Algebrai struktúrák

Diszkrét modellek alkalmazásai

1. Gyűrű

Az eddigiekben számos olyan matematikai objektumot láttunk, amelyekkel a számokhoz hasonlóan lehet műveleteket végezni (pl. összeadni, kivonni, szorozni): mátrixok, polinomok, maradékosztályok 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, 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:
   $\forall a, b, c \in R : \ a \cdot (b + c) = a \cdot b + a \cdot c \ \wedge \ (b + c) \cdot a = b \cdot a + c \cdot a$.

A legkézenfekvőbb példa az egész számok, azaz $(\mathbb{Z}, +, \cdot)$, amelyre minden fent leírt tulajdonság teljesül, tehát gyűrű. 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 $a + (-a) = 0$.

Látható, hogy a multiplikatív művelettől sokkal kevesebbet várunk el, mint az additív művelettől. Ez azért van így, hogy minél többféle objektum férjen bele a gyűrű fogalmába (pl. 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 lehetnek tetszőleges műveletek, nemcsak ténylegesen összeadás és szorzás. Viszont itt legtöbbször mégis erről a két műveletről lesz szó, ezért gyakran – kissé pontatlanul – elhagyjuk őket a jelölésből, például $(\mathbb{Z}, +, \cdot)$ helyett csak annyit mondunk, 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.)

Példák gyűrűre:

1. Az ismert számhalmazok többsége gyűrű:
   (a) $\mathbb{Z}$ (az egész számok halmaza),
   (b) $\mathbb{Q}$ (a racionális számok halmaza),
   (c) $\mathbb{R}$ (a valós számok halmaza),
   (d) $\mathbb{C}$ (a komplex számok halmaza)

   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 $A + (-A)$ a nullmátrix.
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 Moduláris aritmetika 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 $\overline{a}$ 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 alkotnak a páros számok 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 viszont gyűrűt a páratlan számok, 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. *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 a számoknál négy alapműveletet ismerünk. Mi a helyzet a többivel? A kivonást például definiálni tudjuk az összeadás és az additív inverz segítségével:
1.3. Definíció (kivonás)**.** Egy R gyűrűben $a, b \in R$ elemekre $a - b := a + (-b)$.
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 szorzásból, de ehhez szükség lesz még további fogalmakra.)

2. Integritási tartomány

A gyűrű definíciója kellően általános, de bizonyos esetekben szükség van további követelményekre, elsősorban a multiplikatív műveletre vonatkozóan (például az additív művelet A/* tulajdonságainak megfelelőire). Ezért bevezetünk még néhány fogalmat.
Minden gyűrű additív művelete kommutatív, de hasznos lehet, ha a multiplikatív művelet is az:
2.1. Definíció (kommutatív gyűrű)**.** Egy R gyűrű *kommutatív*, ha a multiplikatív művelete $(\cdot)$ kommutatív, azaz: $\forall a, b \in R : \ a \cdot b = b \cdot a$.
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 (egységelem)**.** Egy R gyűrű $e \in R$ eleme *egységelem*, ha $\forall a \in R : \ ae = a \ \wedge \ ea = a$.
Az olyan gyűrűt, amelyben van egységelem, *egységelemes gyűrű*nek nevezzük.
2.3. Tétel. *Az egységelem egyértelmű, azaz ha e_1 és e_2 is egységelem, akkor $e_1 = e_2$.*
Nézzük meg, hogy a fent felsorolt gyűrűk közül melyeknek van egységeleme:

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 $(2^H, \triangle, \cap)$ gyűrű egységeleme a H halmaz, hiszen minden $A \in 2^H$ (azaz $A \subseteq H$) halmazra $A \cap H = A$ és $H \cap A = A$. (Itt tehát az egységelem a nullelemhez képest a másik 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.)

A következő fogalom a számok körében ismeretlen, és néha kifejezetten kellemetlen lehet:

2.4. Definíció (nullosztó)**.** Egy R gyűrű $a \in R \setminus \{z\}$ eleme *nullosztó*, ha létezik olyan $b \in R \setminus \{z\}$, hogy $ab = z$ vagy $ba = z$ (ahol z a nullelem). Egy gyűrű *nullosztómentes*, ha nincs benne nullosztó. Más szóval 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 számtalanszor 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.

