiszen tetszőleges $f' \in F[x]$ polinomhoz pontosan egy olyan f polinom létezik F fölött, amelyre $f' = f + gm$, ahol $f, g \in F[x]$ és $\deg f < \deg m$.

8. Polinomfüggvények, gyökök, interpoláció.

8.1. Definíció. *Az* $f = a_n x^n + \ldots + a_1 x + a_0 \in F[x]$ *polinom* $c \in F$ *helyen vett* **helyettesítési értéke** *az* $f(c) = a_n c^n + \ldots + a_1 c + a_0 \in F$ *elem. Az*

$$f\colon F \to F, \quad c \mapsto f(c)$$

leképezést az $f \in F[x]$ *polinomhoz tartozó* **polinomfüggvénynek** *nevezzük.*

Jelölés. A polinomot és a hozzá tartozó polinomfüggvényt ugyanazzal a betűvel jelöljük. Az, hogy polinomról, vagy polinomfüggvényről van szó, mindig a szövegkörnyezetből derül ki. Polinomfüggvény esetén az x-et általában **változónak** nevezzük (nem pedig határozatlannak, mint a polinomoknál).

Megjegyzés. Nagyon fontos a polinom és a polinomfüggvény fogalmának elkülönítése, megkülönböztetése. Erre a következő példák is rámutatnak.

Példák.

1. Ha F véges test, mondjuk $|F| = q$, akkor az $F \to F$ leképezések száma q^q, míg az F fölötti polinomok száma végtelen.
2. Tekintsük az $f = x^3$ és a $g = x$ $\mathbb{Z}_3$ test fölötti polinomokat. Ekkor

$$f\colon\ \overline{0} \mapsto \overline{0^3} = \overline{0},\ \overline{1} \mapsto \overline{1^3} = \overline{1},\ \overline{2} \mapsto \overline{2^3} = \overline{2},$$

azaz ugyanúgy az identikus függvény, mint a g polinomhoz tartozó. Ez azt (is) mutatja, hogy különböző polinomok ugyanazt a polinomfüggvényt határozhatják meg.

8.2. Definíció. *Azt mondjuk, hogy az* $a \in F$ *elem* **gyöke (zéróhelye)** *az* $f \in F[x]$ *polinomnak, ha* $f(a) = 0$.

8.1. Tétel. *(Bezout tétele) Bármely* $f \in F[x]$ *és* $a \in F$ *esetén*

$$f(a) = 0 \qquad \Leftrightarrow \qquad x - a | f.$$

8.2. Következmény. *Tetszőleges* $f, g \in F[x]$ *esetén e két polinom közös gyökei éppen a legnagyobb közös osztójuk,* $\ln.\,k.\,o.(f, g)$ *gyökei.*

8.3. Következmény. *Ha* $a_1, \ldots, a_k \in F$ *páronkint különböző elemek, akkor*

$$f(a_1) = \ldots = f(a_k) = 0 \qquad \Leftrightarrow \qquad (x - a_1) \ldots (x - a_k) | f.$$

8.3. Definíció. *Azt mondjuk, hogy az* $f \in F[x]$ *polinomnak az* $\alpha \in F$ *elem* **k-szoros gyöke**, *ha* $(x - \alpha)^k | f$, *de* $(x - \alpha)^{k+1} \nmid f$. *A* k *számot az* α *gyök* **multiplicitásának** *nevezzük.*

Megjegyzés. Vegyük észre, hogy nem zártuk ki a $k = 0$ esetet. Valamely α pontosan akkor 0-szoros gyök, ha nem gyök.

8.4. Következmény. *Ha az* $f \in F[x]$ *(nemzéró) polinom fokszáma* n, *akkor legföljebb* n *különböző gyöke van* F*-ben.*

Megjegyzés. A polinom és a zéróhely fogalmát egységelemes gyűrű fölött is bevezethetjük, de akkor nem érvényes már az előbbi következmény. Például, a $\mathbb{Z}_{12}$ gyűrű fölötti $x^2 - \overline{1}$ polinomnak 4 gyöke is van az alapgyűrűben.

8.5. Következmény. *Ha az $f, g \in F[x]$ polinomok legföljebb n-edfokúak, és $n+1$ helyen ugyanaz a helyettesítési értékük, akkor $f = g$.*

8.6. Következmény. *Ha az F test végtelen, akkor két F fölötti polinom akkor és csak akkor egyenlő, ha a hozzájuk tartozó polinomfüggvények megegyeznek.*

Megjegyzés. Ha az F test véges, akkor könnyen találhatók olyan különböző polinomok F fölött, amelyek ugyanazt a polinomfüggvényt határozzák meg. Például, ha $|F| = p$ prím, akkor ilyenek az x^p és az x polinomok.

8.7. Tétel. *(Lagrange-interpoláció) Tetszőleges, páronként különböző $c_1, \ldots, c_{n+1}$ és tetszőleges $d_1, \ldots, d_{n+1}$ (nem föltétlenül különböző) F-beli elemekhez pontosan egy olyan $f \in F[x]$ legföljebb n-edfokú polinom létezik, amelyre $f(c_i) = d_i$ minden $i \in \{1, 2, \ldots, n+1\}$-re.*

8.4. Definíció. *Az előbbi tételbeli f polinomot* **Lagrange-féle interpolációs polinomnak** *nevezzük.*

Megjegyzés. Előfordulhat, hogy az $n+1$ pontra illeszkedő Lagrange-polinom fokszáma kisebbnek adódik n-nél. Pontosan n-edfokú polinom létezése nem garantálható. Ha azonban semmit sem kötünk ki a fokszámra, akkor elvész az unicitás. Ugyanis tetszőleges $g \in F[x]$ polinomra az

$$f + (x - c_1) \ldots (x - c_{n+1})g$$

polinomra is teljesül a helyettesítési értékre vonatkozó föltétel.

Példa. Meghatározzuk azt a legalacsonyabb fokszámú valós együtthatós f polinomot, amelyre $f(0) = 1,\ f(1) = 2,\ f(2) = 4,\ f(3) = 8$. A számolás menete a következő.

(1) Meghatározunk 4 polinomot a következőképp:

$$\begin{aligned} \Phi_1 &= (x-1)(x-2)(x-3) & \Phi_1(0) &= -6 \\ \Phi_2 &= x(x-2)(x-3) & \Phi_2(1) &= 2 \\ \Phi_3 &= x(x-1)(x-3) & \Phi_3(2) &= -2 \\ \Phi_4 &= x(x-1)(x-2) & \Phi_4(3) &= 6 \end{aligned}$$

(2)

$$\begin{aligned} f &= 1 \cdot \frac{\Phi_1}{-6} + 2 \cdot \frac{\Phi_2}{2} + 4 \cdot \frac{\Phi_3}{-2} + 8 \cdot \frac{\Phi_4}{6} \\ &= \mathbf{\frac{1}{6}x^3 + \frac{5}{6}x + 1} \end{aligned}$$

8.1. Irreducibilis polinomok, gyöktényezős alak.

8.5. Definíció. *A $p \in F[x]$ polinom* **irreducibilis (az $F[x]$ polinomgyűrűben, ill. irreducibilis F fölött)**, *ha legalább elsőfokú és csak triviális módon bontható föl F fölötti polinomok szorzatára, azaz ha valamely $f, g \in F[x]$ polinomokra $p = fg$, akkor $f \sim p$, vagy $g \sim p$. (Ekkor nyilván $g \sim 1$, vagy $f \sim 1$.) Formálisan:*

$$\forall f, g \in F[x] \colon p = fg \;\Rightarrow\; (f \sim p \text{ vagy } g \sim p).$$

8.8. Állítás. *Egy legalább elsőfokú $p \in F[x]$ polinom akkor és csak akkor irreducibilis F fölött, hs nem bontható föl $\deg p$-nél alacsonyabb fokú, $F[x]$-beli polinomok szorzatára.*

Megjegyzés. Vegyük észre, hogy az irreducibilitás fogalmánál lényeges, hogy mely test fölött tekintjük a polinomot. Hiszen az $x^2 - 2$ polinom $\mathbb{Q}$ fölött irreducibilis, de pl. $\mathbb{R}$ fölött már nem.

