Láng Csabáné

# TESTBŐVÍTÉS, VÉGES TESTEK HIBAJAVÍTÓ KÓDOK

Példák és megoldások

ELTE Budapest 2007-11-26
IK Digitális Könyvtár
3. javított kiadás

Felsőoktatási tankönyv

Lektorálta: Gonda János

# Tartalomjegyzék

# 1. Bevezetés

Ez a példatár elsősorban az ELTE Informatikai Kar programtervező informatikus, programtervező matematikus, programozó és informatika tanár szakos hallgatói számára készült. Megkönnyíti a hallgatók önálló tanulását azzal, hogy minden példa részletesen ki van dolgozva.

A 2. fejezetben a példákat soroltuk fel, a 3. fejezetben pedig ezek a példák megoldással együtt szerepelnek.

A példákhoz szükséges elméleti anyag megtalálható Gonda János: *Bevezető fejezetek a matematikába III.* ELTE TTK, Budapest, 1998 könyvében. A kódelmélet példákhoz szükséges fogalmak rövid összefoglalása a 3.2.1. és a 3.2.3. fejezetben szerepel.

A példák egy része más könyvekből, példatárakból, mások által összeállított feladatsorokból származik. Azok a források, amelyekről tudomásunk van, szerepelnek az *Ajánlott irodalom* fejezetben. A feladatok más része pedig ebben a példatárban jelenik meg először.

Ajánljuk Gonda János: *Gyakorlatok és feladatok a Bevezetés a matematikába c. tárgyhoz Polinomok, véges testek, kongruenciák, kódolás* ELTE TTK, Budapest, 2001 példatárát is, amelyik mindkét témakörből bőségesen tartalmaz kidolgozott példákat.

A könyvben található hibákra, hiányosságokra vonatkozó észrevételeket köszönettel fogadjuk.

Budapest, 2006. június

Láng Csabáné

szerző

zslang@compalg.inf.elte.hu

ELTE Informatikai Kar Komputer Algebra Tanszék

1117 Budapest, Pázmány Péter sétány I/C.

# 2. Példák

## 2.1. Testbővítés, véges testek

### 2.1.1. Testbővítés, véges testek, felbonthatatlan (irreducibilis) polinomok

**2.1-1.** Van-e a valós számoknak olyan részteste, amelyet a valós számok minden részteste tartalmaz?
**2.1-2.** Testet alkotnak-e a szokásos műveletekre a következő halmazok?

a. $T_1 = \left\{a + b\sqrt[4]{2} \mid a, b \in \mathbb{Q}\right\}$ b. $T_2 = \left\{a + bi\sqrt{5} \mid a, b \in \mathbb{Q}\right\}$

**2.1-3.** Mi a kapcsolat a $\mathbb{Q}(\sqrt{2})$, a $\mathbb{Q}(1+\sqrt{2})$ és a $\mathbb{Q}(\sqrt{8})$ testek között?
**2.1-4.** Mely $a, b$ racionális számokra teljesül, hogy $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(a + b\sqrt{2})$?
**2.1-5.** Van-e olyan szám, amellyel bővítve a racionális számok testét, rögtön a $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ testet kapjuk?
**2.1-6.** Felbonthatatlan-e az $x^5+5$ polinom $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, illetve $\mathbb{Z}_5$ felett?

**2.1-7.** Keressük meg $\mathbb{Z}_2$ fölött az összes másod-, harmad-, és negyedfokú felbonthatatlan (irreducibilis) polinomot.
**2.1-8.** Igazoljuk, hogy az alábbi polinomok felbonthatatlanok (irreducibilisek) $\mathbb{F}_2$ felett.

**a.** $x^5 + x^2 + \overline{1}$,

**b.** $x^6 + x + \overline{1}$,

**c.** $x^7 + x^3 + \overline{1}$.

**2.1-9.** Hány másodfokú normált (1 főegyüttható́jú) irreducibilis polinom van egy $q$ elemű testben?

**2.1-10.** Készítsünk 9 elemű testet.

a. Adjuk meg a művelettáblákat.

b. Határozzuk meg az egyes elemek multiplikatív rendjét, keressünk primitív elemeket.

c. Határozzuk meg az egyes elemek additív rendjét.

**2.1-11.** Készítsünk 4 elemű testet.

a. Adjuk meg a művelettáblákat.

b. Határozzuk meg az egyes elemek multiplikatív rendjét, keressünk primitív elemeket.

**2.1-12.**

a. Bizonyítsuk be, hogy az $f(x) = x^3 + x + \overline{1} \in \mathbb{Z}_5[x]$ polinom irreducibilis $\mathbb{Z}_5$ felett.

b. Hány eleme van a $\mathbb{Z}_5[x]/\overline{f}$ maradékosztálygyűrűnek (testnek), ahol $\overline{f}$ az $f$ többszöröseiből álló ideál? Adjunk meg egy reprezentánsrendszert.

**2.1-13.**

a. Bizonyítsuk be, hogy az $f(x) = x^2 + x + \overline{1} \in \mathbb{Z}_5[x]$ polinom irreducibilis $\mathbb{Z}_5$ felett.

b. Hány eleme van a $\mathbb{Z}_5[x]/\overline{f}$ maradékosztálygyűrűnek (testnek), ahol $\overline{f}$ az $f$ többszöröseiből álló ideál? Adjunk meg egy reprezentánsrendszert.

**2.1-14.**

a. Igazoljuk, hogy $f(x) = x^3 + x + \overline{2}$ reducibilis $\mathbb{Z}_7$ felett.

b. Hány eleme van a $\mathbb{Z}_7[x]/\overline{f}$ maradékosztálygyűrűnek ($\overline{f}$ az $f$ polinom többszöröseiből álló ideál)? Adjunk meg egy reprezentánsrendszert.

c. Mutassuk meg, hogy a $\mathbb{Z}_7[x]/\overline{f}$ maradékosztálygyűrű tartalmaz nullosztót.

### 2.1.2. Elem felírása bázisban

**2.1-15.** Legyen $u \in \mathbb{C}$ a $\mathbb{Q}$ feletti $x^3 - 2x + 2$ polinom egyik gyöke. Lássuk be,

hogy a polinom $\mathbb{Q}$ felett irreducibilis. Írjuk fel $\mathbb{Q}(u) \mid \mathbb{Q}$ $\{1,\ u,\ u^2\}$ bázisában a következő elemeket:

a. $u^7$ b. $u^{-1}$ c. $u^4 + u^{-2}$

**2.1-16.** Legyen $u \in \mathbb{C}$ az $x^3 - 6x^2 + 9x + 3$ $\mathbb{Q}$ felett irreducibilis polinom gyöke. Fejezzük ki $\mathbb{Q}(u) \mid \mathbb{Q}$ $\{1,\ u,\ u^2\}$ bázisában a következő elemeket:

a. $3u^5 - 2u$ b. $\frac{1}{1+u}$

### 2.1.3. Minimálpolinom, felbontási test

**2.1-17.** Határozzuk meg $\sqrt{2 - \sqrt[3]{2}}$ minimálpolinomját $\mathbb{Q}$ felett.

**2.1-18.** Mutassuk meg, hogy

$$\sqrt[3]{9 + 4\sqrt{5}} + \sqrt[3]{9 - 4\sqrt{5}}$$

egész szám.

**2.1-19.** Határozzuk meg az $(x^2+1)(x^2-2x+1)$ polinom felbontási testét $\mathbb{Q}$ felett.

**2.1-20.** $\mathbb{Q}(\sqrt[3]{2})$ megegyezik-e $\sqrt[3]{2}$ minimálpolinomjának a felbontási testével?

**2.1-21.** Van-e racionális gyöke az $f(x) = x^3 - x^2 - x - 2$ polinomnak? Mi az $f(x)$ felbontási teste $\mathbb{Q}$ felett?

**2.1-22.** Bizonyítsuk be, hogy ha $\alpha \in \mathbb{C}$ megoldása a $10x^3 - 105x^2 + 84x + 210 = 0$ racionális együtthatós egyenletnek, és valamely $K$ testre fennáll, hogy $\mathbb{Q}(\alpha)|K$ és $K|\mathbb{Q}$, akkor $K = \mathbb{Q}(\alpha)$ vagy $K = \mathbb{Q}$.

**2.1-23.** Legyen $K = \mathbb{F}_q$, és $f(x)$ $K$ fölötti irreducibilis $n$-edfokú polinom. Lássuk be, hogy

$$f(x)|x^{q^n} - x.$$

($\mathbb{F}_q$ a $q$ elemű testet jelöli.)

**2.1-24.** Legyen $K = \mathbb{F}_q$, $f(x)$ $K$ fölötti irreducibilis $n$-edfokú polinom, és legyen $\alpha$ gyöke $f$-nek. Lássuk be, hogy $K$-t $\alpha$-val bővítve megkapjuk $f$ $K$ fölötti felbontási testét. (Más szóval lássuk be, hogy ha $f$ egyik gyöke a bővített véges testben van, akkor $f$ mindegyik gyöke benne van.) ($\mathbb{F}_q$ a $q$ elemű testet jelöli.)

**Megjegyzés.** 0 karakterisztikájú testben ez általában nem igaz (lásd a 20. példát).

### 2.1.4. Bővítés foka, véges és algebrai bővítés

**2.1-25.** A következő bővítések közül melyik véges és melyik algebrai? ($A$ az algebrai számok halmaza)

a. $\mathbb{C}|\mathbb{R}$ b. $\mathbb{Q}(\sqrt{5})|\mathbb{Q}$ c. $A|\mathbb{Q}$ d. $A|\mathbb{Q}(\sqrt{5})$ e. $\mathbb{R}|\mathbb{Q}(\pi)$

**2.1-26.** Mennyi a $\mathbb{Q}(\pi)|\mathbb{Q}(\pi^2)$ testbővítés foka?

**2.1-27.** Határozzuk meg a $T|\mathbb{Q}$ testbővítés fokát, ahol $T$ az alábbi. Mi a bővítő elem minimálpolinomja $\mathbb{Q}$ fölött? Adjunk meg egy bázist.

**a.** $\mathbb{Q}(\sqrt{7})$ **b.** $\mathbb{Q}(i\sqrt{5})$
**c.** $\mathbb{Q}(1+i\sqrt{3})$ **d.** $\mathbb{Q}(i+\sqrt{5})$
**e.** $\mathbb{Q}(u+i\sqrt{v}),\ u,v\in\mathbb{Q}, \sqrt{v}\notin\mathbb{Q}$

**2.1-28.** Határozzuk meg a $T|\mathbb{Q}$ testbővítés fokát, ahol $T$ az alábbi. Adjunk meg egy bázist.

**a.** $\mathbb{Q}(\sqrt{2},\sqrt{3})$ **b.** $\mathbb{Q}(i,\sqrt{8})$

### 2.1.5. Véges test elemeinek összege, szorzata, Vieta-formulák, gyökök és együtthatók közötti összefüggések

**2.1-29.** Bizonyítsuk be a Wilson-tételt: $(p-1)!\equiv -1 \pmod{p}$, ha $p$ prím.

**2.1-30.** Mennyi valamely véges test nem nulla elemeinek a szorzata?

**2.1-31.** Véges testben mi az elemek számának paritása?

**Vieta-formulák, gyökök és együtthatók közötti összefüggések**

Legyen $R$ egységelemes integritási tartomány, és tegyük fel, hogy az

$f(x)=a_nx^n+a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\ldots+a_1x+a_0\in R[x]$

$n$-edfokú polinom – multiplicitással együtt vett – $n$ gyöke mind $R$-ben van. Legyenek ezek a gyökök $c_1,\ c_2,\ \ldots,\ c_n$. Ekkor

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 = \\ &= a_n(x-c_1)(x-c_2)\cdots(x-c_n) = \\ &= a_n\left(x^n - (c_1+c_2+\ldots+c_n)x^{n-1} + \right. \\ &\quad +(c_1\cdot c_2 + c_1\cdot c_3 + \ldots + c_{n-1}\cdot c_n)x^{n-2} + \\ &\quad \vdots \\ &\quad \left. +(-1)^n(c_1\cdot c_2\cdots c_n)\right) \end{aligned}$$

amiből

$$\begin{aligned} \frac{a_{n-1}}{a_n} &= -(c_1+c_2+\ldots+c_n) \\ \frac{a_{n-2}}{a_n} &= (c_1\cdot c_2 + c_1\cdot c_3 + \ldots + c_{n-1}\cdot c_n) \\ &\vdots \\ \frac{a_0}{a_n} &= (-1)^n(c_1\cdot c_2\cdots c_n) \end{aligned}$$

**2.1-32.** Legyen $L$ véges test, $|L| = q^k$. Számítsuk ki a következő összeget:

$$\sum_{l\in L} l.$$

**2.1-33.** Legyen $L$ véges test, $|L| = q^k$. Jelölje $L^*$ az $L$ multiplikatív csoportját. Számítsuk ki a következő szorzatot:

$$\prod_{l\in L^*} l.$$

(Lásd a 30. példát is.)

## 2.2. Hibajavító kódok

A feladatok általában bináris kódokra vonatkoznak, vagyis olyanokra, amelyek esetén az $S$ alaphalmaz a $\{0,1\}$ halmaz. Néhány feladat általánosabban van megfogalmazva, ezekben az $S$ alaphalmaz tetszőleges nem üres halmaz.

### 2.2.1. Alapfogalmak

A részleteket lásd a megoldásnál.

### 2.2.2. Blokk-kódok

**2.2-1.** Tegyük fel, hogy az üzenetek bináris jelsorozatok, vagyis az $S = \{0, 1\}$ halmaz elemeiből épülnek fel. Rendeljünk hozzá a kettő hosszú üzenetekhez öt hosszú kódokat a következő szabály szerint.

$$(0\ 0) \to (0\ 0\ 0\ 0\ 0)$$
$$(0\ 1) \to (0\ 1\ 1\ 1\ 0)$$
$$(1\ 0) \to (1\ 0\ 1\ 0\ 1)$$
$$(1\ 1) \to (1\ 1\ 0\ 1\ 1)$$

Így négy elemből álló blokk-kódot kapunk. Ha a csatornán például a (0 1 0 0 0) jelsorozat érkezik, tudjuk, hogy hiba történt, hiszen ez a szó nem szerepel a kódszavak között.

Mekkora az $u = (0\ 1\ 1\ 1\ 0)$ és $v = (1\ 0\ 1\ 0\ 1)$ kódszavak távolsága, a kód távolsága, a $z = (1\ 1\ 0\ 1\ 1)$ vektor súlya, valamint a kód súlya?

**2.2-2.** Az 1. példa $S$ halmaza legyen $\mathbb{F}_2$, a kételemű test. $\mathbb{F}_2$ az összeadásra csoportot alkot. Az $\mathbb{F}_2$ elemeiből készített $n$ hosszú vektorok is csoportot alkotnak az elemenkénti összeadásra nézve. Lássuk be, hogy a példa $K$ kódhalmaza részcsoport $S^n$-ben, így $K$ *csoportkód*.

**2.2-3.** Legyen $K$ az 1. példabeli kód, $u = (0\ 0\ 0\ 0\ 0)$, $t = 1$. Adjuk meg az $u$ körüli 1 sugarú gömbben szereplő sorozatokat.

**2.2-4.** Az 1. példa kódját alkalmazva tegyük fel, hogy a (0 1 0 0 0) hibás jelsorozat érkezik. Minimális távolságú dekódolás esetén melyik szót választjuk helyette?

**2.2-5.** Legyen $S = \mathbb{F}_2$, a közleményszavak pedig $k$ hosszú sorozatok. Állapítsuk meg, hogy az alábbi kódok esetén mi jellemzi a kódszavakat, mennyi a kód minimális távolsága, hibajelző és (minimális távolságú dekódolással) a hibajavító képessége.

**a. Kétszeri ismétlés kódja.** A kódszót megkapjuk, ha a közleményszót kétszer egymásután leírjuk. Az $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ közleményszóból az

$$(\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_1, \alpha_2, \ldots, \alpha_k)$$

kódszó keletkezik.

**b. Háromszori ismétlés kódja.** A kódszót megkapjuk, ha a közleményszót háromszor egymásután leírjuk. Az $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ közleményszóból az

$$(\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_1, \alpha_2, \ldots, \alpha_k)$$

kódszó keletkezik.

**c. Paritásvizsgálat kódja.** A kódszót megkapjuk, ha a közleményszó végére az elemek ($\mathbb{F}_2$-ben számított) összegét írjuk. Az $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ közleményszóból az

$$(\alpha_1, \alpha_2, \ldots, \alpha_k, \beta), \quad \beta = \sum_{i=1}^{k} \alpha_i$$

kódszó keletkezik.

