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 *absztrakció*t 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 "$\cdot$". Az $(R, +, \cdot)$ hármast **gyűrű**nek 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** $(\cdot)$:
   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. "$\cdot$" 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 A/4-ben előírt *nullelem* a nulla szám ($z = 0$), hiszen $a + 0 = a$, az 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 "$\cdot$" 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. Az ismert számhalmazok többsége gyűrű:

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

   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. 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 nulleleme a nullmátrix, azaz amelynek minden eleme a 0 szám, pl. $\left(\begin{smallmatrix}0 & 0\\ 0 & 0\end{smallmatrix}\right)$. Egy $A \in \mathbb{R}^{n\times n}$ mátrix additív inverze a $-A \in \mathbb{R}^{n\times n}$ mátrix, azaz amelynek minden eleme az A megfelelő elemének ellentettje (pl. ha $A = \left(\begin{smallmatrix}2 & 1\\ 0 & -3\end{smallmatrix}\right)$, akkor $-A = \left(\begin{smallmatrix}-2 & -1\\ 0 & 3\end{smallmatrix}\right)$), hiszen ekkor lesz $A + (-A) = \left(\begin{smallmatrix}0 & 0\\ 0 & 0\end{smallmatrix}\right)$.
3. Gyűrűt alkot a polinomok halmaza, pl. $\mathbb{R}[x]$ is. A nullelem a nullpolinom ($0 \in \mathbb{R}[x]$), egy p polinom additív inverze pedig $-p = -1 \cdot p$ (pl. ha $p = 2x^2 - 3$, akkor $-p = -2x^2 + 3$).
4. Gyűrűt alkot a maradékosztályok halmaza is adott $m \in \mathbb{N}^+$ modulusra: $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}$ (lásd a Kongruenciák c. jegyzetet). Emlékeztető: a műveletek modulárisan történnek, azaz minden eredménynek vesszük a maradékát m szerint, például $\mathbb{Z}_5$-ben $\overline{3} + \overline{4} = \overline{2}$ és $\overline{3} \cdot \overline{3} = \overline{4}$. A nullelem a $\overline{0}$ maradékosztály. Egy $\overline{a} \in \mathbb{Z}_m$ elem additív inverze $-\overline{a} = \overline{m - a}$, pl. $\mathbb{Z}_5$-ben $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$ additív inverzei rendre $\overline{0}, \overline{4}, \overline{3}, \overline{2}, \overline{1}$ (mert $\overline{0} + \overline{0} = \overline{0},\ \overline{1} + \overline{4} = \overline{0}$ stb.).
5. 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 már az összeadás zártsága (A/1) sem teljesül: pl. $1 + 3 = 4$, azaz két páratlan szám összege nem páratlan.
6. 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 $(2^H, \triangle, \cap)$ gyűrű, azaz H részhalmazai a szimmetrikus differencia ($\triangle$) 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 $\triangle$, a multiplikatív művelet pedig a $\cap$. Például a disztributivitás (első fele) így néz ki: $\forall A, B, C \in 2^H : A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$. A gyűrű nulleleme az üres halmaz, $\emptyset$ (hiszen $A \triangle \emptyset = A$), egy halmaz additív inverze pedig önmaga (hiszen $A \triangle A = \emptyset$).
7. 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 triviális módon teljesül (pl. kommutativitás: $a + a = a + a$ stb.). A nullelem a halmaz egyetlen eleme (a), annak additív inverze pedig önmaga. Ezt a gyűrűt **nullgyűrű**nek 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 szorzással 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 alapművelettel? A kivonást például definiálni tudjuk az összeadás és az additív inverz segítségével:

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

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 **inverzé**nek. Például a fenti $(2^H, \triangle, \cap)$ gyűrűben a $\triangle$ 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 művelet 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 $A = \left(\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ és $B = \left(\begin{smallmatrix} 2 & 2 \\ 2 & 2 \end{smallmatrix}\right)$, akkor $AB = \left(\begin{smallmatrix} 4 & 4 \\ -4 & -4 \end{smallmatrix}\right)$, de $BA = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

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 gyűrű**nek nevezzük.