Példák nullosztókra:

1. A mátrixok körében pl. $\left(\begin{smallmatrix} 2 & 2 \\ 2 & 2 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & 1 \\ -1 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, 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.
2. $\mathbb{Z}_6$-ban pl. $\overline{2} \cdot \overline{3} = \overline{0}$ (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 (integritási tartomány)**.** Az R gyűrűt *integritási tartomány*nak nevezzük, ha

0. legalább két eleme van,
1. kommutatív,
2. egységelemes és
3. nullosztómentes.

Például 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 felesleges bonyodalmakhoz vezetne.)

3. Test

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

3.1. Definíció (multiplikatív inverz)**.** Egy R egységelemes gyűrűben $a \in R$ *multiplikatív inverze* x, ha $ax = e$ és $xa = e$ (ahol e az egységelem). Jelölés: a^{-1}. (Néha jelző nélkül *inverz*nek is nevezik.) Az olyan elemet, amelynek van multiplikatív inverze, *invertálható*nak nevezzük.

Példák multiplikatív inverzre:

1. $2 \in \mathbb{Q}$ multiplikatív inverze $1/2 \in \mathbb{Q}$, mert $2 \cdot 1/2 = 1$. Általában $a \in \mathbb{Q} \setminus \{0\}$ inverze $1/a$.
2. $\mathbb{Z}$-ben csak 1 és -1 invertálható (mindkettőnek önmaga az inverze).
3. 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 $\det B = 0$.
4. $\mathbb{Z}_m$-ben azon $\overline{a} \in \mathbb{Z}_m$ elemek invertálhatóak, melyekre $\operatorname{lnko}(a, m) = 1$.

3.2. Tétel (a multiplikatív inverz tulajdonságai)**.**

1. *A multiplikatív inverz egyértelmű.*
2. *Az egységelem multiplikatív inverze önmaga: $e^{-1} = e$.*
3. *A nullelem nem invertálható.*
4. *Nullosztó nem invertálható.*

Most már definiálhatjuk a gyűrű melletti másik legfontosabb algebrai struktúrát:

3.3. Definíció (test)**.** Az R gyűrűt *test*nek nevezzük, 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).

(Megjegyzés: 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.)

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*, 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, például a disztributivitásnak elég csak az egyik irányát kimondani.)

A 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 $a/b := ab^{-1}$.

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

A definícióból következik, hogy $(a/b)\, b = a$ és $(ab)/b = a$.

4. Gyűrűk Sage-ben

Sage-ben a főbb gyűrűket a következőképpen hozhatjuk létre ("gyűrű" = "ring", "test" = "field"):

```
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
sage: CC
Complex Field with 53 bits of precision
sage: Mat(QQ, 5)    # QQ fölötti 5×5-ös mátrixok
Full MatrixSpace of 5 by 5 dense matrices over Rational Field
sage: ZZ["x"]
Univariate Polynomial Ring in x over Integer Ring
sage: Zmod(6)
Ring of integers modulo 6
```

A gyűrűk elemeit különféle módokon érhetjük el:

```
sage: type(12)      # az egész számok eleve ZZ-ben vannak
<class 'sage.rings.integer.Integer'>
sage: type(2/3)     # a törtek pedig QQ-ban
<class 'sage.rings.rational.Rational'>
sage: type(QQ(12))  # konvertálás másik gyűrűbe: ZZ -> QQ
<class 'sage.rings.rational.Rational'>
sage: ZZ(2/3)       # QQ -> ZZ nem mindig működik
[...]
TypeError: no conversion of this rational to integer
sage: RR(2/3)       # RR és CC csak közelítőleg ábrázolható, ezért kerülendők
0.666666666666667
sage: Zmod(5)(13)   # ZZ -> Zmod(5)
3
sage: Zmod(10).list()  # ha véges, akkor felsorolhatjuk az elemeit
[0, 1, 2, 3, 4, 5, 6, 7, 8, 9]
sage: [a^2 for a in Zmod(10)]
[0, 1, 4, 9, 6, 5, 6, 9, 4, 1]
sage: ZZ.zero()     # nullelem
0
sage: ZZ.one()      # egységelem
1
sage: Mat(ZZ, 3).one()
[1 0 0]
[0 1 0]
[0 0 1]
```