8.6. Definíció. *A $p \in F[x]$ polinom* **prím**, *ha legalább elsőfokú, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat valamelyik tényezőjének.*

Megjegyzés. Az előbb definiált fogalomra gyakran úgy hivatkozunk, mint **prímtulajdonság**.

8.9. Tétel. *Test fölötti polinomgyűrűkben az irreducibilitás és a prímtulajdonság ekvivalens, azaz egy test fölötti polinom pontosan akkor prím, ha irreducibilis.*

Bizonyítás. Legyen a $p \in F[x]$ polinom prím. Ha léteznek olyan $f, g \in F[x]$ polinomok, hogy $p = fg$, akkor valamely tényezőnek osztója a p. Ha $p|f$, akkor egyrészt $\deg p \leq \deg f$, másrészt a $\deg p = \deg f + \deg g$ egyenlőségből $\deg f \leq \deg p$. A két egyenlőtlenség maga után vonja, hogy $\deg g = 0$, azaz $g \in F$, vagyis f, p asszociáltak.

Megfordítva, ha legyen most p irreducibilis és $p|fg$ valamely $f, g \in F[x]$ polinomra. Ha p osztója valamelyik tényezőnek, akkor készen vagunk, így föltehető, hogy $p \nmid f$. Ekkor $\ln.\,\mathrm{k.\,o.}(p, f) \sim 1$, ezért léteznek olyan $u, v \in F[x]$ polinomok, hogy $pu + fv = 1$. Ezt g-vel szorozva kapjuk, hogy $p|g$.

8.10. Tétel. *Minden legalább elsőfokú F fölötti polinom fölbontható irreducibilis polinomok szorzatára. A fölbontás a tényezők sorrendjétől, és asszociáltságtól eltekintve egyértelműen meghatározott.*

Megjegyzés. Az előbbi tételben szereplő egyértelműségi követelmény azt jelenti, hogy ha valamely $f \in F[x]$ polinomnak $f = p_1 \cdot \ldots \cdot p_n$, és $f = q_1 \cdot \ldots \cdot q_m$ egyaránt irreducibilis fölbontása, akkor egyrészt $n = m$, másrészt minden $1 \leq i \leq n$-hez van olyan $1 \leq j \leq m$, hogy $p_i \sim q_j$.

Bizonyítás. Legyen $f \in F[x]$ legalább elsőfokú polinom. Ha $\deg f = 1$, akkor készen vagyunk, és ugyanez a helyzet, ha f irreducibilis. Így

föltehető egyrészt, hogy $\deg f \geq 2$, és léteznek olyan $g_1, g_2 \in F[x]$ nemkonstans polinomok, hogy $f = g_1 g_2$, és $\deg g_i < \deg f$. Ha valamelyik tényező nem irreducibilis, akkor azzal ugyanúgy járunk el, mint tettük az f polinommal. Az eljárás nem folytatható minden határon túl, mert $\deg f \in \mathbb{N}$. Az eljárás pontosan akkor áll le, ha mindegyik tényező irreducibilis.

A fölbontás egyértelműsége abból adódik, hogy az irreducibilis polinomok prímek.

8.11. Állítás. *Az elsőfokú polinomok bármely test fölött irreducibilisek.*

8.12. Tétel. *Ha a legalább másodfokú $f \in F[x]$ polinom irreducibilis, akkor nincs gyöke F-ben.*

Megjegyzés. Az előbbi tétel megfordítása nem igaz. Egy ellenpélda az $x^4 + 1 \in \mathbb{R}[x]$ polinom.

8.13. Tétel. *Legyen $f \in F[x]$ és $2 \leq \deg f \leq 3$. F pontosan akkor irreducibilis, ha nincs gyöke.*

8.14. Tétel. *Az $F[x]/(f)$ maradékosztály-gyűrű pontosan akkor test, ha az f polinom irreducibilis F fölött.*

Bizonyítás. Tudjuk, hogy az $F[x]/(f)$ maradékosztály-gyűrű kommutatív és egységelemes. Azt kell igazolni, hogy az összes nemzéró elemeknek pontosan akkor van multiplikatív inverze, ha az f polinom irreducibilis $F[x]$-ben.

Világos, hogy $F[x]/(f)$ elemei $\overline{g} = g + (f)$ alakban írhatók, ahol $g \in F[x]$ és $g \neq 0$ esetén $\deg g < \deg f$.

Ha az $F[x]/(f)$ maradékosztály-gyűrű test, akkor bármely $\overline{g}$-hez, ha $g \neq 0$, van olyan $\overline{h} \in F[x]/(f)$, amelyre $\overline{g} \cdot \overline{h} = \overline{1}$, azaz $gh \equiv 1 \pmod{f}$. Ez utóbbi maga után vonja, hogy alkalmas $h' \in F[x]$ polinomra $gh + fh' = 1$, amiből $\ln.\,k.\,o.(g, f) | 1$ következik. Ez pedig csak akkor állhat fönn minden $\deg f$-nél alacsonyabb fokú g polinomra, ha f irreducibilis.

Ha f irreducibilis polinom, akkor az előbbi gondolatmeneten visszafelé haladva: bármely $\deg f$-nél alacsonyabb fokú $g \in F[x]$ polinomra megoldható a $gu + fv = 1$ egyenlet. Ha u egy egymegoldás, akkor $gu \equiv 1 \pmod{f}$, azaz $\overline{u}$ a $\overline{g}$ inverze az $F[x]/(f)$ gyűrűben, azaz bármely $\overline{g} \neq \overline{0}$ elemnek van multiplikatív inverze, s így az $F[x]/(f)$ maradékosztály-gyűrű test.

8.2. Irreducibilis polinomok a $\mathbb{R}$ és $\mathbb{C}$ testek fölött. Gyöktényezős alak, Viète formulák.

8.15. Tétel. (a klasszikus algebra alaptétele) *Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.*

8.16. Következmény. *A komplex számok teste fölött pontosan az elsőfokú polinomok irreducibilisek, így minden komplex együtthatós legalább elsőfokú polinom elsőfokú polinomok szorzatára bontható. Ha* $f = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{C}[x]$, $a_n \neq 0$, *akkor léteznek olyan (nem föltétlenül különböző)* $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ *komplex számok, hogy* $f = a_n(x - \alpha_1)\ldots(x - \alpha_n)$.

Megjegyzés. Az utóbbi alakot az f polinom **gyöktényezős alakjának** nevezzük.