Példa. Nézzük végig a fent 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 $I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.
3. A polinomgyűrű egységeleme az 1 konstans polinom.
4. A $\mathbb{Z}_m$ egységeleme az $\overline{1}$ maradékosztály.
5. A páros számoknak ($2\mathbb{Z}$) nincs egységeleme.
6. A $(2^H, \triangle, \cap)$ 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 néha kifejezetten kellemetlen lehet, ezért legtöbbször 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 $\left(\begin{smallmatrix} 2 & 2 \\ 2 & 2 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, azaz $\left(\begin{smallmatrix} 2 & 2 \\ 2 & 2 \end{smallmatrix}\right)$ és $\left(\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ nullosztók $\mathbb{R}^{2\times 2}$-ben.

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

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

1. *$\overline{a} \in \mathbb{Z}_m$ akkor és csak akkor nullosztó, ha $\overline{a} \neq \overline{0}$ és* $\operatorname{lnko}(a, m) \neq 1$.
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, amelyekben 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,
2. egységelemes és
3. nullosztómentes.

Példa. Integritási tartomány a négy alapvető számgyűrű ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), az ezeken alapuló polinomgyűrűk ($\mathbb{Z}[x]$, $\mathbb{R}[x]$ stb.), valamint prímszámokra $\mathbb{Z}_p$.

(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: a^{-1}. (Néha jelző nélkül **inverz**nek is nevezik.) Az olyan elemet, amelynek van multiplikatív inverze, **invertálható**nak 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 $A = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 5 \end{smallmatrix}\right) \in \mathbb{R}^{2\times 2}$ mátrix multiplikatív inverze $A^{-1} = \left(\begin{smallmatrix} -5 & 2 \\ 3 & -1 \end{smallmatrix}\right)$, mert $AA^{-1} = I = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ és $A^{-1}A = I$. Nem invertálható viszont a $B = \left(\begin{smallmatrix} 1 & 2 \\ 3 & 6 \end{smallmatrix}\right)$, mert $\det B = 0$.

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

(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 **számtest**eknek.
2. $\mathbb{Z}_p$, ahol p prímszám, mert ott a $\overline{0}$-n kívül minden elem invertálható.

Nem test viszont $\mathbb{Z}$, 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 $a, b \in F$, $b \neq z$ elemekre $\boldsymbol{a/b} := ab^{-1}$.

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 a számgyűrűket ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) dupla betűkkel jelöli (duplavonalas betűk helyett):

```
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
0.666666666666667
```

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

```
sage: Mat(ZZ, 3)     # 3×3-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 `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 $\overline{a} \in \mathbb{Z}_m$ elemeket egyszerűbben is létrehozhatjuk a `mod(a, m)` függvénnyel, amely ekvivalens a `Zm = Zmod(m); Zm(a)` konverzióval, csak nem kell hozzá létrehozni a `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: [4*a for a in Zmod(10)]
[0, 4, 8, 2, 6, 0, 4, 8, 2, 6]
sage: for a in Zmod(10):
....:     print(a, a^2)
0 0
1 1
2 4
3 9
4 6
5 5
6 6
7 9
8 4
9 1
```

5. Gyűrű fölötti polinomok

Az előző jegyzetben (Polinomok alapjai) foglalkoztunk polinomokkal, de feltettük, hogy az együtthatók számok (pl. $\mathbb{Z}[x]$, $\mathbb{R}[x]$). Most ezt általánosítani fogjuk gyűrűkre.

Ebben a szakaszban legyen K tetszőleges kommutatív gyűrű, és tekintsük $K[x]$-et, a ***K* fölötti polinom**ok halmazát, azaz olyan polinomokat, amelyben az együtthatók a K gyűrűből valók.