**2.2-6. Hamming-korlát.**

Bizonyítsuk be a következőt. Legyen az alaphalmaz $S$, a $K \subseteq S^n$ kód $t$-hiba javító. Ekkor

$$|K| \cdot \sum_{i=0}^{t} \binom{n}{i} (s-1)^i \leq s^n,$$

ahol $s = |S|$.

**2.2-7.** Bináris blokk-kódot készítünk 3 hosszú üzenetekhez. Legalább mekkora legyen a kódszavak hossza, ha azt akarjuk, hogy a kód (minimális távolságú dekódolással) pontosan 1-hiba javító legyen?

**2.2-8.** $k$ hosszú bináris szavakból (üzenet) 19 hosszú bináris szavakat (kódszót) készítünk. Legfeljebb mekkora lehet az üzenetek hossza, ha azt akarjuk, hogy a kód minimális távolsága 8 legyen?

**2.2-9.** Állapítsuk meg, hogy van-e 6 minimális távolságú, 13 hosszú perfekt bináris kód?

A $K$ blokk-kód *tökéletes* (*perfekt*), ha a Hamming-korlát egyenlőséggel teljesül. Perfekt kód esetén a kódszavak körüli $\lfloor \frac{d-1}{2} \rfloor$ sugarú gömbök teljesen kitöltik az $n$ hosszú sorozatok terét, s így minden szóhoz pontosan egy kódszó van, amelytől legfeljebb $\lfloor \frac{d-1}{2} \rfloor$ távolságra van.

**2.2-10.** Létezik-e 3 minimális távolságú perfekt bináris kód $n = 147$ esetén?

**2.2-11.** Van-e 12 hosszú kódszavakból álló 1-hiba javító perfekt bináris kód?

### 2.2.3. Lineáris kód alapfogalmai

A részleteket lásd a megoldásnál.

### 2.2.4. Lineáris kód

**2.2-12.** Valamely kód generátormátrixa legyen a következő:

$$G = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

Ezt a mátrixot használva kódolásra, adjuk meg az összes közleményszót, valamint a megfelelő kódszavakat.

**2.2-13.** Állapítsuk meg, hogy az 5. példa kódjai közül melyik lineáris, és a lineárisoknak adjuk meg a generátormátrixát.

**2.2-14.** Az alábbi bináris kódok esetében állapítsuk meg a minimális távolságot, a hibajelző illetve (minimális távolságú dekódolással) a hibajavító képességet, valamint azt, hogy melyik lineáris, a lineárisoknak pedig adjuk meg a generátormátrixát.

a. Legyen $k = 3$, $n = 4$, és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat.

$$\alpha_1, \alpha_2, \alpha_3 \to \alpha_1, \alpha_2, \alpha_3, \alpha_1 + \alpha_2 + \alpha_3 + 1$$

b. Legyen $k = 3$, $n = 5$, és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat.

$$\alpha_1, \alpha_2, \alpha_3 \to \alpha_1, \alpha_2, \alpha_3, \alpha_1, \alpha_2 + \alpha_3$$

c. Legyen $k = 3$, $n = 5$, és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat.

$$\alpha_1, \alpha_2, \alpha_3 \to \alpha_1, \alpha_2, \alpha_3, \alpha_1, \max(\alpha_2, \alpha_3)$$

**2.2-15.** Lássuk be, hogy ha az $\mathbb{F}_k$ fölötti $[n, k]$ kód generátormátrixa $G = (I_k \;\; P)$ alakú, akkor a $H = (-P^T \;\; I_{n-k})$ mátrix a kód ellenőrző mátrixa. ($I_k$ a $k \times k$ méretű egységmátrixot jelöli, $P$ pedig tetszőleges $k \times (n-k)$ méretű, $\mathbb{F}_k$ fölötti mátrix.) A kételemű test fölött $-P$ helyett $P$ is irható, mert $\mathbb{F}_2$-ben $1 = -1$.

**Megjegyzés.** Hasonlóan igaz az is, hogy ha egy $[n, k]$ kód ellenőrző mátrixa $H = (I_{n-k} \;\; R)$ alakú, ahol $R$ tetszőleges $((n-k) \times k)$ méretű, $\mathbb{F}_k$ fölötti mátrix, akkor a $G = (-R^T \;\; I_k)$ mátrix megfelel generátormátrixnak.

**2.2-16.** Adjuk meg a 14. példában szereplő lineáris kód ellenőrző mátrixát a

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

generátormátrix felhasználásával.

**2.2-17.** Lássuk be, hogy egy $[n, k, d]$ kód $H$ ellenőrző mátrixában van $d$ lineárisan összefüggő oszlop, de bármely $d$-nél kevesebb oszlop lineárisan független.

**2.2-18.** Adjuk meg a 14. és 16. példában szereplő lineáris kód

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

ellenőrző mátrixának segítségével a kód távolságát és hibajelző, valamint (minimális távolságú dekódolással) a hibajavító képességét.

**2.2-19.** Legyen egy bináris lineáris kód generátormátrixa:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Adjuk meg az (egyik) ellenőrző mátrixát. Az ellenőrző mátrix felhasználásával mondjuk meg a kódtávolságot.

**2.2-20.** Egy bináris kód generátormátrixa

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Adjuk meg a kód paritásellenőrző mátrixát és távolságát.

**2.2-21.** Egy bináris kód generátormátrixa

$$G = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

Adjuk meg a kód paritásellenőrző mátrixát és távolságát.

**2.2-22.** Egy bináris kód generátormátrixa

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Mennyi a kód számossága? Adjuk meg a kód paritásellenőrző mátrixát, és ennek segítségével határozzuk meg a távolságát.

**2.2-23.** Egy bináris kód paritásellenőrző mátrixa

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Lássuk be, hogy 1-hiba javító perfekt lineáris kódról van szó.

### 2.2.5. Hamming-kód

Az 1-hiba javító perfekt lineáris kódot *Hamming-kódnak* nevezzük.

**2.2-24. Hamming-kód készítése.**

Bináris Hamming-kódot készíthetünk a következőképpen. Legyen

$r$ pozitív egész szám (ellenőrző jegyek száma),

$n = 2^r - 1$ a kódszavak hossza,

$k = 2^r - 1 - r$ a közleményszavak hossza.

A $H$ $r \times n$-es ellenőrző mátrix $j$-edik oszlopában a $j$ 2-es számrendszerbeli alakjának jegyei szerepelnek.

Legyen például $r = 3, n = 7, k = 4$. Adjuk meg a kód ellenőrző mátrixát.

**2.2-25.** Adjuk meg az előző példában megismert szabály szerinti Hamming-kód ellenőrző mátrixát, ha $r = 2$, és ha $r = 4$.

**2.2-26. A Hamming-kód generátormátrixa.** Adjuk meg a 24. példabeli $[7, 4]$ Hamming-kód $H$ ellenőrző mátrixának ismeretében a kód (egyik) generátormátrixát. Ha ezt a generátormátrixot alkalmazzuk a kódolásnál, mi lesz a $(0\ \ 1\ \ 1\ \ 1)$ üzenet kódja?

**2.2-27.** Hibajavítás bináris Hamming-kóddal.

A részleteket lásd a megoldásnál.

**2.2-28.** $[7, 4]$ bináris Hamming-kódnál, feltételezve, hogy egynél több hiba nem lépett fel az átvitelnél, mi volt a továbbított kódvektor, ha

**a.** $a^T = (0\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 0)$ illetve

**b.** $b^T = (0\ \ 0\ \ 1\ \ 0\ \ 1\ \ 1\ \ 0)$ érkezett.

# 3. Példák és megoldások

## 3.1. Testbővítés, véges testek

### 3.1.1. Testbővítés, véges testek, felbonthatatlan (irreducibilis) polinomok

**3.1-1. Van-e a valós számoknak olyan részteste, amelyet a valós számok minden részteste tartalmaz?**

**Megoldás.** Ebben a $T$ testben természetesen benne van a 0 és az 1. Mivel test zárt az összeadásra, benne van az $1+1=2$, $1+1+1=3$, ..., tehát a természetes számok halmaza része ennek a testnek,

$$\mathbb{N} \subseteq T.$$

Mivel minden elem additív inverze is benne van a testben, benne van a $-1$, $-2$, ..., tehát az egész számok halmaza is része ennek a testnek,

$$\mathbb{Z} \subseteq T.$$

Test az osztásra is zárt, ha nem nulla elemmel osztunk, s így $m, n \in \mathbb{Z}$, $n \neq 0$ esetén $m/n \in T$ is teljesül. Tehát a racionális számok halmaza is része $T$-nek,

$$\mathbb{Q} \subseteq T.$$

$\mathbb{Q}$ azonban maga is testet alkot, s így megtaláltuk a keresett résztestet,

$$T = \mathbb{Q}.$$

**Megjegyzés.** Azt mondjuk, hogy $\mathbb{Q}$ az $\mathbb{R}$ *prímteste.* ■

**3.1-2. Testet alkotnak-e a szokásos műveletekre a következő halmazok?**

**a.** $T_1 = \left\{a + b\sqrt[4]{2} \mid a, b \in \mathbb{Q}\right\}$ **b.** $T_2 = \left\{a + bi\sqrt{5} \mid a, b \in \mathbb{Q}\right\}$

**Megoldás.**

**a.** Nem, mert például $\sqrt{2} = (\sqrt[4]{2})^2 \notin T_1$.

Tegyük fel ugyanis indirekt módon, hogy $\sqrt{2} = a + b\sqrt[4]{2}$, ahol $a, b \in \mathbb{Q}$. Ebből $\sqrt{2} - a = b\sqrt[4]{2}$, amit négyzetre emelve $2 - 2\sqrt{2}a + a^2 = b^2\sqrt{2}$. Ezt rendezve $2 + a^2 = \sqrt{2}(b^2 + 2a)$. Vizsgáljuk meg először a $b^2 + 2a = 0$ esetet. Ekkor $2 + a^2 = 0$, ebből $a^2 = -2$, ami ellentmondás. Ha pedig $b^2 + 2a \neq 0$, akkor $\sqrt{2} = \frac{2+a^2}{b^2+2a}$, s ez azt jelentené, hogy $\sqrt{2}$ racionális.

Tehát egy $T_1$-beli szám négyzete nem $T_1$-beli, s így $T_1$ nem test.

**b.** Igen. A test axiómák teljesülnek. Most csak azt vizsgáljuk meg, hogy az osztás is elvégezhető a halmazon belül, ha a nevező nem nulla. Legyen ugyanis $a + bi\sqrt{5},\ c + di\sqrt{5} \in T_2,\ c + di\sqrt{5} \neq 0$. Ekkor

$$\frac{a + bi\sqrt{5}}{c + di\sqrt{5}} = \frac{(a + bi\sqrt{5})(c - di\sqrt{5})}{c^2 + 5d^2} \in T_2.$$

■

**3.1-3. Mi a kapcsolat a $\mathbb{Q}(\sqrt{2})$, a $\mathbb{Q}(1+\sqrt{2})$ és a $\mathbb{Q}(\sqrt{8})$ testek között?**

**Megoldás.** Azonosak. Felhasználjuk a test tulajdonságait, nevezetesen azt, hogy testbeli elemek összege, különbsége, szorzata és (ha a nevező nem nulla) a hányadosa is testbeli. Másrészt, ha valamely $a \in \mathbb{Q}(b)$, akkor $\mathbb{Q}(a) \subseteq \mathbb{Q}(b)$

is fennáll.

Először megmutatjuk, hogy $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1+\sqrt{2})$.

$$\begin{array}{rcccccc} 1+\sqrt{2} & \in & \mathbb{Q}(\sqrt{2}) & \to & \mathbb{Q}(1+\sqrt{2}) & \subseteq & \mathbb{Q}(\sqrt{2}), \\ \sqrt{2}=(1+\sqrt{2})-1 & \in & \mathbb{Q}(1+\sqrt{2}) & \to & \mathbb{Q}(\sqrt{2}) & \subseteq & \mathbb{Q}(1+\sqrt{2}), \end{array}$$

és így

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1+\sqrt{2}).$$

Most megmutatjuk, hogy $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{8})$.

$$\begin{array}{rcccccc} \sqrt{8}=2\sqrt{2} & \in & \mathbb{Q}(\sqrt{2}) & \to & \mathbb{Q}(\sqrt{8}) & \subseteq & \mathbb{Q}(\sqrt{2}), \\ \sqrt{2}=\frac{\sqrt{8}}{2} & \in & \mathbb{Q}(\sqrt{8}) & \to & \mathbb{Q}(\sqrt{2}) & \subseteq & \mathbb{Q}(\sqrt{8}), \end{array}$$

és így

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{8}).$$

■

**3.1-4. Mely $a, b$ racionális számokra teljesül, hogy $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(a + b\sqrt{2})$?**

**Megoldás.** $b \neq 0$, egyébként bármelyik racionális szám lehet $a$, illetve $b$. Ugyanis egyrészt

$$a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2}),$$

tehát

$$\mathbb{Q}(a + b\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2})$$

Másrészt, ha $b \neq 0$, akkor

$$\sqrt{2} = \frac{a + b\sqrt{2} - a}{b} \in \mathbb{Q}(a + b\sqrt{2})$$

miatt

$$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(a + b\sqrt{2}),$$

s így a két test megegyezik. ■

**3.1-5. Van-e olyan szám, amellyel bővítve a racionális számok testét, rögtön a $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ testet kapjuk?**

**Megoldás.** Ilyen például az $A = \sqrt{2} + \sqrt{3}$. Ugyanis $A \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ miatt $\frac{1}{A} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$ és

$$\frac{1}{A} = \frac{1}{\sqrt{2}+\sqrt{3}} = \frac{\sqrt{3}-\sqrt{2}}{(\sqrt{3})^2-(\sqrt{2})^2} = \sqrt{3}-\sqrt{2},$$

tehát $\sqrt{3}-\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Másrészt

$$\frac{A-\frac{1}{A}}{2} = \sqrt{2} \quad \text{és} \quad \frac{A+\frac{1}{A}}{2} = \sqrt{3}$$

miatt

$$\begin{array}{rcccccc} \sqrt{2} \text{ és } \sqrt{3} & \in & \mathbb{Q}(\sqrt{2}+\sqrt{3}) & \to & \mathbb{Q}(\sqrt{2},\sqrt{3}) & \subseteq & \mathbb{Q}(\sqrt{2}+\sqrt{3}), \\ \sqrt{2}+\sqrt{3} & \in & \mathbb{Q}(\sqrt{2},\sqrt{3}) & \to & \mathbb{Q}(\sqrt{2}+\sqrt{3}) & \subseteq & \mathbb{Q}(\sqrt{2},\sqrt{3}), \end{array}$$

és így

$$\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2},\sqrt{3}).$$

■

**3.1-6. Felbonthatatlan-e az $x^5+5$ polinom $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, illetve $\mathbb{Z}_5$ felett?**

**Megoldás.**

| Mi felett? | Felbont-hatatlan? | Indoklás |
|---|---|---|
| $\mathbb{Z}$ | igen | $p=5$ választással a Schönemann–Eisenstein tétel. |
| $\mathbb{Q}$ | igen | Az előző és a Gauss-tétel miatt. |
| $\mathbb{C}$ | nem | 5 elsőfokú tényező szorzatára bontható. |
| $\mathbb{Z}_2$ | nem | $x^5+\overline{5} = x^5+\overline{1} = (x-\overline{1})(\ldots)$ (az $\overline{1}$ gyöke) |
| $\mathbb{Z}_3$ | nem | $x^5+\overline{5} = x^5-\overline{1} = (x-\overline{1})(\ldots)$ (az $\overline{1}$ gyöke) |
| $\mathbb{Z}_5$ | nem | $x^5+\overline{5} = x^5$ (a $\overline{0}$ gyöke) |

■

**3.1-7. Keressük meg $\mathbb{Z}_2$ fölött az összes másod-, harmad-, és negyedfokú felbonthatatlan (irreducibilis) polinomot.**

