Véges testek

Diszkrét modellek alkalmazásai

Ebben a jegyzetben *test*ekről lesz szó (lásd: Algebrai struktúrák). Emlékeztető: a test a gyűrű speciális esete, amelyben – többek között – minden elemnek van multiplikatív inverze (vagy leegyszerűsítve: ahol osztani is lehet). A főbb testek a számtestek: $\mathbb{Q}$, $\mathbb{R}$ és $\mathbb{C}$ (de *nem* test a $\mathbb{Z}$), valamint fontos test még a $\mathbb{Z}_p$, ahol p tetszőleges prímszám. Ebben a jegyzetben az ismert testekből újakat fogunk létrehozni.

1. Testbővítés

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

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

1.2. Definíció. Az F testnek **egyszerű bővítése** a G test, ha $\exists \theta \in G \setminus F$, hogy G a legszűkebb olyan testbővítése F-nek, amely tartalmazza θ-t. Jelölés: $G = F(\theta)$. Ekkor G-t az $\boldsymbol{\theta}$ **által generált test**nek nevezzük (F fölött), θ-t pedig a testbővítés **primitív elem**ének. (θ kiejtése: "teta".)

Példa. $\mathbb{C}$ egyszerű bővítése $\mathbb{R}$-nek: $\mathbb{C} = \mathbb{R}(i)$, mert $i \in \mathbb{C} \setminus \mathbb{R}$, de nincs olyan $\mathbb{C}$-nél szűkebb 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 $\mathbb{C}$.

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

Példa. Hozzunk létre egy új testet: $\mathbb{Q}(\sqrt{2})$, azaz bővítsük a racionális számtestet, $\mathbb{Q}$-t a $\sqrt{2}$-vel (ugye $\sqrt{2} \notin \mathbb{Q}$). Ez tartalmaz minden racionális számot, tartalmazza a $\sqrt{2}$-t, valamint minden olyan számot, hogy a műveletek elvégezhetőek legyenek, azaz pl. $2\sqrt{2}$, $1+\sqrt{2}$, $5/2+\sqrt{2}/3 \in \mathbb{Q}(\sqrt{2})$. Belátható, hogy $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Ebben a műveletek így végezhetőek el:

- Az összeadás és a kivonás triviális, csak tagonként történik, például:
$$(1+3\sqrt{2}) + (3-2\sqrt{2}) = 4+\sqrt{2}.$$
- A szorzás is nagyon egyszerű, csak azt kell kihasználni, hogy $\sqrt{2}\cdot\sqrt{2} = 2$, például:
$$(1+\sqrt{2})(3+2\sqrt{2}) = 3+2\sqrt{2}+3\sqrt{2}+2\sqrt{2}^2 = 3+5\sqrt{2}+4 = 7+5\sqrt{2}.$$
- Multiplikatív inverzet számítani (vagy osztani) pedig *gyöktelenítéssel* lehet, például:
$$(5+2\sqrt{2})^{-1} = \frac{1}{5+2\sqrt{2}} = \frac{5-2\sqrt{2}}{(5+2\sqrt{2})(5-2\sqrt{2})} = \frac{5-2\sqrt{2}}{25-8} = \frac{5}{17} + \frac{-2}{17}\sqrt{2}.$$

Vegyük észre, hogy a $\mathbb{Q}(\sqrt{2})$-ben való számolás mennyire hasonlít $\mathbb{C} = \mathbb{R}(i)$-re. Ez nem véletlen, hiszen mindkettő egy egyszerű testbővítés. A különbség az, hogy ott $\sqrt{2}$ helyett i van, amelyre $i^2 = -1$, és hogy az együtthatók $\mathbb{Q}$ helyett $\mathbb{R}$-ben vannak.