8.17. Következmény. *Bármely* $f, g \in \mathbb{C}[x]$ *esetén* $f|g$ *pontosan akkor teljesül, ha* f *minden gyöke egyúttal gyöke* g*-nek is, mégpedig legalább akkora multiplicitással, mint* f*-nek.*

8.18. Tétel. *Legyenek az* $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{C}[x]$ n*-edfokú főpolinom komplex gyökei (mindegyiket annyiszor föltüntetve, ahányszoros gyök)* $\alpha_1, \ldots, \alpha_n$. *Ekkor érvényesek az alábbi egyenlőségek.*

$$\begin{aligned}
-a_{n-1} &= \alpha_1 + \ldots + \alpha_n \\
a_{n-2} &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \ldots + \alpha_{n-1}\alpha_n \\
-a_{n-3} &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \ldots + \alpha_{n-2}\alpha_{n-1}\alpha_n \\
&\vdots \\
(-1)^{n-1}a_1 &= \alpha_1\alpha_2\cdot\ldots\cdot\alpha_{n-2}\alpha_{n-1} + \alpha_1\alpha_2\cdot\ldots\cdot\alpha_{n-2}\alpha_n + \\
&\quad \ldots + \alpha_2\alpha_3\cdot\ldots\cdot\alpha_{n-1}\alpha_n \\
(-1)^n a_0 &= \alpha_1\alpha_2\cdot\ldots\cdot\alpha_{n-1}\alpha_n.
\end{aligned}$$

Megjegyzés. A fönti egyenlőségeket **Viète-formuláknak/képleteknek** nevezzük. A k-adik sor bal oldalán $(-1)^k a_{n-k}$ áll, míg a jobb oldalán az $\alpha_1, \ldots, \alpha_n$ betűkből álló összes k-tényezős szorzat összege, azaz egy $\binom{n}{k}$-tagú összeg. Formálisan:

$$(-1)^k a_{n-k} = \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} \alpha_{i_1}\cdot\alpha_{i_2}\cdot\ldots\cdot\alpha_{i_k}.$$

8.19. Tétel. *Legyen* $f \in \mathbb{R}[x]$. *Valamely* $\alpha \in \mathbb{C}$ *pontosan akkor gyöke* f*-nek, ha konjugáltja is gyök.* α *és* $\overline{\alpha}$ *multiplicitása megegyezik.*

8.20. Következmény. *Egy valós együtthatós polinom pontosan akkor irreducibilis a valós számok teste fölött, ha elsőfokú, vagy olyan másodfokú polinom, amelynek nincs valós gyöke. Tehát az* $\mathbb{R}$ *fölött irreducibilis polinomok a következők:*

- $ax + b$ $(a, b \in \mathbb{R},\ a \neq 0)$*;*
- $ax^2 + bx + c$ $(a, b, c \in \mathbb{R},\ a \neq 0,\ b^2 - ac < 0)$.

8.3. Irreducibilis polinomok $\mathbb{Q}$ fölött.

8.7. Definíció. *Az* $a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *polinomot* **primitív polinomnak** *nevezzük, ha* $\ln.\,k.\,o.(a_0, \ldots, a_n) = 1$.

8.21. Állítás. *Minden racionális együtthatós polinom fölbontható egy racionális szám és egy primitív polinom szorzatára, formálisan:*

$$\forall f \in \mathbb{Q}[x]\ \exists r \in \mathbb{Q}\ \exists f^* \in \mathbb{Z}[x]\colon f = r f^* \text{ ahol } f^* \text{ primitív polinom.}$$

Megjegyzés. Mivel az előbbi állításban szereplő polinomokra $f \sim f^*$, a $\mathbb{Q}[x]$ polinomgyűrűben mindig lehet — asszociáltság erejéig — primitív polinomokkal számolni.

8.22. Tétel. (Gauss lemma) *Primitív polinomok szorzata primitív polinom.*

8.23. Tétel. *Ha egy legalább elsőfokú egész együtthatós polinom nem bontható föl nála alacsonyabb fokszámú egész együtthatós polinomok szorzatára, akkor* $\mathbb{Q}$ *fölött sem, és megfordítva. Formálisan megfogalmazva: ha* $f \in \mathbb{Z}[x]$, $\deg f = n \geq 1$, *akkor a következő két állítás ekvivalens.*

(1) $\exists g, h \in \mathbb{Z}[x]\colon f = gh$ *és* $0 < \deg g, \deg h < n$;
(2) $\exists g, h \in \mathbb{Q}[x]\colon f = gh$ *és* $0 < \deg g, \deg h < n$.

8.8. Definíció. *Azt mondjuk, hogy a* p *prímszám* **pontos osztója** *az* a *egész számnak, ha* $p|a$, *de* $p^2 \nmid a$. *Jelölése:* $p||a$.

8.24. Tétel. (Schönemann-Eisenstein-féle irreducibilitási kritérium) *Legyen* $f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$. *Ha létezik olyanp prímszám, hogy* $p \nmid a_n$, $p|a_i$ *minden* $1 \leq i \neq n-1$, *és* $p||a_0$, *akkor* f *irreducibilis a racionális számok teste fölött.*

Bizonyítás. A tegyük föl, hogy a tételbeli p prímszám létezik, de az f polinom reducibilis, azaz léteznek olyan nemkonstans $g, h \in \mathbb{Z}[x]$ polinomok, hogy $f = gh$.

Tekintsük az egész problémát a $\mathbb{Z}_p$ test fölött, $\overline{f} = \overline{g}\overline{h}$. Mivel $p \nmid a_n$, de az f többi együtthatójának osztója a p prím, $ovf = \overline{a_n} x^n$. Világos, hogy $\overline{f}$ minden osztója sx^m alakú, ahol $s \in \mathbb{Z}_p$ és $0 \leq m \leq n$ egész. Ezért

$$\overline{g} = ux^k \quad \text{és} \quad \overline{h} = vx^l, \qquad \text{valamely} \quad u, v \in \mathbb{Z}_p\text{-re.}$$

Mivel $\mathbb{Z}_p$ test, így zérusosztómentes, tehát $\deg \overline{g} + \deg \overline{h} = k + l = n$. Azonban

$$k = \deg \overline{g} \leq \deg g, \qquad l = \deg \overline{h} \leq \deg h.$$

A föltételezett fölbontás miatt $0 < k, l < n$. Mindebből az adódik, hogy $\overline{g}, \overline{h}$ konstans tagja 0, ami maga után vonja, hogy g, h konstans tagja is 0. Így mindkettő osztható a p prímszámmal, tehtát az f konstans tagja, amely az iménti polinomok konstans tagjainak szorzata, osztható p^2-tel, ami ellentmond a tétel föltételeinek, nevezetesen, hogy $p^2 \nmid a_0$.

Megjegyzés. Az előbbi tétel megfordítása nem igaz! Abból, hogy nem létezik a tételbeli föltételnek megfelelő prímszám, nem következik a polinom reducibilitása.

8.25. Következmény. *Minden $n \geq 1$-re létezik $\mathbb{Q}$ fölött irreducibilis n-edfokú polinom.*

8.26. Tétel. (Rolle-tétele) *Legyen $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha létezik olyan $\frac{p}{q}$ racionális szám, amelyre $p, q \in \mathbb{Z}$, $\ln.\,k.\,o.(p,q) = 0$, akkor*

$$f\left(\frac{p}{q}\right) = 0 \qquad \Rightarrow \qquad q|a_n \text{ és } p|a_0.$$

Speciálisan, az egész együtthatós főpolinomok minden racionális gyöke egész szám.

Bizonyítás. Legyen $p, q \in \mathbb{Z}$, $\ln.\,k.\,o.(p,q) \sim 1$ és $f\left(\frac{p}{q}\right) = 0$. Az utóbbi egyenlőséget q^n-nel szorozva adódik az állítás.

8.27. Következmény. *Az előbbi tétel föltételei mellett, ha $f(\frac{p}{q}) = 0$, akkor tetszőleges $m \in \mathbb{Z}$-re $p - mq | f(m)$. Speciálisan: $p - q | f(1)$ és $p + q | f(-1)$.*

Bizonyítás. Legyen $m \in \mathbb{Z}$, p, q mint az előbb, és írjuk föl az f polinomot $x - m$ hatványai szerint. Ekkor

$$f = a_n(x-m)^n + c_{n-1}(x-m)^{n-1} + \ldots + c_1(x-m) + c_0,$$

ahol $c_{n-1}, \ldots, c_1, c_0 = f(m) \in \mathbb{Z}$.