**Megoldás.**

| fokszám | polinom | felbonthatóság |
|---|---|---|
| elsőfokú | $x$ | irreducibilis |
| | $x+\overline{1}$ | irreducibilis |
| másodfokú | $x^2$ | $= x \cdot x$ |
| | $x^2+\overline{1}$ | $= (x+\overline{1}) \cdot (x+\overline{1})$ |
| | $x^2+x$ | $= x \cdot (x+\overline{1})$ |
| | $x^2+x+\overline{1}$ | irreducibilis |
| harmadfokú | $x^3$ | $= x \cdot x \cdot x$ |
| | $x^3+\overline{1}$ | $= (x+\overline{1}) \cdot (x^2+x+\overline{1})$ |
| | $x^3+x$ | $= x \cdot (x^2+\overline{1}) = x \cdot (x+\overline{1})^2$ |
| | $x^3+x+\overline{1}$ | irreducibilis |
| | $x^3+x^2$ | $= x^2 \cdot (x+\overline{1})$ |
| | $x^3+x^2+\overline{1}$ | irreducibilis |
| | $x^3+x^2+x$ | $= x \cdot (x^2+x+\overline{1})$ |
| | $x^3+x^2+x+\overline{1}$ | $= (x+\overline{1}) \cdot (x^2+\overline{1}) = (x+\overline{1})^3$ |
| negyedfokú | $x^4$ | $= x \cdot x \cdot x \cdot x$ |
| | $x^4+\overline{1}$ | $= (x+\overline{1}) \cdot (x^3+x^2+x+\overline{1}) = (x+\overline{1})^4$ |
| | $x^4+x$ | $= x \cdot (x^3+\overline{1}) = x \cdot (x+\overline{1}) \cdot (x^2+x+\overline{1})$ |
| | $x^4+x+\overline{1}$ | irreducibilis |
| | $x^4+x^2$ | $= x^2 \cdot (x^2+\overline{1}) = x^2 \cdot (x+\overline{1})^2$ |
| | $x^4+x^2+\overline{1}$ | $= (x^2+x+\overline{1})^2$ |
| | $x^4+x^2+x$ | $= x \cdot (x^3+x+\overline{1})$ |
| | $x^4+x^2+x+\overline{1}$ | $= (x+\overline{1}) \cdot (x^3+x^2+\overline{1})$ |
| | $x^4+x^3$ | $= x^3 \cdot (x+\overline{1})$ |
| | $x^4+x^3+\overline{1}$ | irreducibilis |
| | $x^4+x^3+x$ | $= x \cdot (x^3+x^2+\overline{1})$ |
| | $x^4+x^3+x+\overline{1}$ | $= (x+\overline{1}) \cdot (x^3+\overline{1}) = (x+\overline{1})^2 \cdot (x^2+x+\overline{1})$ |
| | $x^4+x^3+x^2$ | $= x^2 \cdot (x^2+x+\overline{1}) = (x+\overline{1})^3$ |
| | $x^4+x^3+x^2+\overline{1}$ | $= (x+\overline{1}) \cdot (x^3+x+\overline{1})$ |
| | $x^4+x^3+x^2+x$ | $= (x+\overline{1}) \cdot (x^3+x^2+x+\overline{1})$ |
| | $x^4+x^3+x^2+x+\overline{1}$ | irreducibilis |

Az elsőfokú polinomok természetesen irreducibilisek. A másod- és harmadfokúak akkor és csak akkor irreducibilisek, ha nincs gyökük a test felett. A negyedfokúak esetében, ha van gyöke a polinomnak, akkor nyilván felbontható, ha nincs gyöke, akkor még előfordulhat, hogy felbontható két másodfokú irreducibilis szorzatára.

Ha $f$ konstans tagja osztható $p$-vel, és a polinom legalább másodfokú, akkor $f$ nem irreducibilis, hiszen a 0 gyöke, így az ilyen polinomokat nem kell külön vizsgálni.

A következő stratégiát alkalmaztuk például a negyedfokúaknál: minden lehetséges módon összeszoroztuk az első-, másod- és harmadfokú irreducibilis polinomokat úgy, hogy az eredmény negyedfokú legyen. Az a negyedfokú polinom, amelyet így nem kaptunk meg, irreducibilis. ■

**3.1-8. Igazoljuk, hogy az alábbi polinomok felbonthatatlanok (irreducibilisek) $\mathbb{F}_2$ felett.**

**a.** $x^5 + x^2 + \overline{1}$,

**b.** $x^6 + x + \overline{1}$,

**c.** $x^7 + x^3 + \overline{1}$.

**Megoldás.** Felhasználjuk, hogy $x^2 + x + \overline{1},\ x^3 + x + \overline{1},\ x^3 + x^2 + \overline{1}$ a másod- és harmadfokú irreducibilis polinomok $\mathbb{F}_2$ felett (lásd az előző példát).

**a.** Ha az $x^5 + x^2 + \overline{1}$ polinom felbontható lenne, akkor lenne elsőfokú vagy másodfokú tényezője.

Ha lenne elsőfokú tényezője, akkor lenne gyöke $\mathbb{F}_2$ felett a polinomnak. Az összes elem ($\overline{0}$ és $\overline{1}$) behelyettesítésével meggyőződhetünk arról, hogy nincs gyöke, így nincs elsőfokú tényezője sem.

Vizsgáljuk meg, hogy van-e másodfokú tényezője. Az egyetlen másodfokú irreducibilis polinom az $x^2+x+1$. Ezzel a polinommal osszuk el maradékosan az $x^5 + x^2 + \overline{1}$ polinomot.

$$
\begin{aligned}
&(x^5 + x^2 + \overline{1}) : (x^2 + x + \overline{1}) = x^3 + x^2 \\
&-(\underline{x^5 + x^4 + x^3}) \\
&\qquad\quad x^4 + x^3 + x^2 + \overline{1} \\
&\qquad -(\underline{x^4 + x^3 + x^2}) \\
&\qquad\qquad\quad \overline{1}
\end{aligned}
$$

A maradék $\overline{1}$, tehát az első polinom nem osztható a másodikkal.

Mivel $x^5 + x^2 + \overline{1}$-nek sem első- sem másodfokú irreducibilis tényezője nincs, ő maga irreducibilis.

**b.** Ha az $x^6 + x + \overline{1}$ polinom felbontható lenne, akkor lenne elsőfokú, másodfokú vagy harmadfokú tényezője.

Ha lenne elsőfokú tényezője, akkor lenne gyöke $\mathbb{F}_2$ felett a polinomnak. Az összes elem ($\overline{0}$ és $\overline{1}$) behelyettesítésével meggyőződhetünk arról, hogy nincs gyöke, így nincs elsőfokú tényezője sem.

Vizsgáljuk meg, hogy van-e másodfokú tényezője. Az egyetlen másodfokú irreducibilis polinom az $x^2+x+1$. Ezzel a polinommal osszuk el maradékosan az $x^6 + x + \overline{1}$ polinomot.

$$
\begin{aligned}
&(x^6 + x + \overline{1}) : (x^2 + x + \overline{1}) = x^4 + x^3 + x + 1\\
&-(\underline{x^6 + x^5 + x^4})\\
&\qquad x^5 + x^4 + x + \overline{1}\\
&\quad -(\underline{x^5 + x^4 + x^3})\\
&\qquad\quad x^3 + x + \overline{1}\\
&\qquad -(\underline{x^3 + x^2 + x})\\
&\qquad\qquad x^2 + \overline{1}\\
&\qquad\quad -(\underline{x^2 + x + \overline{1}})\\
&\qquad\qquad\quad x
\end{aligned}
$$

A maradék $x$, tehát az első polinom nem osztható a másodikkal.

Most osszuk el az $x^6 + x + \overline{1}$ polinomot sorban a két harmadfokú irreducibilis polinommal is.

$$
\begin{aligned}
&(x^6 + x + \overline{1}) : (x^3 + x^2 + \overline{1}) = x^3 + x^2 + x\\
&-(\underline{x^6 + x^5 + x^3})\\
&\qquad x^5 + x^3 + x + \overline{1}\\
&\quad -(\underline{x^5 + x^4 + x^2})\\
&\qquad\quad x^4 + x^3 + x^2 + x + \overline{1}\\
&\qquad -(\underline{x^4 + x^3 + x})\\
&\qquad\qquad x^2 + \overline{1}
\end{aligned}
$$

A maradék $x^2 + \overline{1}$, tehát az első polinom nem osztható a másodikkal.

$$
\begin{aligned}
&(x^6+x+\overline{1}) : (x^3+x+\overline{1}) = x^3+x+\overline{1}\\
&-(\underline{x^6+x^4+x^3})\\
&\qquad x^4+x^3+x+\overline{1}\\
&\quad -(\underline{x^4+x^2+x})\\
&\qquad\quad x^3+x^2+\overline{1}\\
&\qquad -(\underline{x^3+x+\overline{1}})\\
&\qquad\qquad x^2+x
\end{aligned}
$$

A maradék $x^2+x$, tehát az első polinom most sem osztható a másodikkal.

Mivel $x^6+x+\overline{1}$-nek sem első-, sem másod-, sem pedig harmadfokú irreducibilis tényezője nincs, ő maga irreducibilis. ■

### 3.1-9. Hány másodfokú normált (1 főegyüttható jú) irreducibilis polinom van egy $q$ elemű testben?

**Megoldás.** Számoljuk meg, hogy összesen hány $x^2+bx+c$ alakú polinom van, ha $b$ és $c$ a test tetszőleges eleme lehet. Mivel a test $q$ elemű, ilyen polinom $q \cdot q = q^2$ darab van.

Ebből el kell vennünk a reducibilisek számát. Ha egy normált másodfokú polinom reducibilis, akkor $(x-\alpha)(x-\beta)$ alakú, ahol $\alpha$ és $\beta$ a test tetszőleges eleme lehet. Ezek számát megkapjuk, ha $q$ elemből kettőt választunk ismétléssel, a tényezők sorrendje nem számít, tehát a keresett számot megadja a $C_q^{2,i}$ ismétléses permutációszám.

$$C_q^{2,i} = C_{q+1}^2 = \binom{q+1}{2} = \frac{q(q+1)}{2}$$

Az irreducibilisek száma így

$$q^2 - \frac{q(q+1)}{2} = \frac{q(q-1)}{2}$$

$q=2$ esetén ez a képlet 1-et ad, $q=3$ esetén pedig 3-at. ■

### 3.1-10. Készítsünk 9 elemű testet.

**a. Adjuk meg a művelettáblákat.**

**b. Határozzuk meg az egyes elemek multiplikatív rendjét, keressünk primitív elemeket.**

**c. Határozzuk meg az egyes elemek additív rendjét.**

**Megoldás.**

**a.** $\mathbb{F}_9$-et úgy készítjük el, hogy $\mathbb{Z}_3$-mat bővítjük például az $m = x^2 + \overline{1}$ $\mathbb{Z}_3$ fölött irreducibilis polinom $u$ gyökével (másodfokú bővítés). $\mathbb{F}_9$ elemei $u$ legfeljebb elsőfokú polinomjai és a 0.
$\mathbb{Z}_3$ elemei :

$$\overline{0} \qquad \overline{1} \qquad \overline{2} = \overline{-1} = -\overline{1}$$

$\mathbb{F}_9$ elemei :

$$\begin{array}{lllllllll} a & = & \overline{0} & & d & = & u & & g & = & 2u \\ b & = & \overline{1} & & e & = & u+\overline{1} & & h & = & 2u+\overline{1} \\ c & = & \overline{2} & & f & = & u+\overline{2} & & i & = & 2u+\overline{2} \end{array}$$

Az elemek összeadását és szorzását úgy végezzük el, mint a polinomokét.

| $+$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ |
|---|---|---|---|---|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ |
| $b$ | $b$ | $c$ | $a$ | $e$ | $f$ | $d$ | $h$ | $i$ | $g$ |
| $c$ | $c$ | $a$ | $b$ | $f$ | $d$ | $e$ | $i$ | $g$ | $h$ |
| $d$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ | $a$ | $b$ | $c$ |
| $e$ | $e$ | $f$ | $d$ | $h$ | $i$ | $g$ | $b$ | $c$ | $a$ |
| $f$ | $f$ | $d$ | $e$ | $i$ | $g$ | $h$ | $c$ | $a$ | $b$ |
| $g$ | $g$ | $h$ | $i$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ |
| $h$ | $h$ | $i$ | $g$ | $b$ | $c$ | $a$ | $e$ | $f$ | $d$ |
| $i$ | $i$ | $g$ | $h$ | $c$ | $a$ | $b$ | $f$ | $d$ | $e$ |

| $\cdot$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ |
|---|---|---|---|---|---|---|---|---|---|
| $a$ | $a$ | $a$ | $a$ | $a$ | $a$ | $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ | $c$ | $d$ | $e$ | $f$ | $g$ | $h$ | $i$ |
| $c$ | $a$ | $c$ | $b$ | $g$ | $i$ | $h$ | $d$ | $f$ | $e$ |
| $d$ | $a$ | $d$ | $g$ | $c$ | $f$ | $i$ | $b$ | $e$ | $h$ |
| $e$ | $a$ | $e$ | $i$ | $f$ | $g$ | $b$ | $h$ | $c$ | $d$ |
| $f$ | $a$ | $f$ | $h$ | $i$ | $b$ | $d$ | $e$ | $g$ | $c$ |
| $g$ | $a$ | $g$ | $d$ | $b$ | $h$ | $e$ | $c$ | $i$ | $f$ |
| $h$ | $a$ | $h$ | $f$ | $e$ | $c$ | $g$ | $i$ | $d$ | $b$ |
| $i$ | $a$ | $i$ | $e$ | $h$ | $d$ | $c$ | $f$ | $b$ | $g$ |

A szorzótábla elkészítésénél felhasználjuk azt, hogy $u^2 + \overline{1} = 0$, hiszen $u$ az $m = x^2 + \overline{1}$ polinom gyöke.

$$
\begin{aligned}
d \cdot d &= u^2 = u^2 + \overline{1} - \overline{1} = \overline{0} - \overline{1} = c \\
d \cdot e &= u^2 + u = u^2 + \overline{1} + u - \overline{1} = \overline{0} + u + \overline{2} = f \\
d \cdot f &= u^2 + 2u = u^2 + \overline{1} + 2u + \overline{2} = \overline{0} + i = i \\
d \cdot g &= 2u^2 = 2u^2 + \overline{2} + \overline{1} = \overline{0} + \overline{1} = b \\
d \cdot h &= 2u^2 + u = 2u^2 + \overline{2} + u + \overline{1} = \overline{0} + u + \overline{1} = e \\
d \cdot i &= 2u^2 + 2u = 2u^2 + \overline{2} + 2u + \overline{1} = \overline{0} + h \\
e \cdot e &= (u + \overline{1})^2 = u^2 + 2u + \overline{1} = \overline{0} + 2u = g \\
e \cdot f &= (u + \overline{1})(u + \overline{2}) = u^2 + 3u + \overline{2} = \overline{1} = b \\
e \cdot g &= (u + \overline{1})2u = 2u^2 + 2u = 2u^2 + \overline{2} + 2u + \overline{1} = h \\
e \cdot h &= (u + \overline{1})(2u + \overline{1}) = 2u^2 + 3u + \overline{1} = \overline{2} = c \\
e \cdot i &= (u + \overline{1})(2u + \overline{2}) = 2u^2 + 4u + \overline{2} = u = d \\
f \cdot f &= (u + \overline{2})^2 = u^2 + 4u + \overline{4} = u = d \\
f \cdot g &= (u + \overline{2})2u = 2u^2 + 4u = 2u^2 + 2 + u + \overline{1} = e \\
f \cdot h &= (u + \overline{2})(2u + \overline{1}) = 2u^2 + 5u + \overline{2} = 2u = g \\
f \cdot i &= (u + \overline{2})(2u + \overline{2}) = 2u^2 + 6u + \overline{4} = c \\
g \cdot g &= (2u)^2 = 4u^2 = u^2 + \overline{1} + \overline{2} = \overline{2} = c \\
g \cdot h &= 2u(2u + \overline{1}) = 4u^2 + 2u = u^2 + \overline{1} + 2u + \overline{2} = i \\
g \cdot i &= 2u(2u + \overline{2}) = 4u^2 + 4u = u^2 + u = f \\
h \cdot h &= (2u + \overline{1})(2u + \overline{1}) = 4u^2 + 4u + \overline{1} = u = d \\
h \cdot i &= (2u + \overline{1})(2u + \overline{2}) = 4u^2 + 6u + \overline{2} = b \\
i \cdot i &= (2u + \overline{2})^2 = 4u^2 + 8u + \overline{4} = 2u = g
\end{aligned}
$$

**Megjegyzés.** A fenti számítások elvégzése során úgy is eljárhattunk volna, hogy felhasználjuk az $u^2 = \overline{-1} = \overline{2}$, összefüggést.

