BUDAPESTI MŰSZAKI
MATEMATIKA
ÉS GAZDASÁGTUDOMÁNYI
INTÉZET
EGYETEM

Lineáris algebra mérnököknek

BMETE93BG20

Komplex számok, testek

2019-09-20, 24

Wettl Ferenc

ALGEBRA TANSZÉK

Célkitűzések

E lecke befejezése után a hallgató

- át tudja alakítani az algebrai vagy trigonometriai alakban megadott komplex számot a másik alakba,
- el tudja végezni komplex számokkal a konjugálás, összeadás, szorzás, hatványozás, gyökvonás műveleteit,
- ellenőrizni tudja, hogy egy adott algebrai struktúra test-e,
- el tudja végezni az alapműveleteket $\mathbb{Z}_m$-ben.

Testek

Testek

A számfogalom bővülése

- pozitív egészek – összeadás, szorzás
- $a + x = b$ megoldhatósága $\rightarrow$ negatív számok és 0
- $ax = b$ megoldhatósága $\rightarrow$ racionális számok
- $x^2 = 2$ megoldása $\rightarrow$ vannak irracionális számok
- sorozatok határértékének fogalma $\rightarrow$ valós számok
- az $x^2 = -1$ egyenlet megoldásával lesz további bővítés???

Egy kis történelem

- Girolamo Cardano (1501–1576) orvos, filozófus, matematikus – 1538 körül értesül arról, hogy Scipione del Ferro és Niccolò Tartaglia egymástól függetlenül felfedezték az $x^3 + px = q$ alakú harmadfokú egyenlet megoldását – 1545-ben megírja „Ars magna sive de regulis algebraicis” című művét, benne a megoldóképlettel – 1552-től kezdődően Európa egyik leghíresebb orvosa – a 60-as évek elején elveszti két fiát (gyilkosságért halál, rablásért száműzetés) – 1570-ben Bolognában bebörtönzik, szabadulása után Rómába költözik
- Scipione del Ferro (1465–1526) felfedezi a harmadfokú egyenlet megoldásának módját – titokban tartja (kivétel Nave, Fiore)

- Niccolò Fontana (1499–1557) gúnynevén Tartaglia (dadogó) (1511 Brescia, francia dúlás) – 1535: Fiore kihívja Tartagliát egy 15 napos versenyre (30 feladat, a vesztes a győztest és 29 barátját megvendégeli) – felkészüléskor Tartaglia rájön a nehezebb típusú harmadfokú egyenletek megoldási módjára
- Cardano (kilátásba helyezve Tartaglia tüzérségi találmányainak pártfogót keres, titoktartás igérete mellett megszerzi a titkot) – amikor Navétól megtudja, hogy del Ferro is ismerte e képleteket, felmentve érzi magát, és publikálja (a negyedfokú esetre is továbbfejlesztve az eredményt)
- Tartaglia leírta „megcsalatásának” történetét
- Milánóban Ferrari (Cardano tanítványa) vitára hívja Tartagliát, aki a vitát elveszti, ennek következtében lehetőségeit (nyilvános előadások) elveszíti

A megoldóképlet egy speciális esetre

Oldjuk meg az $x^3 = bx + c$ egyenletet! A Tartaglia képlete:

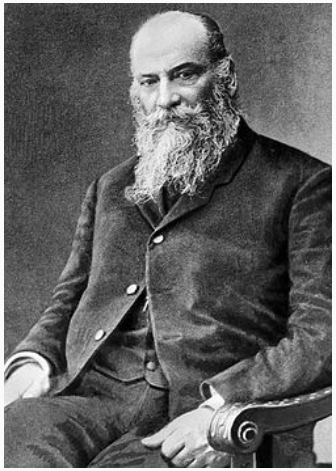
$$x = \sqrt[3]{\frac{c}{2} + \sqrt{\left(\frac{c}{2}\right)^2 - \left(\frac{b}{3}\right)^3}} + \sqrt[3]{\frac{c}{2} - \sqrt{\left(\frac{c}{2}\right)^2 - \left(\frac{b}{3}\right)^3}}$$

Oldjuk meg a $x^3 = 7x + 6$ egyenletet!

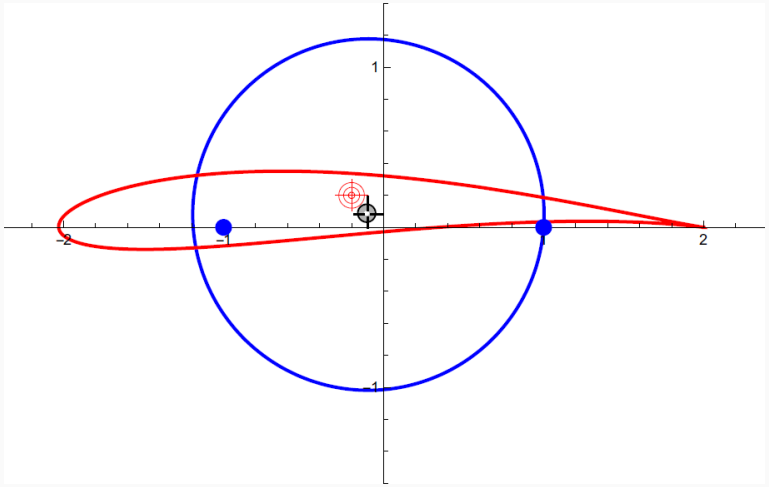
$$\begin{aligned} x &= \sqrt[3]{\frac{6}{2} + \sqrt{\left(\frac{6}{2}\right)^2 - \left(\frac{7}{3}\right)^3}} + \sqrt[3]{\frac{6}{2} - \sqrt{\left(\frac{6}{2}\right)^2 - \left(\frac{7}{3}\right)^3}} \\ &= \frac{1}{3}\sqrt[3]{81 + 30\sqrt{-3}} + \frac{1}{3}\sqrt[3]{81 - 30\sqrt{-3}} \\ &= \frac{1}{3}\left(9/2 + 1/2\sqrt{-3}\right) + \frac{1}{3}\left(9/2 - 1/2\sqrt{-3}\right) \\ &= 3 \end{aligned}$$

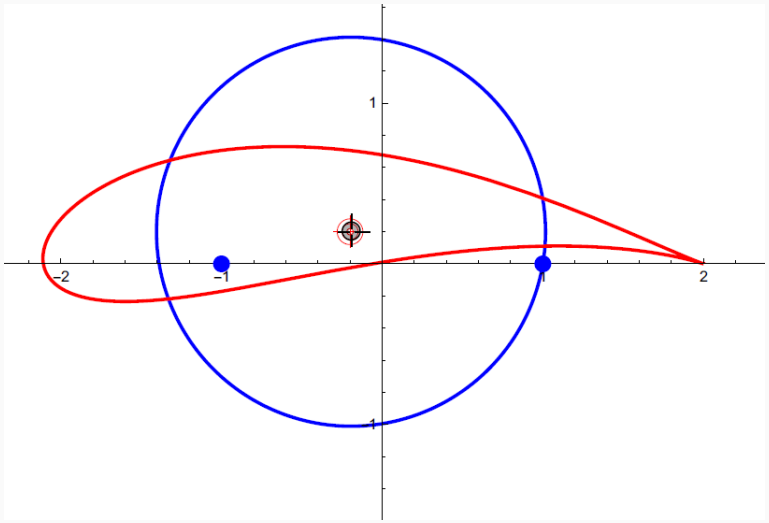
Alkalmazások

hidrodinamika, áramlások vizsgálata, Zsukovszkij-féle szárnyprofil (Joukowski / Zhukovskii / Zhukovsky Airfoil, Nikolay Yegorovich Zhukovsky, Никола́й Его́рович Жуко́вский)



