Klasszikus algebra előadás

Waldhauser Tamás
2014. február 24.

Gyűrűk

2.7. Definíció.

Ha egy nemüres halmazon kettő kétváltozós művelet is értelmezve van (nevezzük az egyiket összeadásnak, a másikat szorzásnak) úgy, hogy az alaphalmaz az összeadás műveletével kommutatív csoportot, a szorzás műveletével pedig félcsoportot alkot, és a szorzás disztributív az összeadásra, akkor ezt a kétműveletes struktúrát *gyűrű*nek nevezzük. Formálisan: $(R; +, \cdot)$ gyűrű, ha R nemüres halmaz, és

(1) $(R; +)$ Abel-csoport;

(2) $(R; \cdot)$ félcsoport;

(3) $\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c$ és $(b + c) \cdot a = b \cdot a + c \cdot a$.

2.8. Definíció.

Az $(R; +)$ csoportot az $(R; +, \cdot)$ gyűrű *additív csoport*jának, nevezzük, és ennek megfelelően beszélhetünk *additív egységelem*ről és *additív inverz*ről is.
Az $(R; \cdot)$ félcsoportot neve: a gyűrű *multiplikatív félcsoport*ja.

(Ellen)példák gyűrűkre

- $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$: gyűrű
- $\mathbb{Z}$: gyűrű
- $\mathbb{R}^+$, $\mathbb{Q}^+$, $\mathbb{N}$: nem gyűrű (nem zárt $-$-ra)
- $\{$páros számok$\}$: gyűrű
- $\{$páratlan számok$\}$: nem gyűrű (nem zárt $+, -$-ra)
- $\{$irracionális számok$\}$: nem gyűrű (nem zárt $+, -, \cdot$-ra)
- $\{$véges tizedestörtek$\}$: gyűrű
- $\mathbb{R}^{n\times n}$: gyűrű

Számolás gyűrűkben

Jelölés.

Korábbi megállapodásunknak megfelelően 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.

2.9. Állítás.

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

2.10. Megjegyzés.

Sok hasonló, az egész számokkal végzett műveleteknél megszokott tulajdonság érvényes tetszőleges gyűrűben, például

$$a\,(b - c) = ab - ac, \qquad -\,(ab) = (-a)\,b = a\,(-b)\,.$$

De vigyázat: a szorzás általában nem kommutatív, így például
$(a + b)\,(a - b) = a^2 - b^2$ vagy $(a + b)^2 = a^2 + 2ab + b^2$
már *nem* teljesül minden gyűrűben!

Integritástartományok

2.11. Definíció.

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

2.12. Definíció.

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

2.13. Állítás.

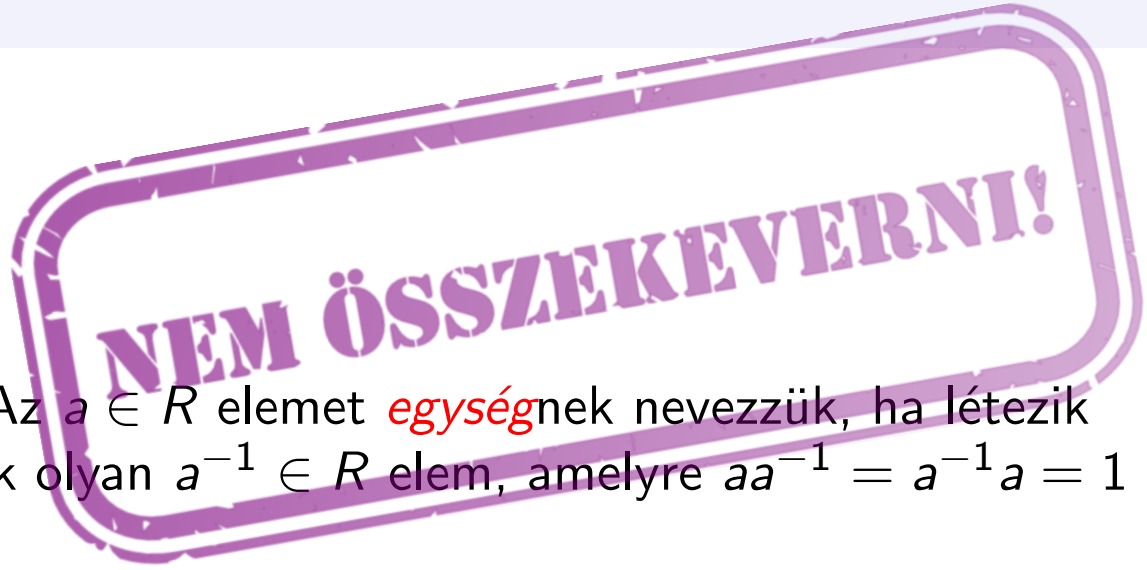
Integritástartományban lehet nemzéró elemmel egyszerűsíteni, azaz tetszőleges $a, b, c \ (c \neq 0)$ *elemekre*