**b.** Most nézzük a nem nulla elemek multiplikatív rendjét. A Lagrange-tételből tudjuk, hogy ez a rend csak olyan szám lehet, ami osztója a test multiplikatív csoportja rendjének, vagyis 8-nak. A szóbajöhető rendek tehát $1, 2, 4, 8$. Azt kell megvizsgálnunk, hogy ezekre a kitevőkre emelve az elemet, mikor kapjuk meg először az egységelemet. A 8. hatvány esetében természetesen mindenképpen megkapjuk.

$$
\begin{array}{llll}
|b| = 1 & & & \\
c^2 = 1 & |c| = 2 & & \\
d^2 = c & d^4 = c^2 = 1 & |d| = 4 & \\
g^2 = c & c^2 = 1 & |g| = 4 & \\
e^2 = g & e^4 = g^2 = c & e^8 = c^2 = 1 & |e| = 8 \\
f^2 = d & f^4 = d^2 = \overline{2} & f^8 = 1 & |f| = 8 \\
h^2 = d & |h| = 8 & & \\
i^2 = g & |i| = 8 & &
\end{array}
$$

Primitív elemek – az $(\mathbb{F}_9^*, \cdot)$ csoport generáló elemei – azok, amelyek rendje megegyezik a multiplikatív csoport rendjével, tehát 8 a rendjük. Ezek $e$, $f$, $h$, $i$.

**c.** Az elemek additív rendje a 0 kivételével 3, mert $\mathrm{Char}(\mathbb{Z}_3)$=$\mathrm{Char}(\mathbb{F}_9)$=3.

■

**3.1-11. Készítsünk 4 elemű testet.**

**a. Adjuk meg a műveletáblákat.**

**b. Határozzuk meg az egyes elemek multiplikatív rendjét, keressünk primitív elemeket.**

**Megoldás.**

**a.** $\mathbb{F}_4$-et úgy készítjük el, hogy $\mathbb{Z}_2$-t bővítjük az $m = x^2 + x + \overline{1}$ $\mathbb{Z}_2$ fölött irreducibilis polinom $u$ gyökével (másodfokú bővítés). Az $m$ polinom valóban irreducibilis $\mathbb{Z}_2$ fölött, mert $m(\overline{1}) = \overline{1}$ és $m(\overline{0}) = \overline{1}$, tehát nincs gyöke $\mathbb{Z}_2$-ben (egyébként lásd a 7. példát). $\mathbb{F}_4$ elemei $u$ legfeljebb elsőfokú polinomjai és a 0.
$\mathbb{Z}_2$ elemei :

$$\overline{0} \qquad \overline{1} = \overline{-1} = -\overline{1}$$

$\mathbb{F}_4$ elemei :

$$a = \overline{0} \qquad b = \overline{1} \qquad c = u \qquad d = u + \overline{1}$$

Az elemek összeadását és szorzását úgy végezzük el, mint a polinomokét.

| $+$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $b$ | $c$ | $d$ |
| $b$ | $b$ | $a$ | $d$ | $c$ |
| $c$ | $c$ | $d$ | $a$ | $b$ |
| $d$ | $d$ | $c$ | $b$ | $a$ |

| $\cdot$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | $a$ | $a$ | $a$ |
| $b$ | $a$ | $b$ | $c$ | $d$ |
| $c$ | $a$ | $c$ | $d$ | $b$ |
| $d$ | $a$ | $d$ | $b$ | $c$ |

A szorzótábla elkészítésénél felhasználjuk azt, hogy $u^2 + u + \overline{1} = 0$, hiszen $u$ az $m = x^2 + x + \overline{1}$ polinom gyöke, és így $u^2 = u + \overline{1}$ is fennáll.

$$c \cdot c = u^2 = u^2 + u + \overline{1} + u + \overline{1} = u + \overline{1} = d$$

$$c \cdot d = u^2 + u = u^2 + u + \overline{1} + \overline{1} = \overline{1} = b$$

$$d \cdot d = (u+1)(u+1) = u^2 + 2u + 1 = u^2 + u + \overline{1} + u = u = c$$

**b.** Primitív elemek: $c = u,\ d = u + 1$.

A multiplikatív csoport generáló eleme a $c$, mert különböző hatványai előállítják a többi elemet:

$$c^1 = c \qquad c^2 = u + \overline{1} = d \qquad c^3 = (u+1) \cdot u = \overline{1} = b$$

Hasonlóan generáló elem a $d$ is:

$$d^1 = d \qquad d^2 = u^2 + \overline{1} = u = c \qquad d^3 = u^2 + u = \overline{1} = b$$

**Megjegyzés.** Az előbbi eredményt más meggondolással is megkaphatjuk: mivel $\mathbb{Z}_3$ multiplikatív csoportjának rendje 3, a csoport ciklikus, sőt az egységelem kivételével a többi két eleme ($c$ és $d$) generálja. ■

**3.1-12.**

**a. Bizonyítsuk be, hogy az $f(x) = x^3 + x + \overline{1} \in \mathbb{Z}_5[x]$ polinom irreducibilis $\mathbb{Z}_5$ felett.**

**b. Hány eleme van a $\mathbb{Z}_5[x]/\overline{f}$ maradékosztálygyűrűnek (testnek), ahol $\overline{f}$ az $f$ többszöröseiből álló ideál? Adjunk meg egy reprezentánsrendszert.**

**Megoldás.**

**a.** Az irreducibilitáshoz elég megvizsgálnunk azt, hogy van-e gyöke a polinomnak $\mathbb{Z}_5$-ben. Ha ugyanis felbontható (reducibilis) lenne, akkor

$$x^3 + x + \overline{1} = (ax + b)(cx^2 + dx + e) \pmod 5$$

alakban lehetne felírni. Mivel $ax + b = 0 \pmod 5$ $a \neq 0$ miatt megoldható, lenne gyöke a polinomnak $\mathbb{Z}_5$-ben. A polinomnak azonban nincs gyöke ebben a testben:

$$f(\overline{0}) = \overline{1}, \qquad f(\overline{1}) = \overline{3}, \qquad f(\overline{2}) = \overline{1}, \qquad f(\overline{3}) = \overline{1}, \qquad f(\overline{4}) = \overline{-1},$$

így $f$ irreducibilis $\mathbb{Z}_5$ felett.

**b.** reprezentánsrendszert alkotnak a legfeljebb másodfokú polinomok:

$$\left\{a + bx + cx^2 \mid a,\ b,\ c \in \{0,\ 1,\ 2,\ 3,\ 4\}\right\}$$

Mivel $a,\ b,\ c$ egymástól függetlenül felveheti az 5 különböző értéket, ezért a reprezentánsrendszer $5^3 = 125$ elemű, s ennyi eleme van a $\mathbb{Z}_5[x]/\overline{f}$ testnek is.

■

**3.1-13.**

**a. Bizonyítsuk be, hogy az $f(x) = x^2 + x + \overline{1} \in \mathbb{Z}_5[x]$ polinom irreducibilis $\mathbb{Z}_5$ felett.**

**b. Hány eleme van a $\mathbb{Z}_5[x]/\overline{f}$ maradékosztálygyűrűnek (testnek), ahol $\overline{f}$ az $f$ többszöröseiből álló ideál? Adjunk meg egy reprezentánsrendszert.**

**Megoldás.**

**a.** Az irreducibilitáshoz elég megvizsgálnunk azt, hogy van-e gyöke a polinomnak $\mathbb{Z}_5$-ben. Ha ugyanis felbontható (reducibilis) lenne, akkor

$$x^2 + x + \overline{1} = (ax + b)(cx + d) \pmod 5$$

alakban lehetne felírni. Mivel $ax + b = 0 \pmod 5$ $a \neq 0$ miatt megoldható, lenne gyöke a polinomnak $\mathbb{Z}_5$-ben. A polinomnak azonban nincs gyöke ebben a testben:

$$f(\overline{0}) = \overline{1}, \qquad f(\overline{1}) = \overline{3}, \qquad f(\overline{2}) = \overline{2}, \qquad f(\overline{3}) = \overline{3}, \qquad f(\overline{4}) = \overline{1},$$

így $f$ irreducibilis $\mathbb{Z}_5$ felett.

**b.** reprezentánsrendszert alkotnak a legfeljebb elsőfokú polinomok:

$$\{a + bx \mid a,\ b \in \{0,\ 1,\ 2,\ 3,\ 4\}\}$$

Mivel $a$ és $b$ egymástól függetlenül felveheti az 5 különböző értéket, ezért a reprezentánsrendszer $5^2 = 25$ elemű, s ennyi eleme van a $\mathbb{Z}_5[x]/\overline{f}$ testnek is.

$\mathbb{Z}_5[x]/\overline{f}$ elemei az alábbi elemek által reprezentált osztályok:

| | | | | |
|---|---|---|---|---|
| $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $x$ | $x+\overline{1}$ | $x+\overline{2}$ | $x+\overline{3}$ | $x+\overline{4}$ |
| $2x$ | $2x+\overline{1}$ | $2x+\overline{2}$ | $2x+\overline{3}$ | $2x+\overline{4}$ |
| $3x$ | $3x+\overline{1}$ | $3x+\overline{2}$ | $3x+\overline{3}$ | $3x+\overline{4}$ |
| $4x$ | $4x+\overline{1}$ | $4x+\overline{2}$ | $4x+\overline{3}$ | $4x+\overline{4}$ |

■

**3.1-14.**

**a. Igazoljuk, hogy $f(x) = x^3 + x + \overline{2}$ reducibilis $\mathbb{Z}_7$ felett.**

**b. Hány eleme van a $\mathbb{Z}_7[x]/\overline{f}$ maradékosztálygyűrűnek ($\overline{f}$ az $f$ polinom többszöröseiből álló ideál)? Adjunk meg egy reprezentánsrendszert.**

**c. Mutassuk meg, hogy a $\mathbb{Z}_7[x]/\overline{f}$ maradékosztálygyűrű tartalmaz nullosztót.**

**Megoldás.**

**a.** A Horner-elrendezéssel azt tapasztaljuk, hogy $f$-nek $\overline{4}$ kétszeres gyöke, $\overline{-1}$ pedig egyszeres gyöke.

| | 1 | 0 | 1 | 2 | |
|---|---|---|---|---|---|
| 4 | | 1 | 4 | 3 | 0 |
| 4 | | | 1 | 1 | 0 |
| $-1$ | | | | 1 | 0 |

**b.** A maradékosztálygyűrű elemeinek reprezentánsai a legfeljebb másodfokú polinomok:

$$\left\{a + bx + cx^2 \mid a,\ b,\ c \in \{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6\}\right\}$$

Mivel $a$, $b$ és $c$ egymástól függetlenül felveheti a 7 különböző értéket, ezért a reprezentánsrendszer $7^3 = 343$ elemű, s ennyi eleme van a $\mathbb{Z}_5[x]/\overline{f}$ maradékosztálygyűrűnek is.

**c.** Nullosztópárt alkot például a következő két osztály:

$$\overline{(x-4)^2}, \quad \overline{x+1},$$

mert

$$\overline{(x-4)^2} \cdot \overline{x+1} = \overline{(x-4^2)\cdot(x+1)} = \overline{f} = 0.$$

Ez a maradékosztálygyűrű nem test, hiszen tartalmaz nullosztót. ■

### 3.1.2. Elem felírása bázisban

**3.1-15. Legyen $u \in \mathbb{C}$ a $\mathbb{Q}$ feletti $x^3 - 2x + 2$ polinom egyik gyöke. Lássuk be, hogy a polinom $\mathbb{Q}$ felett irreducibilis. Írjuk fel $\mathbb{Q}(u) \mid \mathbb{Q}$ $\{1,\ u,\ u^2\}$ bázisában a következő elemeket:**

**a.** $u^7$ **b.** $u^{-1}$ **c.** $u^4 + u^{-2}$

**Megoldás.** A polinom irreducibilis $\mathbb{Z}$ felett: $p = 2$-vel alkalmazzuk a Schönemann–Eisenstein-tételt. A $\mathbb{Q}$ feletti irreducibilitás ebből és a Gauss-tételből következik.

$u$ az $x^3 - 2x + 2$ polinom gyöke, ezért $u^3 - 2u + 2 = 0$, amiből $u^3 = 2u - 2$. Ezt használjuk fel többször is a továbbiakban.

**a.**

$$u^7 = u^4 \cdot u^3 = u^4(2u-2) = u(2u-2)u^3 = u(2u-2)(2u-2) =$$

$$= u(4u^2 - 8u + 4) = 4u^3 - 8u^2 + 4u = 4(2u-2) - 8u^2 + 4u = -8u^2 + 12u - 8$$

**b.** $u \neq 0$, így létezik inverze. Az $u^3 - 2u + 2 = 0$ egyenletet megszorozzuk $u^{-1}$-gyel, ekkor

$$(u^3 - 2u + 2) \cdot u^{-1} = 0.$$

Ebből $u^2 - 2 + 2u^{-1} = 0$, $\qquad u^{-1} = 1 - \frac{u^2}{2}$.

**c.** Először számítsuk ki $u^4$-t. $u^4 = u(2u-2) = 2u^2 - 2u$

Most nézzük $u^{-2}$ kiszámítását. Az $u^3-2u+2=0$ egyenletet megszorozzuk $u^{-2}$-vel.

$$(u^3 - 2u + 2)u^{-2} = 0$$

$$u - 2u^{-1} + 2u^{-2} = 0$$

$$u^{-2} = 1 - \frac{u^2+u}{2}$$

Végül a két kifejezés összege:

$$u^4 + u^{-2} = 2u^2 - 2u + 1 - \frac{u^2+u}{2} = \frac{3}{2}u^2 - \frac{5}{2}u + 1$$

■

**3.1-16. Legyen $u \in \mathbb{C}$ az $x^3 - 6x^2 + 9x + 3 \quad \mathbb{Q}$ felett irreducibilis polinom gyöke. Fejezzük ki $\mathbb{Q}(u) \mid \mathbb{Q} \quad \{1,\ u,\ u^2\}$ bázisában a következő elemeket:**

**a.** $3u^5 - 2u$ **b.** $\frac{1}{1+u}$

**Megoldás.** $u \notin \mathbb{Q}$, mert a polinom irreducibilis. $u$ az $x^3-6x^2+9x+3$ polinom gyöke, ezért $u^3 - 6u^2 + 9u + 3 = 0$, amiből $u^3 = 6u^2 - 9u - 3$. Ezt használjuk fel többször is a továbbiakban.

**a.**

$$3u^5 - 2u = 3u^2 \cdot u^3 - 2u = 3 \cdot u^2(6u^2 - 9u - 3) - 2u = 18u^4 - 27u^3 - 9u^2 - 2u =$$

$$= 18u(u^3) - 27u^3 - 9u^2 - 2u = 18u \cdot (6u^2 - 9u - 3) - 27(6u^2 - 9u - 3) - 9u^2 - 2u =$$

$$= 108u^3 - 162u^2 - 54u - 162u^2 + 243u + 81 - 9u^2 - 2u =$$

$$= 108(6u^2 - 9u - 3) - 333u^2 + 187u + 81 =$$

$$= 315u^2 - 785u - 243$$

**b.** Az $u^3 - 6u^2 + 9u + 3 = 0$ egyenletet megszorozzuk $(u+1)^{-1}$-gyel.

$$\frac{u^3 - 6u^2 + 9u + 3}{u+1} = 0$$

A számlálóval és a nevezővel maradékos osztást végzünk:

$$\begin{array}{r} (u^3-6u^2+9u+\ 3) : (u+1) = u^2-7u+16 \\ \underline{-(u^3+u^2)} \\ -7u^2+9u+\ 3 \\ \underline{-(-7u^2-7u)} \\ 16u+\ 3 \\ \underline{16u+16} \\ -13 \end{array}$$

A maradékos osztás eredménye:

$$u^3-6u^2+9u+3 = (u^2-7u+16)(u+1)-13 \tag{1}$$

Felhasználva, hogy $u^3-6u^2+9u+3=0$, azt kapjuk, hogy:

$$\frac{1}{u+1} = \frac{u^2-7u+16}{13}$$

Az $u+1$ kifejezéssel való maradékos osztás helyett Horner-elrendezést is alkalmazhatunk:

| | 1 | −6 | 9 | 3 | |
|---|---|---|---|---|---|
| −1 | | 1 | −7 | 16 | −13 |

Ebből a táblázatból is leolvashatjuk (1) együtthatóit. ■

### 3.1.3. Minimálpolinom, felbontási test

**3.1-17. Határozzuk meg $\sqrt{2-\sqrt[3]{2}}$ minimálpolinomját $\mathbb{Q}$ felett.**

**Megoldás.** Legyen

$$\alpha = \sqrt{2-\sqrt[3]{2}}$$

Ebből a következőkhöz jutunk:

$$\alpha^2 = 2-\sqrt[3]{2}$$

$$-\alpha^2+2 = \sqrt[3]{2}$$

$$(-\alpha^2+2)^3 = 2$$

$$-\alpha^6 + 6\alpha^4 - 12\alpha^2 + 6 = 0,$$

vagyis $\alpha$ gyöke az

$$f = x^6 - 6x^4 + 12x^2 - 6$$

polinomnak. Másrészt ez a polinom irreducibilis, amit beláthatunk úgy, hogy alkalmazzuk a Schönemann-Eisenstein tételt $p = 2$-vel (vagy 3-mal). Ebből pedig következik, hogy $f$ minimálpolinomja $\sqrt{2 - \sqrt[3]{2}}$-nek. ■

**3.1-18. Mutassuk meg, hogy**

$$\sqrt[3]{9 + 4\sqrt{5}} + \sqrt[3]{9 - 4\sqrt{5}}$$

**egész szám.**

**Megoldás.** Legyen

$$\alpha = \sqrt[3]{9 + 4\sqrt{5}} + \sqrt[3]{9 - 4\sqrt{5}}.$$

Számítás közben felhasználjuk, hogy

$$(a + b)^3 = a^3 + b^3 + 3a^2b + 3ab^2 = a^3 + b^3 + 3ab(a + b)$$

és alkalmazzuk a következő jelölést: $a = \sqrt[3]{9 + 4\sqrt{5}}$, $b = \sqrt[3]{9 - 4\sqrt{5}}$. Ekkor

$$\alpha^3 = 9 + 4\sqrt{5} + 9 - 4\sqrt{5} + 3\sqrt[3]{81 - 80}(a + b) = 18 + 3(a + b) = 18 + 3\alpha$$

Így az alábbi polinomhoz jutottunk.

$$x^3 = 18 + 3x$$

$$x^3 - 3x - 18 = 0$$

Ennek a polinomnak gyöke a $\sqrt[3]{9 + 4\sqrt{5}} + \sqrt[3]{9 - 4\sqrt{5}}$ szám.

