MBL212E Klasszikus algebra

(előadás vázlat)
2016-17. 2. 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 é az 1.
3. Egyszerű számolással kaphatók a következők:

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

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. 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 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.

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

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

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.

1.3. 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.

1.4. 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

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

komplex számok. Ezek a számsíkon az egységkörön helyezkednek el, 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.

1.5. 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* $\ln.\,\mathrm{k.\,o.}(n, k) = 1$.

1.6. 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).*

1.7. 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.*

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

2. Az absztrakt algebra néhány alapvető fogalma

2.1. Definíció. *Legyen A nemüres halmaz. Az $f\colon A^2 \to A$ leképezéseket* **kétváltozós műveleteknek**, *pontosabban A-n definiált kétváltozós műveleteknek nevezzük. Ha $a, b \in A$ és $f(a, b) = c$, akkor helyette általában $a \cdot b = c$-t, vagy röviden $ab = c$-t írunk, és azt mondjuk, hogy az a és a b elemek szorzata c. Az (A, f), ill. az $(A, \cdot)$ rendezett párt* **grupoidnak** *nevezzük. E grupoid* **véges**, *ha A véges halmaz.*

Megjegyzések.
(1) Általában a műveleti jel-szerű, tehát a másodiknak említett jelölésmódot fogjuk használni.
(2) Amennyiben valamely adott A halmazon több kétváltozós műveletet kell megadnunk, akkor a $+, \circ, *$ jelek valamelyikét alkalmazzuk a további műveletekre.

2.2. Definíció. *Legyen $(A, \circ)$ grupoid. Azt mondjuk, hogy a*

- $\circ$ *művelet* **asszociatív**, *ha bármely $a, b, c \in A$ elemre $(a \circ b) \circ c = a \circ (b \circ c)$;*
- $\circ$ *művelet* **kommutatív**, *ha bármely $a, b \in A$ elemre $a \circ b = b \circ a$.*
- $\circ$ *művelet* **invertálható**, *ha minden $a, b \in A$-ra az $a \circ x = b$ és $y \circ a = b$ egyenletek megoldhatók, azaz létezik olyan $c, d \in A$, hogy*

$$a \circ c = b \qquad \text{és} \qquad d \circ a = b$$

.

- $\circ$ *művelet* **egyszerűsítéses**, *vagy másképpen mondva* **kancelatív**, *ha az előbbi pontbeli egyenleteknek legföljebb 1-1 megoldása van.*
- *Az $e \in A$ elem* **egységelem** *ha bármely $a \in A$-ra $a \circ e = e \circ a = a$, ilyenkor azt (is) mondjuk, hogy a grupoid* **egységelemes**. *Az olyan $o \in A$ elemet, amelyre minden $a \in A$ esetén fönnállnak az $a \circ o = o$, $o \circ a = o$ egyenlőségek, e grupoid* **zéróelemének** *nevezzük.*

Az $(A, \circ)$ véges grupoidot az alábbi művelettáblázatal, az ún. **Cayley-táblával** is megadhatjuk, ahol a két bemeneten az A halmaz elemeit soroljuk föl:

$\circ$	$\cdots$	b	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$
a	$\cdots$	$a \circ b$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Vegyük észre, hogy az imént definiált műveleti tulajdonságok — az asszociativitás kivételével — egyszerűen láthatók a művelettáblán. Valóban, a művelet kommutatív volta azt jelenti, hogy a tábla szimmetrikus a főátlójára. Továbbá, a művelet invertálható, ha a művelettábla

minden sorában és minden oszlopában valamennyi elem előfordul legalább egyszer, míg pontosan akkor egyszerűsítéses, ha minden elem minden sorban ill. oszlopban legföljebb egyszer fordul elő.

2.1. Állítás. *Egy grupoidban legföljebb egy egységelem, ill. egy zéróelem lehet.*

Megjegyzések.
1. Amennyiben félreértést nem okoz, az egységelemet 1-gyel, míg a zéróelemet 0-val fogjuk jelölni, továbbá az $(A, \circ)$ grupoidot egyszerűen A-val jelöljük, és $a \circ b$ helyett ab-t írunk. Ezt **multiplikatív írásmódnak** nevezzük.
2. Abban a speciális esetben, ha a műveletet $+$-szal jelöljük, az egységelemet 0 fogja jelölni. Ebben az esetben azt mondjuk, hogy **additív írásmódot** használunk.

2.2. Állítás. *Ha valamely véges grupoid művelete invertálható, akkor egyszerűsítéses is, és megfordítva amennyiben egyszerűsítéses, akkor invertálható.*

2.3. Definíció. *Legyen A egységelemes grupoid. Az $a \in A$ elem* **invertálható/létezik inverze**, *ha van olyan $a' \in A$, hogy $aa' = a'a = 1$. Azt mondjuk, hogy az a' elem a-nak egy* **inverze**.

2.4. Definíció. *Az asszociatív műveletű grupoidot* **félcsoportnak**, *az egységelemez félcsoportot* **monoidnak nevezzük**.

2.3. Tétel. *Monoidban bármely elemnek legföljebb egy inverze lehet. Ha $a, b \in A$ az A monoid invertálható elemei, akkor ab is invertálható.*

Bizonyítás. Legyen A monoid, továbbá $a, a', a'' \in A$ olyanok, hogy $aa' = a'a = aa'' = a''a = 1$. Ekkor

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

Az állítás további része ezek után egyszerűen kapható.
Jelölés. Monoidban egy a elem inverzét a^{-1} fogja jelölni, ha a műveletet szorzásként írjuk, míg ha összeadásként, akkor $-a$. Használni fogjuk az $a + (-b) = a - b$ írásmódot is.

2.4. Következmény. *Ha az $a, b \in A$ elemek az A monoid invertálható elemei, akkor $(ab)^{-1} = b^{-1}a^{-1}$.*

2.5. Definíció. *Ha egy monoidban minden elemnek van inverze, akkor* **csoportnak** *nevezzük, a kommutatív műveletű csoportot pedig* **Abel-csoportnak**.

Példák.
(1) Legyen A tetszőleges nemüres halmaz, és jelölje S_A az A halmaz összes önmagára való bijektív leképezései (permutációi) halmazát. E halmaz a leképezésszorzással csoport: az **A-fölötti szimmetrikus csoport**.

(2) A szabályos n szög szimmetriái (önmagára való egybevágósági transzformációi: forgatások és tengelyes tükrözések) D_n halmaza a leképezésszorzással ugyancsak csoport, az **n-edfokú diédercsoport**.
(3) Abel-csoportok: $(\mathbb{Z}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathcal{P}(A), \triangle)$, $(\mathbb{Z}/n, +)$, $(R_n, \cdot)$ (a modulo n maradékosztályok additív csoportja, ill. a modulo n relatív prím maradékosztályok multiplikatív csoportja)
(4) Tetszőleges $n \in \mathbb{N}$-re az $\mathbb{R}$ fölötti összes $n \times n$ típusú invertálható mátrixok a mátrixszorzással, mint művelettel csoportot alkotnak. E csoportot $\mathrm{GL}(n, \mathbb{R})$-fel szokás jelölni, s elnevezése: $\mathbb{R}$ **fölötti n-edrendű általános lineáris csoport.** Az 1 determinánsú $n \times n$ típusú $\mathbb{R}$ fölötti mátrixok szintén csoportot alkotnak $\mathrm{SL}(n, \mathbb{R})$ jelöli, amelyet $\mathbb{R}$ **fölötti n-edrendű speciális lineáris csoportnak.** szokás nevezni.

2.6. 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.
$(\mathbb{Z}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$, $(\mathbb{C}; +, \cdot)$, $(\mathbb{R}^{n \times n}; +, \cdot)$, $(\mathbb{Z}_n; +, \cdot)$, $(n \in \mathbb{N})$,
$(\mathcal{P}(U); \triangle, \cap)$.

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

Jelölés. Tetszőleges gyűrűben 0 jelöli majd az additív egységelemet, $-a$ az a elem additív inverzét, továbbá 1 a multiplikatív egységelemet (ha van).
Megjegyzés. Használni fogjuk az $a - b = a + (-b)$ írásmódot.

2.7. Definíció. *Legyen R egységelemes gyűrű. Azt mondjuk hogy az $a \in R$* **invertálható**, *ha van olyan $a' \in R$ elem, hogy $aa' = a'a = 1$. Az R gyűrű invertálható elemei halmazát R^* fogja jelölni.*

2.6. Állítás. *Tetszőleges egységelemes R gyűrű invertálható elemei R^* halmaza csoportot alkot a szorzással.*

2.8. Definíció. *Az előbbi R^* csoportot az R gyűrű* **egységcsoportjának** *nevezzük.*

2.9. 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 jóbboldali zérusosztót, azaz bármely $a, b \in R \setminus \{0\}$ elemekre $ab \neq 0$. Kommutatív gyűrű esetén nyilván egyszerűen zérusosztót mondhatunk.*

2.10. Definíció. *Az egységelemes, kommutatív, zérusosztómentes gyűrűt* **integritástartománynak** *nevezzük.*

2.7. Állítás. *Integrtástartományban lehet nemzéró elemel egyszerűsíteni, azaz tetszőleges a, b, c $(c \neq 0)$ elemekre*

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

2.11. Definíció. *Legyen $(T; +, \cdot)$ integritástartomány, és $T^* = T \setminus \{0\}$. Ha T legalább kételemű és $(T^*, \cdot)$ csoport, akkor azt mondjuk, hogy T* **test**.

Példák.
A $(\mathbb{Q}; +, \cdot)$, $(\mathbb{R}; +, \cdot)$, $(\mathbb{C}; +, \cdot)$ algebrák testek.