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

(Ellen)példák integritástartományokra

- $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$: integritástartomány
- $\mathbb{Z}$: integritástartomány
- $\mathbb{R}^+$, $\mathbb{Q}^+$, $\mathbb{N}$: nem is gyűrű
- $\{$páros számok$\}$: *csak* kommutatív, zérusosztómentes gyűrű (nem egységelemes)
- $\{$páratlan számok$\}$: nem is gyűrű
- $\{$irracionális számok$\}$: nem is gyűrű
- $\{$véges tizedestörtek$\}$: integritástartomány
- $\mathbb{R}^{n\times n}$: *csak* egységelemes gyűrű (nem kommutatív és nem zérusosztómentes)

Egységek



2.14. Definíció.

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

2.15. Tétel.

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

2.16. Definíció.

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

Testek

2.17. Definíció.

*Test*nek nevezünk egy integritástartományt, ha legalább kételemű, és minden nemnulla elemének van multiplikatív inverze.

2.18. Definíció.

Ha T test, akkor $(T \setminus \{0\}; \cdot)$ Abel-csoport, amelyet a T test *multiplikatív csoport*jának hívjuk.

2.19. Megjegyzés.

A definíció alapján világos, hogy egy legalább kételemű R kommutatív egységelemes gyűrű akkor és csak akkor test, ha egységcsoportja a nulla kivételével minden elemet tartalmaz, azaz $R^* = R \setminus \{0\}$.

Jelölés.

Mivel gyűrűben és testben a két műveletet általában $+$ és $\cdot$ jelöli, ezeket nem írjuk mindig ki, tehát $(R; +, \cdot)$ illetve $(T; +, \cdot)$ helyett egyszerűen csak R gyűrűről, illetve T testről beszélünk.

(Ellen)példák testekre

- $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$: test
- $\mathbb{Z}$: *csak* integritástartomány (egységcsoportja: $\{1, -1\}$)
- $\mathbb{R}^+$, $\mathbb{Q}^+$, $\mathbb{N}$: nem is gyűrű
- $\{$páros számok$\}$: nem is integritástartomány
- $\{$páratlan számok$\}$: nem is gyűrű
- $\{$irracionális számok$\}$: nem is gyűrű
- $\{$véges tizedestörtek$\}$: *csak* integritástartomány (mi az egységcsoportja?)
- $\mathbb{R}^{n\times n}$: nem is integritástartomány (egységcsoportja: $\mathrm{GL}_n(\mathbb{R})$)

Ré(s)zgyűrűk és altestek

2.20. Definíció.

Legyen R egy gyűrű és $S \subseteq R$. Ha S az R-ből „örökölt” műveletekkel maga is gyűrű, akkor azt mondjuk, hogy S *részgyűrű*je az R gyűrűnek. Hasonlóan definiálható a *résztest*, *részcsoport*, *részfélcsoport* fogalma is.

Példa.

- $(\mathbb{Z}; +)$ részcsoportja a $(\mathbb{C}; +)$ csoportnak
- $(\mathbb{N}; +)$ részfélcsoportja a $(\mathbb{C}; +)$ csoportnak
- $(\mathbb{Z}; \cdot)$ részfélcsoportja a $(\mathbb{C}; \cdot)$ félcsoportnak
- $(\mathbb{Q}^+; \cdot)$ részcsoportja az $(\mathbb{R}^*; \cdot)$ csoportnak
- $(\mathrm{GL}_n(\mathbb{R}); \cdot)$ részcsoportja az $(\mathbb{R}^{n\times n}; \cdot)$ félcsoportnak
- $(S_A; \circ)$ részcsoportja a $(T_A; \circ)$ félcsoportnak
- $(\mathbb{Z}; +, \cdot)$ részgyűrűje a $(\mathbb{C}; +, \cdot)$ testnek
- $(\mathbb{Q}; +, \cdot)$ részteste a $(\mathbb{C}; +, \cdot)$ testnek

Maradékosztály-gyűrűk

2.21. 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.*

2.22. Definíció.

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

Gauss-egészek

2.23. Definíció.

*Gauss-egész*eknek nevezzük azokat a komplex számokat, melyeknek valós és képzetes része is egész szám.

Jelölés.

A Gauss-egészek halmazát $\mathbb{Z}[i]$ jelöli: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

2.24. Állítás.

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

2.25. Állítás.

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

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