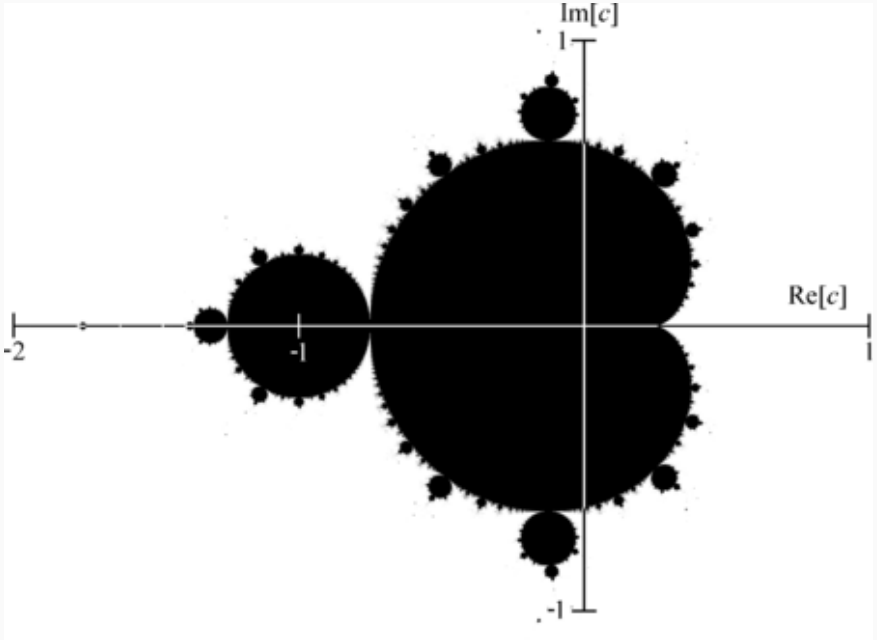
- $z \mapsto z + \frac{1}{z}$:

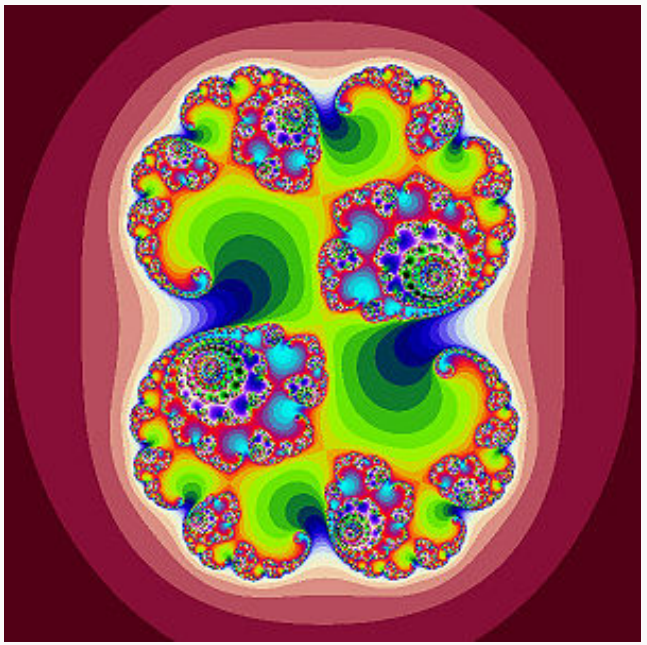


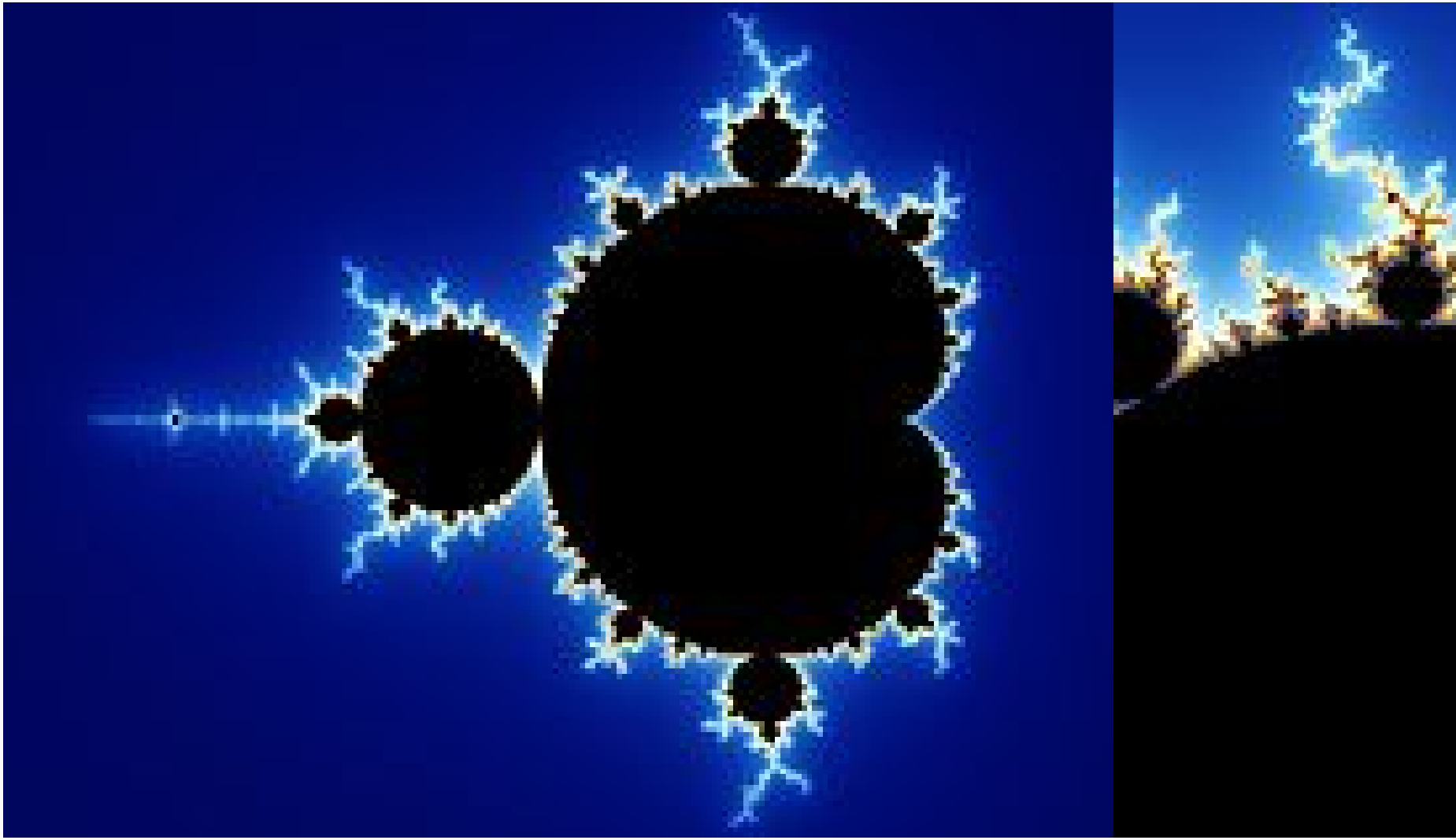


- Egy „Wolfram demonstration” animáció.