2.12. Definíció. *Legyen R gyűrű és $S \subseteq R$. Ha S az R-ből „örökölt" műveletekkel gyűrű, akkor azt mondjuk, hogy S* **részgyűrűje** *R-nek. Analóg módon definiálható test, csoport, monoid, félcsoport, grupoid részteste, részcsoportja, részmonoidja, részfélcsoportja, ill. részgrupoidja.*

2.13. Definíció. *Legyenek $(A; +)$ és $(B; \cdot)$ két grupoid, továbbá $\varphi\colon A \to B$ egy leképezés. Azt mondjuk, hogy a φ* **leképezés megőrzi a $+$ műveletet**, *ha tetszőleges $a_1, a_2 \in A$ elemekre $(a_1 + a_2)\varphi = a_1\varphi \cdot a_2\varphi$. A műveletőrző leképezéseket* **homomorfizmusnak**, *a bijektív homorfizmusokat* **izomorfizmusnak** *nevezzük. Ha az A, B algebrák között létezik izomorfizmus, akkor azt mondjuk, hogy eten algebrák* **izomorfak**, *jelölése: $A \cong B$.*

Megjegyzés. Gyűrűk, testek esetén analóg módon definiálható a homomorfizmus (izomorfizmus) fogalma: a műveletőrzést minden egyes műveletre megköveteljük.

Egyszerűen igazolható a következő tétel.

2.8. Tétel. *Félcsoport, monoid, csoport, gyűrű homomorf képe félcsoport, monoid, csoport, gyűrű.*

Ekvivalenciák és osztályozások, maradékosztálygyűrűk

2.14. Definíció. *Legyen A nemüres halmaz és $\varrho \in A \times A$. Azt mondjuk, hogy ϱ* **ekvivalencia reláció** *röviden* **ekvivalencia** *az A halmazon, ha reflexív, szimmetrikus és tranzitív reláció.*

2.15. Definíció. *Legyen ϱ egy ekvivalencia reláció az A halmazon és $a \in A$. A $\{b \in A\colon a \varrho b\}$ halmazt az a* **elem ϱ szerinti (ekvivalencia)osztályának**, *az összes ϱ-szerinti ekvivalenciaosztályok halmazát pedig az A halmaz ϱ* **szerinti faktorhalmazának** *nevezzük.*

Jelölés. Valamely a elem ϱ szerinti osztályát $[a]\varrho$-val, vagy ha nem okoz félreértést, egyszerűen $\overline{a}$-val jelöljük. A faktorhalmazt pedig A/ϱ jelöli, azaz $A/\varrho = \{\overline{a}\colon a \in A\}$.

2.16. Definíció. *Legyen A nemüres halmaz, és $\mathcal{C} \subseteq \mathcal{P}(A)$. Azt mondjuk, hogy $\mathcal{C}$ az A halmaz egy* **osztályozása***, ha*

(1) $\forall X \in \mathcal{C}\colon X \neq \emptyset$,
(2) $\forall X \neq Y \in \mathcal{C}\colon X \cap Y = \emptyset$,
(3) $\cup_{X\in\mathcal{C}} X = A$.

2.9. Tétel. *Legyen A nemüres halmaz. Ha ϱ ekvivalenciareláció A-n, akkor A/ϱ egy osztályozás A-n. Ha pedig $\mathcal{C} \subseteq \mathcal{P}(A)$ egy osztályozás, akkor az $a\varrho b \Leftrightarrow \exists C \in \mathcal{C}\colon a, b \in C$ formulával definiált ϱ reláció ekvivalencia az A halmazon. Az imént megadott „ekvivalencia $\mapsto$ osztályozás”, és az „osztályozás $\mapsto$ ekvivalencia” megfeleltetések egymás inverzei.*

Jelölés. Legyen $m > 2$ és $\varrho \in \mathbb{Z} \times \mathbb{Z}$ a modulo m kongruencia, azaz $a\varrho b \iff a \equiv b \pmod m$. Tudjuk, hogy ezen ϱ ekvivalencia $\mathbb{Z}$-n, és az $a \in \mathbb{Z}$ osztályát jelölje $\overline{a}$, azaz $\overline{a} = \{b \in \mathbb{Z}\colon a \equiv b \pmod m\}$. Az $\overline{a}$ osztályra használni fogjuk a (modulo m) **maradékosztály** elnevezést. A megfelelő faktorhalmazt azonban az ilyen esetekben nem $\mathbb{Z}/\varrho$, hanem $\mathbb{Z}_m$ fogja jelölni. Nyilván $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$

2.10. Tétel. *Legyen $m \geq 2$ egész és definiáljuk $\mathbb{Z}_m$-en a következő két műveletet:*

$$\overline{a} + \overline{b} = \overline{a + b}$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

E két művelet jól definiált, azaz az eredmény nem függ attól, hogy az adott osztályok mely eleneivel végeztük el azoka. A $(\mathbb{Z}_m; +, \cdot)$ algebra egységelemes kommutatív gyűrű.

2.17. Definíció. *Az imént kapott $\mathbb{Z}_m$ gyűrűt* **modulo m maradékosztálygyűrűnek** *nevezzük.*

2.11. Tétel. *Egy $\mathbb{Z}_m$ maradékosztály pontosan akkor test, ha m prímszám. Ha m összetett szám, akkor a $\mathbb{Z}_m$ gyűrű tartalmaz zérusosztót*

3. Egyhatározatlanos polinomok

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

3.1. 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.*

3.2. 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: $(f)_n = a_n$.*

3.3. 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 $\deg = 1, -\infty$, 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**.

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

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

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

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

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

3.2. Tétel. *A 3.4. Definícióbeli műveletekkel $R[x]$ integritástartomány.*

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

3.3. 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.

3.4. 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 $F^* = F \setminus \{0\}$.

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

3.7. Definíció. *Azt mondjuk, hogy az $f, g \in F[x]$ polinomok* **asszociáltak***, ha $f|g$ és $g|f$. Jelölése: $f \sim g$.*

3.5. Tétel. *Tetszőleges $f, g \in F[x]$ polinomokra*

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

3.6. 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) $f|g \ \Leftrightarrow \ fh|gh, \text{ ha } h \neq 0$;

Megjegyzés. Az előbbi tételbeli (1) és (2) állítások azt jelentik, hogy az oszthatóság reflexív és tranzitív reláció test fölötti polinomgyűrűkben.

3.7. Tétel. *Legyen F test. Az asszociáltság ekvivalenciareláció $F[x]$-en. Két polinom pontosan akkor asszociált, ha egymástól csak egy nemzéró konstans (F^*-beli elem) faktorban különböznek. A nulla osztályt kivéve minden asszociáltsági osztály tartalmaz főpolinomot, mégpedig pontosan egyet.*

3.8. Definíció. *Legyenek $f, g \in F[x]$ tetszőleges polinomok. Azt mondjuk, hogy a $h \in F[x]$ polinom az f és g polinomok egy* **legnagyobb közös osztója***, ha*

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

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

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

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

Jelölés. A legnagyobb közös osztóra és a legkisebb közös többszörösre használni fogjuk az $\text{ln. k. o.}(f,g)$, ill. $\text{lk. k. t.}(f,g)$ jelöléseket.

3.9. 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. Tekintsük az $f - gh,\ h \in F[x]$ polinomokat. Ha szerepel közöttük a zérópolinom, akkor az első állítást már igazoltuk is, így föltehető, hogy egyik ilyen polinom sem zéró. Legyen $q \in F[x]$ egy olyan polinom, amelyre az $f - gq = r$ polinom fokszáma minimális.

Ha $\deg r \geq \deg g$, akkor az $f - gq$ polinomból az $u_t b_m^{-1} x^t g \in F[x]$ polinomot levonva — ahol u_t, b_m rendre az r, g polinomok főegyüttható — egy olyan $f - gq'$ polinomot kapunk, amelynek fokszáma kisebb r fokszámánál, ami ellentmond a q választásának.

Az egyértelműség igazolása egyszerű rutinfeladat.

3.10. Tétel. *Bármely két $f, g \in F[x]$ 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* $\text{ln. k. o.}(f,g) = fu + gv$.

Bizonyítás. Az f, g polinomokon maradékos osztások sorozatát végezzük a következőképp:

$$\begin{aligned} f &= gq_1 + r_1 \\ g &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \end{aligned}$$

Tudjuk, hogy $\deg g > \deg r_1 > \deg r_2 > \ldots$, így az osztás sorozat véges sok lépés után végetér. Ez csak úgy következhet be, hogy lesz olyan r_{k+1} maradék, amely zéró. Egyszerű számolással kapható (ugyanúgy, mint az elemi számelméletben), hogy $\text{ln. k. o.}(f,g) \sim r_k$, azaz egy legnagyobb közös osztó az utolsó nemzéró maradék.

A kívánt előállítás — hasonlóan az egész számokra megismerthez — az osztás sorozaton visszafelé haladva — kapható meg.

Nyilvánvaló, hogy tetszőleges f, g polinomokra, ha legalább az egyik nemzéró, akkor egy legkisebb közös többszörösük: $fg/\operatorname{ln.k.o.}(f,g)$. Továbbá, $\operatorname{lk.k.t.}(0,0) = 0$.

3.9. Definíció. *Az iménti bizonyításban szereplő osztás sorozatot* **Euklideszi algoritmusnak** *fogjuk nevezni.*

3.11. Tétel. *Legyenek $f, g, h \in F[x]$ tetszőleges polinomok.*

(1) $\operatorname{ln.k.o.}(\operatorname{ln.k.o.}(f,g),h) \sim \operatorname{ln.k.o.}(f,\operatorname{ln.k.o.}(g,h))$,
(2) $\operatorname{ln.k.o.}(f,g) \sim \operatorname{ln.k.o.}(g,h)$,
(3) $\operatorname{ln.k.o.}(f,f) \sim f \sim \operatorname{ln.k.o.}(f,0)$,
(4) $\operatorname{ln.k.o.}(f,g) \sim f \;\Leftrightarrow\; f|g$,
(5) $(\operatorname{ln.k.o.}(f,g))h \sim \operatorname{ln.k.o.}(fh,gh)$.
(6) *Ha* $d \sim \operatorname{ln.k.o.}(f,g)$ *és* $d \neq 0$, *továbbá* $f = f'd$, $g = g'd$, *akkor* $\operatorname{ln.k.o.}(f',g') \sim 1$.
(7) *Ha* $\operatorname{ln.k.o.}(f,g) \sim 1$, *akkor* $\operatorname{ln.k.o.}(f,gh) \sim \operatorname{ln.k.o.}(f,h)$.

Megjegyzés. Az előbbi tétel bizonyítása a legnagyobb közös osztó definíciója alapján egyszerűen elvégezhető.

