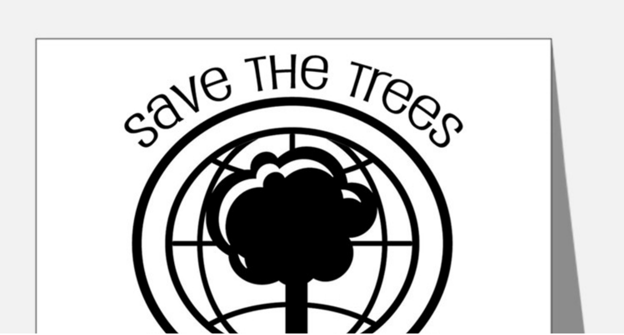
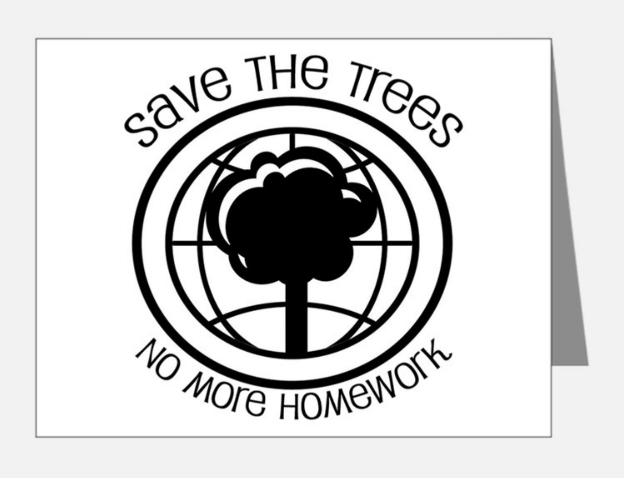
Algebra és számelmélet előadás

Waldhauser Tamás
2016. szeptember 22.


save THE Trees


Save The Trees
No More Homework

Házi feladat a gyakorlatra

7. feladat. Egységgyökök-e a következő komplex számok, és ha igen, akkor hányadik egységgyökök?

(a) $\frac{1}{2}+\frac{1}{2}i$ (nem), $\quad -\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$ $(8, 16, 24, \dots)$, $\quad \operatorname{cis}\frac{5\pi}{12}$ $(24, 48, 72, \dots)$

(b) $\operatorname{cis}\sqrt{2}$ (nem), $\quad -\frac{1}{2}+\frac{\sqrt{3}}{2}i$ $(3, 6, 9, \dots)$

(c) $-\frac{1}{2}+\frac{\sqrt{2}}{2}i$

(d) $-\frac{\sqrt{3}}{2}+\frac{1}{2}i$

(e) $\operatorname{cis}\frac{6\pi}{7}$

Harmadik házi feladat az előadásra

Készítsen Wolfram Mathematica-ban dinamikus vizualizációt, ami az $(a+bi)^k$ komplex számokat ábrázolja a Gauss-féle számsíkon $k = 1, 2, \ldots, n$ esetén. Az $a, b \in \mathbb{R}$ és $n \in \mathbb{N}$ paramétereket dinamikusan lehessen változtatni (pl. csúszkával).

- beküldendő emailben: `twaldha@math.u-szeged.hu`
- Mathematica notebook legyen
- fájlnév: `EHA-eahf3.nb` (például `WATHAAS-eahf3.nb`)
- határidő: október 5, reggel 8 óra

Házi feladat a gyakorlatra

8. feladat. Döntse el, hogy igazak-e az alábbi állítások. A választ minden esetben indokolni kell!

(a) Van olyan z komplex szám, amelyre $\operatorname{Re} z = 1$ és $|z - i| = 3$.

Igaz, pl. $z = 1 + \left(2\sqrt{2} + 1\right) i$.

(b) Tetszőleges $z \in \mathbb{C}$ és $n \in \mathbb{N}$ esetén, ha $\sqrt[n]{z}$ értékei között van valós szám, akkor z is valós.

Igaz, mert, ha $u \in \mathbb{R}$ egy n-edik gyöke z-nek, akkor $z = u^n \in \mathbb{R}$.

(c) Tetszőleges $z \in \mathbb{C}$ esetén, ha z^2 harmadik egységgyök, akkor z is harmadik egységgyök.

(d) Tetszőleges $z, w \in \mathbb{C}$ esetén $|z + w| = |z| + |w|$.

(e) Van olyan z komplex szám, amelyre $\operatorname{Re} z = 2$ és $|z| = 1$.

2. Absztrakt algebrai struktúrák

Csoport, gyűrű, integritástartomány, test

Gyűrűk

2.1. Definíció.

Ha egy nemüres R halmazon kettő kétváltozós művelet is értelmezve van (nevezzük az egyiket összeadásnak, a másikat szorzásnak) úgy, hogy $(R;+)$ Abel-csoport, $(R;\cdot)$ félcsoport, és a szorzás disztributív az összeadásra, akkor az $(R;+,\cdot)$ struktúrát *gyűrűnek* nevezzük.