- elektromosságtan, jelfeldolgozás, villamosmérnöki tudományok
- lineáris rendszerek, lineáris differenciálegyenletek megoldása
- relativitáselmélet, kvantummechanika
- fraktálok (Mandelbrot-halmazok: ahol a $z_0 = c$, $z_n = z_{n-1}^2 + c$ sorozat korlátos; Julia-halmazok)







Testek

Komplex számok

Komplex szám és algebrai alakja

D

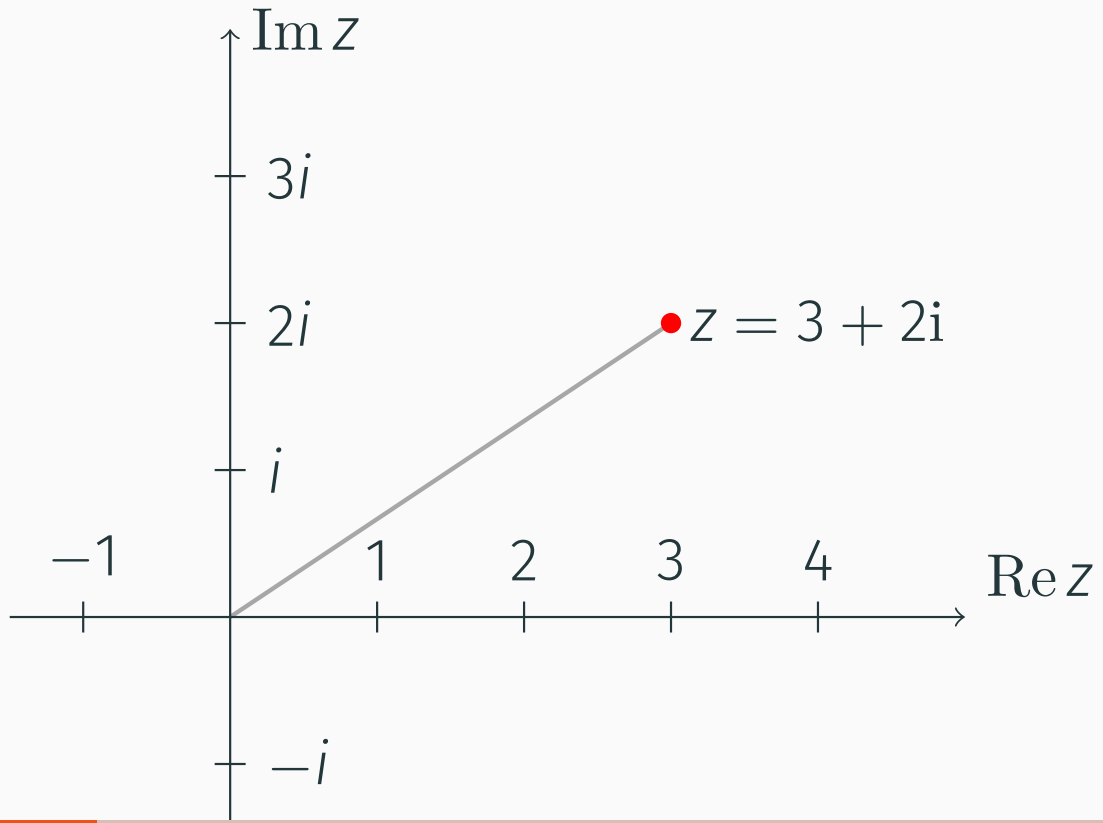
Komplex szám algebrai alakja

Az $a + b\mathrm{i}$ alakú számokat komplex számoknak nevezzük, ahol a és b valósok, i az imaginárius egység, melyre $\mathrm{i}^2 = -1$. a-t a komplex szám valós részének, b-t az imaginárius részének nevezzük. A komplexek halmazát $\mathbb{C}$, az $a + b\mathrm{i} \mapsto a$ függvényt $\Re$ vagy Re, az $a + b\mathrm{i} \mapsto b$ függvényt $\Im$ vagy Im jelöli. Az $a + b\mathrm{i}$ alakot a komplex szám algebrai alakjának nevezzük.

- Algebrai alakban megadott komplex számok összeadása, kivonása, szorzása és pozitív egész kitevős hatványozása úgy végezhető, mintha egyváltozós polinomokkal számolnánk i változóval, de ahol i^2 helyébe -1-et helyettesítünk.
- Az imaginárius egységet – megkülönböztetendő az *i* betű egyéb jelentéseitől – a villamosmérnöki szakirodalomban j betű jelöli, míg bizonyos programnyelvekben I.

D Komplex számsík (Argand-diagram, Gauss-számsík): a komplex számok szemléltetésére az $a + b\mathrm{i}$ komplex számnak a sík (a, b) koordinátájú pontját feleltetjük meg. Ez kölcsönösen egyértelmű. A vízszintes tengelyt valós, a függőlegest imaginárius tengelynek nevezzük.

P Legyen $z = 3 + 2\mathrm{i}$. Ekkor $\operatorname{Re} z = 3$, $\operatorname{Im} z = 2$. E szám a komplex számsíkon ábrázolva:



P

Összeadás, kivonás, szorzás, hatványozás

Számítsuk ki az alábbi kifejezések értékét:

1. $(1-\mathrm{i})+2(1-\mathrm{i})-(1-\mathrm{i})$,
2. $(2-3\mathrm{i})(1+2\mathrm{i})$,
3. $(1-\mathrm{i})^4$.

M

1. $(1-\mathrm{i})+2(1-\mathrm{i})-(1-\mathrm{i}) = 1-\mathrm{i}+2-2\mathrm{i}-1+\mathrm{i} = 2-2\mathrm{i}$.
2. $(2-3\mathrm{i})(1+2\mathrm{i}) = 2-3\mathrm{i}+4\mathrm{i}-6\mathrm{i}^2 = 8+\mathrm{i}$.
3. Hatványozáshoz a binomiális tétel használható:

$$(1-\mathrm{i})^4 = 1-\binom{4}{1}\mathrm{i}+\binom{4}{2}\mathrm{i}^2-\binom{4}{3}\mathrm{i}^3+\mathrm{i}^4 = 1-4\mathrm{i}-6+4\mathrm{i}+1 = -4$$

P **Osztás**

Számítsuk ki az alábbi kifejezések értékét:

1. $\frac{1}{\mathrm{i}}$,
2. $\frac{1+\mathrm{i}}{3+4\mathrm{i}}$,
3. $\frac{a+b\mathrm{i}}{c+d\mathrm{i}}$.