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

3.12. Állítás. *Legyenek az $f, g \in F[x]$ polinomok relatív prímek. Ha valamely $h \in F[x]$ polinomra $f|h$ és $g|h$, akkor $fg|h$.*

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

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

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

azaz a két hányados relatív prím;

(2) *ha f és g relatív prím, akkor*

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

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

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

3.14. 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* $\operatorname{ln.k.o.}(f,g)|h$. *Ha (u_0, v_0) egy megoldás, akkor tetszőleges $t \in F[x]$-re*

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

is megoldás, és minden megoldás ilyen alakban írható.

3.11. 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 $m|f-g$*

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

3.16. 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 $hf \equiv hg \pmod{m} \Leftrightarrow f \equiv g \pmod{m}$.*

3.12. 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 $F[x]/(m) = \{\overline{f} \colon f \in F[x]\}$.*

Megjegyzés. Az elemi számelméletbeli ismereteink alapján: $\overline{f} = \{f + gm \colon g \in F[x]\}$.

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

3.18. Tétel. *Legyen F test és $m \in F[x]$ legalább elsőfokú polinom. Az $F[x]/(m)$ faktorhalmaz az $\overline{f} + \overline{g} = \overline{f+g}$, $\overline{f} \cdot \overline{g} = \overline{fg}$ műveletekkel egységelemes kommutatív gyűrű.*

3.13. Definíció. *Az előző tételbeli $F[x]/(m)$ gyűrűt — és a hozzá hasonlóan konstruáltakat —* **maradékosztálygyűrűnek** *nevezzük.*

3.19. Tétel. *Egy $F[x]/(m)$ maradékosztálygyűrű pontosan akkor test, ha az m polinom ireducibilis F fölött.*

Irreducibilis polinomok, irreducibilis faktorizáció test fölötti polinomgyűrűben

3.14. Definíció. *Legyenek $p, q \in F[x]$ legalább elsőfokú polinomok. Azt mondjuk, hogy a q polinom* **irreducibilis az F test fölött**, *ha nem bontható föl $\deg q$-nál alacsonyabb fokú polinomok szorzatára, azaz valahányszor $q = fg$ valamely $f, g \in F[x]$ polinomokra, mindannyiszor*

$f \sim q$ és $g \in F$, vagy $f \in F$ és $q \sim g$. A p polinom **prím**, *ha valahányszor $p|fg$ valamely $f, g \in F[x]$ polinomokra, mindannyiszor $p|f$ vagy $p|g$.*

3.20. Állítás. *Test fölötti polinomgyűrűben a prím polinomok irreducibilisek.*

Bizonyítás. Legyen $p, f, g \in F[x]$, és $p|fg$. p prím volta maga után vonja, hogy $p|f$, vagy $p|g$. Ha $p|f$, akkor egyrészt

$$\deg p = \deg f + \deg g \quad \Rightarrow \quad \deg p \leq \deg f,$$

másrészt $\deg p \leq \deg f$, és így $\deg p = \deg f$, azaz $\deg g = 0$. Mivel a $p|g$ eset hasonlóan tárgyalható, az állítást igazoltuk.

3.21. Állítás. *Test fölötti polinomgyűrűben az irreducibilis polinomok prímek.*

Bizonyítás. Legyen q irreducibilis polinom és valamely $f, g \in F[x]$ polinomokra $q|fg$. Ha $q|f$ készen vagyunk, míg ha $q \nmid f$, akkor $\ln.\,k.\,o.(q, f) \sim 1$. Így léteznek olyan $u, v \in F[x]$ polinomok, hogy $qu + fv = 1$. Ekkor $qug + fgv = g$, amiből már adódik állításunk.

3.22. Következmény. *Ha $q \in F[x]$ irreducibilis és valamely $f_1, \ldots, f_k \in F[x]$ polinomokra $q|f_1 \ldots f_k$, akkor van olyan $1 \leq i \leq k$, hogy $q|f_i$.*

3.23. Tétel. *Test fölötti polinomgyűrűben minden legalább elsőfokú polinom fölbontható irreducibilis polinomok szorzatára. E fölbontés a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű. Ez utóbbi állítás azt jelenti, hogy ha valamely $f \in F[x]$ polinomra $f = q_1 \ldots q_k = q'_1 \ldots q'_m$, ahol a q_i, q'_j-k irreducibilis F fölötti polinomok, akkor egyrészt $k = m$, másrészt minden $1 \leq i \leq k$-hoz van olyan $1 \leq j \leq m$, hogy $q_i \sim q'_j$.*

Bizonyítás. E tétel azt állítja, hogy test fölötti polinomgyűrűkben érvényes a számelmélet alaptételének megfelelő általánosítása. A bizonyítás is lényegében ugyanúgy végezhető el, mit e klasszikus tételé.

Megjegyzés. Az irreducibilis- ill. a prím elem fogalma tetszőleges integritástartományban is definiálható, amit később meg is teszünk. Ezen általánosabb kontextusban könnyen kapható, hogy a prímelemek irreducibilisek, de nem minden irreducibilis elem prím. A legegyszerűbb példák a $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \colon a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ integritástartományban adhatók meg. Ezzel később még foglalkozni fogunk.

4. Polinom gyökei, gyöktényezős alak, irreducibilitás $\mathbb{C}$, $\mathbb{R}$ és $\mathbb{Q}$ fölött

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

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

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

Bizonyítás. f-en és $x - a$-n végzett maradékos osztásból azonnal kapható az állítás.

4.2. Következmény. *Ha $a_1, \ldots, a_k \in F$ páronként különböző elemek és $f \in F[x]$, akkor*

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

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

4.2. 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.

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

4.5. 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.

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

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

4.8. 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.

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

4.10. Tétel. *Legyen $f \in \mathbb{R}[x]$ nemkonstans polinom, és $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy gyöke, azaz $f(\alpha) = 0$. Ekkor $f(\overline{\alpha}) = 0$ is teljesül, továbbá az α és $\overline{\alpha}$ gyökök multiplicitása megegyezik.*

Bizonyítás. Legyen $f = \sum_{i=0}^{n} a_k x^k$. Ekkor

$$f(\overline{\alpha}) = \sum_{i=0}^{n} a_k \overline{\alpha}^k = \sum_{i=0}^{n} \overline{a_k} \cdot \overline{\alpha^k} = \sum_{i=0}^{n} \overline{a_k \alpha^k} = \overline{\sum_{i=0}^{n} a_k \alpha^k} = \overline{f(\alpha)} = \overline{0} = 0.$$

A multiplicitásra vonatkozó állítás ezután triviális.

4.11. 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:*

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

4.12. Következmény. *Minden páratlan fokszámú valós együtthatós polinomnak van valós gyöke.*

Bizonyítás. Az állítás azonnal adódik abból, hogy a valós együtthatós polinomok folytonos függvények, és a páratlan fokszámúak pozitív és negatív értékeket is fölvesznek. A Bolzano-Darboux tétel alapján a 0 értéket is föl kell vennie.

Egy kombinatorikus bizonyítás is adható, hiszen a nem valós komplex gyökök konjugált párokban fordulnak elő.

4.13. Állítás. *Legyen F_1 részteste F-nek, és $f \in F_1[x]$. Ha f irreducibilis F fölött, akkor irreducibilis F_1 fölött is.*

4.14. 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.*

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

Bizonyítás. Az állítás egyszerűen kapható a 4.8. Következmény alapján.

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:

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

Irreducibilis polinomok $\mathbb{Z}$ és $\mathbb{Q}$ fölött

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

4.15. 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.

4.16. Állítás. *Ha $p \in \mathbb{Z}$ prímszám, akkor p a $\mathbb{Z}[x]$ gyűrűben mint konstans polinom is prímtulajdonságú.*

Bizonyítás. Legyen p prímszám és $f, g \in \mathbb{Z}[x]$ olyanok, hogy $p|fg$. Számoljunk most a $\mathbb{Z}_p[x]$ polinomgyűrűben. Tudjuk, hogy $\overline{fg} = \overline{f} \cdot \overline{g}$. Mivel $p|fg$, $\overline{fg} = \overline{0}$, azaz $\overline{f} \cdot \overline{g} = \overline{0}$. A $\mathbb{Z}_p[x]$ polinomgyűrű zérusosztómentes, így $\overline{f} = \overline{0}$, vagy $\overline{g} = \overline{0}$, ami azt jelenti, hogy $p|f$, vagy $p|g$.

4.17. Következmény. (Gauss lemma) *Primitív polinomok szorzata primitív polinom.*

Bizonyítás. Legyen $f, g \in \mathbb{Z}[x]$ két primitív polinom. Ha ± 1-en kívül lenne osztója fg-nek, akkor lenne egy p prímosztója is, de ekkor $p|f$, vagy $p|g$.

4.18. 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 $f \in \mathbb{Z}[x]$, $\deg f = n \ge 1$, 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* $0 < \deg g, \deg h < n$.

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

4.19. Tétel. (Schönemann-Eisenstein-féle irreducibilitási kritérium) *Legyen* $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *nemkonstans polinom. Ha létezik olyan* p *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. Tegyük föl, hogy az f polinomra és a p prímszámra teljesülnek a tételbeli föltételek, mégis léteznek olyan $\mathbb{Q}$ fölötti g, h polinomok, hogy $f = gh$. A 4.18. Tétel alapján föltehető, hogy $g, h \in \mathbb{Z}[x]$.

Tekintsük az f, g, h polinomokat, mint a $\mathbb{Z}_p$ test fölötti polinomokat. Ekkor $\overline{f} = \overline{a_n}x^n$, ahol $\overline{a_n} \neq 0$. Egyszerűen kapható, hogy ekkor $\overline{g}(x) = ux^k$ és $\overline{h}(x) = vx^l$ alkalmas $u, v \in \mathbb{Z}_p$-re. Mivel $\mathbb{Z}_p$ zérusosztómentes, $k + l = n$, és $k \leq \deg g$, $l \leq \deg h$. Másrészt $n = k + l$, ahol egyik összeadandó sem zérus, így mindkettő kisebb n-nél. Egyikük sem zéró $\mathbb{Z}_p[x]$-ben, ezért a konstans tagok a $\overline{g}, \overline{h}$ polinomokban zérók, azaz oszthatók p-vel. E két tag szorzata azonban megegyezik f konstans tagjával, így az szükségképp osztható p^2-tel, ami ellentmondás.