Megjegyzés.

Adott R halmaz és $+$, $\cdot$ műveletek esetén tehát a következőket kell ellenőrizni, hogy meggyőződjünk róla, hogy $(R;+,\cdot)$ gyűrű:

0. a $+$, $\cdot$ műveletek valóban értelmezettek az R halmazon;
1. az összeadás asszociatív;
2. az összeadás kommutatív;
3. létezik additív egységelem;
4. minden elemnek létezik additív inverze;
5. a szorzás asszociatív;
6. a szorzás disztributív az összeadásra.

Gyűrűk

2.2. Definíció.

Az $(R;+)$ csoportot az $(R;+,\cdot)$ gyűrű *additív csoportjának* nevezzük, és ennek megfelelően beszélhetünk *additív egységelemről* és *additív inverzről* is. Az $(R;\cdot)$ félcsoport neve: a gyűrű *multiplikatív félcsoportja*.

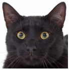
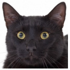
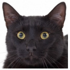
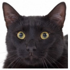
Jelölés.

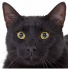
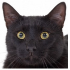
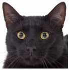
Tetszőleges gyűrűben 0 jelöli az additív egységelemet, az a gyűrűelem additív inverzét pedig $-a$ jelöli, és értelmezhetjük a kivonás műveletét a $b-a=b+(-a)$ képlettel.

2.3. Állítás.

Ha $(R;+,\cdot)$ gyűrű, akkor minden $a \in R$ esetén $a\cdot 0 = 0\cdot a = 0$ teljesül.

Izomiaúrfizmus

$+$		
		
		

$\cdot$		
		
		

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Testek

2.4. Definíció.

Testnek nevezünk egy $(T; +, \cdot)$ gyűrűt, ha $(T \setminus \{0\}; \cdot)$ Abel-csoport (ebből következik, hogy $|T| \geq 2$).

Megjegyzés.

Adott $(T; +, \cdot)$ gyűrű esetén tehát a következőket kell ellenőrizni, hogy meggyőződjünk róla, hogy $(T; +, \cdot)$ test:

7. a nemzéró elemek halmaza nem üres, és zárt a szorzásra;
8. a szorzás kommutatív;
9. létezik multiplikatív egységelem;
10. minden nemzéró elemnek létezik multiplikatív inverze.

Megjegyzés.

A 7. pontból a zártsági feltétel elhagyható, mert következik a többiből.

~~Harmadik házi feladat az előadásra~~

2.5. Definíció.

Ha egy gyűrűben nemcsak az összeadás, hanem a szorzás is kommutatív, akkor *kommutatív gyűrűnek* nevezzük. Ha pedig nemcsak additív, de *multiplikatív egységelem* is létezik (amelyet általában 1 jelöl), akkor *egységelemes gyűrűről* beszélünk.

Bizonyítsa be, hogy ha egy egységelemes gyűrűben az additiív és a multiplikatív egységelem megegyezik (azaz $0 = 1$), akkor a gyűrűnek csak egyetlen eleme van.

- beküldendő emailben: `twaldha@math.u-szeged.hu`
- pdf fájl legyen (lehet szkennelt is)
- fájlnév: `EHA-eahf3.pdf` (például `WATHAAS-eahf3.pdf`)
- határidő: október 5, reggel 8 óra

Egységek

2.6. Definíció.

Legyen R egységelemes gyűrű. Az $a \in R$ elemet *egységnek* nevezzük, ha létezik *multiplikatív inverze*, azaz létezik olyan $a^{-1} \in R$ elem, amelyre $aa^{-1} = a^{-1}a = 1$ teljesül.

2.7. Tétel.

Az egységek bármely egységelemes gyűrűben csoportot alkotnak a szorzás műveletére nézve.

2.8. Definíció.

Az R gyűrű egységeinek multiplikatív csoportját R *egységcsoportjának* nevezzük és R^*-gal jelöljük.

2.9. Definíció.

Ha T test, akkor a $(T^*; \cdot) = (T \setminus \{0\}; \cdot)$ Abel-csoportot a T test *multiplikatív csoportjának* hívjuk.

Integritástartományok

2.10. Definíció.

Ha egy gyűrű a, b elemeire $ab = 0$ teljesül, de se a, se b nem nulla, akkor azt mondjuk, hogy a és b *zérusosztók*.
Ha egy gyűrűben nincsenek zérusosztók (azaz nullától különböző elemek szorzata sosem nulla), akkor *zérusosztómentes gyűrűnek* nevezzük.
A kommutatív, egységelemes, zérusosztómentes gyűrű neve *integritástartomány*.

Megjegyzés.

Az integritástartomány definíciójában szokás még feltenni azt is, hogy $1 \neq 0$, vagyis az egyelemű $\{0\}$ gyűrűt nem (mindig) tekintjük integritástartománynak.

2.11. Állítás.