Például vehetjük $\mathbb{Z}_4[x]$-et, a modulo 4 maradékosztályok ($\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$) fölötti polinomokat:

```
sage: P4.<x> = Zmod(4)[]
sage: P4
Univariate Polynomial Ring in x over Ring of integers modulo 4
sage: p = 2*x + 3
sage: q = 3*x + 1
sage: p * q
2*x^2 + 3*x + 3
sage: p + q
x
```

Azért lett $p+q = x$, mert $\mathbb{Z}_4$-ben $\overline{2}+\overline{3} = \overline{1}$ és $\overline{3}+\overline{1} = \overline{0}$. Általában $\mathbb{Z}_m[x]$-ben elvégezhetjük a polinomműveleteket úgy, hogy először kiszámítjuk az eredményt $\mathbb{Z}[x]$-ben, majd vesszük az együtthatókat modulo m. Például $\mathbb{Z}[x]$-ben a fenti $p \cdot q = 6x^2 + 11x + 3$, ezért $\mathbb{Z}_4[x]$-ben $p \cdot q = \overline{2}x^2 + \overline{3}x + \overline{3}$.

Visszatérve általános K-ra, könnyen belátható, hogy $K[x]$ is gyűrűt alkot, sőt, megörökli a K konstansgyűrű legtöbb tulajdonságát:

5.1. Tétel ($K[x]$ tulajdonságai)**.**

1. *Ha K kommutatív gyűrű, akkor $K[x]$ is kommutatív gyűrű.*
2. *Ha K egységelemes gyűrű, akkor $K[x]$ is egységelemes gyűrű.*
3. *Ha K nullosztómentes gyűrű, akkor $K[x]$ is nullosztómentes gyűrű.*
4. *Ha K integritási tartomány, akkor $K[x]$ is integritási tartomány.*

Azaz például $K[x]$ örökli K egységelemét, és ha K-ban nem voltak nullosztók, akkor $K[x]$ sem hoz létre újakat. Viszont van egy tulajdonság, amely nem öröklődik:

5.2. Tétel. *Az $x \in K[x]$ polinomnak nincs multiplikatív inverze.*

Vagyis semmilyen $K[x]$ polinomgyűrű nem lehet test, még akkor sem, ha K test.

Példa. $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ és $\mathbb{C}[x]$ integritási tartomány, de egyik sem test.

Példa. $\mathbb{Z}_p[x]$, ahol p prímszám, szintén integritási tartomány, de nem test (hiába test a $\mathbb{Z}_p$).

Most vizsgáljuk meg az előző jegyzet (Polinomok alapjai) megállapításait, és nézzük meg, milyen feltételeket kell-e előírni K-ra, hogy igazak maradjanak:

1. Először is, ha K nem lenne kommutatív, akkor már a polinomszorzással is probléma lenne, hiszen pl. már a $2x \cdot 2x = 4x^2$ szorzásnál is felhasználtuk, hogy $x \cdot 2 = 2 \cdot x$. Ezért kötöttük ki, hogy K csak kommutatív gyűrű lehet.
2. Ha pedig K nem egységelemes, akkor a gyöktényezőknél ütközünk problémába: az $x - c$-nek, bár nem tüntetjük fel, a főegyütthatója az egységelem (pl. $1x - c$); ha viszont K-ban nincs egységelem, akkor $x - c \notin K[x]$. Ezért a továbbiakban K legyen egységelemes gyűrű.