Keressük először a polinom racionális gyökeit. Felhasználjuk, hogy ha van $\alpha$ racionális gyök, akkor az egész szám, osztója 18-nak, valamint $1-\alpha | \sum a_i = f(1)$ és $1+\alpha | \sum(-1)^i a_i = f(-1)$, ahol $a_i$ a polinom együtthatóit jelöli. (Lásd a Polinomok kötetben.)

Azt kapjuk, hogy a 3 lehetséges gyök, behelyettesítéssel (Horner-elrendezés) pedig azt kapjuk, hogy valóban gyök.

| $\alpha$ | 1 | 0 | $-3$ | $-18$ | $f(\alpha)$ |
|---|---|---|---|---|---|
| 3 | | 1 | 3 | 6 | 0 |

A Horner-elrendezés együtthatóiból azt is leolvashatjuk, hogy mi a hányados polinom, ha $x-3$-mal osztjuk a polinomunkat:

$$x^2+3x+6$$

Ennek a polinomnak a gyökei

$$x_{1,2}=\frac{-3\pm\sqrt{9-24}}{2}=\frac{-3\pm i\sqrt{15}}{2},$$

tehát nem valósak. A $\sqrt[3]{9+4\sqrt{5}}+\sqrt[3]{9-4\sqrt{5}}$ szám valós, s ennek a gyökök közül csak a 3 felel meg. Tehát

$$\sqrt[3]{9+4\sqrt{5}}+\sqrt[3]{9-4\sqrt{5}}=3.$$

■

**3.1-19. Határozzuk meg az $(x^2+1)(x^2-2x+1)$ polinom felbontási testét $\mathbb{Q}$ felett.**

**Megoldás.**

$$(x^2+1)(x^2-2x+1)=(x-i)(x+i)(x-1)^2,$$

így a polinom gyökei $\pm i$ és 1, tehát a polinom $\mathbb{Q}$ feletti felbontási teste $\mathbb{Q}(i)$.

■

**3.1-20. $\mathbb{Q}(\sqrt[3]{2})$ megegyezik-e $\sqrt[3]{2}$ minimálpolinomjának a felbontási testével?**

**Megoldás.** $\sqrt[3]{2}$ minimálpolinomja $x^3-2$. Ennek gyökei $\sqrt[3]{2}$ mellett

$$\sqrt[3]{2}\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right),\quad \sqrt[3]{2}\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right).$$

Ez utóbbi két gyök nincs benne $\mathbb{Q}(\sqrt[3]{2})$-ben (mert ennek a testnek minden eleme valós), tehát a két test nem egyezik meg. ■

**3.1-21. Van-e racionális gyöke az $f(x) = x^3 - x^2 - x - 2$ polinomnak? Mi az $f$ felbontási teste $\mathbb{Q}$ felett?**

**Megoldás.** A polinom racionális gyökei 2 osztói lehetnek. 2 valóban gyöke, amint erről a Horner-elrendezéssel meggyőződhetünk:

| | 1 | −1 | −1 | −2 | |
|---|---|---|---|---|---|
| 2 | | 1 | 1 | 1 | 0 |

Az előbbi táblázat második sorában a hányados polinom együtthatói is megjelennek, amely $x^2 + x + 1$. Ennek (s így az eredeti polinomnak is) a gyökei $\frac{-1 \pm i\sqrt{3}}{2}$. Az $f$ polinom $\mathbb{Q}$ feletti felbontási teste így $\mathbb{Q}(i\sqrt{3})$. ■

**3.1-22. Bizonyítsuk be, hogy ha $\alpha \in \mathbb{C}$ megoldása a $10x^3 - 105x^2 + 84x + 210 = 0$ racionális együtthatós egyenletnek, és valamely $K$ testre fennáll, hogy $\mathbb{Q}(\alpha)|K$ és $K|\mathbb{Q}$, akkor $K = \mathbb{Q}(\alpha)$ vagy $K = \mathbb{Q}$.**

**Megoldás.** Ha $p = 7$-tel alkalmazzuk a Schönemann–Eisenstein-tételt, akkor azt tapasztaljuk, hogy a polinom $\mathbb{Z}$ felett irreducibilis. Ebből a Gauss-tétel alkalmazásával azt kapjuk, hogy $\mathbb{Q}$ felett is irreducibilis a polinom, tehát $\mathbb{Q}(\alpha)|\mathbb{Q}$ harmadfokú bővítés. A testbővítések fokszámtétele szerint

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : K] \cdot [K : \mathbb{Q}] = 3.$$

Ebből $[\mathbb{Q}(\alpha) : K]$ és $[K : \mathbb{Q}]$ egyike 1, tehát $K = \mathbb{Q}(\alpha)$ vagy $K = \mathbb{Q}$. ■

**3.1-23. Legyen $K = \mathbb{F}_q$, és $f(x)$ $K$ fölötti irreducibilis $n$-edfokú polinom. Lássuk be, hogy**

$$f(x)|x^{q^n} - x.$$

**($\mathbb{F}_q$ a $q$ elemű testet jelöli.)**

**Megoldás.** Legyen $\alpha$ az $f$ polinom gyöke, és bővítsük $K$-t $\alpha$-val:

$$L = \mathbb{F}_q(\alpha)$$

Belátjuk, hogy $\alpha$ gyöke az $x^{q^n} - x$ polinomnak. $L$ $q^n$ elemszámú test, multiplikatív csoportjának elemszáma eggyel kevesebb:

$$|L \setminus \{0\}| = q^n - 1.$$

Legyen $\beta$ a test tetszőleges nem nulla eleme. Ekkor

$$\beta^{q^n-1} = e,$$

ahol $e$ a test egységeleme, ugyanis ha csoport valamely elemét a csoport rendje nagyságú kitevőre emeljük, akkor megkapjuk az egységelemet (Lagrange-tétel következménye). Így az is igaz, hogy

$$\alpha^{q^n-1} = e.$$

Innen

$$\alpha^{q^n} = \alpha,$$

vagyis

$$\alpha^{q^n} - \alpha = 0$$

tehát $\alpha$ valóban gyöke az $x^{q^n} - x$ polinomnak is.

Másrészről $f$ az $\alpha$ $K$ fölötti minimálpolinomja, és ha a $K$ fölötti valamely $g$ polinomnak gyöke $\alpha$, akkor $f|g$ is teljesül. Tehát

$$f(x)|x^{q^n} - x$$

■

**3.1-24. Legyen $K = \mathbb{F}_q$, $f(x)$ $K$ fölötti irreducibilis $n$-edfokú polinom, és legyen $\alpha$ gyöke $f$-nek. Lássuk be, hogy $K$-t $\alpha$-val bővítve megkapjuk $f$ $K$ fölötti felbontási testét. (Más szóval lássuk be, hogy ha $f$ egyik gyöke a bővített véges testben van, akkor $f$ mindegyik gyöke benne van.) ($\mathbb{F}_q$ a $q$ elemű testet jelöli.)**

**Megjegyzés. 0 karakterisztikájú testben ez általában nem igaz (lásd a 20. példát).**

**Megoldás.** Legyen $L = \mathbb{F}_q(\alpha)$. Beláttuk az előző példában, hogy $\alpha$ gyöke az $x^{q^n} - x$ $L$ fölötti polinomnak. Sőt azt is beláttuk, hogy a test bármelyik nem nulla $\beta$ eleme is gyöke a polinomnak. Ennek a polinomnak – mint könnyen látható – gyöke a 0 is, tehát a test minden eleme gyöke. Mivel a $q^n$-fokú polinomnak megtaláltuk $q^n$ gyökét, több gyöke pedig nem lehet egy test fölötti

polinomnak, mint a fokszáma, ebből következik, hogy a polinom $L$ fölött $q^n$ darab elsőfokú tényező szorzatára bomlik.

$$x^{q^n} - x = \prod_{\beta \in L} (x - \beta)$$

Másrészt szintén az előbbi példából tudjuk, hogy

$$f(x) | x^{q^n} - x,$$

tehát $L$ fölött $f$ is elsőfokú polinomok szorzatára bomlik. Ez pedig azt jelenti, hogy $f$ egyetlen gyökével bővítve, a kapott testben $f$ mindegyik gyöke megtalálható. ■

### 3.1.4. Bővítés foka, véges és algebrai bővítés

**3.1-25. A következő bővítések közül melyik véges és melyik algebrai? ($A$ az algebrai számok halmaza)**

**a.** $\mathbb{C}|\mathbb{R}$ **b.** $\mathbb{Q}(\sqrt{5})|\mathbb{Q}$ **c.** $A|\mathbb{Q}$ **d.** $A|\mathbb{Q}(\sqrt{5})$ **e.** $\mathbb{R}|\mathbb{Q}(\pi)$

**Megoldás.**

**a.** Véges, algebrai, $\{1,\ i\}$ egy bázis.

**b.** Véges, algebrai, $\{1,\ \sqrt{5}\}$ egy bázis.

**c.** Nyilván algebrai a bővítés, ugyanakkor nem véges. Ha véges lenne, akkor lenne véges bázisa, s így véges sok algebrai szám lineáris kombinációjaként az összes többit elő lehetne állítani. Ez azonban nem lehetséges.

**d.** Nem véges, algebrai.

**e.** Nem véges, nem algebrai, pl. belátható, hogy $e$ nem írható fel $\mathbb{Q}(\pi)$-beli nem nulla polinom gyökeként. ■

**3.1-26. Mennyi a $\mathbb{Q}(\pi)|\mathbb{Q}(\pi^2)$ testbővítés foka?**

**Megoldás.** A bővítés foka 2. Egyrészt $\pi \notin \mathbb{Q}(\pi^2)$, másrészt $x^2 - \pi^2 \quad \mathbb{Q}(\pi^2)$ feletti polinom, ennek gyöke $\pi$, s így másodfokú a bővítés. ■

**3.1-27. Határozzuk meg a $T|\mathbb{Q}$ testbővítés fokát, ahol $T$ az alábbi. Mi a bővítő elem minimálpolinomja $\mathbb{Q}$ fölött? Adjunk meg egy bázist.**

**a.** $\mathbb{Q}(\sqrt{7})$ **b.** $\mathbb{Q}(i\sqrt{5})$
**c.** $\mathbb{Q}(1+i\sqrt{3})$ **d.** $\mathbb{Q}(i+\sqrt{5})$
**e.** $\mathbb{Q}(u+i\sqrt{v}),\ u,v\in\mathbb{Q},\sqrt{v}\notin\mathbb{Q}$

**Megoldás.**

**a.** Legyen $\alpha=\sqrt{7}$. Mivel $\alpha\notin\mathbb{Q}$, $\alpha$ minimálpolinomja legalább másodfokú. $\alpha^2=7$, s így $\sqrt{7}$ minimálpolinomja $\mathbb{Q}$ fölött $x^2-7$. A bővítés foka 2, egy bázis $\{1,\sqrt{7}\}$.

**b.** Legyen $\alpha=i\sqrt{5}$. Mivel $\alpha\notin\mathbb{Q}$, $\alpha$ minimálpolinomja legalább másodfokú. $\alpha^2=-5$, s így $i\sqrt{5}$ minimálpolinomja $\mathbb{Q}$ fölött $x^2+5$, a bővítés foka 2, egy bázis $\{1,i\sqrt{5}\}$.

**c.** Legyen $\alpha=1+i\sqrt{3}$. Mivel $\alpha\notin\mathbb{Q}$, $\alpha$ minimálpolinomja legalább másodfokú. $\alpha$ minimálpolinomja $\mathbb{Q}$ fölött $x^2-2x+4$. Ezt a következőképpen találhatjuk meg:

$$\alpha=1+i\sqrt{3}$$

$$\alpha^2=1-3+2i\sqrt{3}=2+2i\sqrt{3}-4=2\alpha-4$$

$\alpha$ gyöke az $x^2-2x+4$ polinomnak, és korábbi megállapításunk alapján ez a minimálpolinomja is.

A bővítés foka 2, egy bázis $\{1,1+i\sqrt{3}\}$. Mivel $\mathbb{Q}(1+i\sqrt{3})=\mathbb{Q}(i\sqrt{3})$, bázis például $\{1,i\sqrt{3}\}$ is.

**d.** $i+\sqrt{5}$ minimálpolinomja $\mathbb{Q}$ fölött $x^4-8x^2+36$. Ezt a következőképpen találhatjuk meg:

$$\alpha=i+\sqrt{5}$$

$$\alpha^2=-1+5+2i\sqrt{5}$$

$$\alpha^2-4=2i\sqrt{5}$$

$$\alpha^4+16-8\alpha^2=-20$$

Ezek szerint $i+\sqrt{5}$ gyöke az $f=x^4-8x^2+36$ polinomnak.

Az $i+\sqrt{5}$ elemmel való bővítés negyedfokú, mert két másodfokú bővítés szorzata ($i$-vel majd $\sqrt{5}$-tel bővítünk). Így a kapott negyedfokú polinom minimálpolinomja $i+\sqrt{5}$-nek.

Egy lehetséges bázis $\{1, i+\sqrt{5}, (i+\sqrt{5})^2, (i+\sqrt{5})^3\}$.

**e.** $u+i\sqrt{v}$ minimálpolinomja $\mathbb{Q}$ fölött $x^2-2ux+u^2+v$. Ezt a következőképpen találhatjuk meg. Legyen

$$\alpha = u+i\sqrt{v},$$

ekkor

$$\alpha^2 = u^2-v+2ui\sqrt{v} = u^2-v+2u(u+i\sqrt{v})-2u^2 = -u^2-v+2u\alpha$$

Vagyis $\alpha$ gyöke a $\mathbb{Q}$ fölötti $x^2-2ux+u^2+v$ polinomnak. Ugyanakkor $\alpha \notin \mathbb{Q}$, így a minimálpolinom legalább másodfokú.

A bővítés foka 2, egy bázis $\{1, u+i\sqrt{v}\}$. Mivel $\mathbb{Q}(u+i\sqrt{v}) = \mathbb{Q}(i\sqrt{v})$, bázis például $\{1, i\sqrt{v}\}$ is. ■

**3.1-28. Határozzuk meg a $T|\mathbb{Q}$ testbővítés fokát, ahol $T$ az alábbi. Adjunk meg egy bázist.**

**a.** $\mathbb{Q}(\sqrt{2},\sqrt{3})$ **b.** $\mathbb{Q}(i,\sqrt{8})$

**Megoldás.**

**a.** $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$. A bővítés tehát felfogható két másodfokú bővítés egymásutánjaként. Az első bővítés bázisa $\{1,\sqrt{2}\}$, a második bővítés bázisa $\{1,\sqrt{3}\}$. A keresett bővítés bázisa a két előbbi bázis szorzatából adódik (lásd testbővítések fokszámtétele): $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$, a bővítés foka pedig 4.