Példa. Tekintsünk $\mathbb{Q}(\sqrt[3]{2})$-t. Ez abban különbözik $\mathbb{Q}(\sqrt{2})$-től és $\mathbb{C} = \mathbb{R}(i)$-től, hogy itt már nem elég a két együttható (a és b): ha ugyanis két $a+b\sqrt[3]{2}$ alakú számot összeszorzunk, akkor az eredményben megjelenik a $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{2}^2$ is, amelyet nem tudunk $a + b\sqrt[3]{2}$ alakban felírni. Ezért itt *három* együtthatóra lesz szükség: $\mathbb{Q}(\sqrt[3]{2}) = \{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2 \mid a, b, c \in \mathbb{Q}\}$. Az ilyen elemek összeszorzásakor megjelennek ugyan $\sqrt[3]{2}$ magasabb kitevőjű hatványai is, de azok már nem jelentenek problémát, mert $\sqrt[3]{2}^3 = 2$ és $\sqrt[3]{2}^4 = 2\sqrt[3]{2}$. Például:

$$\begin{aligned}(5 + \sqrt[3]{2}^2)(\sqrt[3]{2} - \sqrt[3]{2}^2) &= 5\sqrt[3]{2} - 5\sqrt[3]{2}^2 + \sqrt[3]{2}^3 - \sqrt[3]{2}^4 = \\ &= 5\sqrt[3]{2} - 5\sqrt[3]{2}^2 + 2 - 2\sqrt[3]{2} = \\ &= 2 + 3\sqrt[3]{2} - 5\sqrt[3]{2}^2.\end{aligned}$$

2. Testbővítések szerkezete

Általában a testbővítéshez használt primitív elemet nem közvetlenül (explicit képlettel) adjuk meg (pl. $\sqrt{2}$), hanem egy szabállyal, amelyet teljesítenie kell (pl. hogy $\theta^2 = 2$). Erre legtöbbször egy polinomot használunk (pl. $x^2 - 2$), amelynek a gyöke kell hogy legyen a primitív elem.

2.1. Tétel. *Legyen $F(\theta)$ az F test egy egyszerű testbővítése, ahol θ egy olyan $m \in F[x]$ polinom gyöke, amely **irreducibilis**, fokszáma $n \geq 2$, és főegyütthatója 1. Ekkor bármely $\alpha \in F(\theta)$ elem egyértelműen felírható a következő alakban:*

$$\alpha = a_0 + a_1\theta + a_2\theta^2 + \ldots + a_{n-1}\theta^{n-1},$$

ahol $a_0, a_1, \ldots, a_{n-1} \in F$; más szóval egyértelműen létezik olyan $p_\alpha \in F[x]$ legfeljebb $n-1$-edfokú polinom, amelyre $\alpha = p_\alpha(\theta)$.

2.2. Definíció. A fenti tételben szereplő m irreducibilis polinom a θ **minimálpolinomja**, annak fokszáma, $n = \deg m$ pedig a testbővítés **foka**.

Példa. $\mathbb{Q}(\sqrt{2})$ egy másodfokú testbővítése $\mathbb{Q}$-nak, ahol $\sqrt{2}$ minimálpolinomja $m = x^2 - 2$, és minden $\alpha \in \mathbb{Q}(\sqrt{2})$ elem egyértelműen felírható $\alpha = a + b\sqrt{2}$ alakban, ahol $a, b \in \mathbb{Q}$ (azaz felírható egy $p_\alpha = a + bx$ legfeljebb elsőfokú polinommal).

Példa. $\mathbb{C} = \mathbb{R}(i)$ egy másodfokú testbővítése $\mathbb{R}$-nek, ahol i minimálpolinomja $m = x^2 + 1$, és minden $z \in \mathbb{C}$ komplex szám komplex szám egyértelműen felírható $z = a + bi$ alakban (ahol $a, b \in \mathbb{R}$).

Példa. $\mathbb{Q}(\sqrt[3]{2})$ egy harmadfokú testbővítése $\mathbb{Q}$-nak, ahol $\sqrt[3]{2}$ minimálpolinomja $m = x^3 - 2$, és minden $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ elem egyértelműen felírható $\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$ alakban (ahol $a, b, c \in \mathbb{Q}$), ami egy $p_\alpha = a + bx + cx^2$ legfeljebb másodfokú polinomnak felel meg.

Egy egyszerű testbővítésnek több primitív eleme is lehet. Például $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(2\sqrt{2} + 1)$, azaz nemcsak a $\sqrt{2}$, hanem a $\theta = 2\sqrt{2} + 1$ (minimálpolinomja: $x^2 - 2x - 7$) segítségével is felírható $\mathbb{Q}(\sqrt{2})$ minden eleme $a + b\theta$ alakban (persze más a-val és b-vel). Például ha $\alpha = 4 + 3\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, akkor ugyanezt $\theta = 2\sqrt{2} + 1$-gyel így írhatjuk fel: $\alpha = 5/2 + 3/2 \cdot \theta$. (De az együtthatók száma továbbra is kettő, azaz a testbővítés foka független a primitív elem választásától.)

