

Algebrai struktúrák

Diszkrét modellek alkalmazásai

1. Gyűrű

Számos olyan matematikai objektumot ismerünk, amelyekkel a számokhoz hasonlóan lehet műveleteket végezni (pl. összeadni, kivonni, szorozni): mátrixok, polinomok, maradékok stb. Ezek műveletei között sok hasonlóság van (például mindegyiknél igaz, hogy $a + b = b + a$), de vannak különbségek is (például számoknál $a \cdot b = b \cdot a$, de ez mátrixokra általában nem igaz). Az alábbiakban *absztrakciót* fogunk végrehajtani: a különböző matematikai objektumoknak csak a közös tulajdonságaival foglalkozunk, "elfelejtve" az egyéni jellegzetességeiket. Így bármilyen megállapításra is jutunk általánosan, az az összes konkrét esetre automatikusan teljesülni fog.

1.1. Definíció (gyűrű). Legyen R egy halmaz, és azon két bináris művelet: "+" és "·". Az $(R, +, \cdot)$ hármast **gyűrűnek** nevezzük [*ring*], ha a következő tulajdonságok (*gyűrűaxiómák*) teljesülnek:

A. **additív művelet** (+):

1. zárt: $\forall a, b \in R : a + b \in R$;
2. asszociatív: $\forall a, b, c \in R : (a + b) + c = a + (b + c)$;
3. kommutatív: $\forall a, b \in R : a + b = b + a$;
4. van **nullelem**: $\exists z \in R : \forall a \in R : a + z = a$;
5. van **additív inverz**: $\forall a \in R : \exists x \in R : a + x = z$ (ahol z a nullelem) (x jelölése: $-a$);

M. **multiplikatív művelet** (·):

1. zárt: $\forall a, b \in R : a \cdot b \in R$;
2. asszociatív: $\forall a, b, c \in R : (a \cdot b) \cdot c = a \cdot (b \cdot c)$;

D. "·" disztributív "+"-ra:

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

Példa. Az egész számok, azaz $(\mathbb{Z}, +, \cdot)$ gyűrű, mert teljesít minden fent leírt tulajdonságot. Az $\mathbb{A}/4$ -ben előírt *nullelem* a nulla szám ($z = 0$), hiszen $a + 0 = a$, az $\mathbb{A}/5$ -beli *additív inverz* pedig a szám ellentettje ($x = -a$), hiszen $a + (-a) = 0$.

A tulajdonságokat három csoportba osztottuk: az első kettő (A és M) a két műveletről szól külön-külön, a harmadik (D, azaz disztributivitás) pedig összekapcsolja a két műveletet (hogy ne két egymástól független műveletről legyen szó). Látható, hogy a gyűrű sokkal kevesebbet vár el a multiplikatív művelettől, mint az additív művelettől. Ez azért van, hogy minél többféle objektum férjen bele a gyűrű fogalmába (például a mátrixok is, ahol a szorzás nem kommutatív). Később majd definiálunk további algebrai struktúrákat is, amelyek a multiplikatív művelettől is többet várnak el.

(Megjegyzés: bár a műveleteket a "+" és a "·" jellel jelöltük, ezek csak jelölések, és általában tetszőleges műveletek lehetnek, nemcsak összeadás és szorzás. Viszont gyakran mégiscsak erről a két műveletről van szó, ezért ilyenkor – kissé pontatlanul – elhagyjuk őket a jelölésből, például $(\mathbb{Z}, +, \cdot)$ helyett csak annyit írunk, hogy " $\mathbb{Z}$ egy gyűrű". Továbbá, ha a művelet szorzás, akkor annak jelét gyakran elhagyjuk, azaz $a \cdot b$ helyett csak annyit írunk, hogy ab .)

