Véges testek

Egy véges test

Az $m = x^3 + x + 1 \in \mathbb{Z}_2[x]$ polinom irreducibilis (mert nincs gyöke, és csak harmadfokú), ezért a $K := \mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ maradékosztály-gyűrű test. Ennek a testnek

Egy véges test

Az $m = x^3 + x + 1 \in \mathbb{Z}_2[x]$ polinom irreducibilis (mert nincs gyöke, és csak harmadfokú), ezért a $K := \mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ maradékosztály-gyűrű test. Ennek a testnek 8 eleme van:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1}.$$

Egy véges test

Az $m = x^3 + x + 1 \in \mathbb{Z}_2[x]$ polinom irreducibilis (mert nincs gyöke, és csak harmadfokú), ezért a $K := \mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ maradékosztály-gyűrű test. Ennek a testnek 8 eleme van:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1}.$$

Vezessük be az $\alpha = \overline{x}$ jelölést, és hagyjuk el a vonásokat a konstansokról. Ezzel a jelöléssel a K test 8 eleme:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

Egy véges test

Az $m = x^3 + x + 1 \in \mathbb{Z}_2[x]$ polinom irreducibilis (mert nincs gyöke, és csak harmadfokú), ezért a $K := \mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ maradékosztály-gyűrű test. Ennek a testnek 8 eleme van:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1}.$$

Vezessük be az $\alpha = \overline{x}$ jelölést, és hagyjuk el a vonásokat a konstansokról. Ezzel a jelöléssel a K test 8 eleme:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

Figyeljük meg, hogy $\{0,1\}$ egy $\mathbb{Z}_2$-vel izomorf résztestet alkot K-ban, tehát kis jóindulattal mondhatjuk, hogy $\mathbb{Z}_2 \subseteq K$, vagyis K kibővítése $\mathbb{Z}_2$-nek.

Egy véges test

Az $m = x^3 + x + 1 \in \mathbb{Z}_2[x]$ polinom irreducibilis (mert nincs gyöke, és csak harmadfokú), ezért a $K := \mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ maradékosztály-gyűrű test. Ennek a testnek 8 eleme van:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1}.$$

Vezessük be az $\alpha = \overline{x}$ jelölést, és hagyjuk el a vonásokat a konstansokról. Ezzel a jelöléssel a K test 8 eleme:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

Figyeljük meg, hogy $\{0,1\}$ egy $\mathbb{Z}_2$-vel izomorf résztestet alkot K-ban, tehát kis jóindulattal mondhatjuk, hogy $\mathbb{Z}_2 \subseteq K$, vagyis K kibővítése $\mathbb{Z}_2$-nek.

Számítsuk ki $m(\alpha)$ értékét:

$$m(\alpha) = \alpha^3 + \alpha + 1 = \overline{x}^3 + \overline{x} + \overline{1} = \overline{x^3 + x + 1} = \overline{m} = \overline{0}.$$

Egy véges test

Az $m = x^3 + x + 1 \in \mathbb{Z}_2[x]$ polinom irreducibilis (mert nincs gyöke, és csak harmadfokú), ezért a $K := \mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ maradékosztály-gyűrű test. Ennek a testnek 8 eleme van:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1}.$$

Vezessük be az $\alpha = \overline{x}$ jelölést, és hagyjuk el a vonásokat a konstansokról. Ezzel a jelöléssel a K test 8 eleme:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

Figyeljük meg, hogy $\{0,1\}$ egy $\mathbb{Z}_2$-vel izomorf résztestet alkot K-ban, tehát kis jóindulattal mondhatjuk, hogy $\mathbb{Z}_2 \subseteq K$, vagyis K kibővítése $\mathbb{Z}_2$-nek.