Megjegyzések.

1. Az előbbi tétel megfordítása nem igaz! Abból, hogy nem létezik a tételbeli föltételnek megfelelő prímszám, nem következik a polinom reducibilitása. A legegyszerűbb példa az $x + 1$ polinom.
2. A tétel — bár egész együtthatós polinomokról szól — alkalmazható racionális együtthatós polinomokra is: be kell szorozni a polinomot a nevezők legkisebb közös többszörösével (vagy egyszerűen a nevezőkkel).

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

4.21. Tétel. (fordított Schönemann-Eisenstein-féle irreducibilitási kritérium)
Legyen $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ *legalább elsőfokú polinom. Ha létezik olyan* p *prímszám, hogy* $p||a_n, p|a_{n-1}, \ldots, p|a_1, p \nmid a_0$, *akkor* f *irreducibilis a racionális számok teste fölött.*

4.22. 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.

4.23. 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* $p + q|f(-1)$.

Megjegyzés. A Schönemann-Eisenstein tételnek egy elemi bizonyítása, valamint a Rolle-tételnek és következményének igazolása megtalálható pl. Szendrei Ágnes Diszkrét matematika c. könyvének IX. fejezetében.

5. Polinomok többszörös gyökei

5.1. 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* $na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + 2a_2 x + a_1 \in \mathbb{C}[x]$ *polinomot értjük.*

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

5.1. 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) $(f^k)' = kf^{k-1}f'$.

5.2. 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.)*

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

5.3. 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* $f^{(k)}(\alpha) \neq 0$.

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

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

5.2. Definíció. *A komplex számok testének résztesteit* **számtesteknek** *nevezzük.*

5.6. 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.

6. Harmad- és negyedfokú egyenletek megoldása

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.

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. 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.

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. Az ötlet egyszerű, az egyenlet bal oldalát két másodfokú polinom szorzatára kell bontani. Ezt pedig úgy érhetjük el, ha előbb két, legföljebb másodfokú, polinom négyzetének különbségeként írjuk.

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

A következő tételként — az olvasó kényelmére — megismételjük a 4.7. Tételt (a klasszikus algebra alaptételét), mert annak egy következménye alapján azonban csak négy — nem föltétlenül különböző — megoldást kapunk.

6.1. 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.*

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

A harmad- és negyedfokú egyenletek megoldóképlete (megoldási eljárása) megtalálása után több, mint 200 évig kiváló matematikusok hada kereste a négynél magasabbfokú egyenlete megoldóképletét, megoldási eljárását. 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 van komplex zéróhelye. Ugyanis csak 1799-ben igazolta (először) Gauss a 4.7. Tételt.

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.

7. Polinomfüggvények, interpoláció.

7.1. 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.

A korábban igazolt Bezout tétel alapján könnyen adódik a következő tétel.

7.1. Tétel. *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 tétel. Például, a $\mathbb{Z}_{12}$ gyűrű fölötti $x^2 - \overline{1}$ polinomnak 4 gyöke is van az alapgyűrűben.

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

7.3. 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.

7.4. Tétel. *(Lagrange-interpoláció) Tetsőleges, 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.*

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

Bizonyítás. Konstruáljuk meg a következő polinomokat minden $1 \leq i \leq n+1$-re

$$\Phi_i(x) = \frac{\prod\limits_{j=1,\ i\neq j}^{n+1} (x - c_j)}{\prod\limits_{j=1,\ i\neq j}^{n+1} (c_i - c_j)}$$

Világos, hogy e polinomok legföjebb n-edfokúak, és $\Phi_i(c_i) = 1$, továbbá minden $k \neq i$-re $\Phi(c_k) = 0$. Így az

$$f(x) = \sum_{i=1}^{n+1} d_i \Phi_i(x)$$

polinom rendelkezik a kívánt tulajdonságokkal.

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:

$$\begin{aligned} \Psi_1 &= (x-1)(x-2)(x-3) & \Psi_1(0) &= -6 \\ \Psi_2 &= x(x-2)(x-3) & \Psi_2(1) &= 2 \\ \Psi_3 &= x(x-1)(x-3) & \Psi_3(2) &= -2 \\ \Psi_4 &= x(x-1)(x-2) & \Psi_4(3) &= 6 \end{aligned}$$

(2) Világos, hogy $\Phi_i(x) = \Psi_i(x)/\Psi_i(c_i)$.

(3)

$$\begin{aligned} f &= 1 \cdot \frac{\Psi_1}{-6} + 2 \cdot \frac{\Psi_2}{2} + 4 \cdot \frac{\Psi_3}{-2} + 8 \cdot \frac{\Psi_4}{6} \\ &= \mathbf{\frac{1}{6}x^3 + \frac{5}{6}x + 1} \end{aligned}$$

8. Többhatározatlanú polinomok

8.1. Definíció. *Legyen F test, továbbá $x_1, \dots, x_n$ határozatlanok (olyan szimbólumok, amelyen nincsenek az F testben.) Az $F[x_1, \dots, x_n] = (F[x_1, \dots, x_{n-1}])[x_n]$ halmaz elemeit F* **fölötti n határozatlanos polinomoknak** *nevezzük.*

8.1. Tétel. *Az imént definiált $F[x_1, \dots, x_n]$ halmaz a szokásos polinom-műveletekkel integritástartomány.*

Megjegyzés. Az oszthatóság és az asszociáltság fogalma a szokásos módon definiálható, és érvényben maradnak a 3.6. és 3.7. Tételek is.

Egy alternatív definíció a következő.

8.2. Definíció. *Egy tetszőleges test F fölötti n* **határozatlanos monomnak** *nevezzük az $ax_1^{k_1} \dots x_n^{k_n}$ alakú formális kifejezéseket, ahol $0 \neq a \in F$, és $k_1, \dots, k_n \in \mathbb{N}$. Az ilyen monomok véges összegeit pedig F* **fölötti n határozatlanos polinomoknak**. *(Az összes F fölötti n határozatlanos polinomok halmazára most is az $F[x_1, \dots, x_n]$ jelölést fogjuk alkalmazni.)*

8.3. Definíció. *Azt mondjuk, hogy az $ax_1^{k_1} \dots x_n^{k_n}$ monom* **lexikográfusan megelőzi** *a $bx_1^{m_1} \dots x_n^{m_n}$ monomot, ha van olyan $i \in \{1, 2, \dots, n\}$ index, hogy $k_1 = m_1, \dots, k_{i-1} = m_{i-1}$ és $k_i > m_i$.*

Jelölés. Azt a tényt, hogy az $K, L \in F[x_1, \dots, x_n]$ monomok esetén K lexikografikusan megelőzi az L monomot, a következőképp jelöljük: $K \succ L$. $K \succeq L$ pedig azt jelenti, hogy $K \succ L$, vagy $K \sim L$.

8.2. Állítás. *A monomok halmazán a $\succeq$ reláció reflexív, tranzitív és dichotom reláció. $K \succ L$ és $L \succ K$ akkor és csak akkor áll fönn egyidejűleg, ha $K \sim L$.*

8.4. Definíció. *A $\succeq$ relációt* **lexikorgrafikus rendezésnek** *nevezzük.*

Megjegyzés. Az előbbi állítás szerint a $\succeq$ reláció teljes rendezés (dichotom részbenrendezés) a monomok halmazán „modulo asszociáltság”. Mi általában csak egy adott polinomban előforduló monomokat vizsgálunk, ezek között pedig nincsenek asszociáltak (hiszen azok ott egyszerűen összevonhatók), így ott valóban egy teljes (lineáris) rendezéssel van dolgunk.

8.3. Állítás. *A monomok szorzása monoton a lexikografikus rendezésre nézva, azaz tetszőleges K, K', L, L' monomokra*

$$M \succeq L \text{ és } M' \succeq L' \quad \Rightarrow \quad MM' \succeq LL',$$

és egyegyenlőség (pontosabban asszociáltság) csak akkor teljesül, ha $M \sim M'$, illetve $L \sim L'$.

8.4. Állítás. *Tetszőleges $f, g \in F[x_1, \dots, x_n]$ polinomokra fg lexikografikusan első tagja a két polinom lexikografikusan első tagjának szorzata.*

Szimmetrikus polinomok

8.5. Definíció. *Azt mondjuk, hogy az* $f \in F[x_1, \ldots, x_n]$ **szimmetrikus polinom**, *ha invariáns a határozatlanok permutációival szemben, azaz*

$$\forall \pi \in S_n \colon f(x_{\pi(1)}, \ldots, x_{\pi(n)}) = f(x_1, \ldots, x_n).$$

8.6. Definíció. *A* k**-adik** n **határozatlanos** $(k \leq n)$ **elemi szimmetrikus polinom** *az* $x_1, \ldots, x_n$ *határozatlanokból képezett összes* k *tényezős szorzat összege:*

$$\sigma_k = \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} x_{i_1} x_{i_2} \ldots x_{i_k} = \sum_{\substack{I \subseteq \{1, \ldots, n\} \\ |I| = k}} \prod_{i \in I} x_i \in F[x_1, \ldots, n_n].$$

Megjegyzés. Emlékezzünk, az elemi szimmetrikus polinomokkal már találkoztunk a Viète-formuláknál.

8.5. Tétel. *Az* F *fölötti szimmetrikus polinomok* $F_S[x_1, \ldots, x_n]$ *halmaza részgyűrűje az* $F[x_1, \ldots, x_n]$ *gyűrűnek.*

8.6. Állítás. *Ha az* $a x_1^{k_1} \ldots x_n^{k_n}$ *monom valamely szimmetrikus polinom lexikografikusan első tagja, akkor* $k_1 \geq k_2 \geq \ldots \geq k_n$.