További példák gyűrűkre:

1. Példa. Az ismert számhalmazok többsége gyűrű:

$$\begin{aligned}\mathbb{Z} &= \{\dots, -2, -1, 0, 1, 2, \dots\} && \text{(az egész számok halmaza),} \\ \mathbb{Q} &= \{a/b \mid a, b \in \mathbb{Z} \wedge b \neq 0\} && \text{(a racionális számok halmaza),} \\ \mathbb{R} &&& \text{(a valós számok halmaza),} \\ \mathbb{C} &= \{a + bi \mid a, b \in \mathbb{R}\} && \text{(a komplex számok halmaza)}\end{aligned}$$

a szokásos összeadással és szorzással. A nullelem minden esetben a 0 szám, egy szám additív inverze pedig az ellentettje ($-a$).

Nem gyűrű viszont a természetes számok halmaza ($\mathbb{N}$), mert ott nincs additív inverz: például nincs olyan x természetes szám, hogy $2 + x = 0$.

2. Példa. Gyűrűt alkot az $n \times n$ -es mátrixok halmaza, pl. $\mathbb{R}^{n \times n}$ (egy rögzített n -re), a mátrixösszeadás és a mátrixszorzás műveletekkel. A gyűrű nulleme a csupa nullából álló *nullmátrix*, pl. $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{R}^{2 \times 2}$. Egy $A \in \mathbb{R}^{n \times n}$ mátrix additív inverze a $-A \in \mathbb{R}^{n \times n}$ mátrix, azaz az A elemeinek ellentettjeiből álló mátrix (pl. ha $A = \begin{pmatrix} 2 & 1 \\ 0 & -3 \end{pmatrix}$, akkor $-A = \begin{pmatrix} -2 & -1 \\ 0 & 3 \end{pmatrix}$), hiszen ekkor lesz $A + (-A) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

3. Példa. Gyűrűt alkotnak a polinomok is (pl. $3x^5 - 4x^3 + x - 2 \in \mathbb{R}[x]$) – ezekről részletesebben a következő jegyzetben lesz szó. A nullelem a konstans nulla polinom ($0 \in \mathbb{R}[x]$), egy p polinom additív inverze pedig $-p = -1 \cdot p$ (pl. ha $p = 2x^2 - 3$, akkor $-p = -2x^2 + 3$).

4. Példa. Gyűrűt alkotnak a maradékosztályok is adott $m \in \mathbb{N}^+$ modulusra: $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}$ (lásd a Kongruenciák c. jegyzetet). Emlékeztető: a műveletek modulárisan történnek, azaz minden eredménynek vesszük a maradékát m szerint, például $\mathbb{Z}_5$ -ben $\bar{3} + \bar{4} = \bar{2}$ és $\bar{3} \cdot \bar{3} = \bar{4}$. A nullelem a $\bar{0}$ maradékosztály. Egy $\bar{a} \in \mathbb{Z}_m$ elem additív inverze $-\bar{a} = \overline{m-a}$, pl. $\mathbb{Z}_5$ -ben $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$ additív inverzei rendre $\bar{0}, \bar{4}, \bar{3}, \bar{2}, \bar{1}$ (mert $\bar{0} + \bar{0} = \bar{0}$, $\bar{1} + \bar{4} = \bar{0}$ stb.).

5. Példa. Gyűrűt alkot a páros számok halmaza is: $2\mathbb{Z} := \{2k \mid k \in \mathbb{Z}\}$. Mivel $2\mathbb{Z} \subseteq \mathbb{Z}$, és $\mathbb{Z}$ -ről már tudjuk, hogy gyűrű, ezért a gyűrűaxiómák egy része automatikusan öröklődik (asszociativitás, kommutativitás, disztributivitás). A többit ellenőrizni kell: a műveletek zártsága (A/1 és M/1) teljesül, mert páros számok összege és szorzata is páros; a nullelem öröklődik, mert a 0 páros szám; és az additív inverz is, mert páros szám ellentettje is páros.

Nem alkotnak gyűrűt viszont a páratlan számok ($2\mathbb{Z} + 1$), mert ott (többek között) már az összeadás zártsága (A/1) sem teljesül: pl. $1 + 3 = 4$, azaz két páratlan szám összege nem páratlan.