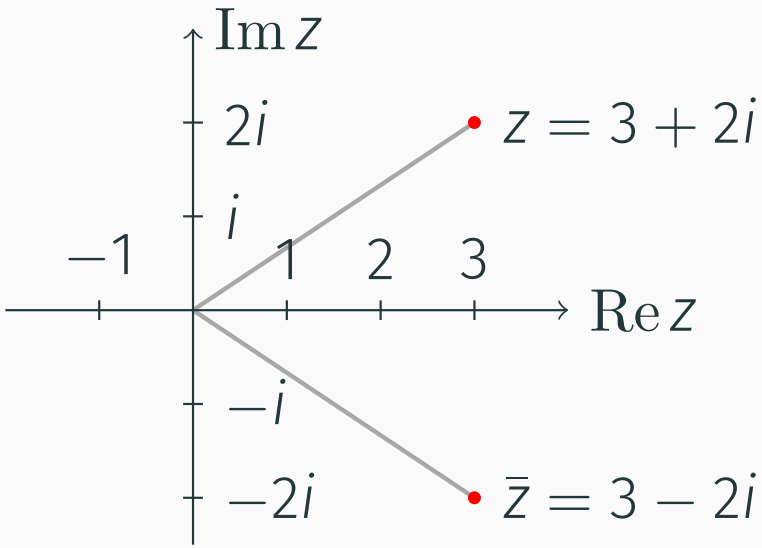
M Kihasználva, hogy $z\bar{z}$ minden komplex z számra valós, komplex számok hányadosának algebrai alakját a nevező konjugáltjával való bővítéssel ki tudjuk számolni.

1. $\frac{1}{\mathrm{i}} = -\mathrm{i}$, mert $-\mathrm{i} \cdot \mathrm{i} = 1$.
2. $\frac{1+\mathrm{i}}{3+4\mathrm{i}} = \frac{(1+\mathrm{i})(3-4\mathrm{i})}{(3+4\mathrm{i})(3-4\mathrm{i})} = \frac{7-\mathrm{i}}{25} = \frac{7}{25} - \frac{1}{25}\mathrm{i}$.
3. $\frac{a+b\mathrm{i}}{c+d\mathrm{i}} = \frac{(a+b\mathrm{i})(c-d\mathrm{i})}{(c+d\mathrm{i})(c-d\mathrm{i})} = \frac{(ac+bd)+(bc-ad)\mathrm{i}}{c^2+d^2}$.

D

Komplex szám konjugáltja

Az $a + bi$ komplex szám konjugáltján az $a - bi$ komplex számot értjük.



T

Konjugált tulajdonságai

1. $\overline{z_1 \pm z_2} = \bar{z}_1 \pm \bar{z}_2$
2. $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$
3. $\overline{z_1 / z_2} = \bar{z}_1 / \bar{z}_2$
4. $\bar{\bar{z}} = z$

A komplex szám trigonometriai alakja

D

Komplex szám abszolút értéke

Az $z = a + b\mathrm{i}$ szám abszolút értékén az $r = |z| := \sqrt{a^2 + b^2}$ nemnegatív valós számot értjük. Ez megegyezik a komplex számsíkon a z számnak a 0-tól való távolságával.

D

Komplex szám irányszöge

A komplex számsíkon az (a, b) vektornak a valós tengellyel bezárt irányított szögét az $a + b\mathrm{i}$ szám irányszögének vagy argumentumának nevezzük.

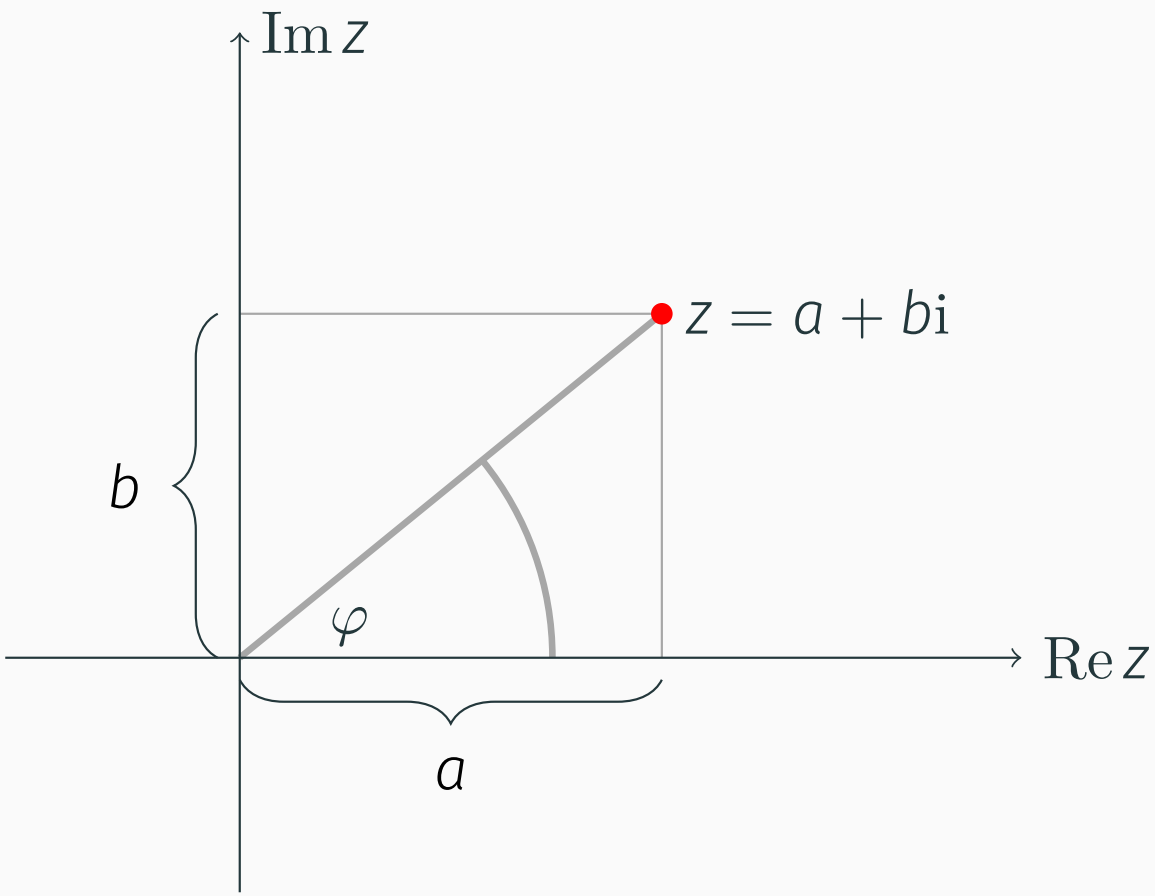
D

Komplex szám trigonometriai alakja

Ha a $z \in \mathbb{C}$ komplex szám abszolút értéke r, irányszöge φ, akkor

$$z = r(\cos\varphi + \mathrm{i}\sin\varphi).$$

Ez a trigonometriai alak.


Im z
z = a + bi
b
φ
Re z
a

T

Az algebrai és trigonometriai alakok közti kapcsolat

Ha $z = a + b\mathrm{i} = r(\cos\varphi + \mathrm{i}\sin\varphi)$, akkor

$$a = r\cos\varphi \tag{1}$$

$$b = r\sin\varphi \tag{2}$$

$$r = |z| = \sqrt{a^2 + b^2} = \sqrt{z\bar{z}} \tag{3}$$

$$\operatorname{tg}\varphi = \frac{b}{a} \text{ ha } a \neq 0, \quad \operatorname{ctg}\varphi = \frac{a}{b} \text{ ha } b \neq 0 \tag{4}$$

B Az első két egyenlőség az $a + b\mathrm{i} = r(\cos\varphi + \mathrm{i}\sin\varphi)$ egyenlőségből azonnal adódik.