5. Gyűrű fölötti polinomok

Az előző jegyzetben (Polinomok) 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, azaz 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; q = 3*x + 1
sage: p + q
x
sage: p * q
2*x^2 + 3*x + 3
```

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 úgy a polinomműveleteket, 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.

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

Most tekintsük át az előző jegyzet (Polinomok) megállapításait aszerint, hogy melyek működnek tetszőleges K fölötti polinomgyűrűre, és melyeknél kell további feltételeket előírni K-ra. Az általános konvenció az volt, hogy ha egy tételben vagy definícióban $K[x]$ szerepelt (és nem konkrétabb, pl. $\mathbb{R}[x]$), akkor az tetszőleges K kommutatív egységelemes gyűrűre igaz, ha pedig konkrétabban volt megadva, akkor az csak speciális K-kra igaz (de nem feltétlenül csak arra, amit megadtunk). Egészen pontosan a következőkre kell figyelni:

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 is van: $\overline{0}, \overline{2}, \overline{3}, \overline{5} \in \mathbb{Z}_6$ (és így a gyöktényezős alak sem egyértelmű: $p = (x - \overline{2})(x - \overline{3}) = x(x - \overline{5})$). Ezért szerepelt a tételben az a feltétel, hogy "K egy számhalmaz", amit most már általánosíthatunk úgy, hogy "K nullosztómentes". (A tétel bizonyításában ezt ott használtuk ki, hogy "ha $p(c) = 0$, akkor valamelyik tényező 0".) Látható, hogy a nullosztók számtalan kellemetlenséget okoznak, ezért legtöbbször integritási tartomány fölötti polinomokkal foglalkozunk.
5. De a maradékos osztáshoz (5.2. Tétel) még integritási tartomány sem elég. Például $f = x^2 + 3$ és $g = 2x$ hányadosa $q = 1/2 \cdot x$, maradéka $r = 3$, tehát $\mathbb{Z}[x]$-ben általában nem tudjuk elvégezni a maradékos osztást, csak $\mathbb{Q}[x]$-ben. Ehhez ugyanis szükség van a főegyütthatóval való osztásra, ami általában csak testben működik. Ezért fogalmaztuk meg a tételt $\mathbb{R}[x]$-re, de általában tetszőleges test fölött megfogalmazhatjuk: $\mathbb{Q}[x]$-re, $\mathbb{Z}_5[x]$-re stb. Hasonlóan, az euklideszi algoritmus (és a Bézout-lemma) is test fölötti polinomokra működik.
6. A polinomok algebrai deriváltja azonban még test fölött is problémás. Először is, hogyan értelmezzük a definíciót, miszerint $a_n x^n$ deriváltja $n a_n x^{n-1}$, ha $a_n \in K$, de $n \in \mathbb{N}$? Azaz mit jelent egy tetszőleges gyűrű elemének n-szerese, ha n egész szám? (A kitevőben ugyanis mindig egész számok vannak, bármilyen gyűrűből is vannak az együtthatók.) Ez még megoldható: $n a_n := a_n + a_n + \ldots + a_n$, ahol pontosan n tag van. Például $\mathbb{Z}_3[x]$-ben $p = \overline{2}x^5$ algebrai deriváltja $p' = 5 \cdot \overline{2}x^4 = (\overline{2} + \overline{2} + \overline{2} + \overline{2} + \overline{2})x^4 = \overline{1}x^4$. (Megjegyzés: itt különösen indokolt az "algebrai" jelző, mert $\mathbb{Z}_3$-ban nincs értelme analízisről beszélni.) Ez azonban nem várt eredményekhez vezethet. Például $\mathbb{R}[x]$-ben megszoktuk, hogy egy n-edfokú polinom deriváltja $n-1$-edfokú, viszont ez $\mathbb{Z}_m[x]$-ben nem mindig igaz: pl. a $p = x^3 + \overline{2}x^2 + \overline{2}x + \overline{1} \in \mathbb{Z}_3[x]$ harmadfokú polinom deriváltja csak elsőfokú: $p' = x + \overline{2}$, ugyanis p' másodfokú együtthatója $\mathbb{Z}_3$-ban eltűnt: $3 \cdot \overline{1}x^2 = (\overline{1} + \overline{1} + \overline{1})x^2 = \overline{0}x^2$. Sőt, az is előfordulhat, hogy az egész polinom eltűnik, pl. $p = x^6 + x^3 + \overline{1} \in \mathbb{Z}_3[x]$ deriváltja $p' = \overline{0}$. Ez azért baj, mert így nem működik a $p \,/\, \mathrm{lnko}(p, p')$ módszer a többszörös gyökök kiszűrésére (lásd a Polinomok jegyzetet) – pedig lenne mit kiszűrni: $p = x^6 + x^3 + \overline{1} = (x - \overline{1})^6$, azaz van egy hatszoros gyöke, $c = \overline{1}$.