6. Példa. A következő példa azt mutatja be, hogy a gyűrű két műveletének nem kell feltétlenül összeadásnak és szorzásnak lennie, lehetnek teljesen mások is. Vegyünk egy tetszőleges H halmazt, és annak összes lehetséges részhalmazát – azaz H hatványhalmazát, 2^H -t (pl. ha $H = \{a, b\}$, akkor $2^H = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$). Ekkor $(2^H, \Delta, \cap)$ gyűrű, azaz H részhalmazai a szimmetrikus differencia (Δ) és a metszet ($\cap$) műveletével (lásd: Diszkrét matematika I) gyűrűt alkotnak. A halmazműveletek szabályaiból ellenőrizhető, hogy minden gyűrűaxióma teljesül, csak itt az additív művelet a Δ , a multiplikatív művelet pedig a $\cap$. Például a disztributivitás (első fele) így néz ki: $\forall A, B, C \in 2^H : A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$. A gyűrű nulleme az üres halmaz, $\emptyset$ (hiszen $A \Delta \emptyset = A$), egy halmaz additív inverze pedig önmaga (hiszen $A \Delta A = \emptyset$).

7. Példa. A legegyszerűbb gyűrű az egyelemű halmaz: $\{a\}$, ahol a műveleteket az egyetlen lehetséges módon értelmezzük: $a + a = a$ és $a \cdot a = a$. Ekkor $(\{a\}, +, \cdot)$ gyűrű, mert az összes gyűrűaxióma triviálisan teljesül (pl. kommutativitás: $a + a = a + a$ stb.). A nullelem a halmaz egyetlen eleme (a), és annak additív inverze önmaga. Ezt **nullgyűrűnek** nevezzük (mert az egyetlen eleme a nullelem).

1.2. Tétel (gyűrűk tulajdonságai).

1. A nullelem egyértelmű (azaz ha z_1 és z_2 is nullelem, akkor $z_1 = z_2$).
2. Az additív inverz egyértelmű (azaz ha a -nak x_1 és x_2 is additív inverze, akkor $x_1 = x_2$).
3. A nullelem additív inverze önmaga: $-z = z$.
4. Az additív inverz additív inverze az eredeti elem: $-(-a) = a$.
5. A nullelem a szorzás során elnyel minden elemet: $\forall a \in R : za = z \wedge az = z$.

(Ezek mind könnyen levezethetők a gyűrűaxiómákból. Például az első abból adódik, hogy mivel z_1 nullelem, ezért $z_1 + z_2 = z_2$, de mivel z_2 is nullelem, ezért $z_1 + z_2 = z_1$, tehát $z_1 = z_2$.)

A gyűrű definíciójában csak két művelet szerepel (összeadás és szorzás), de mi a helyzet a többi alpművelettel? A kivonást például definiálni tudjuk az összeadás és az additív inverz segítségével:

1.3. Definíció (kivonás). Egy R gyűrűben $a, b \in R$ elemekre $\mathbf{a - b} := a + (-b)$.

A definícióból következik, hogy $(a - b) + b = a$ és $(a + b) - b = a$, ahogy azt várnánk.

(Megjegyzés: ha a gyűrű additív művelete nem az összeadás, akkor ezt a műveletet sem kivonásnak hívjuk, hanem az adott művelet **inverzének**. Például a fenti $(2^H, \Delta, \cap)$ gyűrűben a Δ inverze önmaga, mert ott minden elem additív inverze is önmaga. Hasonlóan fogjuk az osztást is definiálni a szorzás segítségével, de ehhez további fogalmak kellenek.)

2. Integritási tartomány

A gyűrű fogalma kellően általános, de bizonyos esetekben szükség van további követelményekre, elsősorban a multiplikatív műveletre vonatkozóan. Ezért bevezetünk még néhány fogalmat.