Most vizsgáljuk meg, hogyan lehet műveleteket végezni $F(\theta)$-ban. Legyen θ minimálpolinomja $m \in F[x]$, annak fokszáma $n = \deg m$. Ekkor tehát $F(\theta)$ elemeit $\alpha = a_0 + a_1\theta + \ldots + a_{n-1}\theta^{n-1}$ alakban írjuk fel, azaz egy legfeljebb $n-1$-edfokú $p_\alpha = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ polinommal. A számolás során alapvetően ezeken az ábrázoló polinomokon végezzük el a megfelelő műveleteket, de ez nem minden műveletnél ilyen egyszerű:

1. **Összeadás, kivonás:** egyszerűen összeadjuk, ill. kivonjuk az ábrázoló polinomokat.
2. **Szorzás:** nem elég összeszorozni a két polinomot, mert a szorzat fokszáma $n-1$-nél nagyobb is lehet, hanem venni kell még a szorzat maradékát a minimálpolinom (m) szerint. Pl. $\mathbb{Q}(\sqrt{2})$-ben:
$$\alpha = 1 + \sqrt{2} \quad \longrightarrow \quad p_\alpha = 1 + x,$$
$$\beta = 3 + 2\sqrt{2} \quad \longrightarrow \quad p_\beta = 3 + 2x,$$
$$p_{\alpha\beta} = p_\alpha p_\beta \bmod m = (1+x)(3+2x) \bmod (x^2-2) = (3 + 5x + 2x^2) \bmod (x^2-2) = 7 + 5x,$$
$$\longrightarrow \quad \alpha\beta \quad = \quad (1+\sqrt{2})(3+2\sqrt{2}) \quad = \quad 3 + 5\sqrt{2} + 2\sqrt{2}^2 \quad = \quad 7 + 5\sqrt{2}.$$
Az $x^2 - 2$-vel való maradékképzés annak felel meg, hogy alkalmazzuk a $\sqrt{2}^2 = 2$ azonosságot. (Megjegyzés: a $p_\alpha p_\beta \bmod m$ műveletsor nagyon hasonlít arra, ahogy kongruenciákkal számoltunk, pl. $3 \cdot 6 \equiv 8 \pmod{10}$, csak itt egész számok helyett polinomok vannak.)
3. **Multiplikatív inverz:** erre többféle módszer is létezik:
   (a) **Gyöktelenítéssel:** ezt fent $\mathbb{Q}(\sqrt{2})$-re már láttuk, és minden olyan másodfokú testbővítésre működik, ahol a minimálpolinom $x^2 - d$ alakú (azaz $\theta = \sqrt{d}$, pl. $\sqrt{2}$ vagy $i = \sqrt{-1}$):
   $$(a+b\theta)^{-1} = \frac{1}{a+b\theta} = \frac{a-b\theta}{(a+b\theta)(a-b\theta)} = \frac{a-b\theta}{a^2-b^2d} = \frac{a}{a^2-b^2d} - \frac{b}{a^2-b^2d}\theta.$$
   (Másfajta testbővítésekre is általánosítható, de nem triviális, hogy mivel gyöktelenítünk.)
   (b) **Egyenletrendszerrel:** írjuk be az $\alpha\alpha^{-1} = 1$ egyenletbe α és α^{-1} felírását, és oldjuk meg a kapott egyenletrendszert α^{-1} ismeretlen együtthatóira. Pl. $\mathbb{Q}(\sqrt{2})$-ben $\alpha = 5 + 2\sqrt{2}$-re:
   $$\alpha\alpha^{-1} = 1,$$
   $$(5 + 2\sqrt{2})(u + v\sqrt{2}) = 1,$$
   $$5u + 5v\sqrt{2} + 2u\sqrt{2} + 4v = 1 + 0\sqrt{2},$$
   ebből különválasztva a racionális és a $\sqrt{2}$-s tagokat (eliminálva $\sqrt{2}$-t):
   $$5u + 4v = 1,$$
   $$2u + 5v = 0,$$
   és ezt megoldva megkapjuk, hogy $u = 5/17$ és $v = -2/17$, azaz $\alpha^{-1} = 5/17 - 2/17 \cdot \sqrt{2}$.
   (c) **Bővített euklideszi algoritmussal:** mint tudjuk, az egész számok moduláris inverzét kiszámíthatjuk a bővített euklideszi algoritmussal (lásd: Kongruenciák):
   $$7x \equiv 1 \pmod{10} \quad \longrightarrow \quad \mathrm{xgcd}(7, 10) = (1, 3, -2) \quad \longrightarrow \quad x = 3.$$
   Ugyanez működik polinomokra is: pl. $\mathbb{Q}(\sqrt{2})$-ben $\alpha = 5 + 2\sqrt{2}$ inverzét $p_\alpha = 5 + 2x$ és $m = x^2 - 2$ bővített euklideszi algoritmusával számíthatjuk ki:
   $$\alpha\alpha^{-1} = 1 \quad \longrightarrow \quad p_\alpha p_{\alpha^{-1}} \bmod m = 1 \quad \longrightarrow$$
   $$\mathrm{xgcd}(p_\alpha, m) = \mathrm{xgcd}(5 + 2x,\ x^2 - 2) = (1,\ 5/17 - 2/17 \cdot x,\ 4/17)$$
   $$\longrightarrow \quad p_{\alpha^{-1}} = 5/17 - 2/17 \cdot x \quad \longrightarrow \quad \alpha^{-1} = 5/17 - 2/17 \cdot \sqrt{2}.$$
4. **Osztás:** multiplikatív inverzzel szorzunk: $\alpha/\beta = \alpha\beta^{-1}$.

