Gyűrűk és testek.

Klukovits Lajos

TTIK Bolyai Intézet

2020. október 2.

Félcsoport, csoport.

Definíció.

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

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

Megjegyzés. Ha csak a művelet asszociatív voltát követeljük meg, akkor a $(G, \cdot)$ algebra **félcsoport**. Ha van egységeleme, akkor egységelemes félcsoportnak nevezzük.

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

Unicitások.

Tétel.

Félcsoportban egyetlen egységelem létezhet, és bármely elemnek legföljebb egy inverze lehet.

Bizonyítás.

Legyen S egységelemes félcsoport, amelyben $e, e' \in S$ egységelemek. Ekkor

$$e = ee' = e',$$

továbbá, ha valamely $a \in S$-re

$$aa' = a'a = aa'' = a''a = e,$$

akkor

$$a' = a'e = a'(aa''') = (a'a)a'' = ea''' .$$

Gyűrű, test.

Definíciók.

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.

Gyűrű, test.

Példák gyűrűkre.

1. $(\mathbb{Z}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$, $(\mathbb{C}; +, \cdot)$;
2. $(\mathbb{Z}_n; +, \cdot)$, $(n \in \mathbb{N})$,
3. $\mathcal{M}_n(\mathbb{R}) = (\mathbb{R}^{n\times n}; +, \cdot)$, a valós számtest fölötti $n \times n$-es teljes mátrixgyűrű;
4. $(\mathcal{P}(U); \triangle, \cap)$, U részhalmazai gyűrűje;
5. $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, $\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z},\ \alpha^3 = 1, \alpha \neq 1\}$, a Gauss-, ill. az Euler egészek gyűrűje.

Gyűrű, test.

Igazoljuk, hogy $\mathbb{Z}[\alpha]$ egységelemes, kommutatív gyűrű..

Mivel $\mathbb{Z}[\alpha] \subseteq \mathbb{C}$, csak a műveletekre zártságot kell igazolni.

Az összeadásra vonatkozó zártság nyilvánvaló.

Ha $a + b\alpha, c + d\alpha \in \mathbb{Z}[\alpha]$, akkor

$$(a + b\alpha)(c + d\alpha) = ac + \alpha(b + d) + (\alpha)^2 bd.$$

Mivel α az $x^2 + x + 1 = 0$ egyenlet egyik gyöke kapjuk, hogy $(\alpha)^2 = -1 - \alpha$, amiből már adódik a szorzásra való zártság.

Gyűrű, test.

Zérusosztó.

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

Példák.

1. Az előbbi példákban az (1) alattiak zérusosztómentesek.
2. A $\mathbb{Z}_6$ maradékosztálygyűrűben $\overline{2}, \overline{3}$ zérusosztók.
3. A teljes mátrixgyűrűk sem zérusosztómentesek. Hasznos gyakorló feladat a zérusosztó keresés pl. az $\mathcal{M}_2(\mathbb{R})$ gyűrűben.
4. A Gauss-, Euler egészek gyűrűje zérusosztómentesek.

Gyűrű, test.

Definíció.

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

Számelmélet integritástartományokban 1.

Oszthatóság.

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

Inverz egyértelműsége.

Ha $a, c \in R$ az előbbi definícióbeliek, akkor egyrészt a szorzás kommutatív volta miatt a $ca = 1$ egyenlőség is fönnáll, másrészt ha $c' \in R$ olyan, hogy $ac' = c'a = 1$, akkor $c = c'$.

Tétel.

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

Számelmélet integritástartományokban 2.

Az oszthatóság tulajdonságai integritástartományokban.

1. Egyetlen különbség van az egész számokra megismertekhez képest.
2. Bármely a, b elemre

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

3. Ha $a|b$ és $b|a$, akkor a, b **asszociáltak.**
4. Az asszociáltság ekvivalenciareláció.

Legnagyobb közös osztó.

Legyen R integritástartomány, $a, b \in R$. Azt mondjuk, hogy $c \in R$ az a, b elemek egy **legnagyobb közös osztója**, ha $c|a$ és $c|b$, továbbá valahányszor egy $d \in R$-re $d|a$ és $d|b$, mindannyiszor $d|c$. Másképpen mondva: a legnagyobb közös osztó egy olyan közös osztó, amelynek mindegyik közös osztó osztója.

Számelmélet integritástartományokban 3.

Fontos!

Az egész számok gyűrűjében bármely két számnak van legnagyobb közös osztója kivéve, ha mindkettő zéró. Ez általában nem igaz.

Egy példa.