Helyettesítsünk be $x = \frac{p}{q}$-t, majd a kapott egyenlőséget szorozzuk meg q^n-nel:

$$0 = f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q} - m\right)^n + c_{n-1}\left(\frac{p}{q} - m\right) + \ldots + c_1\left(\frac{p}{q} - m\right) + c_0$$

$$0 = a_n(p - qm)^n + c_{n-1}(p - qm)^{n-1}q + \ldots + c_1(p - qm)q^{n-1} + c_0 q^n.$$

A második egyenlőségből következik, hogy $p - mq | c_n q^n$, de $\ln.\,k.\,o.(p - mq, q^n) \sim \ln.\,k.\,o.(p - mq, q) \sim \ln.\,k.\,o.(p, q) \sim 1$, így $p - mq | c_0 = f(m)$. Az állítás többi része ezek után nyilvánvaló.

8.4. Derivált, többszörös gyökök

8.9. Definíció. *Az $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{C}[x]$ polinom* **deriváltján** *az $n a_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2 x + a_1 \in \mathbb{C}[x]$ polinomot értjük.*

Jelölés. Az f polinom deriváltját f', míg a második,..., k-adik deriváltját $f'', \ldots f^{(k)}$ jelöli.

8.28. Tétel. *Tetszőleges $f, g \in \mathbb{C}[x]$ polinomokra és $k \in \mathbb{N}$ egészre érvényesek az alábbi egyenlőségek:*

(1) $(f+g)' = f'+g'$, (2) $(fg)' = f'g+fg'$, (3) $(f^k)' = kf^{k-1}f'$.

8.29. Tétel. *Ha $k \geq 1$ egész, és az $\alpha \in \mathbb{C}$ k-szoros gyöke az f polinomnak, akkor α f'-nek $k-1$-szeres gyöke. (Ha $k = 1$, akkor α nem gyöke f'-nek.)*

Bizonyítás. Ha α k-szoros gyöke f-nek, akkor $f = (x-\alpha)^k g$, ahol $g(\alpha) \neq 0$. Ekkor $f' = k(x-\alpha)^{k-1}g + (x-\alpha)^k g'$, ami már maga után vonja az állítást.

Megjegyzés. E tétel megfordítása nem igaz. Abból, hogy $f'(\beta) = 0$, általában nem következik, hogy $f(\beta) = 0$.

8.30. Következmény. *Legyen $f \in \mathbb{C}[x]$, $\alpha \in \mathbb{C}$, és $f(\alpha) = 0$. Az a legkisebb $k \in \mathbb{N}$ kitevő, amelyre $f^{(k)}(\alpha) \neq 0$, éppen az α gyök multiplicitása. Másképpen mondva, α pontosan akkor k-szoros gyöke az f polinomnak, ha $f(\alpha) = f'(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$, de $f^{(k)}(\alpha) \neq 0$.*

8.31. Következmény. *Az α komplex szám ponosan akkor többszörös gyöke az f polinmnak, ha gyöke az* $\mathrm{ln.\,k.\,o.}(f, f')$ *polinomnak.*

8.32. Következmény. *Bármely legalább elsőfokú f polinomnak és az $\frac{f}{\mathrm{ln.k.o.}(f,f')}$ polinomnak ugyanazok a gyökei, csak az utóbbi polinom minden gyöke egyszeres.*

8.10. Definíció. *Legyen F tetszőleges test. Az olyan $K \subseteq F$ részhalmazokat, amelyek szintén testet alkotnak az F test műveleteivel — másképpen mondva K zárt az F-beli műveletekre — F* **résztesteinek** *nevezzük. A komplex számok testének résztesteit* **számtesteknek** *nevezzük.*

8.33. Következmény. *Ha T egy számtest és az $f \in T[x]$ polinom irreducibilis T-fölött, akkor f minden komplex gyöke egyszeres.*

Horner módszer

Ha egy $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in F[x]$ n-edfokú polinom helyettesítési értékét akarjuk kiszámítani valamely $c \in F$ helyen és mechanikusan elvégezzük a helyettesítéseket, akkor $2n-1$ szorzást és n összeadást kell elvégeznünk. Ez nagy n-re elég hosszadalmas. Van azonban gyorsabb, kevesebb műveletet igénylő eljárás is, amely egyszerűen a szorzás összeadásra vonatkozó disztributivitásán alapul. Ehhez írjuk fel $f(c)$-t a következő alakban:

$$f(c) = ((\cdots(((a_n \cdot c + a_{n-1}) \cdot c + a_{n-2}) \cdot c + a_{n-3}) \ldots + a_2) \cdot c + a_1) \cdot c + a_0.$$

Ezt az alakot **Horner-elrendezésnek** nevezzük. Ebben balról jobbra haladva elvégezve a műveleteket a következő részeredmény (egy zárójelben levő kifejezés) mindig úgy adódik, hogy az előzőt megszorozzuk c-vel, és hozzáadjuk az f soronkövetkező együtthatóját.

A számolást kényelmesebb a következő táblázat segítségével végezni:

	a_n	a_{n-1}	$\cdots$	$\diamondsuit$	$\spadesuit$	$\cdots$	a_0
c	a_n	$a_n \cdot c + a_{n-1}$	$\cdots$	$\clubsuit$	$\clubsuit \cdot c + \spadesuit$	$\cdots$	$f(c)$

Alkalmazzuk most az előbbi Horner-módszert az $f = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ polinomra és a $c \in F$ elemre, majd egészítsük ki a táblázatot egy újabb, az előzőnél eggyel rövidebb sorral a fentebb leírt számolási szabályt követve. Folytassuk újabb, egyre rövidebb sorokkal, míg végül egy háromszög alakú táblázatot kapunk.

	a_n	a_{n-1}	$\cdots$	a_1	a_0
c			$\cdots$		d_0
c			$\cdots$	d_1	
$\vdots$	$\vdots$	$\vdots$	$\ddots$		
c		d_{n-1}			
c	d_n				

A táblázat jobb szélén átlósan elhelyezkedő elemek — $d_0, d_1, \ldots, d_n$ — megadják annak a polinomnak az együtthatóit, amelyet f-ből az $x - c$ határozatlanra való áttéréssel kapunk:

$$a_n x^n + \ldots + a_1 x + a_0 = d_n (x - c)^n + \ldots + d_1 (x - c) + d_0.$$

Kiolvasható a táblázatból az is, hogy c hányszoros gyöke f-nek: a c gyök multiplicitása nem más, mint a legkisebb k, amelyre $d_k \neq 0$ (megengedve a $k = 0$ esetet is).

Az iménti eljárást **iterált Horner-módszernek** nevezzük.

9. Bevezetés az absztrakt algebrába 2. Csoportok.

Megjegyzés. E fejezetben — a téma fontossága és nehézsége miatt — néhány olyan definíciót és tételt megismétlünk, amelyek már szerepeltek a Diszkrét matematika kurzuson.

9.1. Definíció.

(1) *Az egyetlen kétváltozós művelettel rendelkező algebrát* **grupoidnak** *nevezzük. Tehát az $(A, *)$ algebra grupoid, ha A nemüres halmaz, $*$ pedig egy kétváltozós művelet A-n, azaz $*\colon A^2 \to A$.*

(2) *Ha egy grupoid művelete asszociatív, akkor* **félcsoportnak** *nevezzük.*

(3) *Ha egy $(A, *)$ félcsoportban van egységelem — azaz van olyan $e \in A$ elem, hogy minden $a \in A$-ra $e * a = a * e = a$ — akkor* **monoidnak** *nevezzük.*

(4) *Ha egy monoidban minden elemnek van inverze, akkor* **csoportnak** *nevezzük. tehát, az $(A, *)$ monoid — egységelemét e jelöli — pontosan akkor csoport, ha*

$$\forall a \in A\ \exists b \in A\colon\ a * b = b * a = e.$$

(5) *Ha egy csoport művelete kommutatív, akkor* **Abel-csoportnak** *nevezzük.*

Jelölés. Grupoidok műveletét általában $\cdot$ (multiplikatív írásmód), vagy $+$ (additív írásmód) fogja jelölni (az előbbit gyakran ki sem írjuk), kivéve ha a körülmények mást indokolnak (pl. halmazok egyesítése, stb). Az egységelemet multiplikatív írásmód esetén 1, additív írásmód esetén 0 fogja jelölni. Valamely a elem inverzére az a^{-1}, ill $-a$ jelölést alkalmazzuk.