8.7. Tétel. (a szimmetrikus polinomok alaptétele)
Bármely szimmetrikus polinom fölírható — mégpedig egyetlen módon — elemi szimmetrikus polinomok ugyanazon test fölötti polinomjaként:

$$\forall f \in F_S[x_1, \ldots, x_n] \;\Rightarrow\; \exists! h \in F[x_1, \ldots, x_n] \colon f = h(\sigma_1, \ldots, \sigma_n).$$

Bizonyítás. (vázlat) A bizonyítás egyszerű számolással végezhető el, első lépésként elemi szimmetrikus polinomok egy olyan szorzatát kell képezni, amelynek lexikografikusan első tagja (megfelelő együtthatóval ellátva) megegyezik az f polinom lexikografikusan első tagjának. E két polinom különbségének lexikografikusan első tagja, már (szigorú értelemben) követi f első tagját, így az eljárást véges sokszor megismételve kaphatjuk a tételbeli előállítást. Az egyértelműség bizonyítása sem bonyolultabb.

8.8. Következmény. *Ha* $f \in \mathbb{Q}[x]$ *egy* n*-edfokú polinom, és komplex gyökei (multiplicitással)* $\alpha_1, \ldots, \alpha_n$, *akkor bármely* $g \in \mathbb{Q}_S[x_1, \ldots, x_n]$ *szimmetrikus polinomra* $g(\alpha_1, \ldots, \alpha_n) \in \mathbb{Q}$.

8.7. Definíció. *Az* $f \in F[x_1, \ldots, x_n, y_1, \ldots, y_m]$ *polinom* **szimmetrikus az** $x_1, \ldots, x_n$ **és** $y_1, \ldots, y_m$ **határozatrendszerekre nézve**, *ha*

$$\forall \pi \in S_n \; \forall \varrho \in S_m \colon f(x_{\pi(1)}, \ldots, x_{\pi(n)}, y_{\sigma(1)}, \ldots, y_{\sigma(m)}) = f(x_1, \ldots, x_n, y_1, \ldots, y_m).$$

Jelölés. A továbbiakban $\sigma_1, \ldots, \sigma_n$ az $x_1, \ldots, x_n$, míg $\tau_1, \ldots, \tau_m$ az $y_1, \ldots, y_m$ határozatlanok elemi szimmetrikus polinomjait fogja jelölni.

8.9. Tétel. *Ha az* $f \in F[x_1, \ldots, x_n, y_1, \ldots, y_m]$ *polinom szimmetrikus az* $x_1, \ldots, x_n$ *és* $y_1, \ldots, y_m$ *határozatlanrendszerekre nézve, akkor fölírható, mégpedig egyetlen módon, ezen határozatlanos elemi szimmetrikus polinomjaként:*

$$\exists! h \in F[x_1, \ldots, x_n, y_1, \ldots, y_m] \colon f = h(\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m).$$

Megjegyzés. A kettőnél több határozatlanrendszerre nézve szimmetrikus polinom fogalma hasonlóan definiálható, és hasonló tétel is igazolható rájuk.

9. Számelmélet integritástartományokban

Integritástartományokban számos olyan állítás érvényes, mint amilyeneket az elemi számelméletben, vagy a test fölötti polinomgyűrűkben — két fajta speciális integritástartományban — bizonyítottunk. Az általános esetben azonban van néhány eltérés, amelyek a korábbi esetekben az ottani speciális elemek miatt voltak csak érvényesek. Ezek, mint látni fogjuk, az általános esetek speciális megjelenései. A már ismert fogalmakat, összefüggéseket, állításokat megismételjük. Javasoljuk az olvasónak ezek összehasonlítását a már ismert speciális esetekkel.

Az elkövetkezőkben R mindig integritástartományt jelöl. Ezt általában nem fogjuk a jövőben külön említeni. Célunk az lesz, hogy keressünk olyan integritástartomány osztályokat, amelyekben igaz a számelmélet alaptételének értelemszerű általánosítása, azaz a nemzéró és nem invertálható elemeknek van tovább már nem bontható szorzatelőállítása.

Először az oszthatóság és a legnagyobb közös osztó fogalmát, majd a prímszám és az irreducibilis polinom fogalmát adjuk meg általánosan.

9.1. Definíció. *Azt mondjuk, hogy $a \in R$* **osztója a** *$b \in R$* **elemnek,** *(b* **többszöröse** *a***-nak)** *ha van olyan $c \in R$, hogy $ac = b$.*

Jelölés. Az oszthatósági relációt (most is) $|$ jelöli:

$$a|b \quad \Leftrightarrow \quad \exists c \in R\colon b = ac.$$

Megjegyzés. Ha $a \neq 0$, akkor egyetlen ilyen c létezik (ez R integritástartomány voltából következik), így ilyenkor használhatjuk a hagyományos $c = \frac{b}{a}$ jelölést. Ha $a \nmid b$, akkor a $\frac{b}{a}$ szimbólumot (egyelőre) nem értelmezzük.

9.1. Tétel. *Bármely $a, b, c, d \in R$ elemekre évényesek a következő állítások.*

(1) $a|a$,
(2) $a|b$ *és* $b|c \implies a|c$,
(3) $a|b$ *és* $a|c \implies a|b+c$ *és* $a|b-c$,
(4) $a|b$ *és* $a \nmid c \implies a \nmid b+c$ *és* $a \nmid b-c$,
(5) $a|b$ *és* $c|d \implies ac|bd$,
(6) $1|a$ *és* $a|0$,
(7) $0|a \iff a = 0$,
(8) $ac|bc$ *és* $c \neq 0 \implies a|b$.

9.2. Definíció. *Az $a, b \in R$ elemek* **asszociáltak,** *ha $a|b$ és $b|a$. Az* **asszociáltsági relációt** *$\sim$ fogja jelölni:*

$$a \sim b \qquad \Longleftrightarrow \qquad a|b \text{ és } b|a.$$

9.3. Definíció. *Azt mondjuk, hogy az $a \in R$ elem* **egység,** *ha $a|1$.*

Megjegyzés. Vegyük észre, hogy az egységek éppen az integritástartomány invertálható elemei.

9.2. Tétel. *Az egységek bármely integritástartományban csoportot alkotnak a szorzással.*

9.4. Definíció. *Az előbbi csoportot az R integritástartomány* **egységcsoportjának** *nevezzük, és R^*-gal jelöljük.*

Példa. A $\mathbb{Z}$ gyűrű egységcsoportja: $\{\pm 1\}$, míg egy $F[x]$ (test fölötti) polinomgyűrű egységcsoportja a nemzéró konstans polinomok halmaza: F^*, az alaptest multiplikatív csoportja.

9.3. Állítás. *Az asszociáltság ekvivalenciareláció. Az $a, b \in R$ elemek pontosan akkor asszociáltak, ha valamely c egységre $ac = b$.*

Megjegyzés. Az asszociált elemeket nem érdemes (nem is lehet) megkülönböztetni, ha csak az oszthatóságot vizsgáljuk. Ha az oszthatósági relációt az asszociáltsági osztályok halmazán értelmezzük, akkor már nemcsak reflexív és tranzitív, hanem antiszimmetrikus is lesz, azaz részbenrendezés.

A legnagyobb közös osztó (és a legkisebb közös többszörös) fogalma is definiálható integritástartományokban, és ha létezik, akkor csak asszociáltság erejéig egyértelmű.

9.5. Definíció. *A $c \in R$ elem (egy)* **legnagyobb közös osztója** *az $a, b \in R$ elemeknek, ha mindkettőnek osztója, és a két elem mindegyik közös osztója osztója neki, azaz*

(1) $c|a \quad$ *és* $\quad c|b$,
(2) $\forall c' \in R\colon (c'|a$ *és* $c'|b) \Longrightarrow\ c'|c$.

Azt mondjuk, hogy $d \in R$ az $a, b \in R$ elemek (egy) **legkisebb közös többszöröse**, *ha mindkettőnek többszöröse, és a két elem bármely közös többszörösének osztója, azaz*

(1) $a|d$ *és* $b|d$,
(2) $\forall \overline{d} \in R\colon (a|\overline{d}$ *és* $\overline{d}|b) \Longrightarrow\ d|\overline{d}$.

Jelölés. A legnagyobb közös osztó és a legkisebb közös többszörös jelölésére az ismert $\ln.\,\mathrm{k.\,o.}(a, b)$, $\mathrm{lk.\,k.\,t.}(a, b)$ jelöléseket fogjuk használni.

9.4. Tétel. *A legnagyobb közös osztó és a legkisebb közös többszörös, ha léteznek, csak asszociáltság erejéig egyértelműek.*

Megjegyzés. Az előbbi tétel alapján a $c = \ln.\,\mathrm{k.\,o.}(a, b)$ helyett korrektebb(és ezt is fogjuk zömmel alkalmazni) a $c \sim \ln.\,\mathrm{k.\,o.}(a, b)$ írásmód. hasonló a helyzet a legkisebb közös többszörössel is.

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

Integritástartományokban általában nem létezik két tetszőleges elem legnagyobb közös osztója, így különös fontossággal bír azoknak az integritástartomány osztályoknak a keresése, ahol ez létezik. Az előbbire példa a következő integritástartomány.

9.5. Állítás. *A* $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} \colon a, b \in \mathbb{Z}\}$ *halmaz a komplex számok ismert műveleteivel olyan integritástartomány, amelyben a* 9*-nek és a* $3(2 + i\sqrt{5})$*-nek nincs legnagyobb közös osztója.*

Bizonyítás. Az világos, hogy $\mathbb{Z}[i\sqrt{5}]$ integritástartomány, továbbá az is világos, hogy $3 \nmid 2 + i\sqrt{5}$. Az pedig, hogy $2 + i\sqrt{5} \mid 3$ szintén lehetetlen, ugyanis ha $3 = (2 + i\sqrt{5})(x + yi\sqrt{5})$ valamely $x, y \in \mathbb{Z}$-re, akkor — fölhasználva, hogy két komplex szám szorzata mikor valós — szükségképp $x + yi\sqrt{5} = a(2 - i\sqrt{5})$-nek kellene teljesülnie valamely $a \in \mathbb{R}$-re, s így a

$$3 = (2 + i\sqrt{5})a(2 - i\sqrt{5}) = 9a$$

egyenlőségből $a = \frac{1}{3}$ adódik, ami lehetetlen, hiszen $\frac{1}{3}(2-i\sqrt{5}) \notin \mathbb{Z}[i\sqrt{5}]$.