3. A polinomműveletek fokszámára vonatkozó tételben (1.7. Tétel) a szorzásra vonatkozó állítás, azaz $\deg(p \cdot q) = \deg p + \deg q$ csak akkor igaz, ha K nullosztómentes. Például $\mathbb{Z}_6[x]$-ben $(\overline{2}x + \overline{1})(\overline{3}x + \overline{1}) = \overline{5}x + \overline{1}$, azaz nem másodfokú a szorzat, mert a nullosztók miatt az eredeti főegyüttható eltűnt: $\overline{2}x \cdot \overline{3}x = \overline{0}x^2$.
4. Azt az állítást, hogy egy n-edfokú polinomnak legfeljebb n gyöke lehet (4.5. Tétel), szintén elronthatják a nullosztók: pl. $\mathbb{Z}_6[x]$-ben a $p = x^2 + x$ polinomnak *négy* gyöke van: $\overline{0}, \overline{2}, \overline{3}, \overline{5} \in \mathbb{Z}_6$ (és így a gyöktényezős alak sem egyértelmű: $p = (x - \overline{2})(x - \overline{3}) = x(x - \overline{5})$). A tétel tehát általában úgy igaz, ha kikötjük, hogy "K nullosztómentes". (A bizonyításban ezt ott használtuk ki, hogy "ha $p(c) = 0$, akkor valamelyik tényező 0".)

Ha viszont K integritási tartomány, azaz a fenti problémák egyikével sem rendelkezik, akkor az előző jegyzet minden tétele és definíciója érvényes marad. Ha pedig csak annyit kötünk ki, hogy K kommutatív egységelemes gyűrű (tehát megengedjük a nullosztókat), akkor a fent említett két tételen kívül (és a ráépülő Lagrange-interpoláción kívül) minden tétel igaz marad.

5.1. Shamir-féle titokmegosztás – folytatás

Az előző jegyzetben megismertük a Lagrange-interpolációt, és az azon alapuló Shamir-féle titokmegosztást. A gyakorlatban azonban nem a bemutatott módon (egész vagy racionális számokkal) használják az algoritmust, ezért most kiegészítjük az ott leírtakat.

A Lagrange-interpolációról láttuk, hogy – az osztások miatt – $\mathbb{Z}[x]$-ben nem használható, csak $\mathbb{Q}[x]$-ben vagy $\mathbb{R}[x]$-ben. Ezt úgy általánosíthatjuk, hogy bármely *test* fölötti polinomgyűrűre működik, például $\mathbb{Z}_p[x]$-ben is, ahol p prímszám.

A Shamir-féle titokmegosztást a gyakorlatban $\mathbb{Z}_p[x]$-ben végzik, ahol p egy olyan nagy prímszám, amelybe belefér S, a titok. Például legyen – az előző jegyzethez hasonlóan – $n = 5$, $k = 3$ és $S = 67$, és generáljunk szintén egy másodfokú polinomot, de most nem $\mathbb{Z}[x]$-ben, hanem $\mathbb{Z}_{89}[x]$-ben:

$$p = \overline{13}x^2 + \overline{38}x + \overline{67} \in \mathbb{Z}_{89}[x].$$

Ekkor az öt helyettesítési érték a következő (ugyanazok, mint korábban, csak modulo 89):

$$p(\overline{1}) = \overline{29}, \quad p(\overline{2}) = \overline{17}, \quad p(\overline{3}) = \overline{31}, \quad p(\overline{4}) = \overline{71}, \quad p(\overline{5}) = \overline{48}.$$

A visszaállítás is ugyanúgy történik, csak most $\mathbb{Q}$ helyett $\mathbb{Z}_{89}$-ben kell számolni.

$\mathbb{Z}_p$-nek több előnye is van a "naiv" módszerrel szemben: egyrészt, mivel test, ezért az előző jegyzetben leírt probléma nem jelentkezik (bár itt is kijön, hogy $S = \overline{5}a + \overline{2}$, de itt ez semmit nem árul el S-ről, hiszen az $5a \equiv S - 2 \pmod{89}$ lineáris kongruencia bármely S esetén megoldható, lásd: Kongruenciák); másrészt a véletlenszám-generálás is triviális, hiszen $\mathbb{Z}_p$-nek véges sok eleme van.

6. 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)
[3] https://en.wikipedia.org/wiki/Integral_domain
[4] https://en.wikipedia.org/wiki/Field_(mathematics)

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