9.1. Állítás. *Egy grupoidban legföljebb egy egységelem lehet, és egy monoidban egy elemnek legföljebb egy inverze van.*

Bizonyítás. Legyen A grupoid és $e, e' \in A$ egységelemek. Ekkor $e = ee' = e'$. Tekintsük az M monoidot, és tegyük föl, hogy az $a \in M$ elemnek $a', a'' \in M$ egyaránt inverze. Ekkor

$$a' = a'1 = a'(aa'') = (a'a)a'' = 1a'' = a''.$$

Megjegyzés. Ha egy grupoid művelete nem asszociatív, akkor egy elemnek több inverze is lehet.

9.2. Definíció. *Legyen $\mathbf{A} = (A, *)$ grupoid, és $B \subseteq A$. Azt mondjuk, hogy a B halmaz* **zárt a $*$ műveletre**, *ha bármely $b_1, b_2 \in B$ elemre $b_1 * b_2 \in B$. Ha $B \neq \emptyset$, és zárt a $*$ műveletre, akkor B grupoidot alkot a $*$ művelettel (pontosabban annak megszorításával). Az ilyen $\mathbf{B} = (B, *)$ grupoidot $\mathbf{A}$ grupoid* **részgrupoidjának** *nevezzük. Jelölése $\mathbf{B} \leq \mathbf{A}$.*

9.3. Definíció. *Ha $(G, \cdot)$ csoport és $\emptyset \neq H \subseteq G$, és $(H, \cdot)$ részgrupoid maga is csoport, akkor azt mondjuk, hogy $(H, \cdot)$* **részcsoportja** *a $(G, \cdot)$ csoportnak.*

9.4. Definíció. *Legyen $*$ egy művelet a nemüres A halmazon. Azt mondjuk, hogy a $*$ művelet*

- **invertálható**, *ha bármely $a, b \in A$-ra az $a * x = b$ és az $x * a = b$ egyenletek megoldhatók, azaz léteznek olyan (esetleg több is) olyan $c, d \in A$ elemek, hogy $a * c = b$, ill. $d * a = b$;*
- **kancellatív** *(vagy* **egyszerűsítéses***), ha bármely $a, b \in A$-ra az $a * x = b$ és az $x * a = b$ egyenleteknek legföljebb egy-egy megoldásuk van.*

Megjegyzés. A kancellativitás kritériuma a következőképp is megfogalmazható (ez indokolja az egyszerűsítéses elnevezést):

$$\forall a, u, v \in A\colon (a * u = a * v \ \Rightarrow \ u = v) \text{ és } (u * a = v * a \ \Rightarrow \ u = v).$$

9.2. Tétel. *Csoport művelete mindig invertálható és kancellatív, és megfordítava, minden invertálható és kancellatív műveletű félcsoport csoport.*

Bizonyítás. E tétel önálló bizonyítása révén az olvasó ellenőrizheti, hogy megértette-e az előbb definiált fogalmakat. Ezért annak elvégzését javasoljuk.

9.3. Állítás. *Véges alaphalmaz esetén az invertálhatóság és a kancellativitás ekvivalens tulajdonságok.*

9.5. Definíció. *Legyen $(A, *)$ és $(B, \circ)$ két csoport (akár csak grupoid). Azt mondjuk, hogy a $\varphi\colon A \to B$ leképezés* **izomorfizmusa** *A-nak B-be, ha bijektív és fölcserélhető a műveletekkel (megőrzi a műveleteket), azaz*

$$\forall a_1, a_2 \in A\colon \ (a_1 * a_2)\varphi = a_1\varphi \circ a_2\varphi.$$

Ha létezik $A \to B$ izomorfizmus, akkor azt mondjuk, hogy A és B **izomorfak**, *jelölése $A \cong B$.*

Példák.
(1) Tetszőleges gyűrű Abel-csoportot alkot az az összeadás műveletével. tetszőleges egységelemes gyűrű egységei csoportot alkotnak a szorzással.
(2) Tetszőleges F test fölötti $n \times n$-es mátrixok gyűrűjének egységcsoportja az F **fölötti** n **dimenziós általános lineáris csoport**, jelölése: $\mathrm{GL}_n(F)$. E csoportban az 1 determinánsú mátrixok részcsoportot alkotnak, ezt **speciális lineáris csoportnak** nevezzük, jelölése: $\mathrm{SL}_n(F)$:

$$\mathrm{GL}_n(F) = \{A \in F^{n\times n}\colon \det(A) \neq 0\},$$
$$\mathrm{SL}_n(F) = \{A \in F^{n\times n}\colon \det(A) = 1\}.$$

(3) Az összes komplex egységgyökök csoportot alkotnak a szorzás műveletével, ezen belül az n-edik egységgyökök bármely rögzített n-re részcsoportot alkotnak. Ha U_n jelöli az n-edik egységgyökök csoportját,

akkor $(U_n, \cdot) \cong (\mathbb{Z}_n, +)$.
(4) Tetszőleges $A \neq \emptyset$ halmaz összes transzformációi T_A halmaza monoidot alkot a leképezésszorzással, amelyben a bijektív transzformációk, a permutációk, csoportot alkotnak. Ez utóbbit az A halmaz fölötti **szimmetrikus csoportnak** nevezzük. Jelölése: S_A. Ha $|A| = n$, akkor használjuk az S_n jelölést is.
(5) Az S_4 csoportban a $V = \{\mathrm{id},\ (12)(34),\ (13)(24),\ (14)(23)\}$ részcsoportot **Klein-féle csoportnak** nevezzük.
(6) A sík összes egybevágósági transzformációi csoportot alkotnak a leképezésszorzással, egy adott síkidomot önmagába vivő egybevágósági transzformációk alkotta részcsoportot az adott alakzat **szimmetriacsoportjának** nevezzük.

9.6. Definíció. *A szabályos n-szög szimmetriacsoportját* **n-edfokú diédercsoportnak** *nevezzük. Jelölése D_n.*

9.4. Tétel. *A D_n csoportnak $2n$ számú eleme van:*

$$D_n = \{\mathrm{id}, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \tau, \alpha\tau, \alpha^2\tau, \ldots, \alpha^{n-1}\tau\},$$

ahol α a szabályos sokszög középpontja körüli $\frac{2\pi}{n}$ szöggel való elforgatást jelöli, mí τ valamely szimmetria-tengelyére való tükrözést.

Megjegyzés. Világos, hogy az α^k-k a középpont körüli $\frac{2k\pi}{n}$ szögű forgatások ($0 \leq k \leq n-1$), míg az $\alpha^k\tau$ transzformációk pedig tengelyes tükrözések (két „szomszédos" szimmetriatengely ugyanis $\frac{\pi}{n}$ szöget zár be egymással. Továbbá fönnáll a $\tau\alpha = \alpha^{-1}\tau$ összefüggés is.