A $\mathbb{Z}[i\sqrt{5}]$ gyűrűben a 9 és $3(2 + i\sqrt{5})$ elempárnak nincs legnagyobb közös osztója. Ugyanis:

a 9 osztói: $\pm 1, \pm 3, \pm 9, \pm(2 \pm i\sqrt{5})$,

a $3(2 + i\sqrt{5})$ osztói: $\pm 1, \pm 3, \pm(2 + i\sqrt{5}), \pm 3(2 + i\sqrt{5})$.

a közösek: $\pm 1, \pm 3, \pm(2 + i\sqrt{5})$.

Nincs közöttük olyan, amelyik az összes többinek osztója lenne.

Nincs általános módszer egy integritástartományban a legnagyobb közös osztó meghatározására.

Faktorizáció integritástartományokban 1.

Definíció

Legyen R integritástartomány. Azt mondjuk, hogy valamely nemzéró $q \in R$ **irreducibilis** R**-ben**, ha $q \nmid 1$ (nem egység) és valahányszor $q = ab$ valamely $a, b \in R$-re, mindannyiszor $a|1$ vagy $b|1$. A $p \in R$ **prím** R**-ben,** ha $p \neq 0$ és $p \nmid 1$, továbbá tetszőleges $a, b \in R$-re $p|ab$ maga után vonja, hogy $p|a$ vagy $p|b$.

Megjegyzések.

1. Gyakran használjuk az irreducibilis-elem, ill. prímelem megnevezéseket is.
2. Lényeges, hogy mely integritástartományt vesszük alapul. Az 5 irreducibilis a $\mathbb{Z}$ gyűrűben, de $\mathbb{Z}[i]$-ben nem, $5 = (2 + i)(2 - i)$.

Faktorizáció integritástartományokban 2.

Tétel.

Bármely integritástartományban a prímek irreducibilis elemek, de nem minden irreducibilis prím.

Bizonyítás.

Legyen R integritástartomány és $p \in R$ prím. Ha valamely $a, b \in R$-re $p = ab$, akkor $p|a$, vagy $p|b$. Ha $p|a$, akkor $a = pt,\ t \in R$. Ekkor azonban

$$p = ptb \implies 1 = tb \implies b|1,$$

ami maga után vonja, hogy p irreducibilis.
A második állítás (a megfordítás) azonnal adódik a $\mathbb{Z}[i\sqrt{5}]$ integritástartománybeli példánkból: ott a 3 irreducibilis, de nem prím.

Faktorizáció integritástartományokban 3.

Definíció.

Az R integritástartomány **Gauss-gyűrű**, ha minden zérótól különböző eleme, amely nem invertálható, sorrendtől és asszociáltaktól eltekintve egyértelműen bomlik irreducibilis elemek szorzatára.

Tétel

Egy R integritástartomány pontosan akkor Gauss-gyűrű, ha

1. nem létezik elemei olyan $a_1, a_2, \ldots$ végtelen sorozata, hogy minden $i < j$-re $a_j|a_i$, de $a_i \nmid a_j$, azaz a sorozat különböző indexű elemei páronként nem-asszociáltak,
2. R-ben az irreducibilis elemek prímek.

Faktorizáció integritástartományokban 4.

Bizonyítás.

Az R integritástartományra fönnállnak a tételbeli föltételek.

Ha $a \in R$ olyan, hogy $a \neq 0$, és $a \nmid 1$, akkor (1) maga után vonja, hogy a irreducibilis elemek szorzatára bomlik,

míg e fölbontás egyértelműsége (2)-ből adódik ugyanúgy, mint a számelmélet alaptételének ismert bizonyításában.

Faktorizáció integritástartományokban 5.

Bizonyítás. (folytatás)

Megfordítva,

ha R Gauss-gyűrű, akkor nyilván teljesül (1).

A (2) igazolásához legyen $q \in R$ irreducibilis elem, továbbá valamely $a, b \in R$ elemekre $q|ab$, s így

$ab = qt,\ t \in I$.

Ha a, b, t irreducibilis fölbontása rendre

$$a = p_1 \ldots p_k, \quad b = p_{k+1} \ldots p_m, \quad t = q_1 \ldots q_n,$$

akkor

$$ab = p_1 \ldots p_k p_{k+1} \ldots p_m = qq_1 \ldots q_n.$$

Az irreducibilis fölbontás egyértelműsége miatt van olyan p_i, hogy $p_i \sim q$. Ha $1 \leq i \leq k$, akkor $q|a$, míg ha $k < i \leq m$, akkor $q|b$.

Példák.