3. Véges testek

Nemcsak számtesteket bővíthetünk a fent megismert módon, hanem a $\mathbb{Z}_p$ testeket is, ahol p prímszám (lásd: Kongruenciák, ill. Algebrai struktúrák). Emlékeztető: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{p-1}\}$, ahol modulo p kell számolni, pl. $\mathbb{Z}_5$-ben $\overline{3}+\overline{4}=\overline{2}$, $\overline{1}-\overline{4}=\overline{2}$, $\overline{3}\cdot\overline{2}=\overline{1}$ és $\overline{3}^{-1}=\overline{2}$.

Példa. Bővítsük $\mathbb{Z}_5$-öt a $\mathbb{Q}(\sqrt{2})$-höz hasonló módon. Itt a "$\sqrt{2}$" egy olyan "képzeletbeli" θ érték, amelyre $\theta^2=\overline{2}\in\mathbb{Z}_5$ (azaz amelynek minimálpolinomja $m=x^2-\overline{2}\in\mathbb{Z}_5[x]$). Fontos, hogy θ ne legyen benne $\mathbb{Z}_5$-ben, mert akkor nem bővítésről lenne szó (mint ahogy $\mathbb{Q}(\sqrt{4})$ sem az, hiszen $\sqrt{4}=2\in\mathbb{Q}$). Ezt egyszerű ellenőrizni: $\overline{0}^2=\overline{0}$, $\overline{1}^2=\overline{1}$, $\overline{2}^2=\overline{4}$, $\overline{3}^2=\overline{4}$ és $\overline{4}^2=\overline{1}$, vagyis $\mathbb{Z}_5$ egyik elemének sem $\overline{2}$ a négyzete, azaz nincs benne "$\sqrt{2}$". Az így kapott $\mathbb{Z}_5(\theta)$ test elemei $a+b\theta$ alakúak (ahol $a,b\in\mathbb{Z}_5$), pl. $\overline{1}+\overline{3}\theta\in\mathbb{Z}_5(\theta)$, és nagyon hasonlóan lehet velük számolni, mint $\mathbb{Q}(\sqrt{2})$-ben:

$$(\overline{1}+\overline{3}\theta)-(\overline{4}+\theta)=(\overline{1}-\overline{4})+(\overline{3}-\overline{1})\theta=\overline{2}+\overline{2}\theta,$$