A továbbiakban néhány olyan integritástartomány osztályt/típust definiálunk/vizsgálunk, ahol bármely két elemnek van legnagyobb közös osztója.

Euklideszi gyűrűk

9.7. Definíció. *Azt mondjuk, hogy az* R *integritástartomány* **euklideszi gyűrű***, ha létezik olyan —* **euklideszi normának** *nevezett —* $\| \| \colon R \to \mathbb{N}_0$ *leképezés, amelyre*

(1) $\|0\| = 0$*, és minden nemzéró* $a \in R$ *elemre* $\|a\| > 0$*;*
(2) *bármely* $a, b \in R$ *elemekre* $a|b$ *és* $b \neq 0$ *maga után vonja, hogy* $\|a\| \leq \|b\|$*;*

(3) *tetszőleges* $a, b \in R$ $b \neq 0$ *elemekhez léteznek olyan* $q, r \in R$ *elemek, hogy* $a = bq + r$ *és* $\|r\| < \|b\|$*.*

Példák.
1. Az egész számok, illetve a test fölötti polinomok gyűrűje egyaránt euklideszi gyűrű az abszolút érték, illetve a $2^{\deg f}$ normával.
2. A $\mathbb{Z}[i] = \{a + bi \colon a, b \in \mathbb{Z}\}$ gyűrű, az ún. **Gauss-egészek** dyűrűje szintén euklideszi az abszolút érték négyzete, mint euklideszi normával.

Megjegyzés. A definícióbeli $a = bq + r$ előállítást ez esetben is **maradékos osztásnak** — olykor használjuk az **euklideszi osztás** terminológiát is — nevezzük. Könnyen belátható, hogy a maradékos osztás elvégzése lehetővé teszi tetszőleges $a, b \in R,\ b \neq 0$ elemeken az euklideszi algoritmus végrahajtását.

9.6. Tétel. *Euklideszi gyűrűben bármely két elemnek létezik legnagyobb közös osztója.*

Bizonyítás. A két elemen végzett euklideszi algoritmus (maradékos osztások sorozata, ugyanúgy végezve, mint polinomokra) véges sok lépés után most is leáll, mert a maradékok normája szigorúan monoton

csökkenő sorozatot alkot. Így el kell jutni zésó maradékhoz. A legnagyobb közös osztó most is az utolsó nemzéró maradék. E tény a korábbi esetekhez hasonlóan látható be.

Főideálgyűrűk

9.8. Definíció. *A nemüres $I \subseteq R$ részhalmazt* **ideálnak** *nevezzük, ha*

(1) *I részcsoportja R additív csoportjának,*
(2) *tetszőleges $a \in I$ és $c \in R$ elemekre $ac \in I$.*

Jelölése: $I \triangleleft R$.

Megjegyzések.
1. A (2) tulajdonságot **szívó tulajdonságnak** szokás nevezni. Vegyük észre, hogy e szívó tulajdonság erősebb a szorzásra való zártságnál. Így minden ideál részgyűrű is.
2. Maga az R gyűrű, és a $\{0\}$ halmaz ideál. Az előbb nem valódi ideál, míg a második triviális ideál. (A „valódi" jelzőt általában akkor használjuk, ha valódi részhalmazról van szó.)

9.9. Definíció. *Az $a \in R$* **elem által generált főideálon** *az $(a) = \{ab \colon b \in R\}$ halmazt értjük.*

Megjegyzés. Vegyük észre, hogy (a) éppen az a-val osztható elemek halmaza. Továbbá, $(0) = \{0\},\ (1) = R$.

9.7. Állítás. *Az a elem által generált főideál valóban ideál, és a legszűkebb olyan ideál, amely tartalmazza a-t. Azaz bármely olyan I ideálra, amelyre $a \in I$, $(a) \subseteq I$.*

9.8. Tétel. *Bármely $a, b \in R$ elemekre:*

(1) $a|b \implies (a) \supseteq (b)$,
(2) $a \sim b \implies (a) = (b)$,
(3) $a \sim 1 \iff (a) = R$.

Megjegyzés. Az előbbi két állítás igazolása rutin számolás, amelynek önálló elvégzése melegen ajánlott.

9.10. Definíció. *Az R integritástartományt* **főideálgyűrűnek** *nevezzük, ha minden ideálja főideál.*

9.9. Tétel. *Minden euklideszi gyűrű főideálgyűrű.*

Bizonyítás. Legyen R Euklideszi gyűrű és $I \triangleleft R$, továbbá legyen $a \in I$ egy minimális normájú nemzéró elem. Megmutatjuk, hogy tetszőleges $b \in I$-re $a|b$, ami maga után vonja, hogy $I = (a)$. Valóban, $b = aq + r$, amiből $r = b - aq \in I$ adódik. Mivel $\|r\| < \|a\|$, $r = 0$.

Megjegyzések.
1. Korábban említettük, hogy $\mathbb{Z}, F[x], \mathbb{Z}[i]$ euklideszi gyűrűk, így főideálgűrűk is.
2. A tétel megfordítása nem igaz. A $\mathbb{Z}[\omega] = \{a + b\omega \colon a, b \in \mathbb{Z},\ \omega = \frac{1+i\sqrt{19}}{2}\}$ integritástartomány főideálgyűrű, de nem euklideszi gyűrű.

9.10. Tétel. *Főideálgyűrűben bármely két elemnek van legnagyobb közös osztója, és előáll a két elem lineáris kombinációjaként. Formálisan*

$$R \text{ főideálgyűrű} \implies \forall a, b \in R\ \exists x, y \in R\colon ax + by \sim \ln.\,\mathrm{k.\,o.}(a, b).$$

Bizonyítás. Legyen R főideálgyűrű és $a, b \in R$. Egyszerűen kapható, hogy ideálok metszete ismét ideál (főideálgyűrűben természetesen főideál). Ha $(a) \cap (b) = (c)$, akkor $c \sim \ln.\,\mathrm{k.\,o.}(a, b)$. A második állítás is egyszerűen kapható abból, hogy az $\{ax + by\colon x, y \in R\}$ halmaz ideál.

9.11. Tétel. *Legyen R főideálgyűrű, és $a, b, c \in R$ tetsőleges elemek. Ekkor*

(1) $\ln.\,\mathrm{k.\,o.}(\ln.\,\mathrm{k.\,o.}(a, b), c) \sim \ln.\,\mathrm{k.\,o.}(a, \ln.\,\mathrm{k.\,o.}(b, c))$,
(2) $\ln.\,\mathrm{k.\,o.}(a, b) \sim \ln.\,\mathrm{k.\,o.}(b, a)$,
(3) $\ln.\,\mathrm{k.\,o.}(a, a) \sim a$,
(4) $\ln.\,\mathrm{k.\,o.}(0, a) \sim a$,
(5) $\ln.\,\mathrm{k.\,o.}(1, a) \sim 1$,
(6) $\ln.\,\mathrm{k.\,o.}(a, b) \sim a \iff a|b$,
(7) $\ln.\,\mathrm{k.\,o.}(a + bc, b) \sim \ln.\,\mathrm{k.\,o.}(a, b)$,
(8) $\ln.\,\mathrm{k.\,o.}(a, b)c \sim \ln.\,\mathrm{k.\,o.}(ac, bc)$,
(9) $\ln.\,\mathrm{k.\,o.}(a, b) \not\sim 0 \implies \ln.\,\mathrm{k.\,o.}\left(\frac{a}{\ln.\mathrm{k.o.}(a,b)}, \frac{b}{\ln.\mathrm{k.o.}(a,b)}\right) \sim 1$,
(10) $\ln.\,\mathrm{k.\,o.}(a, b) \sim 1 \implies \ln.\,\mathrm{k.\,o.}(a, bc) \sim \ln.\,\mathrm{k.\,o.}(a, c)$.

Megjegyzés. Az előbbi tétel nemcsak főideálgyűrűkben igaz, hanem minden olyan integritástartományban, amelyben bármely két elemnek van legnagyobb közös osztója. Ezen általánosabb tétel igazolása azonban nehezebb.

9.12. Következmény. *Legyen R főideálgyűrű, $a, b, c \in R$, és $\ln.\,\mathrm{k.\,o.}(a, b) \sim 1$. Ekkor*

$$a|bc \implies a|c, \quad \text{valamint } (a|c \text{ és } b|c) \implies ab|c.$$

9.13. Következmény. *Ha R főideálgyűrű és $a, b, c \in R$ olyanok, hogy $\ln.\,\mathrm{k.\,o.}(a, b) \not\sim 0$, akkor*

$$a|bc \iff \frac{a}{\ln.\,\mathrm{k.\,o.}(a, b)}\,|c\,.$$

9.14. Következmény. *Főideálgyűrűben bármely két elemnek létezik legkisebb közös többszöröse, ugyanis tetszőleges $a, b \in R$-re*

$$\ln.\,\mathrm{k.\,o.}(a, b)\,\mathrm{lk.\,k.\,t.}(a, b) \sim ab.$$

Főideálgyűrűben ugyanazon föltétel mellett oldhatók meg a kétismeretlenes lineáris diofantoszi egyenletek, mint az egész számok gyűrűjében. Igazolható ugyanis a következő tétel.

9.15. Tétel. *Legyen R főideálgyűrű, és $a, b, c \in R$ tetszőleges elemek. Az $ax + by = C$ egyenlet pontosan akkor oldható meg, ha $\ln.\,\mathrm{k.\,o.}(a, b)|c$.*

Ha (x_0, y_0) *egy megoldás, akkor bármely* $t \in R$*-re*

$$\left(x_0 + \frac{b}{\text{ln. k. o.}(a,b)}t, y_0 + \frac{a}{\text{ln. k. o.}(a,b)}t\right)$$

is megoldás, és az egyenletünk minden megoldása előáll ilyen alakban.

Gauss-gyűrűk

Az irreducibilis- és a prím elem fogalma nemcsak polinomgyűrűkben, hanem tetszőleges integritástartományban is bevezethető. E részben a legbővebb olyan integritástartomány osztályra adunk egyfajta jellemzést, amelyben érvényes a számelmélet alaptételének egy olyasfajta általánosítása, amilyet egyhatározatlanos polinomok gyűrűire adtunk.