Számítsuk ki $m(\alpha)$ értékét:

$$m(\alpha) = \alpha^3 + \alpha + 1 = \overline{x}^3 + \overline{x} + \overline{1} = \overline{x^3 + x + 1} = \overline{m} = \overline{0}.$$

Ez azt jelenti, hogy a K testben már van gyöke az m polinomnak!

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x}$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1}$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1}$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x}$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x}$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x}$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1}$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / \left(x^3+x+1\right)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo x^3+x+1 kell számolni.

$$\overline{x+1}+\overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1}\cdot\overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába...

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / \left(x^3 + x + 1\right)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

$$(\alpha+1) + (\alpha^2+\alpha)$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

$$(\alpha+1) + (\alpha^2+\alpha) = \alpha^2 + 2\alpha + 1$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

$$(\alpha+1) + (\alpha^2+\alpha) = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

$$(\alpha+1) + (\alpha^2+\alpha) = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1 \qquad \text{(s.v.)}$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

$$(\alpha+1) + (\alpha^2+\alpha) = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1 \qquad \text{(s.v.)}$$

$$(\alpha+1) \cdot (\alpha^2+\alpha)$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

$$(\alpha+1) + (\alpha^2+\alpha) = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1 \qquad \text{(s.v.)}$$

$$(\alpha+1) \cdot (\alpha^2+\alpha) = \alpha^3 + 2\alpha^2 + \alpha$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

$$(\alpha+1) + (\alpha^2+\alpha) = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1 \qquad \text{(s.v.)}$$

$$(\alpha+1) \cdot (\alpha^2+\alpha) = \alpha^3 + 2\alpha^2 + \alpha = \alpha^3 + \alpha$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

$$(\alpha+1) + (\alpha^2+\alpha) = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1 \qquad \text{(s.v.)}$$

$$(\alpha+1) \cdot (\alpha^2+\alpha) = \alpha^3 + 2\alpha^2 + \alpha = \alpha^3 + \alpha = (\alpha+1) + \alpha$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

$$(\alpha+1) + (\alpha^2+\alpha) = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1 \qquad \text{(s.v.)}$$

$$(\alpha+1) \cdot (\alpha^2+\alpha) = \alpha^3 + 2\alpha^2 + \alpha = \alpha^3 + \alpha = (\alpha+1) + \alpha = 1$$

Egy véges test

Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! A test elemei:

$$\overline{0},\ \overline{1},\ \overline{x},\ \overline{x+1},\ \overline{x^2},\ \overline{x^2+1},\ \overline{x^2+x},\ \overline{x^2+x+1},$$

és modulo $x^3 + x + 1$ kell számolni.

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \qquad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0,\ 1,\ \alpha,\ \alpha+1,\ \alpha^2,\ \alpha^2+1,\ \alpha^2+\alpha,\ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

$$(\alpha+1) + (\alpha^2+\alpha) = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1 \qquad \text{(s.v.)}$$

$$(\alpha+1) \cdot (\alpha^2+\alpha) = \alpha^3 + 2\alpha^2 + \alpha = \alpha^3 + \alpha = (\alpha+1) + \alpha = 1 \qquad \text{(sz.sz.)}$$

A nyolcelemű test művelettáblázatai

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

Polinomgyűrű faktorteste

3.39. Tétel.

Legyen T test, $m \in T[x]$ irreducibilis polinom, és jelölje n az m polinom fokszámát. Ekkor a $K = T[x]/(m)$ faktorgyűrű olyan test, amelyben az m polinomnak van gyöke. A K test minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \quad (a_{n-1}, \ldots, a_0 \in T)$$

alakban. Ha $T = \mathbb{Z}_p$, akkor $|K| = p^n$.

Polinomgyűrű faktorteste

3.39. Tétel.

Legyen T test, $m \in T[x]$ irreducibilis polinom, és jelölje n az m polinom fokszámát. Ekkor a $K = T[x]/(m)$ faktorgyűrű olyan test, amelyben az m polinomnak van gyöke. A K test minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \quad (a_{n-1}, \ldots, a_0 \in T)$$

alakban. Ha $T = \mathbb{Z}_p$, akkor $|K| = p^n$.