$$(\overline{1}+\overline{3}\theta)(\overline{4}+\theta)=\overline{4}+\theta+\overline{4}\cdot\overline{3}\theta+\overline{3}\theta^2=\overline{4}+\theta+\overline{2}\theta+\overline{3}\cdot\overline{2}=\overline{4}+\overline{3}\theta+\overline{1}=\overline{3}\theta,$$

$$(\overline{1}+\overline{3}\theta)^{-1}=\frac{\overline{1}}{\overline{1}+\overline{3}\theta}=\frac{\overline{1}-\overline{3}\theta}{(\overline{1}+\overline{3}\theta)(\overline{1}-\overline{3}\theta)}=\frac{\overline{1}-\overline{3}\theta}{\overline{1}^2-\overline{3}^2\cdot\overline{2}}=\frac{\overline{1}}{\overline{3}}-\frac{\overline{3}}{\overline{3}}\theta=\overline{2}-\theta=\overline{2}+\overline{4}\theta.$$

Ennek a testnek véges sok eleme van ($5^2=25$, hiszen $a+b\theta$ mindkét együtthatója 5-5-féle lehet):

$$\begin{array}{ccccc}
\overline{0}, & \overline{1}, & \overline{2}, & \overline{3}, & \overline{4},\\
\theta, & \theta+\overline{1}, & \theta+\overline{2}, & \theta+\overline{3}, & \theta+\overline{4},\\
\overline{2}\theta, & \overline{2}\theta+\overline{1}, & \overline{2}\theta+\overline{2}, & \overline{2}\theta+\overline{3}, & \overline{2}\theta+\overline{4},\\
\overline{3}\theta, & \overline{3}\theta+\overline{1}, & \overline{3}\theta+\overline{2}, & \overline{3}\theta+\overline{3}, & \overline{3}\theta+\overline{4},\\
\overline{4}\theta, & \overline{4}\theta+\overline{1}, & \overline{4}\theta+\overline{2}, & \overline{4}\theta+\overline{3}, & \overline{4}\theta+\overline{4}.
\end{array}$$

3.1. Definíció. A véges sok elemből álló testet **véges test**nek (vagy **Galois-test**nek) nevezzük.

A fenti konstrukció általánosan a következőképpen működik:

- Vegyünk egy $\mathbb{Z}_p$ alaptestet (ahol p prímszám).
- Vegyünk afölött egy $m\in\mathbb{Z}_p[x]$ irreducibilis polinomot, amelynek fokszáma $n\geq 2$.
- Ez lesz a minimálpolinom, amelynek gyöke a θ primitív elem. (θ-nak nem kell "létező" értéknek lennie, mint ahogy a komplex i is csak egy "képzeletbeli" érték volt, amelynek a négyzete -1.)
- Az így kapott $\mathbb{Z}_p(\theta)$ test elemei $a_0+a_1\theta+\ldots+a_{n-1}\theta^{n-1}$ alakban írhatók fel, ahol $a_i\in\mathbb{Z}_p$.
- Mivel minden a_i együttható p-féle lehet, ezért a testben összesen $pp\cdots p=p^n$ elem van.

Ennek a konstrukciónak az a jelentősége, hogy így *minden* véges testet megkapunk:

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

1. *A fenti konstrukció minden p prímszámra és minden $n\geq 2$ fokszámra elvégezhető.*
2. *A p^n-elemű véges test izomorfizmus erejéig egyértelmű.*
3. *Minden véges test elemszáma p^n alakú, ahol p prímszám és $n\geq 1$.*

3.3. Definíció. A q elemből álló véges test jelölése: $\mathbb{F}_q$ (vagy $\mathrm{GF}(q)$ [*Galois field*]).

Vagyis minden prímhatvány elemszámra egyértelműen létezik véges test:

- $\mathbb{F}_2(=\mathbb{Z}_2)$, $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_{16}$, …,
- $\mathbb{F}_3(=\mathbb{Z}_3)$, $\mathbb{F}_9$, $\mathbb{F}_{27}$, …,
- $\mathbb{F}_5(=\mathbb{Z}_5)$, $\mathbb{F}_{25}$, …,
- …;

más véges test pedig nem létezik, például nincs $\mathbb{F}_6$ 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. (pl. $\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$, de $\mathbb{F}_4 = \{\overline{0}, \overline{1}, \theta, \theta + \overline{1}\}$), ráadásul a legtöbb $\mathbb{Z}_m$ nem is test. Csak prímszámokra igaz, hogy $\mathbb{F}_p = \mathbb{Z}_p$.