9.1. Permutációcsoportok

9.7. Definíció. *Legyen $A \neq \emptyset$ tetszőleges halmaz. Az S_A szimmetrikus csoport részcsoportjait A* **fölötti permutációcsoportoknak** *nevezzük.*

9.8. Definíció. *Az $A = \{1, 2, \ldots, n\}$ halmaz összes permutációi alkotta csoportok* **n-edfokú szimmetrikus csoportnak** *nevezzűk, és S_n-nel jelöljük.*

9.9. Definíció. *Azt mondjuk, hogy a $\pi \in S_A$ permutáció* **mozgatja** *az $a \in A$ elemet, ha $a\pi \neq a$. A π permutáció által mozgatott elemek halmazát M_π fogja jelölni.*

9.10. Definíció. *Legyenek $a_1, \ldots, a_k \in \{1, 2, \ldots, n\}$ páronként különböző elemek, valamint $\pi \in S_n$ az a permutáció, amelyre*

$$a_1\pi = a_2,\ a_2\pi = a_3, \ldots, a_{k-1}\pi = a_k,\ a_k\pi = a_1,$$
$$\text{és} \quad b\pi = b\ \forall b \notin \{a_1, \ldots, a_k\}.$$

Ezen π permutációt röviden $\pi = (a_1a_2 \ldots a_k)$-val jelöljük, és **ciklikus permutációnak**, *vagy röviden* **ciklusnak** *nevezzük. E* **ciklus hossza** *k.*

9.11. Definíció. *Két permutáció — $\alpha, \beta \in S_n$ —* **idegen**, *ha mozgatott elemeik halmaza diszjunkt, azaz $M_\alpha \cap M_\beta = \emptyset$.*

A következő négy tétel és állítás bizonyítása megtalálható Klasszikus és lineáris algebra c. jegyzetemben (Polygon Jegyzettár, 1999.).

9.5. Tétel. *Ha a $\pi, \varrho \in S_A$ permutációk idegenek, akkor a szorzásnál fölcserélhetők, azaz $\pi\varrho = \varrho\pi$.*

9.6. Tétel. *Minden S_n-beli permutáció előáll páronként idegen ciklusok szorzataként. Ezen előállítás a ciklusok sorrendjétől eltekintve egyértelmű.*

9.12. Definíció. *Az (ij) alakú, azaz a 2 hosszúságú ciklusokat* **transzpozícióknak** *nevezzük.*

9.7. Tétel. *Minden permutáció előállítható transzpozíciók szorzataként, azaz az S_n csoportot generálják a transzpozíciók.*

9.8. Tétel. *Egy S_n-beli permutáció többféleképp is előállítható transzpozíciók szorzataként, de a tényezők számának paritása egyértelműen meghatározott.*

9.13. Definíció. *Azt mondjuk, hogy a $\pi \in S_n$ permutáció* **páros permutáció**, *ha páros sok transzpozíció szorzatára bontható. Ellenkező esetetben π* **páratlan permutáció**.

9.9. Állítás. *A páros hosszúságú ciklusok páratlan-, míg a páratlan hosszúságú ciklusok páros permutációk.*

9.14. Definíció. *Az S_n csoport imént definiált részcsoportját n-edfokú* **alternáló csoportnak** *nevezzük, és A_n-nel jelöljük.*

9.10. Tétel. *Az alternálócsoportot generálják a 3 hosszúságú ciklusok, azaz minden páros permutáció előáll 3 hosszúságú ciklusok szorzataként.*

9.2. Hatványozás, elemrend, ciklikus csoportok

Jelölés. Az elkövetkezőkben G mindig egy tetszőleges multiplikatív csoportot jelöl, amelynek műveletét a legtöbbször nem írjuk ki. A korábban említettekkel összhangban, a csoportok egységelemét 1, míg valamely a elem inverzét a^{-1} fogja jelölni.

9.15. Definíció. *(egész kitevős hatványozás csoportban) Legyen $a \in G$ és $n \in \mathbb{N}$. Az a elem n-edig hatványa az $a^n = a \cdot \ldots \cdot a$ n tényezős szorzat. Továbbá legyen $a^{-n} = a^{-1} \cdot \ldots \cdot a^{-1}$, amely szintén egy n tényezős szorzat. Végül, $a^0 = 1$.*

9.11. Tétel. *Legyen G csoport, $a, b \in G$ és $m, n \in \mathbb{Z}$. Ekkor érvényesek az alábbi egyenlőségek.*

(1) $a^m \cdot a^n = a^{m+n}$,
(2) $(a^m)^n = a^{mn}$,
(3) *ha* $ab = ba$, *akkor* $(ab)^m = a^m \cdot b^m$.

9.16. Definíció. *Az $a \in G$* **elem rendje** *az a legkisebb $n \in \mathbb{N}$, amelyre $a^n = 1$. Ha ilyen kitevő nem létezik, azaz az a elem egyetlen természetes szám kitevős hatványa sem 1, akkor azt mondjuk, hogy a rendje végtelen. Az a elem rendjét* $\mathrm{o}(a)$ *jelöli. A G* **csoport rendjén** *pedig elemei számát értjük.*

9.12. Állítás. *Ha $a \in G$ véges rendű elem, mondjuk $\mathrm{o}(a) = n$, akkor bármely $r, s \in \mathbb{Z}$-re*

(1) $a^r = 1 \quad \Leftrightarrow \quad n | r$,
(2) $a^r = a^s \quad \Leftrightarrow \quad r \equiv s \pmod{n}$,
(3) $\mathrm{o}(a^r) = \frac{n}{\text{ln.k.o.}(r,n)}$.

Megjegyzés. A $\mathbb{C}^*$ csoport (a nemzéró komplex számok multiplikatív csoportja) véges rendű elemei épp az egységgyökök. Ha valamely $\varepsilon \in \mathbb{C}^*$-ra $\mathrm{o}(\varepsilon) = n$, akkor ε primitív n-edik egységgyök.
Jelölés. Tetszőleges $a \in G$-re legyen $[a] = \{a^k : k \in \mathbb{Z}\}$, azaz $[a]$ az a elem összes egész kitevős hatványának halmaza.

9.17. Definíció. *Azt mondjuk, hogy G* **ciklikus csoport**, *ha $G = [a]$ valamely $a \in G$-re.*

9.13. Tétel. *Legyen G egy tetszőleges csoport és $a \in G$. Ha $\mathrm{o}(a) = n$, akkor $([a], \cdot) \cong (\mathbb{Z}_n, +)$, míg ha a rendje végtelen, akkor $([a], \cdot) \cong (\mathbb{Z}, +)$.*

9.14. Következmény. *Egy csoport akkor és csak akkor ciklikus, ha izomorf a $\mathbb{Z}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \ldots$ additív csoportok valamelyikével.*

9.15. Tétel. *Ciklikus csoport minden részcsoportja ciklikus.*

Bizonyítás. Egy csoport ciklikus volta legegyszerűbben úgy bizonyítható, hogy megadjuk generátorelemét. Ha $G = [a]$ ciklikus csoport, és $H \subseteq G$ egy részcsoport, akkor H nyilván tartalmazza a-nak legalább egy pozitív kitevős hatványát is (kivéve, ha H egyelemű, de akkor az állítás triviális). E hatványkitevők között van legkisebb, moondjuk $k > 0$. Ekkor $H = [a^k]$.

9.16. Állítás. *Tetszőleges $n \in \mathbb{N}$ természetes számra az összes n-edik egységgyökök a $\mathbb{C}^*$ csoport egy ciklikus részcsoportját alkotják.*

9.3. Részcsoport, generálás

9.17. Állítás. *Legyen G csoport és $H \subseteq G$. H* **részcsoportja G-nek,** *ha*

(1) $1 \in H$,
(2) $\forall a, b \in H \quad \Rightarrow \quad ab \in H$;
(3) $\forall a \in H \quad \Rightarrow \quad a^{-1} \in H$.