6. Oszthatóság gyűrűkben

A korábbiakban megismertük az oszthatóság fogalmát egész számokra és polinomokra. Most ezt általánosítjuk gyűrűkre, egészen pontosan integritási tartományokra. Emlékeztető: a főbb integritási tartományok a $\mathbb{Z}$, a polinomgyűrűk ($K[x]$, ahol K integritási tartomány) és bármely test.
Legyen tehát ebben a szakaszban R tetszőleges integritási tartomány.

6.1. Definíció (osztó)**.** *$a \in R$ osztója $b \in R$-nek, ha $\exists c \in R : b = ac$.* Jelölés: $a \mid b$.

A definíció pontosan ugyanaz, mint egész számokra (pl. $2 \mid 6$) és polinomokra (pl. $x + 1 \mid x^2 + x$). Testben a fogalom triviális, mert minden elem osztható minden nemnull elemmel (hiszen $c := b/a$), pl. $\mathbb{Q}$-ban 5 osztható 2-vel, mert $5 = 2 \cdot (5/2)$.

Az oszthatóság általános tárgyalásához szükségünk lesz a következő két fogalomra:

6.2. Definíció (egység)**.** $u \in R$ *egység*, ha osztója az egységelemnek: $u \mid e$, ahol e az egységelem.

Ne keverjük össze az *egység* és az *egységelem* fogalmát: egységelemből csak egy van, egységből viszont több is lehet. Például:

1. $\mathbb{Z}$-ben két egység van: 1 és -1 (az 1 osztói).
2. $\mathbb{R}[x]$-ben minden nulladfokú polinom (azaz nemnulla konstans polinom) egység.
3. Általában $K[x]$-ben az egységek a K egységei (mint konstans polinomok), pl. $\mathbb{Z}[x]$-ben 1 és -1.
4. Testben minden elem egység, kivéve a nullelemet.

Megjegyzés: az egységek pontosan az invertálható elemek.

6.3. Definíció (asszociált)**.** $a \in R$ és $b \in R$ *asszociáltak*, ha egymás osztói: $a \mid b$ és $b \mid a$.

Például:

1. $\mathbb{Z}$-ben az asszociáltak az azonos abszolút értékű számok, pl. 5 és -5;
2. $\mathbb{R}[x]$-ben az asszociáltak az egymás nemnulla konstansszorosai, pl. $x-1$, $2x-2$, $-x+1$, $-x/2+1/2$ stb. mind asszociáltak.
3. Testben bármely két elem asszociált, kivéve a nullelemet.

Az asszociáltak mindig egymás egységszeresei, pl. $\mathbb{Z}$-ben $-5 = -1 \cdot 5$, $\mathbb{R}[x]$-ben $2x-2 = 2(x-1)$ stb. Az asszociáltaknak az a jelentősége, hogy oszthatóság szempontjából pontosan ugyanúgy viselkednek (pl. $2 \mid 6 \implies 2 \mid -6$ stb.). Azt is mondhatnánk, hogy az asszociáltak "lényegében" ugyanazok.

6.4. Definíció (triviális osztó)**.** $b \in R$ *triviális osztói* az egységek és b asszociáltjai.

Ez megfelel a $\mathbb{Z}$-beli definíciónak, pl. 6 triviális osztói 1, -1, 6 és -6.

A prímszám fogalmát a következőképpen általánosíthatjuk:

6.5. Definíció (irreducibilis elem)**.** Egy elem *irreducibilis* (vagy *felbonthatatlan*), ha nem a nullelem, nem egység, és csak triviális osztói vannak.

(A "nem a nullelem, nem egység" annak felel meg, hogy a prímszámoknál kizártuk a 0-t és az 1-et.)

Például:

1. $\mathbb{Z}$-ben az irreducibilis elemek a prímszámok és azok ellentettjei: $2, 3, 5, 7, \ldots, -2, -3, -5, -7, \ldots$ (A prímszámokat az egyszerűség kedvéért úgy definiáltuk, hogy pozitívak legyenek, de az általános esetben nem tudunk ilyen egyszerűen kiválasztani egyet az asszociáltak közül.)