(A tétel "izomorfizmus erejéig egyértelmű" kitétele azt jelenti, hogy két azonos elemszámú test 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 ugyanaz (= "izomorfak"), mert a $\mathrm{H} \to \overline{0}$, $\mathrm{I} \to \overline{1}$ átnevezésekkel megkapjuk az egyikből a másikat, 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.)

4. Testbővítések Sage-ben

Sage-ben az $\mathbb{F}_q$ véges testet a `GF(q)` jelöléssel hozhatjuk létre:

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

Megadhatunk egy minimálpolinomot is, ezáltal előírhatjuk, hogy az elemek ábrázolásához melyik θ primitív elemet használja, például a fenti $\mathbb{F}_{25} = \mathbb{Z}_5(\theta)$ testre (θ-t a kódban `g`-vel jelöljük):

```
sage: F = GF(25, "g", modulus = x^2 - 2)
sage: g = F.gen()
sage: g^2
2
sage: 1/(1 + 3*g)
4*g + 2
```

A polinomokhoz hasonlóan itt is van egy egyszerűsített szintaxis `F` és `g` együttes létrehozására:

```
sage: F.<g> = GF(25, modulus = x^2 - 2)   # F = GF(...) és g = F.gen()
sage: g^2
2
sage: F.<g> = GF(25, modulus = x^2 - 3)   # GF(25) egy másik ábrázolása
sage: g^2
3
sage: (2*g)^2     # "fenti g" == "itteni 2*g"
2
sage: F.<g> = GF(25, modulus = x^2 - 4)   # irreducibilis minimálpolinom kell
[...]
ValueError: finite field modulus must be irreducible but it is not
```

A test elemeit létrehozhatjuk az együtthatók listájából, valamint az ábrázoló polinomból is:

```
sage: F.<g> = GF(27)      # Zmod(3) harmadfokú bővítése (minimálpolinom mindegy)
sage: P.<x> = Zmod(3)[]   # ilyenek az ábrázoló polinomok
sage: F([1,1,2])
2*g^2 + g + 1
sage: F(2*x^2 + x + 1)
2*g^2 + g + 1
sage: P(2*g^2 + g + 1)
2*x^2 + x + 1
sage: P(2*g^2 + g + 1).list()
[1, 1, 2]
```

Létrehozhatunk véges test fölötti polinomgyűrűt is, pl. $\mathbb{F}_{25}[x]$-et (ahol tehát a polinomok minden együtthatója $\mathbb{F}_{25}$-ben van, vagyis maguk is külön-külön polinomokként ábrázolhatók):

```
sage: F.<g> = GF(25, modulus = x^2 - 2)
sage: P.<x> = F[]
sage: P([1 + g, 3 + 2*g, 4*g, 2])
2*x^3 + 4*g*x^2 + (2*g + 3)*x + g + 1
sage: _.list()
[g + 1, 2*g + 3, 4*g, 2]
sage: (x-g)*(x-g-1)*(x-g-2)*(x-g-3)*(x-g-4)
x^5 + 4*x + 2*g
sage: _.roots()
[(g, 1), (g + 4, 1), (g + 3, 1), (g + 2, 1), (g + 1, 1)]
```

Nemcsak véges testeket, hanem a $\mathbb{Q}$ testbővítéseit is létrehozhatjuk, például $\mathbb{Q}(\sqrt{2})$-t:

```
sage: F.<g> = NumberField(x^2 - 2)
sage: g^2
2
sage: 1/(5 + 2*g)
-2/17*g + 5/17
```

5. Advanced Encryption Standard (AES)

Az **Advanced Encryption Standard (AES)** (eredeti nevén: Rijndael) az egyik leggyakrabban használt titkosítási (kriptográfiai) algoritmus. Rengeteg helyen használják, az internetes kommunikációtól (pl. HTTPS) a háttértáron lévő fájlok titkosításán keresztül az USA kormányának legtitkosabb dokumentumaiig. Népszerűségét nemcsak biztonsága, hanem rendkívüli gyorsasága is adja.