**b.** $\mathbb{Q}(i,\sqrt{8}) = \mathbb{Q}(i)(\sqrt{8})$. A bővítés tehát felfogható két másodfokú bővítés egymásutánjaként. Az első bővítés bázisa $\{1,i\}$, a második bővítés bázisa $\{1,\sqrt{8}\}$. A keresett bővítés bázisa a két előbbi bázis szorzatából adódik (lásd testbővítések fokszámtétele): $\{1,i,\sqrt{8},i\sqrt{8}\}$, a bővítés foka pedig 4. ■

### 3.1.5. Véges test elemeinek összege, szorzata, Vieta-formulák, gyökök és együtthatók közötti összefüggések

**3.1-29. Bizonyítsuk be a Wilson-tételt:** $(p-1)! \equiv -1 \pmod{p}$, **ha** $p$

**prím.**

**Megoldás.** $\mathbb{Z}_p$ elemeivel dolgozunk. Minden $\overline{a} \neq \overline{0}$ maradékosztályhoz párosítjuk azt a $\overline{b}$ maradékosztályt, amellyel szorozva $\overline{1}$-et ad. Mivel $\mathbb{Z}_p$ test, minden $\overline{a} \neq \overline{0}$-hoz van ilyen $\overline{b}$. Ha $\overline{a}$ párja $\overline{b}$, akkor nyilván $\overline{b}$ párja $\overline{a}$. E párosítás során csak az $\overline{1}$ és $\overline{-1}$ osztály lesz önmaga párja. Ha ugyanis $\overline{u}$ párja önmaga, akkor

$$u^2 \equiv 1 \pmod{p},$$

vagyis

$$0 \equiv u^2 - 1 = (u-1)(u+1) \pmod{p}.$$

Ebből, mivel $p$ prím

$$p|u-1 \quad \text{vagy} \quad p|u+1,$$

tehát

$$u \equiv 1 \pmod{p} \quad \text{vagy} \quad u \equiv -1 \pmod{p}.$$

Szorozzuk össze tehát mindegyik osztályt a párjával, ha az különbözik tőle. Ezeket az értékeket egymással is összeszorozva $\overline{1}$-et kapunk, amit még meg kell szoroznunk a kimaradt osztályokkal, az $\overline{1}$-gyel, és – ha ettől különbözik – akkor a $\overline{-1}$-gyel is.

Ha $\overline{1} \neq \overline{-1}$, akkor $(p-1)! \equiv 1(-1) = -1 \pmod{p}$.

$p = 2$ esetén $\overline{1} = \overline{-1}$ s így $(p-1)! \equiv 1 \equiv -1 \pmod{2}$ szintén teljesül. ■

### 3.1-30. Mennyi valamely véges test nem nulla elemeinek a szorzata?

**Megoldás.** Az előző példa gondolatmenetét alkalmazzuk. Tetszőleges véges testben is megtehetjük, hogy mindegyik elemet megszorozzuk az inverzével, s a szorzatok értéke 1-et ad (most 1 az adott véges test egységeleme). Csupán azt kell most is megvizsgálnunk, hogy van-e olyan elem, amelyik önmaga

inverze. Ha $u$ inverze önmaga, akkor

$$u = \frac{1}{u},$$

amiből

$$0 = u^2 - 1 = (u-1)(u+1).$$

Mivel testben nincs nullosztó, ez csak úgy lehet, ha

$$u - 1 = 0 \quad \text{vagy} \quad u + 1 = 0,$$

ebből pedig

$$u = 1 \quad \text{vagy} \quad u = -1.$$

Szorozzuk össze mindegyik elemet az inverzével, ha az különbözik tőle. Ha ezeket az értékeket egymással is összeszorozzuk, 1-et kapunk, amit még meg kell szoroznunk a kimaradt $-1$-gyel, s így az eredmény $-1$ lesz. Ha a véges testben $1 \neq -1$, akkor az eddigi eredményt még 1-gyel is szoroznunk kell – ami természetesen nem változtat a szorzat értékén. Így tetszőleges véges test nem nulla elemeinek a szorzata $-1$-et ad. ■

**3.1-31. Véges testben mi az elemek számának paritása?**

**Megoldás.** Lásd az előző példa magyarázatát.

Ha $1 = -1$, akkor az elemszám páros, mert a párosításból csak az 1 és a 0 marad ki.

Ha pedig $1 \neq -1$, akkor páratlan az elemszám, hiszen a párosításból az $1$, $-1$ és a 0 marad ki. ■

**Vieta-formulák, gyökök és együtthatók közötti összefüggések**

**Legyen $R$ egységelemes integritási tartomány, és tegyük fel, hogy az**

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 \in R[x]$$

**$n$-edfokú polinom – multiplicitással együtt vett – $n$ gyöke mind $R$-ben van. Legyenek ezek a gyökök $c_1,\ c_2,\ \ldots,\ c_n$. Ekkor**

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1 x + a_0 = \\ &= a_n(x-c_1)(x-c_2)\cdots(x-c_n) = \\ &= a_n\left(x^n - (c_1+c_2+\ldots+c_n)x^{n-1} + \right. \\ &\quad +(c_1\cdot c_2 + c_1\cdot c_3 + \ldots + c_{n-1}\cdot c_n)x^{n-2} + \\ &\quad \vdots \\ &\quad \left. +(-1)^n(c_1\cdot c_2\cdots c_n)\right) \end{aligned}$$

**amiből**

$$\begin{aligned} \frac{a_{n-1}}{a_n} &= -(c_1+c_2+\ldots+c_n) \\ \frac{a_{n-2}}{a_n} &= (c_1\cdot c_2 + c_1\cdot c_3 + \ldots + c_{n-1}\cdot c_n) \\ &\vdots \\ \frac{a_0}{a_n} &= (-1)^n(c_1\cdot c_2\cdots c_n) \end{aligned}$$

**3.1-32. Legyen $L$ véges test, $|L| = q^k$. Számítsuk ki a következő összeget:**

$$\sum_{l\in L} l.$$

**Megoldás.** A $g(x) = x^{q^k} - x$ polinom gyökei éppen az $L$ test elemei.

A Vieta-formulákat alkalmazzuk:

$$\frac{a_{n-1}}{a_n} = -(c_1+c_2+\ldots+c_n)$$

Ha $n = q^k \geq 3$, akkor $a_{n-1} = 0$, a fenti érték is nulla, tehát a test elemeinek összege nulla.

Ha $n = q^k = 2$, akkor a test elemeinek összege 1, hiszen ennek a testnek egyik eleme a 0, másik eleme az 1. ∎

**3.1-33. Legyen $L$ véges test, $|L| = q^k$. Jelölje $L^*$ az $L$ multiplikatív csoportját. Számítsuk ki a következő szorzatot:**

$$\prod_{l \in L^*} l.$$

**(Lásd a 30. példát is.)**

**Megoldás.** A $k(x) = x^{q^k-1} - 1$ polinom gyökei az $L$ test nem nulla elemei.

A Vieta-formulákat alkalmazzuk:

$$\frac{a_0}{a_n} = (-1)^n (c_1 \cdot c_2 \cdots c_n)$$

ahol $a_0 = -1,\ a_n = 1$.

Ha $n = q^k - 1$ páros ($q^k$ páratlan), akkor a nem nulla elemek szorzata $-1$.

Ha $n = q^k - 1$ páratlan ($q^k$ páros), akkor a nem nulla elemek szorzata 1. Ekkor azonban a test karakterisztikája 2, így $1 + 1 = 0$, vagyis $1 = -1$. Tehát mondhatjuk ilyenkor is, hogy a nem nulla elemek szorzata $-1$. ■

## 3.2. Hibajavító kódok

A feladatok általában bináris kódokra vonatkoznak, vagyis olyanokra, amelyek esetén az $S$ alaphalmaz a $\{0, 1\}$ halmaz. Néhány feladat általánosabban van megfogalmazva, ezekben az $S$ alaphalmaz tetszőleges nem üres halmaz.

### 3.2.1. Alapfogalmak

Az alábbiakban blokk-kódokkal foglalkozunk. A blokk-kódokat az jellemzi, hogy a kódszavak mind ugyanolyan hosszúak.

Legyen $S \neq \emptyset$ véges halmaz, $u, v \in S^n$. $u$ és $v$ *Hamming-távolsága* $u$ és $v$ különböző komponenseinek a száma. Jelölése $d(u, v)$.

Legyen $K \subseteq S^n$ az előbbiek mellett még legalább kételemű. $K$ (*minimális*) *távolsága* az egymáshoz legközelebbi két különböző kódszónak a távolsága. Jelölése $d(K)$ vagy $d$.

Legyen $S$ Abel csoport és $\underline{0} = \{0, ..., 0\}$, ahol 0 az S egységeleme. $u \in S^n$ *Hamming-súlya* az $u$ nem nulla komponenseinek a száma. Jelölése $w(u)$. Ha $K$-nak van eleme a $\underline{0}$-n kívül, akkor $K$ (*minimális*) *súlya* a nem nulla elemei közül a minimális súlyúnak a súlya. Jelölése $w(K)$, vagy $w$.

Legyen $K$ blokk-kód. $K$ *csoportkód,* ha $S$ Abel-csoport és $K$ részcsoport $S^n$-ben, amennyiben $S^n$-ben a művelet a komponensenként végzett $S$-beli művelet.

Legyen $u \in S^n$, $k$ természetes szám. Az $u$ középpontú $k$ sugarú gömbben $S^n$-nek azok az elemei szerepelnek, amelyek $u$-tól legfeljebb $k$ távolságra vannak.

Egy kód *$t$-hiba jelző,* ha bármelyik üzenetben előforduló legfeljebb $t$ számú hibát képes jelezni, *pontosan $t$-hiba jelző,* ha $t$-hiba jelző, de van olyan $t+1$ hiba, amelyet nem jelez.

Egy kód *$t$-hiba javító,* ha bármelyik üzenetben előforduló legfeljebb $t$ számú hibát képes javítani, *pontosan $t$-hiba javító,* ha $t$-hiba javító, de van olyan $t+1$ hiba, amelyet hibásan javít.

Legyen K blokk-kód és $d(K) = d$. A kód akkor és csak akkor $t$-hiba jelző, ha $t < d$, pontosan $t$-hiba jelző, ha $t = d - 1$.

Hiba javítása során alkalmazhatjuk azt a stratégiát, hogy a hibás vektor helyett azt a kódszót választjuk, amelyik hozzá a legközelebb van. Ha több ilyen kódszó van, akkor közülük az egyiket választjuk. Ekkor minimális távolságú dekódolásról beszélünk.

Minimális távolságú dekódolás esetén a $d$ távolságú kód $t$-hiba javító, ha $t \leq \frac{d-1}{2}$, pontosan $t$-hiba javító, ha $t = \lfloor \frac{d-1}{2} \rfloor$.

### 3.2.2. Blokk-kódok

#### 3.2-1.

**Tegyük fel, hogy az üzenetek bináris jelsorozatok, vagyis az $S = \{0, 1\}$ halmaz elemeiből épülnek fel. Rendeljünk hozzá a kettő hosszú üzenetekhez öt hosszú kódokat a következő szabály szerint.**

$$(0\ 0) \to (0\ 0\ 0\ 0\ 0)$$

$$(0\ 1) \to (0\ 1\ 1\ 1\ 0)$$

$$(1\ 0) \to (1\ 0\ 1\ 0\ 1)$$

$$(1\ 1) \to (1\ 1\ 0\ 1\ 1)$$

**Így négy elemből álló blokk-kódot kapunk. Ha a csatornán például a** $(0\ 1\ 0\ 0\ 0)$ **jelsorozat érkezik, tudjuk, hogy hiba történt, hiszen ez a szó nem szerepel a kódszavak között.**

**Mekkora az** $u = (0\ 1\ 1\ 1\ 0)$ **és** $v = (1\ 0\ 1\ 0\ 1)$ **kódszavak távolsága, a kód távolsága, a** $z = (1\ 1\ 0\ 1\ 1)$ **vektor súlya, valamint a kód súlya?**

**Megoldás.** Az $u = (0\ 1\ 1\ 1\ 0)$ és $v = (1\ 0\ 1\ 0\ 1)$ kódszavak távolsága $d(u, v) = 4$, magának a kódnak a távolsága 3, a $z = (1\ 1\ 0\ 1\ 1)$ vektor súlya $w(z) = 4$, a kód súlya 3. ■

**3.2-2. Az 1. példa** $S$ **halmaza legyen** $\mathbb{F}_2$**, a kételemű test.** $\mathbb{F}_2$ **az összeadásra csoportot alkot. Az** $\mathbb{F}_2$ **elemeiből készített** $n$ **hosszú vektorok is csoportot alkotnak az elemenkénti összeadásra nézve. Lássuk be, hogy a példa** $K$ **kódhalmaza részcsoport** $S^n$**-ben, így** $K$ ***csoportkód.***

**Megoldás.** Mivel a megadott halmaz nem üres, ezért ehhez csak arról kell meggyőződnünk, hogy bármely két kódszó különbsége is kódszó. Mivel $\mathbb{F}_2$-ben $1 = -1$, ehelyett elegendő azt megvizsgálnunk, hogy bármely két kódszó összege is kódszó. ■

**3.2-3. Legyen** $K$ **az 1. példabeli kód,** $u = (0\ 0\ 0\ 0\ 0)$, $t = 1$. **Adjuk meg az** $u$ **körüli 1 sugarú gömbben szereplő sorozatokat.**

**Megoldás.** Az $u$ körüli 1 sugarú gömbben a következő sorozatok találhatók:

$$(0\ 0\ 0\ 0\ 0), (\ 1\ 0\ 0\ 0\ 0), (\ 0\ 1\ 0\ 0\ 0), (\ 0\ 0\ 1\ 0\ 0), (\ 0\ 0\ 0\ 1\ 0), (\ 0\ 0\ 0\ 0\ 1).$$

Figyeljük meg, hogy nincs a gömb elemei között a $(0\ 0\ 0\ 0\ 0)$-t leszámítva kódszó, ami összhangban van azzal, hogy a kód távolsága nagyobb 1-nél (nevezetesen 3). ■

**3.2-4. Az 1. példa kódját alkalmazva tegyük fel, hogy a** $(0\ \ 1\ \ 0\ \ 0\ \ 0)$ **hibás jelsorozat érkezik. Minimális távolságú dekódolás esetén melyik szót választjuk helyette?**

**Megoldás.** Minimális távolságú dekódolás esetén a hibásan beérkező szó helyett a hozzá legközelebbi kódszót, a (0 0 0 0 0) szót választjuk. ■

**3.2-5. Legyen $S = \mathbb{F}_2$, a közleményszavak pedig $k$ hosszú sorozatok. Állapítsuk meg, hogy az alábbi kódok esetén mi jellemzi a kódszavakat, mennyi a kód minimális távolsága, hibajelző és (minimális távolságú dekódolással) a hibajavító képessége.**

**a. Kétszeri ismétlés kódja. A kódszót megkapjuk, ha a közleményszót kétszer egymásután leírjuk. Az $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ közleményszóból az**

$$(\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_1, \alpha_2, \ldots, \alpha_k)$$

**kódszó keletkezik.**

**b. Háromszori ismétlés kódja. A kódszót megkapjuk, ha a közleményszót háromszor egymásután leírjuk. Az $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ közleményszóból az**

$$(\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_1, \alpha_2, \ldots, \alpha_k)$$

**kódszó keletkezik.**

**c. Paritásvizsgálat kódja. A kódszót megkapjuk, ha a közleményszó végére az elemek ($\mathbb{F}_2$-ben számított) összegét írjuk. Az $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ közleményszóból az**

$$(\alpha_1, \alpha_2, \ldots, \alpha_k, \beta), \quad \beta = \sum_{i=1}^{k} \alpha_i$$

**kódszó keletkezik.**

**Megoldás.**

**a. Kétszeri ismétlés kódja.** A kódszavak $n = 2k$ hosszúak. Az $n$ hosszú bináris szavak közül azok a kódszavak, amelyekre az $i$-edik és $k+i$-edik elem megegyezik minden $1 \leq i \leq k$ esetén.

Állapítsuk meg a kód távolságát. Minden közleményszóhoz más és más kódszó tartozik, így a távolság legalább 1. Másrészt tekintsünk két olyan közleményszót, amelyek egymástól csak 1 távolságra vannak. A hozzájuk tartozó kódszavak távolsága 2. Az egymástól legalább 2 távolságra lévő közleményszavakhoz tartozó kódszavak egymástól való távolsága pedig nagyobb 2-nél. Így a kód távolsága $d = 2$.