Bizonyítás.

A maradékos osztás tétele (3.5. Tétel) szerint

$$\forall f \in T[x] \ \exists! r \in T[x] : \ f \equiv r \pmod{m} \text{ és } \deg r \leq n-1.$$

Polinomgyűrű faktorteste

3.39. Tétel.

Legyen T test, $m \in T[x]$ irreducibilis polinom, és jelölje n az m polinom fokszámát. Ekkor a $K = T[x]/(m)$ faktorgyűrű olyan test, amelyben az m polinomnak van gyöke. A K test minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \quad (a_{n-1}, \ldots, a_0 \in T)$$

alakban. Ha $T = \mathbb{Z}_p$, akkor $|K| = p^n$.

Bizonyítás.

A maradékos osztás tétele (3.5. Tétel) szerint

$$\forall f \in T[x] \ \exists! r \in T[x] : \ f \equiv r \pmod{m} \text{ és } \deg r \leq n-1.$$

Ezért $T[x]/(m)$ minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \quad (a_{n-1}, \ldots, a_0 \in T)$$

alakban.

Polinomgyűrű faktorteste

3.39. Tétel.

Legyen T test, $m \in T[x]$ irreducibilis polinom, és jelölje n az m polinom fokszámát. Ekkor a $K = T[x]/(m)$ faktorgyűrű olyan test, amelyben az m polinomnak van gyöke. A K test minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \quad (a_{n-1}, \ldots, a_0 \in T)$$

alakban. Ha $T = \mathbb{Z}_p$, akkor $|K| = p^n$.

Bizonyítás.

A maradékos osztás tétele (3.5. Tétel) szerint

$$\forall f \in T[x] \ \exists! r \in T[x] : \ f \equiv r \pmod{m} \text{ és } \deg r \leq n-1.$$

Ezért $T[x]/(m)$ minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \quad (a_{n-1}, \ldots, a_0 \in T)$$

alakban.
Ha $T = \mathbb{Z}_p$, akkor p választási lehetőségünk van minden a_i-re ezért összesen p^n-féleképp tudjuk az $a_{n-1}, \ldots, a_1, a_0$ (n db) együtthatókat megválasztani.

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a + b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a + b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a + b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\overline{f} \;=\; \overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0}$$

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\begin{aligned} \overline{f} &= \overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{a_0} + \overline{a_1}\,\overline{x} + \cdots + \overline{a_{n-1}}\,\overline{x}^{n-1} \end{aligned}$$

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\begin{aligned} \overline{f} &= \overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{a_0} + \overline{a_1}\,\overline{x} + \cdots + \overline{a_{n-1}}\,\overline{x}^{n-1} \\ &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \end{aligned}$$

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\begin{aligned} \overline{f} &= \overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{a_0} + \overline{a_1}\,\overline{x} + \cdots + \overline{a_{n-1}}\,\overline{x}^{n-1} \\ &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = f(\alpha) \quad (a_0, a_1, \ldots, a_{n-1} \in T). \end{aligned}$$

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\begin{aligned} \overline{f} &= \overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{a_0} + \overline{a_1}\,\overline{x} + \cdots + \overline{a_{n-1}}\,\overline{x}^{n-1} \\ &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = f(\alpha) \quad (a_0, a_1, \ldots, a_{n-1} \in T). \end{aligned}$$

Hasonló számolás mutatja, hogy

$$m(\alpha)$$

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\begin{aligned} \overline{f} &= \overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{a_0} + \overline{a_1}\,\overline{x} + \cdots + \overline{a_{n-1}}\,\overline{x}^{n-1} \\ &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = f(\alpha) \quad (a_0, a_1, \ldots, a_{n-1} \in T). \end{aligned}$$