2. $\mathbb{Z}[x]$-ben pl. az x^2-2 polinom irreducibilis, de $\mathbb{R}[x]$-ben nem az, mert $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$.
3. Testben nincsenek irreducibilis elemek (mert minden elem nullelem vagy egység).

Megjegyzés: az irreducibilis elemek asszociáltjai is irreducibilisek.

Polinomgyűrűkben vizsgáljuk meg alaposabban is az irreducibilis polinomokat:

1. Test fölött minden elsőfokú polinom irreducibilis, hiszen $p = ax + b$ osztói csak konstans és elsőfokú polinomok lehetnek, az előbbiek egységek, az utóbbiak pedig p asszociáltjai.
2. Magasabbfokú irreducibilis polinomnak nincs gyöke (az adott K alapgyűrűben), mert ha lenne, akkor kiemelhetnénk belőle egy gyöktényezőt, és akkor nem lenne irreducibilis.
3. $\mathbb{C}[x]$-ben csak az elsőfokú polinomok irreducibilisek, mert az algebra alaptétele miatt (lásd a Polinomok c. jegyzetet) minden nemkonstans polinomnak van gyöke.
4. $\mathbb{R}[x]$-ben csak első- és másodfokú polinomok lehetnek irreducibilisek (pl. $2x + 3$ és $x^2 + 1$ irreducibilisek $\mathbb{R}$ fölött).
5. $\mathbb{Z}[x]$-ben és $\mathbb{Q}[x]$-ben viszont az irreducibilis polinomok fokszáma tetszőlegesen nagy lehet, pl. minden $x^n - 2$ polinom irreducibilis.

Az egész számok körében a számelmélet alaptétele (lásd: Osztók, prímszámok) garantálta, hogy a prímtényezős felbontás egyértelmű. Ha ezt megpróbáljuk általánosítani integritási tartományokra, az nem mindegyikben fog működni, ezért külön kiemeljük azokat, amelyekben igen:

6.6. Definíció (Gauss-gyűrű)**.** Az R integritási tartományt *Gauss-gyűrű*nek nevezzük, ha a nullelem és az egységek kivételével minden elem egyértelműen felírható irreducibilis elemek szorzataként, ahol az egyértelműséget sorrendtől és asszociáltságtól eltekintve értjük. A Gauss-gyűrű angol neve: *unique factorization domain* (UFD).

A Gauss-gyűrű tehát az, amelyben az elemeket egyértelműen lehet faktorizálni. Az "asszociáltságtól eltekintve" azt jelenti, hogy pl. a $6 = 2 \cdot 3 = (-2) \cdot (-3)$ felbontásokat nem tekintjük különbözőnek, mert az egyetlen eltérés az, hogy 2 és 3 helyett azok asszociáltjai, -2 és -3 szerepelnek. (A számelmélet alaptételénél ezt a kitételt megúsztuk, mert azt csak pozitív számokra mondtuk ki.)

Példák:

1. $\mathbb{Z}$ a számelmélet alaptétele miatt Gauss-gyűrű. Például $-10 \in \mathbb{Z}$-t többféleképpen is fel lehet bontani: $-10 = (-2) \cdot 5 = 2 \cdot (-5) = 5 \cdot (-2) = (-5) \cdot 2$, de ezek mind csak sorrendben és asszociáltságban (azaz előjelban) térnek el egymástól.
2. Minden test triviálisan Gauss-gyűrű (mert minden eleme nullelem vagy egység).
3. Ha K Gauss-gyűrű, akkor $K[x]$ is Gauss-gyűrű, azaz $\mathbb{Z}[x]$, $\mathbb{R}[x]$, $\mathbb{Z}_5[x]$ stb. mind Gauss-gyűrű. Például $\mathbb{R}[x]$-ben $x^2 - 1 = (x+1)(x-1) = (2x+2)(x/2-1/2) = (-3x+3)(-x/3-1/3)$ stb., de ezek csak sorrendben és asszociáltságban (azaz konstans szorzóban) térnek el egymástól.

Sage-ben az egész számokra megismert `factor()` függvény tetszőleges Gauss-gyűrűre működik, a következő kiegészítéssel: az irreducibilis tényezőket úgy választja meg (az asszociáltak közül), hogy a lehető legegyszerűbbek legyenek (pl. $\mathbb{Z}$-ben pozitívak), viszont ha így nem jönne ki a szorzat (mert pl. negatív számot bontunk fel), akkor a szorzat elejére kiemel egy egységet (pl. -1). A `factor()` eredménye sorozatként viselkedik (pl. egy `for`-ciklussal felsorolható), de az esetleges egység ebben nem szerepel, hanem külön lekérdezhető a `unit()` tagfüggvénnyel. Például:

```
sage: F = factor(-40)
sage: F
-1 * 2^3 * 5
sage: for (p, n) in F:
....:     print(p, n)
2 3
5 1
sage: F.unit()
-1
sage: P.<x> = QQ[]
sage: F = factor(2*x^2 - 1/2)
sage: F
(2) * (x - 1/2) * (x + 1/2)
sage: [p for (p, n) in F]
[x - 1/2, x + 1/2]
sage: F.unit()
2
```

Végezetül még két ismerős fogalmat általánosítunk tetszőleges integritási tartományra:

6.7. Definíció (lnko)**.** $a \in R$ és $b \in R$ *legnagyobb közös osztója* $c \in R$, ha
$c \mid a \ \wedge \ c \mid b \ \wedge \ \forall d \in R : d \mid a \ \wedge \ d \mid b \implies d \mid c$. Jelölés: $\text{lnko}(p, q)$ (angolul: $\gcd(p, q)$).

6.8. Definíció (lkkt)**.** $a \in R$ és $b \in R$ *legkisebb közös többszöröse* $c \in R$, ha
$a \mid c \ \wedge \ b \mid c \ \wedge \ \forall d \in R : a \mid d \ \wedge \ b \mid d \implies c \mid d$. Jelölés: $\text{lkkt}(a, b)$ (angolul: $\text{lcm}(a, b)$).

Ezekkel a fogalmakkal általánosan, integritási tartományokban két probléma van: egyrészt nem biztos, hogy léteznek, másrészt nem egyértelműek. Ezért bizonyos megszorításokat kell tenni:

6.9. Tétel. *Gauss-gyűrűben bármely két elemnek van legnagyobb közös osztója és legkisebb közös többszöröse.*

Tehát $\mathbb{Z}$-ben, $\mathbb{Z}[x]$-ben, $\mathbb{R}[x]$-ben stb. létezik lnko és lkkt. (A tétel nem meglepő, gondoljunk csak arra, hogy $\mathbb{Z}$-ben hogyan lehet ezeket kiszámítani a faktorizáció segítségével.)

6.10. Tétel. *A legnagyobb közös osztó és a legkisebb közös többszörös, ha létezik, asszociáltságtól eltekintve egyértelmű.*

Ez azt jelenti, hogy két elemnek lehet több lnko-ja, de azok mind egymás asszociáltjai (és hasonlóan az lkkt-ra is). A polinomoknál már láttuk, hogy ez mit jelent: az lnko-k mind egymás konstansszorosai. Az egész számoknál pedig csak azért volt egyértelműség, mert ott kikötöttük, hogy az eredménynek $\mathbb{N}$-ben kell lennie (különben pl. $\text{lnko}(6, 4)$ lehetne 2 és -2 is).

7. Testbővítések

7.1. Definíció. Az F test *testbővítése* a G testnek, ha $G \subseteq F$, és a megfelelő műveleteik ($+$ és $\cdot$) G-ben egybeesnek.

Például $\mathbb{Q}$-nak testbővítése az $\mathbb{R}$, és mindkettőnek testbővítése a $\mathbb{C}$.

7.2. Definíció. Az F test *egyszerű bővítése* a G testnek, ha $\exists \alpha \in F \setminus G$, hogy F a legszűkebb olyan testbővítése G-nek, amely tartalmazza α-t. Jelölés: $F = G(\alpha)$. Ekkor F-et az α *által generált test*nek nevezzük (G fölött), α-t pedig a testbővítés *primitív elem*ének.