- Az r értéke a $z\bar{z} = (a + ib)(a - ib) = a^2 + b^2$ összefüggés következménye.
- A $\operatorname{tg}\varphi$ és a $\operatorname{ctg}\varphi$ értéke leolvasható a számsíkról.

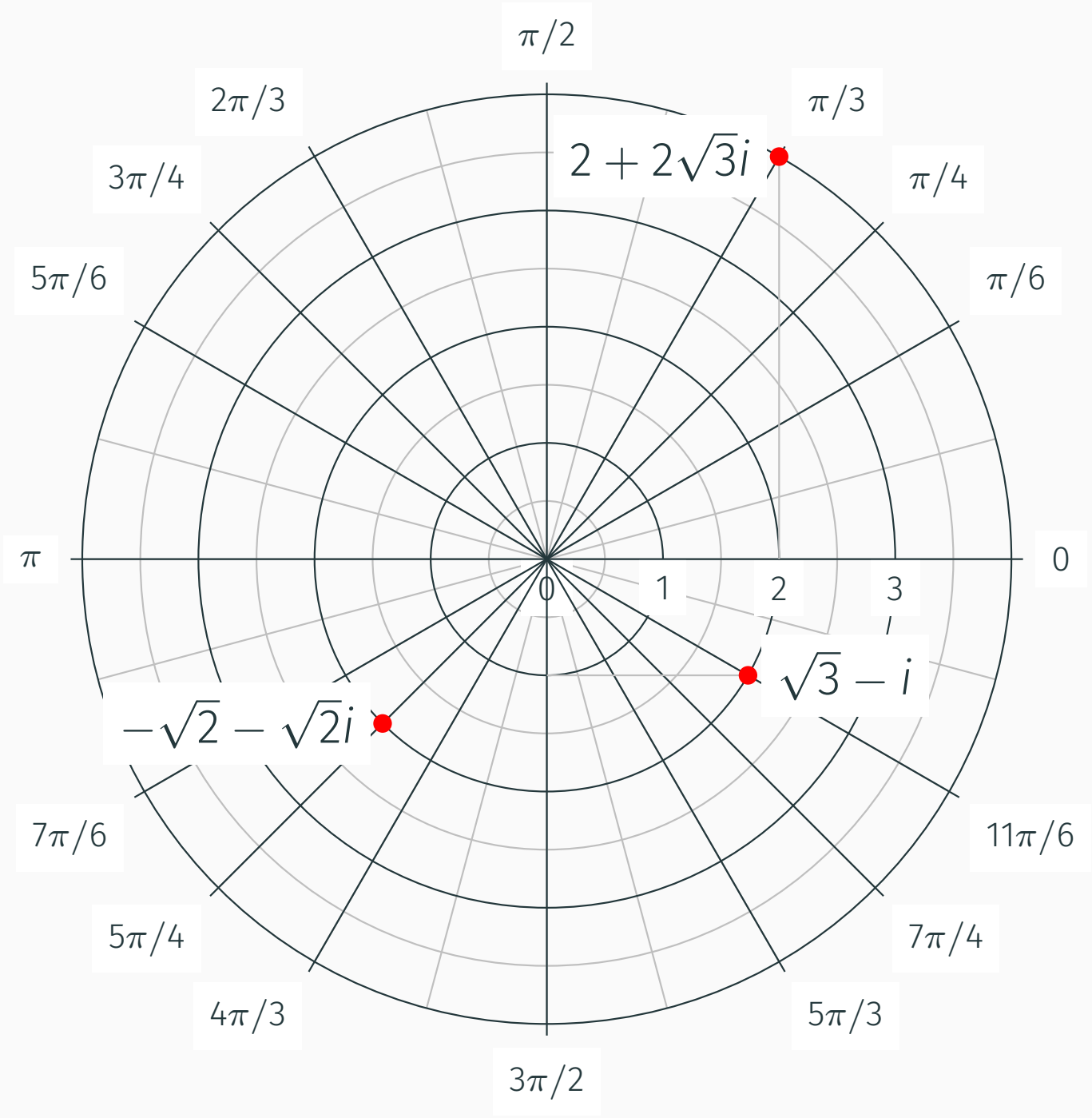
Az algebrai és trigonometriai alak kapcsolata

P **Példa**

Írjuk fel a $2+2\sqrt{3}\mathrm{i}$, $-\sqrt{2}-\sqrt{2}\mathrm{i}$, $\sqrt{3}-\mathrm{i}$ komplex számok trigonometriai alakját, és ábrázoljuk mindegyiket a komplex számsíkon!

M $|2+2\sqrt{3}\mathrm{i}| = \sqrt{2^2+(2\sqrt{3})^2} = \sqrt{4+12} = 4$, a φ irányszögre: $\operatorname{tg}\varphi = \frac{2\sqrt{3}}{2} = \sqrt{3}$, és mivel a komplex szám a számsík első negyedébe esik, ezért $\varphi = \frac{\pi}{3} \rightsquigarrow 2+2\sqrt{3}\mathrm{i} = 4(\cos\frac{\pi}{3} + \mathrm{i}\sin\frac{\pi}{3})$.

- $|-\sqrt{2}-\sqrt{2}\mathrm{i}| = \sqrt{(-\sqrt{2})^2+(-\sqrt{2})^2} = \sqrt{2+2} = 2$. $\operatorname{tg}\varphi = \frac{-\sqrt{2}}{-\sqrt{2}} = 1$, a komplex szám a számsík harmadik negyedébe esik, ezért $\varphi = \frac{5\pi}{4}$: $-\sqrt{2}-\sqrt{2}\mathrm{i} = 2(\cos\frac{5\pi}{4} + \mathrm{i}\sin\frac{5\pi}{4})$.
- $|\sqrt{3}-\mathrm{i}| = \sqrt{3+1} = 2$. $\operatorname{tg}\varphi = -\frac{1}{\sqrt{3}}$, de a komplex szám a számsík negyedik negyedébe esik, ezért $\varphi = -\frac{\pi}{6}$, vagy a $[0, 2\pi)$ intervallumból $\varphi = \frac{11\pi}{6} \rightsquigarrow \sqrt{3}-\mathrm{i} = 2\left(\cos\frac{11\pi}{6} + \mathrm{i}\sin\frac{11\pi}{6}\right)$.


π/2
2π/3
π/3
3π/4
π/4
5π/6
π/6
π
0
0
1
2
3
$2+2\sqrt{3}i$
$\sqrt{3}-i$
$-\sqrt{2}-\sqrt{2}i$
7π/6
11π/6
5π/4
7π/4
4π/3
5π/3
3π/2

A trigonometriai alak tulajdonságai

T **Szorzás, osztás trigonometriai alakban**

Legyen $z_1 = r_1(\cos\varphi_1 + \mathrm{i}\sin\varphi_1)$, $z_2 = r_2(\cos\varphi_2 + \mathrm{i}\sin\varphi_2)$. Ekkor

$$z_1 z_2 = r_1 r_2(\cos(\varphi_1 + \varphi_2) + \mathrm{i}\sin(\varphi_1 + \varphi_2)),$$
$$\frac{z_1}{z_2} = \frac{r_1}{r_2}(\cos(\varphi_1 - \varphi_2) + \mathrm{i}\sin(\varphi_1 - \varphi_2))$$

M A szögek összegére vonatkozó trigonometriai azonosságokból:

$$\begin{aligned} z_1 z_2 &= r_1(\cos\varphi_1 + \mathrm{i}\sin\varphi_1)\cdot r_2(\cos\varphi_2 + \mathrm{i}\sin\varphi_2) \\ &= r_1 r_2(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2 + \\ &\qquad \mathrm{i}(\sin\varphi_1\cos\varphi_2 + \cos\varphi_1\sin\varphi_2)) \\ &= r_1 r_2\left(\cos(\varphi_1 + \varphi_2) + \mathrm{i}\sin(\varphi_1 + \varphi_2)\right) \end{aligned}$$

Az osztás hasonlóan bizonyítható.