Az AES egy *szimmetrikus* titkosítás, azaz ugyanazzal a kulccsal titkosítja az üzenetet, mint amellyel megfejti (ellentétben pl. az RSA-val, amely *aszimetrikus*, lásd: Euler–Fermat-tétel és RSA).

Az AES teljes algoritmusát nem írjuk le, mert viszonylag bonyolult, csak egyes – matematikailag érdekesebb – részeit. A teljes algoritmus megtalálható a specifikációban: [3].

Az üzenetet 128-bites blokkonként titkosítjuk. Egy ilyen blokk 16 byte-ból áll, ezeket képzeletben egy 4×4-es mátrixba írjuk fel oszlopfolytonosan:

$$B = \begin{pmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{pmatrix}.$$

A byte-okat az $\mathbb{F}_{2^8} = \mathbb{F}_{256}$ véges test elemeiként ábrázoljuk, ahol a $\theta \in \mathbb{F}_{256}$ primitív elem az $m = x^8 + x^4 + x^3 + x + \overline{1}$ minimálpolinom gyöke. A byte bitjei az ábrázoló polinom együtthatói, például a [01001011] byte a $\theta^6 + \theta^3 + \theta + \overline{1} \in \mathbb{F}_{256}$ elemnek felel meg.

A titkosítási algoritmus ciklusonként négy lépésből áll, ezekre az angol nevükkel hivatkozunk:

1. *SubBytes*: a byte-ok egyenkénti transzformációja;
2. *ShiftRows*: a sorok ciklikus permutációja;
3. *MixColumns*: a mátrix szorzása egy konstans mátrixszal;
4. *AddRoundKey*: a kulcs alkalmazása a blokkra.

A teljes algoritmus ezt a négy lépést ismétli 10-14-szer (a paraméterektől függően). A megfejtéshez a lépések inverzét kell végrehajtani fordított sorrendben. Az alábbiakban részletezzük a négy lépést.

5.1. AES: *SubBytes*

Ebben a lépésben a mátrix byte-jait egyenként transzformáljuk egy $S : \mathbb{F}_{256} \to \mathbb{F}_{256}$ invertálható függvénnyel, de nem változtatjuk meg a helyüket a mátrixban ($\forall i : b'_i := S(b_i)$). Ezt a transzformációt angolul **Rijndael S-box**nak is nevezik (S = substitution, azaz helyettesítés).

Az S transzformáció két lépésből áll ($S(b) = S_2(S_1(b))$):

1. Először vegyük az elem multiplikatív inverzét $\mathbb{F}_{256}$-ban: $S_1(b) := b^{-1}$ – kivéve ha $b = 0$, amely nem invertálható, arra legyen $S_1(0) := 0$.
2. A második lépés egy affin transzformáció, amely kivételesen nem $\mathbb{F}_{256}$-ban történik, hanem az elemek egy másik ábrázolásával. Kétféle ekvivalens módon is megfogalmazható:
   (a) A $b \in \mathbb{F}_{256}$ elem polinomos ábrázolása ($p_b = b_0 + b_1 x + \ldots + b_7 x^7 \in \mathbb{Z}_2[x]$) segítségével:
   $$S_2(b) := \big(p_b \cdot (x^4 + x^3 + x^2 + x + 1)\big) \bmod (x^8 + 1) \quad + \quad (x^6 + x^5 + x + 1).$$
   (b) A $b \in \mathbb{F}_{256}$ elem együtthatóvektorával ($v_b = (b_0, b_1, \ldots, b_7) \in \mathbb{Z}_2^8$), mátrixszorzással ($\mathbb{Z}_2^{8\times 8}$):
   $$S_2(b) := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}.$$
   Fontos, hogy bármelyik ábrázolást is nézzük, a bitek – azaz a polinomok együtthatói, ill. a vektorok elemei – továbbra is $\mathbb{Z}_2$-ben vannak, azaz modulo 2 kell velük számolni.

Ez az S transzformáció adja az AES lelkét: az inverz miatt erősen *nemlineáris* (lineáris lenne például egy egyszerű mátrixszorzás), ezáltal nagyon nehezen követhető, hogy mi történik a byte-okkal.

Mivel a transzformációnak csak 256 lehetséges értéke van, ezért a gyakorlatban ezeket előre ki szokták számítani, és eltárolják egy táblázatban, hogy a titkosítás gyorsabb legyen.