Például $\mathbb{C}$ egyszerű bővítése $\mathbb{R}$-nek: $\mathbb{C} = \mathbb{R}(i)$, mert nincs más olyan $F \subset \mathbb{C}$ testbővítése $\mathbb{R}$-nek, amely tartalmazza az i-t. A test ugyanis zárt az összeadásra és a szorzásra, tehát ha benne van az i, akkor tartalmaznia kell a $2i$, $-5i$, $i + 1$, $2i - 3/2$ stb. elemeket is, vagyis az összes $a + bi$ alakú számot, ahol $a, b \in \mathbb{R}$, ez pedig már maga a $\mathbb{C}$.

Viszont $\mathbb{R}$ *nem* egyszerű bővítése $\mathbb{Q}$-nak, mert nem tudunk olyan α számot találni, amelyre $\mathbb{R} = \mathbb{Q}(\alpha)$ lenne. (Ennek oka a halmazok számosságában keresendő: $\mathbb{Q}$ megszámlálhatóan végtelen, $\mathbb{R}$ viszont kontinuum, azaz "sokkal nagyobb".)

Testbővítéssel új testeket is létre tudunk hozni. Például mi lesz $\mathbb{Q}(\sqrt{2})$? (Ugye $\sqrt{2} \notin \mathbb{Q}$.) Ennek a racionális számokon kívül tartalmaznia kell a $\sqrt{2}$-t, valamint minden olyan számot, hogy a műveletek elvégezhetőek legyenek. Belátható, hogy $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Például a szorzás így végezhető el: $(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$, a multiplikatív inverz pedig gyöktelenítéssel számítható ki: $(a + b\sqrt{2})^{-1} = \dfrac{a}{a^2 - 2b^2} + \dfrac{-b}{a^2 - 2b^2}\sqrt{2}$. (Vegyük észre, hogy $\mathbb{Q}(\sqrt{2})$ mennyire hasonlít $\mathbb{C} = \mathbb{R}(i)$-re. Ez nem véletlen: az egyszerű testbővítések hasonlóan működnek.)

Most nézzünk olyan testeket, amelyeknek véges sok elemük van. Ilyen például minden $\mathbb{Z}_p$, ha p prímszám. Ezeket is bővíthetjük a fenti módon, például hozzuk létre a $\mathbb{Z}_3(\sqrt{2})$ testet. De mit jelent itt az, hogy $\sqrt{2}$? Olyan értéket, amelynek a négyzete $\overline{2} \in \mathbb{Z}_3$. Ilyen elem $\mathbb{Z}_3$-ban nincs (mert

$\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$ és $\overline{2}^2 = \overline{1}$), tehát valóban bővítjük a testet. A kapott test hasonlít $\mathbb{Q}(\sqrt{2})$-höz: $\mathbb{Z}_3(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}_3\}$, pl. $\overline{1} + \overline{2}\sqrt{2} \in \mathbb{Z}_3(\sqrt{2})$, és számolni is hasonlóan lehet benne. Így tehát előállítottunk egy új véges testet, amelynek $3^2 = 9$ eleme van (mert a és b is 3-3-féle lehet).
Ennek a konstrukciónak az a jelentősége, hogy így *minden* véges testet megkapunk:

7.3. Tétel (a véges testek tulajdonságai)**.**

1. *Minden véges test elemszáma p^k alakú, ahol p prímszám és $k \geq 1$.*
2. *Minden p^k-ra létezik ilyen elemszámú véges test, és ez izomorfizmus erejéig egyértelmű.*
3. *A p^k-elemű véges test a $\mathbb{Z}_p$ egyszerű testbővítése (ha $k \geq 2$, különben pedig izomorf vele).*