A kód 1-hiba jelző, és hiba javítására nem alkalmas. Ugyanis ha egy helyen romlik el a kószó, akkor valamilyen $i$-re az $i$-edik és $k+i$-edik elem különbözik, tehát érzékeljük a hibát, de javítani nem tudjuk. Van azonban olyan 2-hiba, amelyet nem is tudunk érzékelni. Az olyan 2-hibáról van szó, amelyik úgy keletkezik, hogy valamilyen $i$-re az $i$-edik és $k+i$-edik elem egyszerre hibásodik meg.

**b. Háromszori ismétlés kódja.** A kódszavak $n = 3k$ hosszúak. Az $n$ hosszú bináris szavak közül azok a kódszavak, amelyekre az $i$-edik, $k+i$-edik valamint a $2k+i$-edik elem megegyezik minden $1 \leq i \leq k$ esetén.

Állapítsuk meg a kód távolságát. Minden közleményszóhoz más és más kódszó tartozik, így a távolság legalább 1. Másrészt tekintsünk két olyan közleményszót, amelyek egymástól csak 1 távolságra vannak. A hozzájuk tartozó kódszavak távolsága 3. Az egymástól legalább 2 távolságra lévő közleményszavakhoz tartozó kódszavak egymástól való távolsága pedig nagyobb 2-nél. Így a kód távolsága $d = 3$.

A kód 2-hiba jelző, és 1-hiba javító. Ugyanis ha egy helyen romlik el a kószó, akkor valamilyen $i$-re az $i$-edik, $k+i$-edik és $2k+i$-edik elem közül kettő azonos, a harmadik más (amelyik elromlott). Amelyik más, mint a többi kettő, azt javítjuk a másik kettő értékére. Ha pedig két helyen romlik el a kószó, akkor előfordulhat, hogy valamilyen $i$-re az $i$-edik, $k+i$-edik és $2k+i$-edik elem közül romlott el kettő. Ekkor érzékeljük a hibát, de nem tudjuk javítani. Ha pedig három helyen hibásodott meg a kódszó, lehet, hogy valamilyen $i$-re az $i$-edik, $k+i$-edik és $2k+i$-edik elem romlott el, ilyenkor nem is érzékeljük a hibát.

**c. Paritásvizsgálat kódja.** A kódszavak $n = k+1$ hosszúak. Az $n$ hosszú bináris szavak közül azok a kódszavak, amelyek páros sok 1-est tartalmaznak. A kód távolsága $d = 2$, 1-hiba jelző, hiba javítására nem alkalmas.

**Megjegyzés.** Figyeljük meg, hogy az a. és c. kód hibajelző és hibajavító képessége megegyezik, ugyanakkor az a. kód hossza $k$ értékével sokkal gyorsabban nő, mint a c. kód hossza. ■

### 3.2-6. Hamming-korlát.

**Bizonyítsuk be a következőt. Legyen az alaphalmaz $S$, a $K \subseteq S^n$ kód $t$-hiba javító. Ekkor**

$$|K| \cdot \sum_{i=0}^{t} \binom{n}{i} (s-1)^i \leq s^n,$$

**ahol $s = |S|$.**

**Megoldás.** $S^n$-ben egy adott kódszótól $i$ távolságra azok a szavak vannak, amelyek pontosan $i$ helyen különböznek tőle. Az $i$ különböző helyet $\binom{n}{i}$-féleképpen választhatjuk ki, mindegyik helyre $(s-1)$ jel kerülhet, és az $i$ helyre összesen $(s-1)^i$ féleképpen rakhatunk jeleket.

Az adott kódszó körüli $t$ sugarú gömbben így $\sum_{i=0}^{t} \binom{n}{i}(s-1)^i$ $S^n$-beli szó található, beleértve magát a kódszót is. Összesen $|K|$ kódszavunk van. A kód $t$-hiba javító, ezért a $|K|$ különböző kódszó körüli $t$-sugarú gömbök diszjunktak kell, hogy legyenek. Összesen tehát nem tartalmazhatnak több elemet, mint az $S^n$ halmaz, vagyis $s^n$-et. ■

**3.2-7. Bináris blokk-kódot készítünk 3 hosszú üzenetekhez. Legalább mekkora legyen a kódszavak hossza, ha azt akarjuk, hogy a kód (minimális távolságú dekódolással) pontosan 1-hiba javító legyen?**

**Megoldás.** Írjuk fel a Hamming-korlátot bináris esetre alkalmazva. Mivel 1-hiba javító a kód, ezért

$$2^k \left( \binom{n}{0} + \binom{n}{1} \right) \leq 2^n$$

$$\binom{n}{0} + \binom{n}{1} \leq 2^{n-k}$$

$$n + 1 \leq 2^{n-k}$$

$$n + 1 \leq 2^{n-3}$$

$n = 6$ esetén teljesül először az egyenlőtlenség:

$$6 + 1 = 7 \leq 8 = 2^3 = 2^{6-3}.$$

Ha $n$ értéke nagyobb, akkor a Hamming-korlát még inkább érvényben lesz, tehát a válasz az, hogy legalább 6 kell, hogy legyen a kódszavak hossza. ■

**3.2-8. $k$ hosszú bináris szavakból (üzenet) 19 hosszú bináris szavakat (kódszót) készítünk. Legfeljebb mekkora lehet az üzenetek hossza, ha azt akarjuk, hogy a kód minimális távolsága 8 legyen?**

**Megoldás.** Mivel $d = 8$, a kód $t = \lfloor \frac{d-1}{2} \rfloor = 3$-hiba javító. A Hamming korlát a következőképpen alakul:

$$\left( \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{t} \right) \leq 2^{n-k}$$

$$\left( \binom{19}{0} + \binom{19}{1} + \binom{19}{2} + \binom{19}{3} \right) \leq 2^{19-k}$$

$$1 + 19 + \frac{19 \cdot 18}{2} + \frac{19 \cdot 18 \cdot 17}{2 \cdot 3} \leq 2^{19-k}$$

$$1160 \leq 2^{19-k}.$$

Mivel $2^{10} = 1024$ és $2^{11} = 2048$, a következőt kapjuk:

$$11 \leq 19 - k$$

$$k \leq 8$$

■

**3.2-9. Állapítsuk meg, hogy van-e 5 minimális távolságú, 13 hosszú perfekt bináris kód?**

**A $K$ blokk-kód *tökéletes* (*perfekt*), ha a Hamming-korlát egyenlőséggel teljesül. Perfekt kód esetén a kódszavak körüli $\lfloor \frac{d-1}{2} \rfloor$ sugarú gömbök teljesen kitöltik az $n$ hosszú sorozatok terét, s így minden szóhoz pontosan egy kódszó van, amelytől legfeljebb $\lfloor \frac{d-1}{2} \rfloor$ távolságra van.**

**Megoldás.** A kódszavak hossza $n = 13$. Mivel $d = 5$ és $\lfloor \frac{d-1}{2} \rfloor = 2$, a kód $t = 2$-hiba javító (minimális távolságú dekódolással). Ha a közleményszavak

$k$ hosszúak, akkor a közleményszavak száma $2^k$, ami megegyezik a kódszavak számával, s így $|K| = 2^k$. Ha a kód perfekt, akkor a Hamming-korlát egyenlőséggel teljesül, tehát fennáll a következő

$$2^k \cdot \left( \binom{13}{0} + \binom{13}{1} + \binom{13}{2} \right) = 2^{13}$$

Ebből

$$2^k \cdot \left( 1 + 13 + \frac{13 \cdot 12}{2} \right) = 2^{13}$$

amiből $2^k \cdot 92 = 2^{13}$. A jobb oldalon 2 hatványa áll, a bal oldalon szereplő 92 azonban nem 2 hatványa, ez az egyenlőség nem teljesülhet semmilyen $k$ esetén. Ilyen kód tehát nem létezik. ■

**3.2-10. Létezik-e 3 minimális távolságú perfekt bináris kód $n = 147$ esetén?**

**Megoldás.** Nincs. A kód $d = 3$ miatt $t = 1$-hiba javító. Ekkor a Hamming-korlát alapján a következőnek kellene teljesülni:

$$\binom{147}{0} + \binom{147}{1} = 2^{n-k}$$

$$1 + 147 = 2^{147-k}$$

$$148 = 2^{147-k}.$$

A bal oldalon lévő 148 nem 2 hatványa, a jobb oldalon pedig 2 hatványa áll, és ez ellentmondás. ■

**3.2-11. Van-e 12 hosszú kódszavakból álló 1-hiba javító perfekt bináris kód?**

**Megoldás.** Nincs. Ugyanis a Hamming-korlát alapján a következőnek kellene teljesülni:

$$\binom{n}{0} + \binom{n}{1} = 2^{n-k}$$

$$n + 1 = 2^{n-k}$$
$$13 = 2^{12-k}$$

A bal oldalon lévő 13 nem 2 hatványa, a jobb oldalon pedig 2 hatványa áll, ez ellentmondás. ■

### 3.2.3. Lineáris kód alapfogalmai

Legyen $S = \mathbb{F}_q$, és $S^n$ az $\mathbb{F}_q$ test feletti vektortér. $K$ *lineáris kód,* ha $K$ az $S^n$-nek $k$-dimenziós altere. Jelölése $[n, k]$.

Lineáris kód esetén a kód súlya és a kód távolsága megegyezik.

Legyen $K$ $[n, k]$ kód. A kód *generátormátrixa* az altér egy bázisának elemeiből mint sorvektorokból álló $G$ mátrix. A kód *(paritás)ellenőrző mátrixa* a $K$ altérre merőleges altér egy bázisának elemeiből mint sorvektorokból álló $H$ mátrix.

Nyilvánvalóan $G$ $(k \times n)$-es, $k$ rangú, míg $H$ $((n-k) \times n)$-es, $n-k$ rangú $\mathbb{F}_q$ fölötti mátrix, továbbá $H \cdot G^T = 0$.

$\underline{v} \in \mathbb{F}_q^n$ akkor és csak akkor kódszó, ha $H \cdot \underline{v} = \underline{0}$.

A definícióból látszik, hogy egy kódnak általában több generátormátrixa és több paritásellenőrző mátrixa is lehet.

**Kódolás lineáris kóddal**

Tekintsünk egy $[n, k]$ kódot. A kódszavak az $n$ dimenziós tér $k$ dimenziós alterének szavai, és az altér bármely bázisa alkalmas generátormátrix képzésére. Ha azonban közleményszavakhoz kívánunk kódszavakat rendelni, egy rögzített $G$ generátormátrixszal dolgozunk. A közleményszavak $k$ hosszú vektorok, az $\mathbb{F}_q^k$ elemei, és az alábbi szabállyal rendelünk egy közleményszóhoz kódszót. Legyen $\underline{u} \in \mathbb{F}_q^k$ egy lehetséges közleményszó és $\underline{u}^T \cdot G = \underline{v}^T$. Ekkor a $\underline{v} \in \mathbb{F}_q^n$ vektor lesz az $\underline{u}$ kódja.

### 3.2.4. Lineáris kód

**3.2-12. Valamely kód generátormátrixa legyen a következő:**

$$G = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

**Ezt a mátrixot használva kódolásra, adjuk meg az összes közleményszót, valamint a megfelelő kódszavakat.**

**Megoldás.** Alkalmazzuk a következő szabályt. Ha $\underline{u} \in \mathbb{F}_q^k$ egy lehetséges közleményszó, és $\underline{u}^T \cdot G = \underline{v}^T$, akkor a $\underline{v} \in \mathbb{F}_q^n$ vektor lesz az $\underline{u}$ kódja.

| közleményszavak | $\mapsto$ | kódszavak |
|---|---|---|
| (0 0 0) | $\mapsto$ | (0 0 0 0 0 0 0) |
| (0 0 1) | $\mapsto$ | (0 1 1 1 0 1 1) |
| (0 1 0) | $\mapsto$ | (1 1 0 0 1 1 0) |
| (0 1 1) | $\mapsto$ | (1 0 1 1 1 0 1) |
| (1 0 0) | $\mapsto$ | (0 1 0 1 0 1 0) |
| (1 0 1) | $\mapsto$ | (0 0 1 0 0 0 1) |
| (1 1 0) | $\mapsto$ | (1 0 0 1 1 0 0) |
| (1 1 1) | $\mapsto$ | (1 1 1 0 1 1 1) |

■

**3.2-13. Állapítsuk meg, hogy az 5. példa kódjai közül melyik lineáris, és a lineárisoknak adjuk meg a generátormátrixát.**

**Megoldás.** Mindhárom kód esetén bármely két kódszó összege is kódszó, így lineáris kódokról van szó.

**a.** A kétszeres ismétlés kód esetén olyan $G$ $k \times 2k$ méretű mátrixot keresünk, amelyikre

$$(\alpha_1, \alpha_2, \ldots, \alpha_k) \cdot G = (\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_1, \alpha_2, \ldots, \alpha_k)$$

teljesül. A megfelelő $G$ generátormátrix

$$G = (I_k \;\; I_k).$$

**b.** A háromszoros ismétlés kód generátormátrixa $G = (I_k \;\; I_k \;\; I_k)$.

**c.** A paritásellenőrző kód generátormátrixa $G = (I_k \;\; I)$, ahol $I$ csupa 1-esből álló oszlopvektor. ■

**3.2-14. Az alábbi bináris kódok esetében állapítsuk meg a minimális távolságot, a hibajelző, illetve (minimális távolságú dekódolással) a hibajavító képességet, valamint azt, hogy melyik lineáris, a lineárisoknak pedig adjuk meg a generátormátrixát.**

**a. Legyen $k = 3$, $n = 4$, és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat:**

$$\alpha_1, \alpha_2, \alpha_3 \to \alpha_1, \alpha_2, \alpha_3, \alpha_1 + \alpha_2 + \alpha_3 + 1$$

**b. Legyen $k = 3$, $n = 5$, és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat:**

$$\alpha_1, \alpha_2, \alpha_3 \to \alpha_1, \alpha_2, \alpha_3, \alpha_1, \alpha_2 + \alpha_3$$

**c. Legyen $k = 3$, $n = 5$, és az üzenetekhez az alábbi szabállyal rendeljük hozzá a kódszavakat:**

$$\alpha_1, \alpha_2, \alpha_3 \to \alpha_1, \alpha_2, \alpha_3, \alpha_1, \mathbf{max}(\alpha_2, \alpha_3)$$

**Megoldás.**

**a.** A kód távolsága $d = 2$. Ugyanis minden közleményszóhoz más és más kódszó tartozik, így a távolság legalább 1. Másrészt tekintsünk két olyan közleményszót, amelyek egymástól csak 1 távolságra vannak. A hozzájuk tartozó kódszavak távolsága 2. Az egymástól legalább 2 távolságra lévő közleményszavakhoz tartozó kódszavak egymástól való távolsága pedig legalább 2.

Ezért a kód $d - 1 = 1$ hibajelző és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibajavító.

A kód nem lineáris, mert például a $\underline{0}$ vektor nem kódszó.

**b.** A kód távolsága $d = 2$. Ugyanis minden közleményszóhoz más és más kódszó tartozik, így a távolság legalább 1. Másrészt tekintsünk két olyan közleményszót, amelyek egymástól csak 1 távolságra vannak. A hozzájuk tartozó kódszavak távolsága 2. Az egymástól legalább 2 távolságra lévő közleményszavakhoz tartozó kódszavak egymástól való távolsága pedig legalább 2.

Ezért a kód $d - 1 = 1$ hibajelző és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibajavító.

A kód lineáris, generátormátrixa

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

**c.** A kód távolsága $d = 1$. Ugyanis minden közleményszóhoz más és más kódszó tartozik, így a távolság legalább 1. Ugyanakkor van egymástól 1 távolságra lévő két kódszó. Például (1 0 1 1 1) és (1 1 1 1 1).

A kód $d-1=0$ hibajelző és $\lfloor \frac{d-1}{2} \rfloor = 0$ hibajavító.