Hasonló számolás mutatja, hogy

$$m(\alpha) = m(\overline{x})$$

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\begin{aligned} \overline{f} &= \overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{a_0} + \overline{a_1}\,\overline{x} + \cdots + \overline{a_{n-1}}\,\overline{x}^{n-1} \\ &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = f(\alpha) \quad (a_0, a_1, \ldots, a_{n-1} \in T). \end{aligned}$$

Hasonló számolás mutatja, hogy

$$m(\alpha) = m(\overline{x}) = \overline{m(x)}$$

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\begin{aligned} \overline{f} &= \overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{a_0} + \overline{a_1}\,\overline{x} + \cdots + \overline{a_{n-1}}\,\overline{x}^{n-1} \\ &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = f(\alpha) \quad (a_0, a_1, \ldots, a_{n-1} \in T). \end{aligned}$$

Hasonló számolás mutatja, hogy

$$m(\alpha) = m(\overline{x}) = \overline{m(x)} = \overline{0},$$

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\begin{aligned} \overline{f} &= \overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{a_0} + \overline{a_1}\,\overline{x} + \cdots + \overline{a_{n-1}}\,\overline{x}^{n-1} \\ &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = f(\alpha) \quad (a_0, a_1, \ldots, a_{n-1} \in T). \end{aligned}$$

Hasonló számolás mutatja, hogy

$$m(\alpha) = m(\overline{x}) = \overline{m(x)} = \overline{0},$$

hiszen $m \equiv 0 \pmod{m}$.

Polinomgyűrű faktorteste

Bizonyítás (folyt.)

Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a} \colon a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **k**ibővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\begin{aligned} \overline{f} &= \overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \\ &= \overline{a_0} + \overline{a_1}\,\overline{x} + \cdots + \overline{a_{n-1}}\,\overline{x}^{n-1} \\ &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} = f(\alpha) \quad (a_0, a_1, \ldots, a_{n-1} \in T). \end{aligned}$$

Hasonló számolás mutatja, hogy

$$m(\alpha) = m(\overline{x}) = \overline{m(x)} = \overline{0},$$

hiszen $m \equiv 0 \pmod{m}$. Tehát $\alpha \in K$ valóban gyöke m-nek. □

ÖRÖMHÍR!

Minden polinomnak van gyöke!

ÖRÖMHÍR!

Minden polinomnak van gyöke! Ha nem az eredeti testben, akkor annak egy alkalmas kibővítésében.

ÖRÖMHÍR!

Minden polinomnak van gyöke! Ha nem az eredeti testben, akkor annak egy alkalmas kibővítésében.

Ha az $m = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in T[x]$ irreducibilis főpolinomnak akarunk „gyököt csinálni”, akkor a $K = T[x] / (m)$ testet kell elkészítenünk.

ÖRÖMHÍR!

Minden polinomnak van gyöke! Ha nem az eredeti testben, akkor annak egy alkalmas kibővítésében.

Ha az $m = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in T[x]$ irreducibilis főpolinomnak akarunk „gyököt csinálni”, akkor a $K = T[x] / (m)$ testet kell elkészítenünk.

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, a_1, \ldots, a_{n-1} \in T).$$

ÖRÖMHÍR!

Minden polinomnak van gyöke! Ha nem az eredeti testben, akkor annak egy alkalmas kibővítésében.

Ha az $m = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in T[x]$ irreducibilis főpolinomnak akarunk „gyököt csinálni”, akkor a $K = T[x] / (m)$ testet kell elkészítenünk.

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, a_1, \ldots, a_{n-1} \in T).$$

Az α szimbólumról csak annyit kell tudni, hogy $m(\alpha) = 0$, azaz $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$.

ÖRÖMHÍR!

Minden polinomnak van gyöke! Ha nem az eredeti testben, akkor annak egy alkalmas kibővítésében.

Ha az $m = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in T[x]$ irreducibilis főpolinomnak akarunk „gyököt csinálni”, akkor a $K = T[x] / (m)$ testet kell elkészítenünk.