5.2. AES: *ShiftRows*

Ez a lépés a sorokon belül átrendezi a mátrix elemeit: az első sor nem változik, a másodikat ciklikusan eggyel balra tolja, a harmadikat kettővel, a negyediket pedig hárommal, azaz:

$$\begin{pmatrix} b_0 & b_4 & \underline{b_8} & \underline{\boldsymbol{b_{12}}} \\ b_1 & b_5 & \underline{b_9} & \underline{\boldsymbol{b_{13}}} \\ b_2 & b_6 & \underline{b_{10}} & \underline{\boldsymbol{b_{14}}} \\ b_3 & b_7 & \underline{b_{11}} & \underline{\boldsymbol{b_{15}}} \end{pmatrix} \longrightarrow \begin{pmatrix} b_0 & b_4 & \underline{b_8} & \underline{\boldsymbol{b_{12}}} \\ b_5 & \underline{b_9} & \underline{\boldsymbol{b_{13}}} & b_1 \\ \underline{b_{10}} & \underline{\boldsymbol{b_{14}}} & b_2 & b_6 \\ \underline{\boldsymbol{b_{15}}} & b_3 & b_7 & \underline{b_{11}} \end{pmatrix}$$

Ez arra jó, hogy az oszlopok keveredjenek, és ne csak egymástól függetlenül manipuláljuk őket.

5.3. AES: *MixColumns*

Ebben a lépésben megszorozzuk a mátrixot egy rögzített mátrixszal (mindkettő $\mathbb{F}_{256}^{4\times4}$-ben van):

$$B' := \begin{pmatrix} \theta & \theta{+}1 & 1 & 1 \\ 1 & \theta & \theta{+}1 & 1 \\ 1 & 1 & \theta & \theta{+}1 \\ \theta{+}1 & 1 & 1 & \theta \end{pmatrix} B,$$

ahol $\theta \in \mathbb{F}_{256}$ a fent definiált primitív elem. A mátrixban szereplő konstansok olyanok, amelyekkel hatékonyan lehet számolni (bitsorozatként: $\overline{1} \to [00000001]$, $\theta \to [00000010]$, $\theta{+}\overline{1} \to [00000011]$).

A lépés neve (*MixColumns*) arra utal, hogy a mátrixszorzás szabályai miatt ez ekvivalens azzal, mintha B oszlopvektorait külön-külön szoroznánk meg ugyanezzel a mátrixszal.

Ez a lépés gondoskodik arról, hogy az elemeket ne csak átrendezzük és külön-külön transzformáljuk, hanem egymással is kombináljuk őket (az oszlopokon belül).

5.4. AES: *AddRoundKey*

Ebben a lépésben a blokkhoz hozzáadjuk az aktuális kulcsot, amely egy szintén 128-bites bitsorozat. Ez a művelet felírható egy mátrixösszeadással $\mathbb{F}_{256}^{4\times4}$-ben, vagy bitsorozatként nézve egy egyszerű bitenkénti "kizáró vagy" (XOR) művelettel a két 128-bites bitsorozat között.

A kulcs a titkosítás minden ciklusában különböző (ettől *RoundKey*), és az algoritmus bemeneteként megadott főkulcsból számítható ki, amely 128 és 256 bit közötti hosszúságú (minél hosszabb, annál biztonságosabb az eljárás). A számítás részleteibe nem megyünk bele.

A kulcstól lesz titkos az algoritmus: aki ismeri, az meg tudja fejteni az ezzel titkosított üzeneteket, aki meg nem, annak pedig az csak egy értelmetlen bitsorozat marad. A kulcs ismerete nélkül az összes lehetőséget végig kellene próbálni, ami a legrövidebb, 128-bites kulcs esetén is $2^{128} = 340282366920938463463374607431768211456$ lehetőség. Ez a gyakorlatban kivitelezhetetlen.

6. Szerző

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

[1] https://en.wikipedia.org/wiki/Simple_extension

[2] Gonda János: Véges testek (2011)

[3] US NIST (2001): Federal Information Processing Standards Publication: Advanced Encryption Standard (AES). https://doi.org/10.6028/NIST.FIPS.197-upd1

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