R a továbbiakban is tetszőleges integritástartományt fog jelölni.

9.11. Definíció. *Azt mondjuk, hogy az* $q \in R,\ q \neq 0,\ q \nmid 1$ *elem* **irreducibilis** *(R-ben), ha csak úgy bontható föl két R-beli elem szorzatára, hogy az egyik tényező asszociáltja q-nak. (Ekkor a másik tényező természetesen egység.) Az ilyen faktorizációkat* **triviális faktorizációnak** *nevezzük. Formálisan:*

$$\forall a, b \in R\colon q = ab \implies (q \sim a,\ \textit{vagy}\ q \sim b).$$

9.12. Definíció. *Azt mondjuk, hogy a* $p \in R,\ p \neq 0,\ p \nmid 1$ *elem* **prím**, *ha valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat valamelyik tényezőjének. Formálisan:*

$$\forall a, b \in R\colon p|ab \implies (p|a,\ \textit{vagy}\ p|b).$$

9.16. Állítás. *Legyen* $p \in R$ *prím és* $n \in \mathbb{N}$, $p|a_1 \dots a_n$ *valamilyen* $a_1, \dots, a_n \in R$ *elemekre, létezik olyan* $1 \leq i \leq n$, *hogy* $p|a_i$.

9.17. Tétel. *Integritástartományban minden prím irreducibilis.*

Bizonyítás. Legyen R integritástartomány $p \in R$ prím, továbbá $p = ab$ valamely $a, b \in R$ elemekre. Mivel p prím, osztója e két elem közül legalább egynek. Ha $p|a$, akkor $p = ptb$ valamely $t \in R$-re, amiből $1 = tb$, azaz $b|1$, és így $p \sim a$.

Megjegyzés. A fordított irányú implikáció már általában nem igaz. Egy korábban már definiált integritástartományban, a $\mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5}\colon a, b \in \mathbb{Z}\}$ gyűrűben, a 3 irreducibilis, de nem prím: $3|(2 + i\sqrt{5})(2 - i\sqrt{5})$, de egyik tényezőnek nem osztója.

9.13. Definíció. *Azt mondjuk, hogy az R integritástartomány* **Gauss-gyűrű**, *ha minden olyan nemzéró eleme, amely nem egység, irreducibilis elemek szorrzatára bontható. E fölbontás sorrendtől és asszociáltaktól eltekintve egyértelmű. Formálisan*

$$\forall a \in R\ \exists q_1, \dots, q_m \in R\colon q_q, \dots, q_m \textit{ irreducibilis, és } a = q_1 \dots q_m,$$

továbbá, ha $a = q'_1 \dots q'_k$ *egy másik irreducibilis fölbontás* R*-beli elemekre, akkor*

$$m = k \text{ és } \forall i \in \{1, \dots, m\} \exists j \in \{1, \dots, k\} \colon q_i \sim q'_j.$$

9.18. Tétel. *Az* R *integritástartomány pontosan akkor Gauss-gyűrű, ha*

(1) R *minden olyan nemzéró eleme, amely nem egység, irreducibilis elemek szorzatára bontható;*
(2) *az irreducibilis elemek prímek.*

Bizonyítás. Világos, hogy csak az szorul bizonyításra, hogy Gauss-gyűrűben az irreducibilis elemek prímek. Legyen R Gauss-gyűrű és $q \in R$ irreducibilis elem, amely osztója az ab szorzatnak $(a, b \in R)$.

Bontsuk föl a-t és b-t irreducibilis elemek szorzatára:

$$a = q_1 \cdot q_k, \qquad b = q_{k+1} \dots q_m,$$

és így szorzatuk (egy) irreducibilis fölbontása

$$ab = q_1 \dots q_k q_{k+1} \dots q_m,$$

amely sorrendtől és aszociáltaktól eltekintve egyértelmű. Mivel q az ab szorzat egy irreducibilis faktora, $ab = q \cdot q'_1 \dots q'_n$ valamely $q'_1, \dots, q'_n \in R$ irreducibilis elemekre. Ezen fölbontásnak azonban sorrendtől és asszociáltaktól eltekintve meg kell egyeznie az előbbivel, léteznie kell egy olyan q_i-nek $(1 \le i \le m)$, hogy $q \sim q_i$. Ha $i \le k$, akkor $q|a$, különben $q|b$.

9.19. Tétel. *Minden főideálgyűrű Gauss-gyűrű.*

Bizonyítás. A Gauss-gyűrűket jellemző tételünk alapján csak azt kell igazolnunk, hogy főideálgyűrűkben minden nemzéró és nem invertálható elem fölbontható irreducibilis elemek szorzatára. Ez pedig pontosan azt jelenti, hogy ha $a \in R$ az R főideálgyűrű egy olyan eleme, amelyre $a \neq 0,\ a \nmid 1$, akkor nem létezik olyan $b_1, b_2, \dots$ végtelen elemlánc R-ben, hogy $b_1|a,\ b_{i+1}|b_i$, de $b_i \not\sim b_{i+1}$ minden $1 \le i$ esetén, azaz nem léteznek végtelen valódi osztóláncok.

Vegyük észre, hogy egy előbbi tulajdonságú osztólánc létezése egyenértékű végtelen fölszálló főideállánc létezésével. Mégpedig olyannak, amelyben a tartalmazások valódiak. Tehát azt kell igazolnunk, hogy főideálgyűrűben nem létezik főideálok végtelen, valódi módón fölszálló főideállánca.

Tegyük föl, hogy létezik egy

$$(b_1) \subset (b_2) \subset \dots$$

főideállánc R-ben. Egyszerűen kapható, hogy

$$\bigcup_{i=1}^{\infty} (b_i) \lhd R \Longrightarrow \exists c \in R \colon \bigcup_{i=1}^{\infty} (b_i) = (c).$$

Mivel $c \in \bigcup_{i=1}^{\infty}(b_i)$, van olyan $k \in \mathbb{N}$, hogy $c \in (b_k)$, ami maga után vonja, hogy $(c) \subseteq (b_k)$, amiből $b_k|c$ következik. Ez azonban azt (is) jelenti, hogy az ideálsorozat a k indextől kezdve már nem növekvő, azaz az osztólánc szükségképp véges.

A bizonyítás további része ugyanúgy végezhető, mint a számelmélet (klasszikus) alaptételéé.

9.20. Következmény. *Minden Euklideszi-gyűrű Gauss-gyűrű.*

9.21. Állítás. *Gauss-gyűrűben bármely két elemnek létezik legnagyobb közös osztója.*

Bizonyítás. Bontsuk a két elemet irreducibilis elemek szorzatára. Ebből ugyanúgy kapható a legnagyobb közös osztó (és mellesleg a legkisebb közös többszörös is), mint az elemi számelméletben a prímfölbontásból.

10. Integritástartomány hányadosteste

10.1. Állítás. *Legyen R integritástartomány, és $Q = R \times (R \setminus \{0\})$. E Q halmazon definiált $\approx$ reláció*

$$(a, b) \approx (c, d) \quad \Longleftrightarrow \quad ad = bc$$

ekvivalenciareláció. Az (a, b) elemet tartalmazó osztályt (a szokásos módon) $\overline{(a, b)}$ fogja jelölni.

10.2. Tétel. *Definiáljuk az előbbi Q halmazon a következő két műveletet:*

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(ad + bc, bd)}$$
$$\overline{(a, b)} \cdot \overline{(c, d)} = \overline{(ac, bd)}.$$

E műveletek jóldefiniáltak (az eredmény független a reprezentánsok megválasztásától), és velük Q testet alkot.

10.1. Definíció. *Az előző tételben megkonstruált testet R* **hányadostestének** *nevezzük, és használni fogjuk a Q_R jelölést.*

10.3. Állítás. *Legyen R integritástartomány. A Q_R hányadostest tartalmaz R-rel izomorf részgyűrűt.*

Bizonyítás. A kívánt $\varphi\colon R \to Q_R$,leképezés: $\varphi\colon a \mapsto \overline{(a, 1)}$.
Megjegyzés. Az előbbiek alapján, amennyiben $\overline{(a, 1)}$ helyett egyszerűen a-t írunk, és nem is különböztetjük meg az a elemtől, akkor R-et a hányadosteste részének tekinthetjük: $R \subset Q_R$.

10.4. Állítás. *Az R integritástartomány hányadostestének minden eleme előáll két R-beli elem hányadosaként.*

Bizonyítás. A kívánt előállítást úgy kapjuk, hogy az $\overline{(a, b)}$ osztályt az $\frac{a}{b}$ $(a, b \in R,\ b \neq 0)$ formális törttel helyettesítjük.
Megjegyzés. Vegyük észre, hogy az előbbiekből az is adódik, hogy Q_R-nek nincs olyan valódi részteste, amely tartalmazza R-et. Ez azt is jelenti, hogy az iménti hányadostest-konstrukció „gazdaságos". Természetesen egy integritástartomány többféleképpen is bővíthető testté, elég csak az egész számok $\mathbb{Z}$ gyűrűje esetén a $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ testekre gondolni. De $\mathbb{Q}$ az egyetlen minimális bővítés.
Megjegyzés. Egyszerüen belátható, hogy a $Q_{\mathbb{Z}}$ hányadostest azonosítható a racionális számok $\mathbb{Q}$ testével, $\mathbb{Q} \cong Q_{\mathbb{Z}}$, de egy korábbi megjegyzésünk alapján $\mathbb{Q} = Q_{\mathbb{Z}}$ is írható.

10.2. Definíció. *Legyen F tetszőleges test. Az $F[x]$ polinogyűrű hányadostetét, a $Q_{F[x]}$ testet. az F* **test fölötti racionális függvénytestnek** *nevezzük, és $F(x)$-szel jelöljük.*

Megjegyzés. A $Q_{F[x]}$ hányadostest elemei az $\frac{f}{g},\ f,g \in F[x],\ g \neq 0$ alakú formális törteknek — racionális törteknek — tekinthetők. Minden $\frac{f}{g}$ törthöz egy $c \mapsto \frac{f(c)}{g(c)}$ függvény tartozik, amely F azon elemein értelmezett, amelyek nem gyökei a g polinomnak.