9.18. Tétel. *Részcsoportok metszete részcsoport: azaz ha $(H_i)_{i\in I}$ a G csoport részcsoportjai tetszőleges rendszere (azaz $H_i \leq G \colon \forall i \in I$), akkor $\bigcap_{i\in I} H_i \leq G$.*

9.18. Definíció. *Legyen G csoport, és $B \subseteq G$. A B halmaz által* **generált részcsoport** *a legszűkebb olyan részcsoport, amely tartalmazza B részhalmazt. Jelölése: $[B]$.*

9.19. Állítás. *Az előbbi definíció jelöléseivel:*

$$[B] = \bigcap_{B\subseteq H\leq G} H.$$

Megjegyzés. Az üres halmaz generátuma a csak az egységelemet tartalmazó (így a legszűkebb) részcsoport: $[\emptyset] = \{1_G\}$.

9.19. Definíció. *Ha $[B] = G$ a G csoport valamely B részhalmazára, akkor azt mondjuk, hogy B a G csoport (egy)* **generátorrendszere**.

9.20. Állítás. *Legyen G csoport. A $B \subseteq G$ részhalmaz által generált részcsoport azokból az elemekből áll, amelyek megkaphatók B elemeiből a szorzás és az inverzképzés véges számú alkalmazásával:*

$$[B] = \{b_1^{\varepsilon_1} \cdot \ldots \cdot b_k^{\varepsilon_k} \colon k \in \mathbb{N}_0,\ b_1, \ldots, b_k \in B,\ \varepsilon_1, \ldots, \varepsilon_k \in \{\pm 1\}\}$$

9.21. Tétel. *Legyen G csoport és $H \leq G$ Tetszőleges $a, b \in G$-re a $a \sim b \ \Leftrightarrow \ a^{-1}b \in H$ reláció ekvivalenciareláció G-n. Egy $a \in G$ elem ekvivalencia-osztálya $aH = \{ah \colon h \in H\}$.*

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

9.22. Következmény. *Egy $H \leq G$ részcsoport szerinti összes bal oldali mellékosztályai G-nek egy osztályozását alkotják.*

9.21. Definíció. *A véges G csoport H részcsoportja szerinti bal oldali mellékosztályai számát H (bal oldali)* **indexének** *nevezzűk. jelölése: $|G \colon H|$*

Megjegyzés. Ugyanúgy, ahogy a bal oldali mellékosztályokat definiáltuk definiálhatjuk a jobb oldali mellékosztályokat, és természetesen az indext is. Az állítások is érvényesek a jobb oldali mellékosztályokra is. Ezért az elövetkezőkben egyszerűen mellékoszályokról és indexről beszélünk.

9.23. Tétel. (Lagrange-tétele) *Tetszőleges G véges csoport és $H \leq G$ részcoportra $|G| = |H| \cdot |G \colon H|$. Másképpen mondva, véges csoport részcsoportjának rendje osztója a csoport rendjének.*

Bizonyítás. A tétel állítása abból adódik, hogy $|H| = |aH|$ bármely $a \in G$-re, ugyanis a $h \mapsto ah$ megfeleltetéssel definiált $H \to aH$ leképezés bijektív.

9.24. Következmény. *Legyen G egy n elemű csoport.*

(1) *Minden $a \in G$-re* $\mathrm{o}(a)|n$.
(2) *Minden $a \in G$-re* $a^n = 1$.
(3) *Minden $a \in G$-re* $a^{-1} = a^{n-1}$.
(4) *Ha n prímszám, akkor a G csoport ciklikus.*

9.25. Tétel. *A legföljebb 7 elemű csoportok izomorfia erejéig a következők:*

$$\{1\},\ \mathbb{Z}_k,\ (2 \leq k \leq 7),\ V,\ S_3.$$

10. Testbővítések.

A második fejezetben — az egyenletek megoldhatóságával (gyökképlet létezésével) kapcsolatban — utaltunk arra, hogy a több évszázados sikertelen próbálkozások után a XIX. század első harmadában a francia E. Galois egy teljesen új megközelítést vezetett be. A korábbi erőfeszítések „gyökképlet" keresésére fókuszáltak, amelyek csak akkor lehettek (volna) sikeresek, ha léteznek, de semmit sem adtak arra az esetre, ha nem is léteznek e keresett képletek/eljárások.

Galois új megközelítése abból állt, hogy kiindulva az egyenlet/polinom együtthatóit tartalmazó legszűkebb testből, azt „gyökmennyiségek", az elemekre alkalmazott egész kitevős gyökvonások eredményeivel bővítve olyan testet konstruáljon, amely már tartalmazza a gyököket, másképpen mondva olyan testet kívánt konstruálni ílymódon, amely fölött a polinom lineáris tényezők szorzatára bontható.

Ezen az úton az első lépés bizonyos testbővítések konstruálása. Most csak egy ilyennel foglalkozunk, a továbbhaladás egy másik kurzus feladata.

10.1. Definíció. *Azt mondjuk, hogy az L test a K test* **bővítése***, ha $K \subseteq L$. Ez esetben használni fogjuk a $L\colon K$ jelölést.*

10.1. Állítás. *Ha $L\colon K$, akkor L vektortér K fölött.*

10.2. Állítás. *Ha $(K_i)_{i\in I}$ az L test résztestei, akkor $\bigcap\limits_{i\in I} K_i$ test.*

10.2. Definíció. *Legyen $L\colon K$ testbővítés, és $\alpha \in L$. Az L test $K \cup \{\alpha\}$-t tartalmazó legszűkebb résztestét (e halmaz által generált résztestét) a K test α-val való* **egyszerű bővítésének** *nevezzük, és $K(\alpha)$-val jelöljük.*

Könnyen igazolható, hogy e test az L test összes $K\cup\{\alpha\}$-t tartalmazó résztestének metszete, azaz

$$K(\alpha) = \bigcap\{L' \subseteq L\colon K \subseteq L',\ \alpha \in L',\ L' \text{ test}\}.$$

Egyszerű számolással igazolható a következő tétel.

10.3. Tétel. *Legyen $L\colon K$ testbővítés és $\alpha \in L$. Ekkor*

$$K(\alpha) = \{f(\alpha)/g(\alpha)\colon f, g \in K[x],\ g(\alpha) \neq 0\}.$$

Bizonyítás. Jelölje a tételbeli egyenlőség jobb oldalán álló halmazt T. Rutin számolással kapjuk, hogy T test, és $\alpha \in T$. Ebből $K(\alpha)$ minimális volta alapján azonnal adódik, hogy $K(\alpha) \subseteq T$.

A fordított irányú tartalmazás igazolásához tekintsünk egy $f \in K[x]$ polinomot. Az $f(\alpha)$ elem α-ból és a K test elemeiből összeadással, kivonással és szorzással kapható, így $f(\alpha) \in K(\alpha)$. Lévén $K(\alpha)$ test, bármely további g K fölötti polinomra, ha $g(\alpha) \neq 0$, akkor $f(\alpha)/g(\alpha) \in K(\alpha)$, azaz $K(\alpha) \supseteq T$.