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, a_1, \ldots, a_{n-1} \in T).$$

Az α szimbólumról csak annyit kell tudni, hogy $m(\alpha) = 0$, azaz $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$. Tehát a számolási szabály:

$$\alpha^n = -b_{n-1}\alpha^{n-1} - \cdots - b_1\alpha - b_0.$$

ÖRÖMHÍR!

Minden polinomnak van gyöke! Ha nem az eredeti testben, akkor annak egy alkalmas kibővítésében.

Ha az $m = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in T[x]$ irreducibilis főpolinomnak akarunk „gyököt csinálni”, akkor a $K = T[x] / (m)$ testet kell elkészítenünk.

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, a_1, \ldots, a_{n-1} \in T).$$

Az α szimbólumról csak annyit kell tudni, hogy $m(\alpha) = 0$, azaz $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$. Tehát a számolási szabály:

$$\alpha^n = -b_{n-1}\alpha^{n-1} - \cdots - b_1\alpha - b_0.$$

(És ha m nem irreducibilis?)

Egyszerű algebrai bővítés

3.40. Következmény.

Tetszőleges T test és $m \in T[x]$ irreducibilis polinom esetén létezik olyan K test, amelyre

1. K *bővítése* T-nek, azaz $K \supseteq T$;
2. létezik olyan $\alpha \in K$ elem, amely gyöke m-nek;
3. K minden eleme egyértelműen előáll $a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$ $(a_{n-1}, \ldots, a_0 \in T)$ alakban, ahol $n = \deg m$.

Bizonyítás.

Legyen $K = T[x]/(m)$, és alkalmazzuk az előző tételt. □

3.41. Definíció.

Azt mondjuk, hogy a K test T-ből az α elem *adjungálásával* keletkezik (jelölés: $K = T(\alpha)$), és az ilyen módon előálló testeket T *egyszerű algebrai bővítéseinek* nevezzük.

A komplex számtest újratöltve

3.42. Megjegyzés.

Ha a K testet a $T = \mathbb{R}$ és $m = x^2 + 1$ esetre felírjuk, éppen a komplex számok testét kapjuk.

A komplex számtest újratöltve

3.42. Megjegyzés.

Ha a K testet a $T = \mathbb{R}$ és $m = x^2 + 1$ esetre felírjuk, éppen a komplex számok testét kapjuk.

Most $n = 2$, tehát

$$K = \{\overline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{R}\}\,.$$

A komplex számtest újratöltve

3.42. Megjegyzés.

Ha a K testet a $T = \mathbb{R}$ és $m = x^2 + 1$ esetre felírjuk, éppen a komplex számok testét kapjuk.

Most $n = 2$, tehát

$$K = \{\overline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{R}\}.$$

Menjünk le alfába...

A komplex számtest újratöltve

3.42. Megjegyzés.

Ha a K testet a $T = \mathbb{R}$ és $m = x^2 + 1$ esetre felírjuk, éppen a komplex számok testét kapjuk.

Most $n = 2$, tehát

$$K = \{\overline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{R}\}\,.$$

Menjünk le alfába...

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha \quad (a_0, a_1 \in \mathbb{R})\,.$$

A komplex számtest újratöltve

3.42. Megjegyzés.

Ha a K testet a $T = \mathbb{R}$ és $m = x^2 + 1$ esetre felírjuk, éppen a komplex számok testét kapjuk.

Most $n = 2$, tehát

$$K = \{\overline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{R}\}.$$

Menjünk le alfába...

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha \quad (a_0, a_1 \in \mathbb{R}).$$

Az α szimbólumra vonatkozó számolási szabály: $m(\alpha) = \alpha^2 + 1 = 0$, vagyis

$$\alpha^2 = -1.$$

A komplex számtest újratöltve

3.42. Megjegyzés.

Ha a K testet a $T = \mathbb{R}$ és $m = x^2 + 1$ esetre felírjuk, éppen a komplex számok testét kapjuk.