Minden gyűrű additív művelete kommutatív, de hasznos lehet, ha a multiplikatív művelete is az:

2.1. Definíció. Egy R gyűrű **kommutatív**, ha a multiplikatív művelete $(\cdot)$ kommutatív, azaz

$$\forall a, b \in R : a \cdot b = b \cdot a.$$

Példa. A fent felsorolt gyűrűk közül majdnem mindegyik kommutatív. A kivétel a mátrixok, például ha $A = \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$ és $B = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$, akkor $AB = \begin{pmatrix} 4 & 4 \\ -4 & -4 \end{pmatrix}$, de $BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

A nullelem megfelelőjét is bevezethetjük a multiplikatív műveletre:

2.2. Definíció. Egy R gyűrű $e \in R$ eleme **egységelem** [*identity element*], ha

$$\forall a \in R : ae = a \wedge ea = a.$$

Az olyan gyűrűt, amelyben van egységelem, **egységelemes gyűrűnek** nevezzük.

Példa. Nézzük végig az előző oldalon felsorolt gyűrűket, hogy van-e egységelemük:

1. A számgyűrűk ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) egységeleme az 1.
2. A mátrixgyűrű egységeleme az *egységmátrix*, pl. $\mathbb{R}^{2 \times 2}$ -ben $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
3. A polinomgyűrű egységeleme az 1 konstans polinom.
4. A $\mathbb{Z}_m$ egységeleme az $\bar{1}$ maradékosztály.
5. A páros számoknak ($2\mathbb{Z}$) nincs egységeleme.
6. A $(2^H, \Delta, \cap)$ egységeleme a teljes H halmaz, hiszen minden $A \in 2^H$ (azaz $A \subseteq H$) halmazra $A \cap H = A$ és $H \cap A = A$. (Itt tehát a nullelem ($\emptyset$) és az egységelem (H) a két véglet.)
7. A nullgyűrű egységeleme az egyetlen elem. (Megjegyzés: ez az egyetlen olyan gyűrű, ahol az egységelem megegyezik a nullelemmel. Nagyobb gyűrűkben ugyanis a nullelem elnyelési tulajdonsága ($za = z$) kizárja, hogy egyúttal egységelem is lehessen.)

2.3. Tétel. Az egységelem egyértelmű, azaz ha e_1 és e_2 is egységelem, akkor $e_1 = e_2$.

A következő fogalom a számok körében ismeretlen, és általában szeretnénk elkerülni:

2.4. Definíció. Egy R gyűrű $a \in R \setminus \{z\}$ eleme **nullosztó** [*zero divisor*], ha

$$\exists b \in R \setminus \{z\} : ab = z \vee ba = z,$$

ahol z a nullelem. Egy gyűrű **nullosztómentes**, ha nincs benne nullosztó.

Másképpen: R nullosztómentes, ha $ab = z$ csak úgy lehet, ha $a = z$ vagy $b = z$. A számok körében nincsenek nullosztók, mert ha $ab = 0$, akkor $a = 0$ vagy $b = 0$. Ezt a tulajdonságot az egyenletek megoldásánál sokszor használtuk, hiszen ez garantálta, hogy ha pl. $(x-1)(x-2) = 0$, akkor $x = 1$ vagy $x = 2$, és más megoldás nem lehet. A nullosztók ezt jelentősen megnehezítenék.

Példa. A mátrixok körében $\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, azaz $\begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}$ és $\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}$ nullosztók $\mathbb{R}^{2 \times 2}$ -ben.

Példa. $\mathbb{Z}_6$ -ban $\bar{2} \cdot \bar{3} = \bar{0}$ (mert $2 \cdot 3 = 6$), azaz $\bar{2}$ és $\bar{3}$ nullosztók $\mathbb{Z}_6$ -ban.