Ai integrálszámításban alapvező fontosságú a következő fogalom.

10.3. Definíció. *Azt mondjuk, hogy az $\frac{f}{g} \in F(x)$ racionális tört* **elemi tört***, ha $g = p^k$ valamely p irreducibilis polinomra és $k \in \mathbb{N}$re, továbbá* $\deg f < \deg p$.

10.5. Tétel. *Minden racionális tört fölbontható egy polinom és véges sok elemi tört összegére. E fölbontás a tagok sorrendjétől eltekintve egyértelmű.*

Megjegyzés. E tétel speciális esete jól ismert az elemi (valós-, komplex) integrálelméletből: ott parciális (elemi) törtekre bontásként említik, és alapvető szerepe van a racionális törtfüggvények (polinomok hányadosai) integrálásában.

Egész együtthatós polinomok irreducibilis faktorizációja

Vegyük észre, hogy a $\mathbb{Z}[x]$ gyűrűbeli irreducibilis faktorizációk gyakran különböznek ugyanazon polinom $\mathbb{Q}[x]$-beli faktorizációjától: például a $2 \cdot x$ faktorizáció $\mathbb{Q}[x]$-ben triviális (lévén ott a 2 egység), de $\mathbb{Z}[x]$-ben már nemtriviális, hiszen e gyűrűben csak a ± 1 egység. Egy másik fontos észrevétel, hogy valamely $a \in \mathbb{Z},\ f \in \mathbb{Z}[x]$-re $a|f$ pontosan akkor teljesül, ha az f polinom minden egyes együtthatója osztható a-val. Következésképp f pontosan akkor primitív, ha ± 1-en kívül nem osztható egyetlen egész számmal sem.

10.6. Tétel. *A $\mathbb{Z}[x]$ gyűrű irreducibilis elemei a prímszámok (mint nulladfokú polinomok), valamint a legalább elsőfokú polinomok közül azok, amelyek primitívek és irreducibilisek $\mathbb{Q}[x]$-ben.*

10.7. Tétel. *$\mathbb{Z}[x]$ Gauss-gyűrű.*

A hányadostest konstrukciót is föhasználva igazolható a következő tétel, amiből előbbi tételünk is következik.

10.8. Tétel. *Ha R Gauss-gyűrű, akkor $R[x]$ szintén Gauss-gyűrű.*

10.9. Következmény. *Bármely F testre az $F[x_1, \ldots, x_n]$ polinomgyűrű Gauss-gyűrű.*

11. Algebrai számok

11.1. 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.*

Jelölés. Az összes algebrai számok halmazát $\mathbb{A}$ fogja jelölni.

11.1. Tétel. (Liouville 1844) *Létezik transzcendens szám.*

Bizonyítás. Az

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

szám transzcendens.

11.2. Tétel. *Tetszőleges $\alpha \in \mathbb{A}$ esetén létezik egy egyértelműen meghatározott $\mathbb{Q}[x]$-beli, e gyűrűben irreducibilis főpolinom, amelynek α gyöke.*

11.2. Definíció. *Az előbbi tételbeli polinomot az α algebrai szám* **minimálpolinomjának** *nevezzük. Az α minimálpolinomjának gyökeit α* **konjugáltjainak** *nevezzük.*

11.3. Definíció. *Legyen $\alpha \in \mathbb{C}$ algebrai szám, és $n \in \mathbb{N}$. Azt mondjuk, hogy α* **n-edfokú algebrai szám**, *ha minimálpolinomja n-edfokú.*

Példák.
(1) Minden racionális szám (elsőfokú) algebrai szám.
(2) A $\sqrt{2}$ másodfokú, míg a $\sqrt[13]{15}$ 13-adfokú algebrai szám. Ugyancsak algebrai szám a $\sqrt{2} + \sqrt[5]{3}$.
(3) A komplex egységgyökök algebrai számok.

11.3. Tétel. *Az összes algebrai számok a komplex számok testének résztestét alkotják.*

Bizonyítás. Egyszerűen belátható, hogy ha $\alpha \in \mathbb{A}$, akkor $-\alpha, \frac{1}{\alpha} \in \mathbb{A}$ is áll. Ha ugyanis az α minimálpolinomja az $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Q}[x]$ polinom akkor az $f_1 = (-1)^n a_n x^n + (-1)^{n-1} a_{n-1} x^{n-1} + \ldots - a_1 x + a_0$, illetve az $f_2 = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n$ polinomok a $-\alpha$, ill. az $\frac{1}{\alpha}$ minimálpolinomja.

A továbbiakban tegyük föl, hogy egyrészt $a_n = 1$, másrészt a $\beta \in \mathbb{A}$ minimálpolinomja $g = x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0 \in \mathbb{Q}[x]$. Írjuk e két polinomot

$$f = \prod_{i=1}^{n}(x - \alpha_i), \quad \text{és} \qquad g = \prod_{j=1}^{m}(x - \beta_j)$$

alakban, ahol $\alpha_1 = \alpha,\ \beta_1 = \beta$.

Tekintsük a következő polinomot:

$$h = \prod_{i=1}^{m}\prod_{j=1}^{n}(x-\alpha_i-\beta_j) = x^{nm} + c_{nm-1}x^{nm-1} + \ldots + c_1 x + c_0.$$

Ennek az $\alpha+\beta$ nyilván gyöke, így annak algebrai voltához csak azt kell megmutatni, hogy $h \in \mathbb{Q}[x]$. Világos, hogy a h polinom

$$h = \prod_{i=1}^{n} g(x-\alpha_i)$$

alakban írható. Vegyük észre, hogy e polinom invariáns az $\alpha_1, \alpha_2, \ldots, \alpha_n$ számok — amelyeket változóknak is tekinthetünk — tetszőleges permutációjával szemben. Ez azt is jelenti, hogy a c_i együtthatók az α_i-k $\mathbb{Q}$ fölötti szimmetrikus polinomjai (hiszen a racionális együtthatós g polinom együtthatóiból kapjuk ezeket). Léteznek tehát olyan F_r szimmetrikus polinomok, hogy

$$c_r = F_r(\alpha_1, \ldots, \alpha_n), \qquad 0 \le r \le nm-1.$$

A szimmetrikus polinomok alaptétele szerint F_r fölírható az $\alpha_1, \ldots, \alpha_n$ határozatlanok elemi szimmetrikus polinomjai $\mathbb{Q}$ fölötti polinomjaként:

$$c_r = F_r(\alpha_1, \ldots, \alpha_n) = G_r(\sigma_1, \ldots, \sigma_n),$$

ahol G_r n határozatlanos racionális együtthatós polinom. Az α_i-k elemi szimmetrikus polinomjai a gyökök és együtthatók közötti összefüggéseket leíró Viète formulák szerint az f polinom együtthatói, ill. azok additív inverzei, tehát racionális számok. Ez pedig azt jelenti, hogy a $c_r = G_r(\sigma_1, \ldots, \sigma_n)$ együtthatók racionális számok, azaz $\alpha+\beta \in \mathbb{A}$.

Hasonlóan látható be (ennek önálló elvégzése ajánlott), hogy $\alpha\beta$ gyöke az ugyancsak racionális együtthatós

$$\prod_{i=1}^{n}\prod_{j=1}^{m}(x-\alpha_i\beta_j) = \prod_{i=1}^{n}\alpha_i^m g\left(\frac{x}{\alpha_i}\right)$$

polinomnak. Vegyük észre, hogy itt föltételeztük, hogy α, β nemzérók, de ezzel nem korlátoztuk az általánosságot.

11.4. Következmény. *Az $\alpha = a+bi$ komplex szám $(a, b \in \mathbb{R})$ pontosan akkor algebrai, ha $a, b \in \mathbb{A}$*

11.5. Tétel. *Az algebrai számok teste algebrailag zárt, azaz az algebrai szám együtthatós polinomok (komplex) gyökei algebrai számok.*

11.6. Következmény. *Ha $\alpha \in \mathbb{A}$ és $n \ge 2$, akkor $\sqrt[n]{\alpha}$ algebrai szám (mind az n értékre).*

11.4. Definíció. *Az α komplex számot* **gyökmennyiségnek** *nevezzük, ha megkapható racionális számokból kiindulva a négy alapművelettel (összeadás, kivonás, szorzás és osztás) és egész kitevős gyökvonások véges sokszori alkalmazásával.*

11.7. Következmény. *A gyökmennyiségek algebrai számok.*

11.8. Tétel. *Van olyan algebrai szám, amely nem gyökmennyiség.*

11.9. Tétel. (Hermite 1873, Lindemann 1882)
Az e és a π transzcendens számok.

Megjegyzés. A mai napig sem ismert, hogy az $e + \pi$ szám algebrai, vagy transzcendens. Azonban az, hogy az $e+i\pi$ transzcendens, triviális.

Az algebrai számok teste hatványozásra nem zárt. Az egyszerűen igazolható, hogy tetszőleges $\alpha \in \mathbb{A}$-ra $\alpha^s \in \mathbb{A}$ valahányszor $s \in \mathbb{Q}$, de több már nem igaz. A nem racionális kitevős hatványok esetén az egyik legegyszerűbb kérdés az, hogy a $2^{\sqrt{2}}$ algebrai szám, vagy transzcendens. Sőt az sem nyilvánvaló, hogy egyáltalán irracionális-e. Ez a kérdés illusztráló példaként szerepel Hilbert VII. problémájában, amelyben az algebrai számok irracionális kitevős hatványainak természetére kérdezett rá.

Ő maga ezt a problémát, az α^β alakú hatványok algebrai vagy transzcendens voltának kérdését irracionális algebrai kitevő esetén, nagyon nehéznek tartotta. Nehezebbnek, mint Fermat- vagy a Riemann sejtést. Sőt még az igen egyszerű speciális esetet, a $2^{\sqrt{2}}$-t is szinte reménytelennek vélte. Vélekedése ellenére 1932-ben igazolták, hogy transzcendens.

A probléma teljes megoldását 1934-ben adták meg: egymástól függetlenül érte el Gelfond és Schneider, akik a megelőző években fontos részeredményeket bizonyítottak.