T

Abszolút érték tulajdonságai

Legyen $z, z_1, z_2 \in \mathbb{C}$. Ekkor

1. $|\bar{z}| = |z|$
2. $|z_1 z_2| = |z_1||z_2|$
3. $|z_1/z_2| = |z_1|/|z_2|$
4. $|z_1 + z_2| \leq |z_1| + |z_2|$ (háromszög-egyenlőtlenség)

B $|\bar{z}| = |a - b\mathrm{i}| = \sqrt{a^2 + b^2} = |a + b\mathrm{i}| = |z|$.

- $|z_1| = r_1$, $|z_2| = r_2$, így az előző tételből $|z_1 z_2| = r_1 r_2 = |z_1||z_2|$ és $|z_1/z_2| = r_1/r_2 = |z_1|/|z_2|$.
- Azonnal következik az $\mathbb{R}^2$-re vonatkozó háromszög-egyenlőtlenségből.

Hatványozás, gyökvonás trigonometriai alakkal

D **Komplex szám gyöke**

Ha $z \in \mathbb{C}$ és $n \in \mathbb{N}^+$, akkor $\sqrt[n]{z} = \{w \in \mathbb{C} : w^n = z\}$, azaz a z komplex szám komplex n-edik gyökén azon w számok halmazát értjük, melyekre $w^n = z$. (nem egyértékű!)

T **Hatványozás, gyökvonás kiszámítása**

Legyen $z = r(\cos\varphi + i\sin\varphi)$. Ekkor

$$z^{-1} = r^{-1}(\cos(-\varphi) + i\sin(-\varphi)) = r^{-1}(\cos\varphi - i\sin\varphi)$$

$$z^n = (r(\cos\varphi + i\sin\varphi))^n = r^n(\cos n\varphi + i\sin n\varphi), \quad n \in \mathbb{Z}$$

$$\sqrt[n]{z} = \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right),\ n \in \mathbb{N}^+,\ k = 0, \ldots, n-1,$$

ahol $\sqrt[n]{\ }$ a komplex, $\sqrt[n]{\ }$ a valós n-edik gyökvonás művelete (és k végigfuthat egészek bármely más n-elemű halmazán, n-nel osztva különböző maradékokat adnak).

B Legyen $z = r(\cos\varphi + i\sin\varphi)$. L! $n \in \mathbb{N}^+$ pozitív egész. A $z^n = r^n\,(\cos n\varphi + i\sin n\varphi)$ képlet a szorzási szabály n-szeri alkalmazásából adódik.

- L! $n = -1$: $z^{-1} = \frac{1}{z}$, így a trigonometrikus alakba felírt számok osztására vonatkozó szabály szerint

$$z^{-1} = \frac{1\,(\cos 0 + \mathrm{i}\sin 0)}{r(\cos\varphi + \mathrm{i}\sin\varphi)} = r^{-1}(\cos(-\varphi) + \mathrm{i}\sin(-\varphi))$$

- L! $n < 0$ és $m = -n > 0$.

$$z^n = z^{-m} = \frac{1}{z^m} = \frac{1\,(\cos 0 + \mathrm{i}\sin 0)}{r^m(\cos m\varphi + \mathrm{i}\sin m\varphi)}$$

$$= r^{-m}(\cos(-m\varphi) + \mathrm{i}\sin(-m\varphi)) = r^n(\cos n\varphi + \mathrm{i}\sin n\varphi)$$

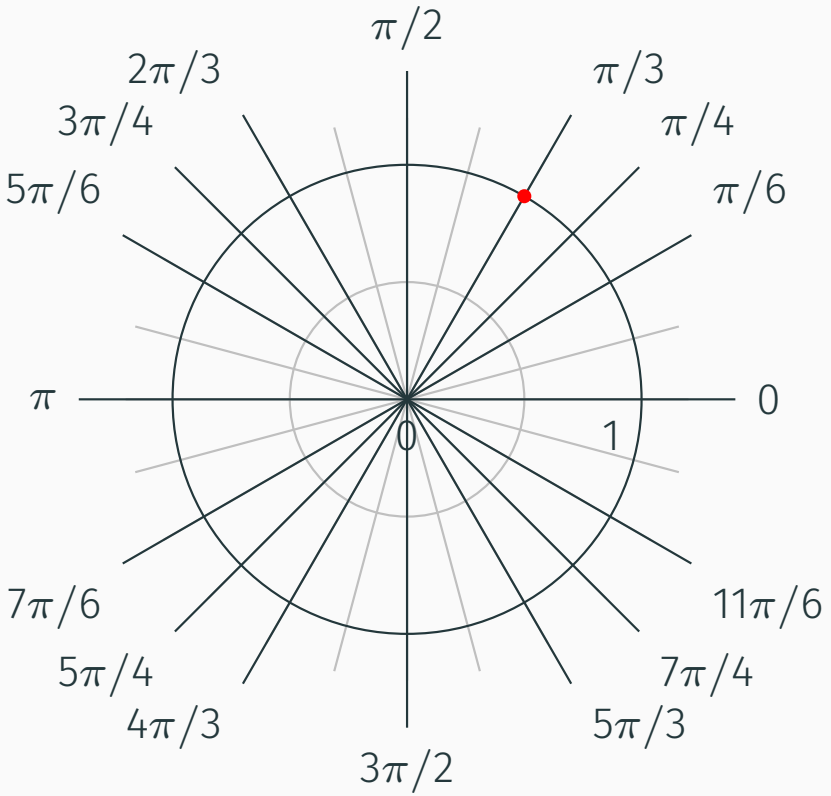
- Legyen $w = R(\cos\alpha + i\sin\alpha)$ és $w^n = z$.
- Ekkor $R^n(\cos(n\alpha) + i\sin(n\alpha)) = r(\cos\varphi + i\sin\varphi)$ ahonnan $R = \sqrt[n]{r}$, $n\alpha = \varphi + 2k\pi$, azaz $\alpha = \frac{1}{n}(\varphi + 2k\pi)$. Ha $\frac{1}{n}(\varphi + 2k\pi)$ és $\frac{1}{n}(\varphi + 2\ell\pi)$ azonos szögek, akkor $(\frac{k}{n} - \frac{\ell}{n})2\pi$ a 2π egész számú többszöröse, így $\frac{k}{n} - \frac{\ell}{n}$ egész, tehát k és ℓ azonos maradékot ad

P Hatványozás: Számítsuk ki

$$\left(\frac{1}{2}+\frac{\sqrt{3}}{2}i\right)^{100}$$

értékét!