10.3. Definíció. *Legyen $L\colon K$ egy testbővítés. Azt mondjuk, hogy az $\alpha \in L$ elem* **algebrai K fölött***, ha van olyan $f \in K[x]$ nemkonstans polinom, hogy $f(\alpha) = 0$. Ellenkező esetnem α* **transzcendens K fölött.**

10.4. Definíció. *Azt mondjuk, hogy $\alpha \in \mathbb{C}$* **algebrai szám***, ha algebrai elem a $\mathbb{Q}$ test fölött. A többi komplex számot* **transzcendens számnak** *nevezzük.*

Megjegyzések.
(1) Először Euler fogalmazta meg azt a sejtést, hogy „bizonyos számok meghaladják sz algebrai módszerek erejét". Ezekre vezette be a transzcendens szám fogalmát. Úgy vélte, hogy az e, π konstansok, továbbá az exponenciális és a trigonometrikus függvények legtöbb értéke transzcendens. Bizonyítani azonban csak azt tudta, hogy az e irracionális szám. Egyik tanítványa, Lambert, ugyanezt mutatta meg a π-ről még a XVIII. században.
(2) Az első transzcendens számot Liouville konstruálta meg, és 1844-ben publikálta:

10.4. Tétel. *Az*

$$\alpha = \sum_{k=1}^{\infty} \frac{1}{10^{k!}} = 0,110001000000000000000001\ldots$$

szám transzcendens.

(3) Az 5. fejezetben még néhány tényt ismertettünk a transzcendens számokkal kapcsolatban.
Példák.
(1) A π, az e és a $2^{\sqrt{2}}$ számok transzcendensek.
(2) Nem ismeretes, hogy $\pi + e$ milyen szám, de a $\pi + ie$ komplex szám transzcendens volta egyszerűen kapható.
(3) Egy K test minden elemei algebrai K fölött.

10.5. Tétel. *Legyen $L\colon K$ testbővítés és $\alpha \in L$ algebrai K fölött. Pontosan egy olyan $f \in K[x]$ főpolinom létezik, amelyre $f(\alpha) = 0$ és ha valamely nemzéró $g \in K[x]$ polinomra $g(\alpha) = 0$, akkor $f|g$. Ezen f polinom irreducibilis K fölött.*

Bizonyítás. Azon K fölötti legalább elsőfokú polinomok J halmaza, amelyeknek α gyöke nem üres, így van közöttük minimális fokszámú főpolinom. Jelöljön egy ilyet f. Rutin számolással (maradékos osztás) kapható, hogy tetszőleges $g \in J$-re $f|g$, valamint az is hogy f irreducibilis.

10.5. Definíció. *Az előbbi tételbeli f polinomot az α elem* **minimálpolinomjának** *nevezzük. Azt mondjuk, hogy $L\colon K$* **egyszerű algebrai bővítés***, ha van olyan $\alpha \in L$ elem, hogy $K(\alpha) = L$.*

10.6. Állítás. *Legyen $L\colon K$ testbővítés, $\alpha \in L$ algebrai elem K fölött, minimálpolinomját jelölje m, $\deg m = n$. Tetszőleges $f \in K[x]$ polinomra $f(\alpha)$ fölírható, mint α legföljebb $n-1$-edfokú polinomja.*

Bizonyítás. Ha r jelöli az f és m-en végzett euklideszi osztás maradékát, akkor az $f(\alpha) = r(\alpha)$ egyenlőségből adódik állításunk.

Megvizsgáljuk, hogy $K(\alpha)$ minden eleme fölírható-e az e az előbbi módon. Ehhez azt nézzük meg, hogy egy $g(\alpha) \neq 0$ elem inverze írható-e, mint α legföljebb $n-1$-edfokú polinomja. Ha igen akkor van olyan $q \in K[x]$ polinom, hogy $1/g(\alpha) = q(\alpha)$, azaz $g(\alpha)q(\alpha)-1 = 0$. Ez pedig azt jelenti, hogy α gyöke a $gq-1$ K fölötti polinomnak. Mivel az α elem minimálpolinomja m, ezért alkalmas $p \in K[x]$ polinomra teljesülnie kellene a $gq - 1 = pm$ egyenlőségnek, vagyis $K[x]$-ben megoldható a

$$gq - mp = 1$$

egyenlet.

Tudjuk, hogy ez akkor teljesül, ha $\ln.\,k.\,o.(g, m) \sim 1$. Ha h jelöli a két polinom legnagyobb közös osztói közül a főpolinomot (ilyen pontosan egy van!), akkor $h|m$ Mivel m irreducibilis főpolinom, ezért $h = m$, vagy $h = 1$. Az első eset lehetetlen, mert abból $m|g$, azaz $g(\alpha) = 0$ következne, ami lehetetlen. Kaptuk tehát hogy g, m relatív prmek, az egyenlet megoldható, ezért $g(\alpha)$ inverze is írható az α legföljebb $n-1$-edfokú polinomja.

Így részben igazoltuk a következő tételt (a benne levő egyértelműségi kritériummal nam foglalkozunk, az érdeklődő olvasók könnyen igazolhatják).

10.7. Tétel. *Legyen $L\colon K$ testbővítés és $\alpha \in L$ egy algebrai elem, amelynek minimálpolinomja n-edfokú. Ekkor a $K(\alpha)$ test elemei fölírhatók*

$$\beta = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$$

alakban, ahol $a_0, \ldots, a_{n-1} \in K$. Ezen elemeket a β elem egyértelműen meghatározza.

10.8. Következmény. *Legyen $L\colon K$ testbővítés és $\alpha \in L$ egy algebrai elem, amelynek minimálpolinomja n-edfokú. Ekkor a $K(\alpha)$ n dimenziós vektortér a K test fölött.*

10.9. Tétel. *Legyen $L\colon K$ testbővítés és $\alpha \in L$ egy algebrai elem, amelynek f minimálpolinomja n-edfokú. Ekkor*

$$K(\alpha) \cong K[x]/(f).$$

Bizonyítás. Legyen $\beta \in K(\alpha)$ egy tetszőleges elem. Léteznek olyan egyértelműen meghatározott $a_0, \ldots, a_{n-1} \in K$ elemek, hogy $\beta = a_0 + a_1\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$. Jelölje g a következő K fölötti polinomot: $g(x) = a_{n-1}x^{n-1} + \ldots + a_1x + a_0$. Egyszerűen igazolható a korábbiak alapján, hogy a

$$\varphi\colon K(\alpha) \to K[x]/(f), \quad \beta \mapsto \overline{g} = g + (f)$$

leképezés a kívánt izomorfizmus.

10.10. Tétel. *Legyen F test és $f \in F[x]$ n-edfokú irreducibilis polnom. Ekkor a $K = F[x]/(f)$ faktorgyűrű olyan test, amelyben az f polinomnak van zéróhelye. A K test minden eleme fölírható $a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ alakban, ahol $a_{n-1}, \ldots, a_1, a_0 \in F$. E fölírás egyértelmű. Ha $F = \mathbb{Z}_p$, akkor $|K| = p^n$.*

10.11. Következmény. *Tetszőleges F test és $f \in F[x]$ irreducibilis polinom estén létezik olyan K test, hogy*

(1) *$K \supseteq F$, azaz K* **bővítése** *F-nek;*
(2) *létezik olyan $\alpha \in K$ elem, amely gyöke f-nek;*
(3) *K minden eleme egyértelműen előáll $a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0$ alakban, ahol $n = \deg f$ és $a_0, a_1, \ldots, a_{n-1} \in F$.*

10.6. Definíció. *Azt mondjuk, hogy az előbbi Következményben leírt K test az F testből az α elem adjungálásával keletkezik — jelölése $K = F(\alpha)$ —, és az ilyen módon előálló testeket F* **egyszerű algebrai bővítéseinek** *nevezzük.*

10.12. Következmény. *Az előbbi jelölésekkel, $K[x]/(f) = K(\overline{x})$, ahol $\overline{x} = x + (f)$.*

Megjegyzés. Ha $F = \mathbb{R}$ és $f = x^2 + 1$, akkor az $\mathbb{R}[x]/(x^2 + 1)$ faktortest megfeleltethető a komplex számok testének.

10.13. Tétel. *Minden véges test elemszáma prímhatvány, és tetszőleges p prímszám és $n \in \mathbb{N}$ esetén létezik p^n elemű test.*