2.5. Tétel (nullosztók $\mathbb{Z}_m$ -ben).

1. $\bar{a} \in \mathbb{Z}_m$ akkor és csak akkor nullosztó, ha $\bar{a} \neq \bar{0}$ és $\text{lko}(a, m) \neq 1$.
2. $\mathbb{Z}_m$ -ben akkor és csak akkor van nullosztó, ha m összetett szám.

Tehát prímszámokra $\mathbb{Z}_p$ nullosztómentes.

Nagyon hasznosak lesznek az olyan gyűrűk, amelyekre mind a három fenti tulajdonság teljesül:

2.6. Definíció. Az R gyűrűt **integritási tartomány**nak nevezzük [*integral domain*], ha

0. legalább két eleme van;
1. kommutatív: $\forall a, b \in R : ab = ba$;
2. egységelemes: $\exists e \in R : \forall a \in R : ae = a \wedge ea = a$;
3. nullosztómentes: $\forall a, b \in R \setminus \{z\} : ab \neq z \wedge ba \neq z$.

Példa. A négy alapvető számgyűrű ($\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$) integritási tartomány.

Példa. Integritási tartományok a polinomgyűrűk is, ha az együtthatók számok ($\mathbb{Z}[x], \mathbb{R}[x]$ stb.).

Példa. $\mathbb{Z}_m$ akkor és csak akkor integritási tartomány, ha m prímszám.

(A "legalább két eleme van" feltétel azért kell, hogy kizárja a nullgyűrűt, ezáltal garantálja, hogy az egységelem ne lehessen azonos a nullelemmel, ami később fölösleges bonyodalmakhoz vezetne.)

3. Test

Egy fontos tulajdonság még hátravan: az additív inverz ($-a$) megfelelője szorzásra:

3.1. Definíció. Egy R egységelemes gyűrűben $a \in R$ **multiplikatív inverze** x , ha

$$ax = e \wedge xa = e,$$

ahol e az egységelem. Jelölés: $x = a^{-1}$. (Néha jelző nélkül **inverz**nek is nevezik.) Az olyan elemet, amelynek van multiplikatív inverze, **invertálhatónak** nevezzük.

Példa. $2 \in \mathbb{Q}$ multiplikatív inverze $1/2 \in \mathbb{Q}$, mert $2 \cdot 1/2 = 1$. Általában $a \in \mathbb{Q} \setminus \{0\}$ inverze $1/a$.

Példa. $\mathbb{Z}$ -ben csak 1 és -1 invertálható (mindkettő inverze önmaga).

Példa. Az $A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix} \in \mathbb{R}^{2 \times 2}$ mátrix multiplikatív inverze $A^{-1} = \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}$, mert $AA^{-1} = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ és $A^{-1}A = I$. Nem invertálható viszont a $B = \begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$, mert $\det B = 0$.

Példa. $\bar{3} \in \mathbb{Z}_{10}$ multiplikatív inverze $\bar{7}$, mert $\bar{3} \cdot \bar{7} = \bar{1}$. Általában $\mathbb{Z}_m$ -ben a multiplikatív inverz egybeesik a *moduláris inverz* fogalmával (lásd: Kongruenciák), azaz pontosan azon $\bar{a} \in \mathbb{Z}_m$ elemek invertálhatóak, amelyekre $\text{lko}(a, m) = 1$. Tehát $\mathbb{Z}_{10}$ -ben pontosan $\bar{1}, \bar{3}, \bar{7}$ és $\bar{9}$ invertálható.

3.2. Tétel (a multiplikatív inverz tulajdonságai).

1. A multiplikatív inverz egyértelmű.
2. Az egységelem multiplikatív inverze önmaga: $e^{-1} = e$.
3. A multiplikatív inverz multiplikatív inverze az eredeti elem: $(a^{-1})^{-1} = a$.
4. A nullelem nem invertálható.
5. Nullosztó nem invertálható.

Most már definiálhatjuk a gyűrű melletti másik legfontosabb algebrai struktúrát:

3.3. Definíció. Az R gyűrűt **testnek** nevezzük $[field]$, ha

0. legalább két eleme van,
1. kommutatív,
2. egységelemes és
3. minden eleme invertálható, kivéve a nullelemet.