M $\frac{1}{2}+\frac{\sqrt{3}}{2}i$ trigonometriai alakja: $\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}$.



- A hatványozás képletét alkalmazva:

$$\left(\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}\right)^{100}=\cos\frac{100\pi}{3}+i\sin\frac{100\pi}{3}$$
$$=\cos\frac{4\pi}{3}+i\sin\frac{4\pi}{3}$$
$$=-\frac{1}{2}-\frac{\sqrt{3}}{2}i.$$

- Egy másik megoldási lehetőség fejben is számolható: mivel $\left(\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}\right)^6=1$, és 100-at 6-tal osztva 4 a maradék, ezért

$$\left(\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}\right)^{100}=\left(\cos\frac{\pi}{3}+i\sin\frac{\pi}{3}\right)^4$$
$$=\cos\frac{4\pi}{3}+i\sin\frac{4\pi}{3}$$
$$=-\frac{1}{2}-\frac{\sqrt{3}}{2}i.$$

P Számítsuk ki

$$\left(\sqrt{3}+i\right)^9$$

értékét!

M $\sqrt{3}+i$ hossza $\sqrt{\sqrt{3}^2+1^2}=2$, trigonometriai alakja: $2(\cos\frac{\pi}{6}+i\sin\frac{\pi}{6})$. Így

$$\begin{aligned}[2(\cos\frac{\pi}{6}+i\sin\frac{\pi}{6})]^9 &= 2^9(\cos\frac{9\pi}{6}+i\sin\frac{9\pi}{6})\\ &= 512(\cos\frac{3\pi}{2}+i\sin\frac{3\pi}{2})\\ &= -512i\end{aligned}$$

P Hatodik egységgyökök Számítsuk ki az 1 hatodik gyökeit!

M Az 1 trigonometriai alakja $1 = 1(\cos 0 + i \sin 0)$. Olyan számokat keresünk, melyek 6-odik hatványa 1, azaz olyanokat, melyekre $r^6(\cos 6\varphi + i \sin 6\varphi) = 1(\cos 0 + i \sin 0)$.

- Innen $r = 1$, és $6\varphi = 0$, de mivel 0 ugyanaz a szög, mint 2π, 4π..., ezért $6\varphi = 2\pi$, $6\varphi = 4\pi$,...$6\varphi = 10\pi$ is lehet! ($6\varphi = 12\pi$, $6\varphi = 14\pi, \ldots$ nem ad új eredményt!) Így φ lehetséges értékei: $0, \frac{\pi}{3}, \frac{2\pi}{3}, \pi, \frac{4\pi}{3}, \frac{5\pi}{3}$. A gyökök listája és azok algebrai alakja tehát

$$\cos 0 + i \sin 0 = 1, \qquad \cos \frac{\pi}{3} + i \sin \frac{\pi}{3} = \frac{1}{2} + \frac{\sqrt{3}}{2} i,$$

$$\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2} i, \qquad \cos \pi + i \sin \pi = -1,$$

$$\cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2} i, \qquad \cos \frac{5\pi}{3} + i \sin \frac{5\pi}{3} = \frac{1}{2} - \frac{\sqrt{3}}{2} i.$$

P Gyökvonás Számítsuk ki $\sqrt[5]{1+\mathrm{i}\sqrt{3}}$ értékeit!

M $z = 1 + i\sqrt{3}$ esetén $|z| = 2$, $\arg(z) = \frac{\pi}{3}$, így $z = 2\left(\cos\frac{\pi}{3} + \mathrm{i}\sin\frac{\pi}{3}\right)$.

- Egy gyök: $\sqrt[5]{2}(\cos\frac{\pi}{15} + \mathrm{i}\sin\frac{\pi}{15})$. Az összes gyök:

$$\sqrt[5]{2}(\cos(\frac{\pi}{15} + \frac{2k\pi}{5}) + \mathrm{i}\sin(\frac{\pi}{15} + \frac{2k\pi}{5}), \quad k = 0, 1, \ldots, 4.$$

Testek

Kétműveletes algebrai struktúrák

Test

A valós, a racionális és a komplex számok közös műveleti tulajdonságai vezetnek a következő absztrakcióhoz:

D **Test**

A test egy legalább két elemet tartalmazó (jelölje ezeket 0 és 1) és két bináris művelettel ($+$ és $\cdot$) ellátott $\mathbb{F}$ halmaz, melyre bármely $a, b, c, d \in \mathbb{F}$, $d \neq 0$ esetén fennállnak a következők:

$a + b = b + a$	$ab = ba$	kommutativitás
$(a + b) + c = a + (b + c)$	$(ab)c = a(bc)$	asszociativitás
$0 + a = a$	$1a = a$	zérus-/egységelem
$\exists x \in \mathbb{F}\colon a + x = 0$	$\exists y \in \mathbb{F}\colon dy = 1$	$\exists$ ellentett/reciprok
$(a + b)c = ac + bc$		disztributivitás

- Reciproka – más néven multiplikatív inverze – csak a nullától különböző elemeknek van.

Á Minden test tetszőleges a elemére igaz, hogy $0 \cdot a = a \cdot 0 = 0$. (B $0a + 0a = (0 + 0)a = 0a$)

Á Egy testnek csak egyetlen zérus- és egyetlen egységeleme van.

J Az a elem ellentettjét $-a$, reciprokát a^{-1} vagy $1/a$ jelöli.

Á $(-1) \cdot a = -a$, $-ab = (-a)b = a(-b)$.

Á $(ab)^{-1} = a^{-1}b^{-1}$.

T A valósok $\mathbb{R}$, a racionálisok $\mathbb{Q}$, a komplexek $\mathbb{C}$ halmaza a szokásos műveletekkel testet alkot.

P Testet alkotnak az $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ alakú számok.

m Nem test az $\mathbb{N}$, mivel pozitív elemeinek ellentettje nem $\mathbb{N}$-beli.

m Nem test a $\mathbb{Z}$, mivel az 1-nél nagyobb elemeinek nem létezik reciproka.

P Tekintsük a kételemű $\{0, 1\}$ halmazt és definiáljunk rajta két műveletet a következő művelettáblákkal:

$+$	0	1
0	0	1
1	1	0

$\times$	0	1
0	0	0
1	0	1

E halmaz e két művelettel testet alkot, melyet $\mathbb{Z}_2$ vagy $\mathbb{F}_2$ jelöl. (A páros és páratlan számokkal való számolásban, vagy a logikai műveletekkel összekapcsolt állításokban már találkozhattunk e testtel.)

M Egyenként ellenőrizzük a test definíciójának minden pontját! Az alsó tagozatban megismert szabályok a következő táblázatba foglalhatók:

$+$	páros	páratlan
páros	páros	páratlan
páratlan	páratlan	páros

$\times$	páros	páratlan
páros	páros	páros
páratlan	páros	páratlan

Jelölje ’h’ a hamis, ’i’ az igaz logikai értékű állítást és AND az „és”, valamint XOR (exclusive or angol kifejezésből) a „kizáró vagy” műveletét. A két művelettábla:

XOR	h	i
h	h	i
i	i	h

AND	h	i
h	h	h
i	h	i

E számítástechnikában is fontos két művelet a hamis $\leftrightarrow$ 0, igaz $\leftrightarrow$ 1, XOR $\leftrightarrow$ összeadás, AND $\leftrightarrow$ szorzás megfeleltetésekkel ismét $\mathbb{Z}_2$-t adja.