7.4. Definíció. A q elemből álló véges testet $\mathbb{F}_q$-val jelöljük.

Vagyis minden prímhatvány elemszámra egyértelműen létezik véges test: $\mathbb{F}_2(= \mathbb{Z}_2)$, $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_{16}$, …, $\mathbb{F}_3(= \mathbb{Z}_3)$, $\mathbb{F}_9(= \mathbb{Z}_3(\sqrt{2}))$, $\mathbb{F}_{27}$, …, $\mathbb{F}_5(= \mathbb{Z}_5)$, $\mathbb{F}_{25}$, …. Viszont nem létezik például $\mathbb{F}_6$ vagy $\mathbb{F}_{10}$, mert azok nem prímhatványok. Fontos: ne keverjük össze az $\mathbb{F}_m$-et a $\mathbb{Z}_m$-mel, mert $\mathbb{F}_4 \neq \mathbb{Z}_4$, $\mathbb{F}_9 \neq \mathbb{Z}_9$ stb., ráadásul a legtöbb $\mathbb{Z}_m$ nem is test. Csak prímszámokra igaz, hogy $\mathbb{F}_p = \mathbb{Z}_p$.

(Az "izomorfizmus erejéig egyértelmű" azt jelenti, hogy két azonos elemszámú test még ha névleg különböző, akkor is izomorf, azaz az egyikből megkaphatjuk a másikat az elemek átnevezésével. Például belátható, hogy a logikai értékek (I = "igaz", H = "hamis") halmaza a "kizáró vagy" ($\oplus$) és az "és" ($\wedge$) művelettel, azaz $(\{\mathrm{I}, \mathrm{H}\}, \oplus, \wedge)$ testet alkot. Ez eléggé különbözőnek tűnik a $(\mathbb{Z}_2, +, \cdot)$ testtől, de "lényegében" mégis ugyanazok (izomorfak), mert a $\mathrm{H} \to \overline{0}$, $\mathrm{I} \to \overline{1}$ átnevezésekkel megkapjuk az elsőből a másodikat, pl. $\mathrm{I} \oplus \mathrm{I} = \mathrm{H} \to \overline{1} + \overline{1} = \overline{0}$, $\mathrm{H} \wedge \mathrm{I} = \mathrm{H} \to \overline{0} \cdot \overline{1} = \overline{0}$ stb.)

A testbővítéshez használt primitív elemet általában nem explicit képlettel adjuk meg (pl. $\sqrt{2}$), hanem egy szabállyal, amit teljesítenie kell (pl. hogy $\alpha^2 = 2$), egészen pontosan egy polinommal (pl. $x^2 - 2$), amelynek gyöke kell hogy legyen. Bebizonyítható, hogy erre bármely legalább másodfokú irreducibilis polinom alkalmas. Ezt hívjuk a primitív elem *minimálpolinom*jának.

Sage-ben az $\mathbb{F}_q$ véges testet a `GF(q)` függvénnyel hozhatjuk létre (GF = "Galois field"):

```
sage: GF(4)
Finite Field in z2 of size 2^2
sage: GF(4).list()
[0, z2, z2 + 1, 1]
sage: a = GF(4).gen()   # primitív elem (a fenti z2)
sage: a.minpoly()       # minimálpolinom
x^2 + x + 1
sage: a^2 + a + 1       # tényleg gyöke?
0
sage: GF(6)
[...]
ValueError: the order of a finite field must be a prime power
```

8. Szerző

Ezt a jegyzetet Uray M. János írta, részben felhasználva Nagy Ádám jegyzetét:
https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa
Hibákat, észrevételeket itt lehet jelezni: uray.janos@inf.elte.hu.