Vegyük észre, hogy minden test egyúttal integritási tartomány is, mert a definícióik csak a 3-as pontban térnek el, és invertálható elem nem lehet nullosztó (a fenti tétel alapján).

(A 3-as pontban azért zártuk ki a nullelemet, mert az semmilyen gyűrűben nem lehet invertálható, hiszen bármely elemmel szorozzuk meg, a nullelemet kapjuk vissza. Ez annak felel meg, hogy a számoknál nem lehet 0-val osztani.)

Példa. Az eddig ismert gyűrűk közül a következők testek:

1. $\mathbb{Q}$, $\mathbb{R}$ és $\mathbb{C}$ – ezeket hívjuk **számtesteknek**.
2. $\mathbb{Z}_p$, ahol p prímszám, mert ott a $\bar{0}$ -n kívül minden elem invertálható.

Nem test viszont a $\mathbb{Z}$, az egész számok halmaza, mert ott csak az 1 és a -1 invertálható.

Összefoglalásképpen megadjuk a test definícióját önállóan is, azaz a gyűrű fogalma nélkül, a gyűrű definíciójához hasonló formában:

3.4. Definíció (test). $(F, +, \cdot)$ **test** $[field]$, ha a következő tulajdonságok (*testaxiómák*) teljesülnek:

A. additív művelet (+):

1. zárt: $\forall a, b \in F : a + b \in F$;
2. asszociatív: $\forall a, b, c \in F : (a + b) + c = a + (b + c)$;
3. kommutatív: $\forall a, b \in F : a + b = b + a$;
4. van **nullelem**: $\exists z \in F : \forall a \in F : a + z = a$;
5. van **additív inverz**: $\forall a \in F : \exists x \in F : a + x = z$ (ahol z a nullelem);

M. multiplikatív művelet ($\cdot$):

1. zárt: $\forall a, b \in F : a \cdot b \in F$;
2. asszociatív: $\forall a, b, c \in F : (a \cdot b) \cdot c = a \cdot (b \cdot c)$;
3. kommutatív: $\forall a, b \in F : a \cdot b = b \cdot a$;
4. van **egységelem**: $\exists e \in F \setminus \{z\} : \forall a \in F : a \cdot e = a$;
5. van **multiplikatív inverz**: $\forall a \in F \setminus \{z\} : \exists x \in F : a \cdot x = e$ (ahol e az egységelem);

D. " $\cdot$ " disztributív "+"-ra:

$$\forall a, b, c \in F : a \cdot (b + c) = a \cdot b + a \cdot c.$$

Látható, hogy a testnél, a gyűrűvel ellentétben, a multiplikatív művelettől is pontosan ugyanannyit várunk el, mint az additívtól. (Kivéve a nullelem invertálhatóságát, mert az lehetetlen.)

(Megjegyzés: a szorzás kommutativitása miatt bizonyos tulajdonságok leegyszerűsödtek a gyűrű definíciójához képest, például a disztributivitásnak elég volt csak az egyik irányát kimondani.)

Testekben már definiálni tudjuk a negyedik alapműveletet is (hasonlóan a kivonáshoz, lásd a gyűrűknél fent):

3.5. Definíció (osztás). Egy F testben az $a, b \in F$, $b \neq 0$ elemekre $\mathbf{a/b} := ab^{-1}$.

Példa. $\mathbb{Q}$ -ban ez azt jelenti, hogy $5/2 = 5 \cdot 2^{-1} = 5 \cdot (1/2)$.

A definícióból következik, hogy $(a/b)b = a$ és $(ab)/b = a$, ahogy azt várnánk.