P Testet alkotnak-e $\mathbb{R}^3$ vektorai a vektorok összeadására és vektori szorzására nézve?

M Nem, hisz például a vektori szorzás nem kommutatív.

Kvaterniók

Kvaterniók: $a+bi+cj+dk$ alakú számok, ahol $a, b, c, d \in \mathbb{R}$, i, j, k olyan „imaginárius” számok, melyekre $i^2 = j^2 = k^2 = ijk = -1$, $ij = k$, $ji = -k$, $jk = i$,..., összeadás „koordinátánként”, szorzás az előző szabályok szerint: az $\mathbf{u} = u_1 i + u_2 j + u_3 k$, $\mathbf{v} = v_1 i + v_2 j + v_3 k$ jelöléssel $(a + \mathbf{u})(b + \mathbf{v}) = ab - \mathbf{u} \cdot \mathbf{v} + a\mathbf{v} + b\mathbf{u} + \mathbf{u} \times \mathbf{v}$.

Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication $i^2 = j^2 = k^2 = ijk = -1$ & cut it on a stone of this bridge

A szorzás nem kommutatív, de a többi testaxióma teljesül: a kvaterniók ferdetestet alkotnak.

D

Gyűrű

A gyűrű egy legalább egy elemet tartalmazó (jelölje ezt 0) és két bináris művelettel ($+$ és $\cdot$) ellátott R halmaz, melyre bármely $a, b, c \in R$ esetén fennállnak a következők:

$a + b = b + a$		kommutativitás
$(a + b) + c = a + (b + c)$	$(ab)c = a(bc)$	asszociativitás
$0 + a = a$		van zéruselem
$\exists x \in R\colon a + x = 0$		ellentett létezése
$(a + b)c = ac + bc$		disztributivitás

A gyűrű kommutatív, ha a szorzás kommutatív, egységelemes, ha van egységelem.

D

Nullosztómentes

Egy G gyűrű nullosztómentes, ha bármely $a, b \in G$ és $ab = 0$ esetén $a = 0$ vagy $b = 0$.

- Definíció szerint minden test gyűrű, sőt egységelemes kommutatív és nullosztómentes gyűrű.
- Egy gyűrűben bármely a elemre $0a = a0 = 0$ és $(-1)a = -a$.
- A természetes számok $\mathbb{N}$ halmaza nem gyűrű a szokásos műveletekkel (a -1 nem természetes szám).
- A páros számok kommutatív gyűrűt alkotnak, de ez a gyűrű nem egységelemes.
- A valós együtthatós polinomok egységelemes kommutatív gyűrűt alkotnak. Általában, ha R egy gyűrű, akkor az R-együtthatós polinomok gyűrűt alkotnak, amit $R[x]$ jelöl.
- Egységelemes kommutatív gyűrűt alkotnak *(1)* az $\mathbb{R} \to \mathbb{R}$ függvények, *(2)* a $[0, 1]$ intervallumon értelmezett függvények, *(3)* a $[0, 1]$ intervallumon értelmezett folytonos függvények a szokásos műveletekkel, *(4)* a végtelen sorozatok az elemenkénti összeadás és szorzás műveletére nézve.

T **Minden test nullosztómentes**

Minden test nullosztómentes.

B Indirekt: tfh van olyan test, és abban két elem, hogy $a \neq 0$, $b \neq 0$, de $ab = 0$.

Egy testben a nemnulla elemeknek van inverzük. Szorozzuk be az $ab = 0$ egyenlőséget $1/b$-vel: $ab\frac{1}{b} = 0$, azaz $a = 0$, ami ellentmondás.

Testek

Véges test

D **A mod művelet**

Legyen $a, m \in \mathbb{Z}$ egészek és legyen $m > 1$. Az a-nak m-mel való osztási maradékát $a \bmod m$ jelöli, és „a modulo m”-nek olvassuk. Az osztás maradéka nem negatív, és kisebb m-nél, tehát $0 \leqslant a \bmod m < m$.

P $12 \bmod 5 = 2$, $-3 \bmod 8 = 5$, $(8 + 6) \bmod 12 = 2$, $2^{10} \bmod 2 = 0$, $3^{10} \bmod 2 = 1$.

m Tudjuk, hogy egy páros és egy páratlan szám szorzata mindig páros, míg összege mindig páratlan. Vagyis a művelet eredményének 2-vel való osztási maradéka csak a két szám maradékától függ. Ezt általánosítjuk a következőkben.

D Ha $a, b, m \in \mathbb{Z}$, $m > 1$ és $a \bmod m = b \bmod m$ (azaz a-nak és b-nek m-mel való osztási maradékai azonosak), akkor azt mondjuk, hogy a és b kongruensek modulo m.
Jelölése: $a \equiv b \pmod{m}$ vagy egyszerűbben $a \equiv b \ (m)$.

T

Szám helyettesítése vele kongruenssel

Ha a, b, c, d, e tetszőleges egészek, $m, n > 1$ egészek, $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor

$$a + c \equiv b + d \pmod{m}$$
$$a - c \equiv b - d \pmod{m}$$
$$ac \equiv bd \pmod{m}$$
$$a^n \equiv b^n \pmod{m}.$$

m E tétel azt jelenti, hogy ha egy egész számokat tartalmazó kifejezésről csak azt akarjuk tudni, hogy mekkora maradékot ad m-mel osztva, akkor az összeadás és kivonás tagjait, a szorzás tényezőit és a pozitív egész kitevős hatványozás alapját (a kitevőjét nem!) kicseréljük egy tetszőleges, vele kongruens egészre.

D

$\mathbb{Z}_m$

Legyen $m > 1$ és tekintsük az m-elemű $\{0, 1, \ldots, m-1\}$ halmazt és elemein vezessük be a következő két műveletet:

$$a \oplus b := a + b \bmod m$$

$$a \otimes b := ab \bmod m$$

A két művelettel ellátott struktúrát $\mathbb{Z}_m$-mel jelöljük, és ha nem okoz félreértést, két műveletét is a szokásos összeadás és szorzásjellel jelöljük.

T

Tétel

$\mathbb{Z}_m$ egységelemes kommutatív gyűrű minden $m > 1$ esetén. $\mathbb{Z}_m$ pontosan akkor test, ha m prím.

P Írjuk fel $\mathbb{Z}_3$, $\mathbb{Z}_5$ és $\mathbb{Z}_6$ műveletábláit:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\times$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Összefoglalás

- A valós számok $\mathbb{R}$ teste kibővíthető az imaginárius $\mathrm{i} = \sqrt{-1}$ hozzávételével úgy, hogy a bővebb struktúra is test maradjon, tehát hogy az összeadás és szorzás műveleti tulajdonságai érvényben maradjanak. A komplex számokat tartalmazó bővebb test már nem létezik.
- Testet alkot a racionális számok $\mathbb{Q}$, a valósok $\mathbb{R}$, a komplexek $\mathbb{C}$ halmaza, és $\mathbb{Z}_p$, ha p prímszám.
- Nem test, csak gyűrű az egészek $\mathbb{Z}$ halmaza, és $\mathbb{Z}_m$, ha $m > 1$ összetett szám. ($\mathbb{N}$ nem gyűrű.)