A kód nem lineáris, mert van két olyan kódszó, amelyek összege nem kódszó, s így az összeadás (valamint a kivonás is) kivezet a kódszavak halmazából. Ez a helyzet például a következő esetben. $\underline{u}_1^T = (1 \;\; 1 \;\; 0 \;\; 1 \;\; 1)$ és $\underline{u}_2^T = (1 \;\; 0 \;\; 1 \;\; 1 \;\; 1)$ kódszavak, de az összegük $\underline{u}_1^T + \underline{u}_2^T = (0 \;\; 1 \;\; 1 \;\; 0 \;\; 0)$ nem kódszó. ■

**3.2-15. Lássuk be, hogy ha az $\mathbb{F}_k$ fölötti $[n,k]$ kód generátormátrixa $G = (I_k \;\; P)$ alakú, akkor a $H = (-P^T \;\; I_{n-k})$ mátrix a kód ellenőrző mátrixa. ($I_k$ a $k \times k$ méretű egységmátrixot jelöli, $P$ pedig tetszőleges $k \times (n-k)$ méretű, $\mathbb{F}_k$ fölötti mátrix.) A kételemű test fölött $-P$ helyett $P$ is írható, mert $\mathbb{F}_2$-ben $1 = -1$.**

**Megjegyzés. Hasonlóan igaz az is, hogy ha egy $[n,k]$ kód ellenőrző mátrixa $H = (I_{n-k} \;\; R)$ alakú, ahol $R$ tetszőleges $((n-k) \times k)$ méretű, $\mathbb{F}_k$ fölötti mátrix, akkor a $G = (-R^T \;\; I_k)$ mátrix megfelel generátormátrixnak.**

**Megoldás.** $H$ nyilván $n-k$ rangú. Elég belátnunk azt, hogy $H \cdot G^T = 0$. Blokkonkénti szorzással a következőt kapjuk:

$$\left(-P^T \;\; I_{n-k}\right) \cdot \begin{pmatrix} I_k \\ P^T \end{pmatrix} = -P^T + P^T = 0$$

■

**3.2-16. Adjuk meg a 14. példában szereplő lineáris kód ellenőrző mátrixát a**

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

**generátormátrix felhasználásával.**

**Megoldás.** Alkalmazzuk az előző példát, ami alapján

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

■

**3.2-17. Lássuk be, hogy egy $[n, k, d]$ kód $H$ ellenőrző mátrixában van $d$ lineárisan összefüggő oszlop, de bármely $d$-nél kevesebb oszlop lineárisan független.**

**Megoldás.**

1. Belátjuk, hogy egy $[n, k, d]$ kód $H$ ellenőrző mátrixában van $d$ lineárisan összefüggő oszlop. A következő módon lehet ilyet találni. Mivel $d$ a kód minimális távolsága és ez az érték megegyezik a kód súlyával, van a kódban olyan $\underline{u}$ vektor, amelyikre $w(\underline{u}) = d$. Ebben a vektorban tehát $d$ helyen nem nulla érték áll, a többi helyen pedig nulla. Tudjuk, hogy $H \cdot \underline{u} = \underline{0}$.

Ez az egyenlet felfogható úgy is, hogy $H$ oszlopainak vesszük a lineáris kombinációit, és $\underline{u}$ elemei az együtthatók. Olyan lineáris kombinációról van szó, amelyben pontosan $d$ számú együttható különbözik nullától. A megfelelő $d$ oszlop $H$-ban lineárisan összefüggő.

2. Most belátjuk, hogy $H$-ban bármely $d$-nél kevesebb oszlop lineárisan független. Legyen $0 < d_1 < d$, és tegyük fel, hogy $H$-ban van $d_1$ összefüggő oszlop. Ekkor van $H$ oszlopainak olyan lineáris kombinációja, amelyben ez a $d_1$ oszlop nem mind nullával szorzódik, a többi együttható azonban mind nulla, s az eredmény a nullvektor. Ezekből az együtthatókból készítsünk egy $\underline{u}_1$ vektort. Egyrészt $H \cdot \underline{u}_1 = \underline{0}$, ami azt jelenti, hogy $\underline{u}_1$ kódvektor. Másrészt $w(\underline{u}_1) = d_1$, így a kód súlya és ezzel együtt a távolsága kisebb lenne $d$-nél, ami ellentmond a kiindulási feltételnek. Így valóban minden $d$-nél kevesebb oszlop lineárisan független $H$-ban. ■

**3.2-18. Adjuk meg a 14. és 16. példában szereplő lineáris kód**

$$H = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

**ellenőrző mátrixának segítségével a kód távolságát és hibajelző, valamint (minimális távolságú dekódolással) a hibajavító képességét.**

**Megoldás.** Az ellenőrző mátrixban van két összefüggő oszlop (a 2. és a 3.), ugyanakkor bármely oszlop önmagában lineárisan független (nem szerepel köztük a nullvektor), így $d = 2$, 1-hibajelző és 0-hiba javító a kód. Más meggondolással a 14.b példában ugyanezt kaptuk. ■

**3.2-19. Legyen egy bináris lineáris kód generátormátrixa:**

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

**Adjuk meg az (egyik) ellenőrző mátrixát. Az ellenőrző mátrix felhasználásával mondjuk meg a kódtávolságot.**

**Megoldás.** Az ellenőrző mátrix:

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Van két összefüggő oszlop $H$-ban (a 3-dik és a 7-dik), de nincs egyetlen önmagában összefüggő oszlop, ugyanis egyik oszlopban sincs csupa nulla. Így a kódtávolság 2. ■

**3.2-20. Egy bináris kód generátormátrixa**

$$G = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

**Adjuk meg a kód paritásellenőrző mátrixát és távolságát.**

**Megoldás.**

A generátormátrixnak nem szerepel az elején az egységmátrix, de az oszlopok 4-3-2 permutációját elvégezve (a negyedik oszlopot rakjuk a harmadikba,

a harmadikat a másodikba, a második pedig a negyedik oszlopba kerül), az így keletkező $G_1$ mátrix már ilyen alakú:

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{pmatrix}.$$

Ehhez a $G_1$ mátrixhoz tartozó $H_1$ mátrixot a 15. példa alkalmazásával megkaphatjuk.

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Ezen a $H_1$ mátrixon hajtsuk végre az előző permutáció inverzét, tehát a 2-3-4 permutációt, a kapott $H$ mátrix a $G$ mátrixnak megfelelő paritásellenőrző mátrix:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

A kód távolsága $d = 3$, mert $H$-ban van három összefüggő oszlop (a második, negyedik és hatodik), de semelyik két oszlop nem összefüggő. ■

### 3.2-21. Egy bináris kód generátormátrixa

$$G = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

**Adjuk meg a kód paritásellenőrző mátrixát és távolságát.**

**Megoldás.** A generátormátrixban nem fordulnak elő az egységmátrix oszlopai, ezért oszlopcserével sem tudjuk a kívánt alakra hozni. Emlékeztetünk azonban arra, hogy a generátormátrix sorai a kódszavakból álló altér bázisának vektorai. Ha valamilyen bázistranszformációt hajtunk végre ezeken a vektorokon, akkor ugyanannak az altérnek másik bázisát kapjuk, az az ellenőrző mátrix, amelyik megfelel az utóbbi bázisból képzett generátormátrixnak,

megfelel az eredeti generátormátrixnak is. Adjuk hozzá a $G$ mátrix első sorát a másodikhoz, s igy a $G_1$ mátrixhoz jutunk:

$$G_1 = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \end{pmatrix}$$

Ebben már ott vannak az egységmátrix oszlopai, s megfelelő oszloppermutációval a mátrix elejére hozhatjuk. Alkalmazzuk $G_1$ oszlopaira a 4-1-3-2 permutációt, így a $G_2$ mátrixhoz jutunk:

$$G_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}$$

A $G_2$-höz tartozó $H_2$ ellenőrző mátrixot a 15. példa alkalmazásával kaphatjuk:

$$H_2 = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Ezen a $H_2$ mátrixon hajtsuk végre az előző permutáció inverzét, tehát a 2-3-1-4 permutációt, a kapott $H_1$ mátrix a $G_1$ mátrixnak megfelelő paritásellenőrző mátrix, de korábban kifejtett gondolatmenet alapján ez a $G$ mátrixnak megfelelő $H$ paritásellenőrző mátrix is.

$$H_1 = H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

A kód távolsága $d = 2$, mert $H$-ban van két összefüggő oszlop (a harmadik és a hetedik), de mindegyik oszlop önmagában független. ■

### 3.2-22. Egy bináris kód generátormátrixa

$$G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

**Mennyi a kód számossága? Adjuk meg a kód paritásellenőrző mátrixát, és ennek segítségével határozzuk meg a távolságát.**

**Megoldás.** Ez egy [5,3] bináris kód, az üzenetek hossza 3, s így a kód számossága $|K| = 2^3 = 8$. $G$-ből bázistranszformációval olyan mátrixot képezünk, amelyiknek az elején ott van az egységmátrix.

Először a második sort a harmadikhoz adjuk, és így kapjuk az alábbi $G1$ mátrixot:

$$G1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Most $G1$ első sorát adjuk a másodikhoz, és így kapjuk az alábbi $G2$ mátrixot:

$$G2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Határozzuk meg a $G2$-höz tartozó ellenőrző mátrixot a 15. példa eredményét felhasználva.

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Mivel $G$ sorai és $G2$ sorai ugyanannak az altérnek két különböző bázisa, így a kapott $H$ mátrix a $G$ generátormátrixhoz tartozó ellenőrző mátrix.

A kód távolsága $d = 2$, mert $H$-nak van két összefüggő oszlopa (a 2-dik és a 4-dik), de egy összefüggő oszlopa nincs (nincs az oszlopok között a nullvektor). ■

### 3.2-23. Egy bináris kód paritásellenőrző mátrixa

$$H = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

**Lássuk be, hogy 1-hiba javító perfekt lineáris kódról van szó.**

**Megoldás.** $H$ a 15 dimenziós tér 4 dimenziós alterének bázisa, mert a sorok lineárisan függetlenek (ugyanis benne vannak az egységmátrix oszlopai). Ennek az altérnek ortogonális altere 11-dimenziós és egyértelműen meghatározott, tehát a kód lineáris.

$d$=3, mert a 3-dik, 7-dik és a 12-dik oszlopok összefüggnek, és nincs két összefüggő oszlop (nincs két azonos oszlop). Ebből $t = 1$-hiba javító a kód.

Vizsgáljuk meg a Hamming-korlátot. $r = 4, n = 15, k = 11$, és

$$2^{11}\left(\binom{15}{0} + \binom{15}{1}\right) = 2^{11}(1+15) = 2^{11}2^4 = 2^{15} = 2^n$$

A Hamming korlát egyenlőséggel teljesül, s így a kód perfekt.

**Megjegyzés:** Ez egy Hamming-kód. Lásd a következő fejezetet. ■

### 3.2.5. Hamming-kód

**Az 1-hiba javító perfekt lineáris kódot *Hamming-kódnak* nevezzük.**

**3.2-24. Hamming-kód készítése.**

**Bináris Hamming-kódot készíthetünk a következőképpen. Legyen**

$r$ **pozitív egész szám (ellenőrző jegyek száma),**

$n = 2^r - 1$ **a kódszavak hossza,**

$k = 2^r - 1 - r$ **a közleményszavak hossza.**

**A** $H$ $r \times n$**-es ellenőrző mátrix** $j$**-edik oszlopában a** $j$ **2-es számrendszerbeli alakjának jegyei szerepelnek.**

**Legyen például** $r = 3, n = 7, k = 4$. **Adjuk meg a kód ellenőrző mátrixát.**

**Megoldás.**

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Ez egy $[7, 4]$ kód ellenőrző mátrixa. ■

**3.2-25. Adjuk meg az előző példában megismert szabály szerinti Hamming-kód ellenőrző mátrixát, ha $r = 2$, és ha $r = 4$.**

**Megoldás.**

$r = 2$ esetén:

$$H = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$r = 3$ esetén:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

■

**3.2-26. A Hamming-kód generátormátrixa.**

**Adjuk meg a 24. példabeli $[7, 4]$ Hamming-kód $H$ ellenőrző mátrixának ismeretében a kód (egyik) generátormátrixát. Ha ezt a generátormátrixot alkalmazzuk a kódolásnál, mi lesz a $(0 \quad 1 \quad 1 \quad 1)$ üzenet kódja?**

**Megoldás.** A

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

mátrixból az oszlopok $(3, 4)$ transzpozíciójával kapható a

$$H_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

mátrix, amely $(I_{n-k} \;\; P)$ alakú. A $H_1$-nek megfelelő $G_1$ mátrix, amely $(P^T \;\; I_k)$ alakú, a 15. példa alkalmazásával kapható:

$$G_1 = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Ebből a transzpozíciót újra alkalmazva megkapjuk a keresett

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

mátrixot. A $(0 \;\; 1 \;\; 1 \;\; 1)$ üzenet kódját megkapjuk, ha ezt a vektort jobbról szorozzuk $G$-vel. Az eredmény: $(0 \;\; 0 \;\; 0 \;\; 1 \;\; 1 \;\; 1 \;\; 1)$. ■

### 3.2-27. Hibajavítás bináris Hamming-kóddal.

**Megoldás.** A $[7, 4]$ Hamming-kód esetén láttuk az előző példában, hogy $b^T = (0 \;\; 0 \;\; 0 \;\; 1 \;\; 1 \;\; 1 \;\; 1)$ kódszó. Ha ellenőrizzük, azt tapasztaljuk, hogy valóban $H \cdot \underline{b} = (0 \;\; 0 \;\; 0) = \underline{0}$. Tegyük fel, hogy az átvitel során egy hiba történt, mégpedig a harmadik helyen. Ekkor $e^T = (0 \;\; 0 \;\; 1 \;\; 0 \;\; 0 \;\; 0 \;\; 0)$ a hibavektor, és a $(b+e)^T = (0 \;\; 0 \;\; 1 \;\; 1 \;\; 1 \;\; 1 \;\; 1)$ vektor érkezik meg a csatornán. $H \cdot (b+e) = (0 \;\; 1 \;\; 1)^T$, ez a $H$ mátrix 3. oszlopa, alulról olvasva éppen a 3 bináris alakja, rámutat arra, hogy a 3. pozícióban van a hiba. Ha pedig $e^T = (0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 1)$ a hibavektor, ellenőrzéskor azt kapjuk, hogy $H \cdot (b + e) = (1 \;\; 1 \;\; 1)^T$, ez a 7 bináris értéke, ami azt mutatja, hogy a 7. jegy hibás. Ezzel a módszerrel mindig megkapjuk a hiba helyét, feltéve, hogy legfeljebb 1 hiba történt. Egynél több hiba esetén nem kapunk helyes eredményt, a kód időnként nem ismeri fel a hibát, vagy rosszul javítja. Ha olyan hibaminta lép fel, mely maga is

kódszó, akkor $H \cdot (b + e) = \underline{0}$, olyan mintha nem történt volna hiba. Ha a hibaminta két 1-est tartalmaz (kettős hiba), akkor a kód egyhibának tekinti.

■

**3.2-28.** $[7, 4]$ **bináris Hamming-kódnál, feltételezve, hogy egynél több hiba nem lépett fel az átvitelnél, mi volt a továbbított kódvektor, ha**

**a.** $a^T = (0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0)$, **illetve**

**b.** $b^T = (0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 0)$ **érkezett.**

**Megoldás.**

**a.** $H \cdot a = (0 \quad 1 \quad 1)^T$, így a 6. hely hibás, $(0 \quad 1 \quad 1 \quad 1 \quad 1 \quad 0 \quad 0)^T$ volt a küldött szó.

**b.** $H \cdot b = (0 \quad 0 \quad 0)^T$. A kapott szó hibátlan. ■

# 4. Ajánlott irodalom


Bagyinszkiné Orosz Anna – Csörgő Piroska – Gyapjas Ferenc:
*Példatár a bevezető fejezetek a matematikába c. tárgyhoz*
Tankönyvkiadó, Budapest, 1983.

Bálintné Szendrei Mária – Czédli Gábor – Szendrei Ágnes:
*Absztrakt algebrai feladatok*
Tankönyvkiadó, Budapest, 1988.

G. Birkhoff - T. C. Bartee: *A modern algebra a számítógéptudományban*
Műszaki Könyvkiadó, Budapest, 1974.

Demetrovics, Denev, Pavlov: *A számítástudomány matematikai alapjai*
Tankönyvkiadó, Budapest, 1985.

Freud Róbert: *Lineáris algebra*
ELTE Eötvös Kiadó, Budapest, 1996.

Gavrilov, Szapozsenko: *Diszkrét matematikai feladatgyűjtemény*
Műszaki Könyvkiadó 1981.

Gonda János: *Bevezető fejezetek a matematikába III.*
ELTE TTK, Budapest, 1998

Gonda János: *Gyakorlatok és feladatok a Bevezetés a matematikába c. tárgyhoz – Polinomok, véges testek, kongruenciák, kódolás*
ELTE TTK, Budapest, 2001

Györfi László – Győri Sándor – Vajda István: *Információ- és kódelmélet*
Typotex Kiadó, 2000, 2002

Járai Antal: *Bevezetés a matematikába*
ELTE Eötvös Kiadó, 2005.

Surányi László: *Algebra. Testek, gyűrűk, polinomok.*
Typotex, Budapest, 1997.