4. Gyűrűk Sage-ben

Sage-ben a számgyűrűkre ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) dupla betűkkel hivatkozhatunk (a matematikai dupla-vonalas betűkre utalva):

```
sage: ZZ
Integer Ring
sage: QQ
Rational Field
sage: RR          # RR és CC csak közelítőleg ábrázolható, ezért kerülendők
Real Field with 53 bits of precision
```

A gyűrűk nevét használhatjuk típuskonvertálásra:

```
sage: type(QQ(12))    # ZZ -> QQ konvertálás
<class 'sage.rings.rational.Rational'>
sage: type(6/3)       # tört mindig QQ-ban van, akkor is, ha egész szám
<class 'sage.rings.rational.Rational'>
sage: type(ZZ(6/3))   # de konvertálható ZZ-be
<class 'sage.rings.integer.Integer'>
sage: ZZ(2/3)         # ez viszont nem
[...]
TypeError: no conversion of this rational to integer
sage: RR(2/3)         # QQ -> RR: kerekítéssel jár, ezért kerülendő
0.6666666666666667
```

Mátrixgyűrűket (pl. $\mathbb{Z}^{3 \times 3}$) a `Mat()` függvénnyel hozhatunk létre:

```
sage: Mat(ZZ, 3)      # 3x3-as egész mátrixok
Full MatrixSpace of 3 by 3 dense matrices over Integer Ring
sage: M = Mat(ZZ, 3)
sage: M([[3,1,-4], [2,5,6], [1,4,8]])
[ 3  1 -4]
[ 2  5  6]
[ 1  4  8]
sage: M.one()         # egységelem
[1 0 0]
[0 1 0]
[0 0 1]
```

A $\mathbb{Z}_m$ gyűrűt a $\text{Zmod}(m)$ függénnyel hozhatjuk létre:

```
sage: Zmod(10)
Ring of integers modulo 10
sage: Z10 = Zmod(10)
sage: Z10(34)          # ZZ -> Zmod(10) konvertálás
4
sage: Z10(34) * 13     # a 13-at már automatikusan konvertálja
2
sage: type(Z10(34))
<class 'sage.rings.finite_rings.integer_mod.IntegerMod_int'>
```

Az $\bar{a} \in \mathbb{Z}_m$ elemeket egyszerűbben is létrehozhatjuk a $\text{mod}(a, m)$ függvénnyel, amely ekvivalens a $\text{Zm} = \text{Zmod}(m)$; $\text{Zm}(a)$ konverzióval, csak nem kell hozzá létrehozni a $\text{Zmod}(m)$ gyűrűt. Ezt azonban ne keverjük a $\%$ művelettel, amely egész számot ad vissza:

```
sage: mod(34, 10)      # ugyanaz, mint a fenti Z10(34)
4
sage: mod(34, 10) ^ 2  # modulárisan számol tovább
6
sage: (34 % 10) ^ 2    # NEM ugyanaz: egész számként számol tovább
16
sage: type(mod(34, 10))
<class 'sage.rings.finite_rings.integer_mod.IntegerMod_int'>
sage: type(34 % 10)
<class 'sage.rings.integer.Integer'>
```

A véges gyűrűknek (pl. $\mathbb{Z}_m$) fel tudjuk sorolni az elemeit:

```
sage: list(Zmod(10))
[0, 1, 2, 3, 4, 5, 6, 7, 8, 9]
sage: for a in Zmod(5):
....:     print(a, a^2)
0 0
1 1
2 4
3 4
4 1
```

5. Szerző

Ezt a jegyzetet Uray M. János írta, részben felhasználva az alábbi forrásokat:

- [1] <https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa>
- [2] [https://en.wikipedia.org/wiki/Ring_\(mathematics\)](https://en.wikipedia.org/wiki/Ring_(mathematics))
- [3] https://en.wikipedia.org/wiki/Integral_domain
- [4] [https://en.wikipedia.org/wiki/Field_\(mathematics\)](https://en.wikipedia.org/wiki/Field_(mathematics))

Hibákat, észrevételeket itt lehet jelezni: uray.janos@inf.elte.hu.