Integritástartományban lehet nemzéró elemmel egyszerűsíteni, azaz tetszőleges $a, b, c \ (c \neq 0)$ elemekre

$$ac = bc \implies a = b.$$

2.12. Állítás.

Minden test integritástartomány.

Számgyűrűk és számtestek

Megjegyzés.

Adott $H \subseteq \mathbb{C}$ számhalmaz esetén a gyűrű (test) definíciójából sok minden automatikusan teljesül a szokásos összeadás és szorzás műveletére.

Ezért elegendő az alábbiakat ellenőrizni:

$$\left.\begin{array}{l} \left.\begin{array}{r} \left.\begin{array}{r} \forall a, b \in H:\ \ a+b \in H \text{ és } ab \in H \\ 0 \in H \\ \forall a \in H:\ \ -a \in H \end{array}\right\} \text{gyűrű} \\ 1 \in H \end{array}\right\} \text{int. tart.} \\ \forall a \in H \setminus \{0\}:\ \ a^{-1} \in H \end{array}\right\} \text{test}$$

(Ellen)példák

Példa.

Az alábbi halmazok közül melyek alkotnak gyűrűt, integritástartományt, testet a szokásos összeadás és szorzás műveletével?

- $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$: test
- $\mathbb{Z}$: integritástartomány (egységcsoportja: $\{1, -1\}$)
- $\mathbb{R}^+$, $\mathbb{Q}^+$, $\mathbb{N}$: nem is gyűrű
- $\{$páros számok$\}$: kommutatív, zérusosztómentes gyűrű
- $\{$páratlan számok$\}$: nem is gyűrű
- $\{$irracionális számok$\}$: nem is gyűrű
- $\{$véges tizedestörtek$\}$: integritástartomány (mi az egységcsoportja?)
- $\mathbb{R}^{n \times n}$: egységelemes gyűrű (egységcsoportja: $\mathrm{GL}_n(\mathbb{R})$)
- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$: integritástartomány (mi az egységcsoportja?)

Házi feladat a gyakorlatra

9. feladat. Döntse el, hogy gyűrűt, integritástartományt, illetve testet alkotnak-e az alábbi számhalmazok a szokásos összeadás és szorzás műveletével.

(a) $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ test

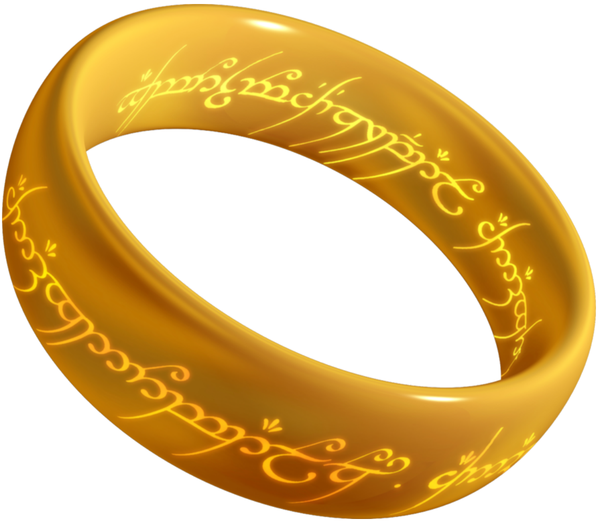
(b) $\{a + bi : a, b \in \mathbb{Z}$ és a is és b is páros$\}$ gyűrű

(c) $\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} : a, b \in \mathbb{Z}\right\}$

(d) $\{a + bi : a, b \in \mathbb{Z}$ és a páros$\}$

(e) $\{a + bi : a, b \in \mathbb{Z}$ és b páros$\}$

Nevezetes gyűrűk



Maradékosztály-gyűrűk

2.13. Állítás.

- Minden $m \geq 2$ egész szám esetén a modulo m maradékosztályok egységelemes kommutatív gyűrűt alkotnak.
- A $\mathbb{Z}_m$ gyűrű egységei éppen a redukált maradékosztályok (innen a $\mathbb{Z}_m^*$ jelölés).
- Ha m prímszám, akkor $\mathbb{Z}_m$ test, ha m nem prím, akkor $\mathbb{Z}_m$ még csak nem is integritástartomány.

2.14. Definíció.

A $\mathbb{Z}_m$ gyűrű neve modulo m *maradékosztály-gyűrű*, illetve prím modulus esetén *maradékosztálytest*.

Gauss-egészek

2.15. Definíció.

Gauss-egészeknek nevezzük azokat a komplex számokat, melyeknek valós és képzetes része is egész szám. A Gauss-egészek halmazát $\mathbb{Z}[i]$ jelöli:

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

2.16. Állítás.

A Gauss-egészek a komplex számok szokásos összeadásával és szorzásával integritástartományt alkotnak.

2.17. Állítás.

A Gauss-egészek gyűrűjében az egységek éppen a negyedik egységgyökök:

$$\mathbb{Z}[i]^* = \{1, -1, i, -i\}.$$