1. A páros számok $\mathbb{P}$ halmaza a szokásos műveletekkel zérusosztómentes gyűrű. Bár nem integritástartomány, az irreducibilis- és a prímelem fogalma definiálható. E gyűrűben a 2 nyilván irreducibilis, de nem prím, hiszen $2|36 = 6 \cdot 6$, de $2 \nmid 6$ $\mathbb{P}$-ben.
2. A $\mathbb{Z}[i\sqrt{5}]$ integritástartományban a 3 irreducibils. Ugyanis — fölhasználva, hogy két komplex szám szorzata mikor valós — a $3 = a(x + iy\sqrt{5})(x - iy\sqrt{5})$ egyenlőségből $3 = a(x^2 - 5y^2)$, így szükségképp $y = 0$. Mivel $a \in \mathbb{Z}$, csak $a = \pm 1$, vagy ± 3 lehet és x is csak ± 1 lehet.
3. A $\mathbb{Z}[i\sqrt{5}]$ integritástartományban a 9-nek két nemtriviális irreducibilis fölbontása is van: $9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5})$

Testek.

Definíció

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

Megjegyzések.

1. Az előbbi példák közül $(\mathbb{Z}; +, \cdot)$, $\mathbb{Z}[i]$ integritástartományok. Az összes páros számok halmaza a szokásos műveletekkel kommutatív zérusosztó mentes gyűrű, DE nem integritástartomány, mert nincs egységeleme.
2. Integritástartományokban, sőt egységelemes gyűrűkben is, az invertálható elemek csoportot alkotnak. Az F test fölötti $\mathcal{M}_n(F)$ teljes mátrixgyűrűk esetént az ilyen csoportokat **általános lineáris csoportnak** nevezzük, és használjuk rájuk a $\mathrm{GL}_n(F)$ jelölést.
3. $(\mathbb{Q}; +, \cdot)$, $(\mathbb{C}; +, \cdot)$, $\mathbb{Q}(\alpha) = \{a + b\alpha \colon a, b \in \mathbb{Q},\ \alpha^3 = 1, \alpha \neq 1\}$, (az ún. Euler-racionálisok) testek;
4. Tetszőleges p prímre $(\mathbb{Z}_p; +, \cdot)$ testek.
5. Vegyük észre, hogy a testek integritástartományok.

Tételek.

1. Legyen F test, $n > 1$ egész. Az F-fölötti $n \times n$-es mátrixok $\mathcal{M}_n(F)$ gyűrűje egységelemes, de se nem kommutatív, se nem zérusosztómentes. E gyűrű egységei (mint speciális esetben már említettük) a nemzéró determinánsú mátrixok.
2. Tetszőleges $m \geq 2$ egészre a modulo m maradékosztályok $\mathbb{Z}_m$ halmaza az ismert összeadással és szorzással egységelemes kommutatív gyűrűt alkot. Ezen gyűrű egységei éppen a redukált maradékosztályok (halmazukat $\mathbb{Z}_m^*$ jelöli). A $\mathbb{Z}_m$ gyűrű pontosan akkor test, ha m prímszám.

Bizonyítás.

A tétel első állítása nyilvánvaló, a második pedig következik a lineáris kongruenciák megoldhatóságára vonatkozó tételből.
Ha m összetett szám, és $r|m$, $r > 1$, akkor $\overline{r}$ zérusosztó, így $\mathbb{Z}_m$ nem lehet test (testben nincs zérusosztó!).

Ha p prím, akkor tetszőleges $1 \leq a < p$-re az $ax \equiv 1 \pmod{p}$ kongruencia megoldható, tehát a $\mathbb{Z}_p$ gyűrű minden nemzéró elemének van multiplikatív inverze, tehát test.

Maradékosztálygyűrűk.

Definition

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

Theorem

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

Bizonyítás.

Az állítások abból következnek, hogy egyrészt $\mathbb{Z}[i] \subseteq \mathbb{C}$, másrészt $\mathbb{Z}[i]$ egységei 1 abszolút értékűek. □

Theorem

A Gauss-egészek gyűrűje Gauss-gyűrű.

Bizonyítás.

Legyenek α, β nemzéró Gauss-egészek. A Gauss-egészek a számsík egész koordinátájú rácspontjai, így az $\frac{\alpha}{\beta}$ ponthoz legalább egy olyan rácspont van, amely 1-nél kisebb távolságra van. Ha γ egy ilyen, akkor $\alpha = \beta\gamma + \varrho$, ahol $|\varrho| < |\beta|$. Ez azt jelenti, hogy e gyűrűben ugyanolyan maradékos osztást lehet végezni, mint a racionális egész számok gyűrűjében. Így formálisan ugyanúgy igazolható az is, hogy bármely két nemzéró Gauss-egésznek van legnagyobb közös osztója, és a fölbonthatatlanok prímek. Ebből — egy korábbi tételünk alapján — már adódik tételünk állítása. □

Észrevételek.

- Nem minden racionális prímszám fölbonthatatlan a $\mathbb{Z}[i]$ gyűrűben. Például: $2 = (1 + i)(1 - i)$, $5 = (2 + i)(2 - i)$.
- Igazolható (bár nem triviális), hogy a $4k + 1$ alakú prímszámok két négyzetszám összegére bonthatók, amiből már adódik a nemtriviális fölbontás létezése.