Most $n = 2$, tehát

$$K = \{\overline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{R}\}.$$

Menjünk le alfába...

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha \quad (a_0, a_1 \in \mathbb{R}).$$

Az α szimbólumra vonatkozó számolási szabály: $m(\alpha) = \alpha^2 + 1 = 0$, vagyis

$$\alpha^2 = -1.$$

Ezzel éppen a

A komplex számtest újratöltve

3.42. Megjegyzés.

Ha a K testet a $T = \mathbb{R}$ és $m = x^2 + 1$ esetre felírjuk, éppen a komplex számok testét kapjuk.

Most $n = 2$, tehát

$$K = \{\overline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{R}\}.$$

Menjünk le alfába...

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha \quad (a_0, a_1 \in \mathbb{R}).$$

Az α szimbólumra vonatkozó számolási szabály: $m(\alpha) = \alpha^2 + 1 = 0$, vagyis

$$\alpha^2 = -1.$$

Ezzel éppen a komplex számok testét kaptuk (csak α helyett i a szokásos jelölés).

A komplex számtest újratöltve

3.42. Megjegyzés.

Ha a K testet a $T = \mathbb{R}$ és $m = x^2 + 1$ esetre felírjuk, éppen a komplex számok testét kapjuk.

Most $n = 2$, tehát

$$K = \left\{ \overline{a_0 + a_1 x} \mid a_0, a_1 \in \mathbb{R} \right\}.$$

Menjünk le alfába...

A K test elemeinek kanonikus alakja:

$$a_0 + a_1 \alpha \quad (a_0, a_1 \in \mathbb{R}).$$

Az α szimbólumra vonatkozó számolási szabály: $m(\alpha) = \alpha^2 + 1 = 0$, vagyis

$$\alpha^2 = -1.$$

Ezzel éppen a komplex számok testét kaptuk (csak α helyett i a szokásos jelölés).

Tehát $\mathbb{C} \cong \mathbb{R}[x] / \left(x^2 + 1\right)$, és ezt tekinthetnénk akár a komplex számok definíciójának is.

Egy végtelen faktortest

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

Egy végtelen faktortest

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

Egy végtelen faktortest

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

$$\overline{2 - x}^{-1} = \overline{u} \iff$$

Egy végtelen faktortest

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

$$\overline{2 - x}^{-1} = \overline{u} \iff \overline{2 - x} \cdot \overline{u} = \overline{1}$$

$$\iff$$

Egy végtelen faktortest

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

$$\overline{2 - x}^{-1} = \overline{u} \iff \overline{2 - x} \cdot \overline{u} = \overline{1}$$

$$\iff (2 - x)\, u \equiv 1 \pmod{x^3 - 7}$$

$$\iff$$

Egy végtelen faktortest

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

$$\begin{aligned}
\overline{2 - x}^{-1} = \overline{u} &\iff \overline{2 - x} \cdot \overline{u} = \overline{1} \\
&\iff (2 - x)\, u \equiv 1 \pmod{x^3 - 7} \\
&\iff \exists v \in \mathbb{Q}[x] : (2 - x)\, u = 1 + \left(x^3 - 7\right) v \\
&\iff
\end{aligned}$$

Egy végtelen faktortest

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

$$
\begin{aligned}
\overline{2 - x}^{-1} = \overline{u} &\iff \overline{2 - x} \cdot \overline{u} = \overline{1} \\
&\iff (2 - x)\, u \equiv 1 \pmod{x^3 - 7} \\
&\iff \exists v \in \mathbb{Q}[x] : (2 - x)\, u = 1 + \left(x^3 - 7\right) v \\
&\iff u \equiv x^2 + 2x + 4 \pmod{x^3 - 7} \\
&\iff
\end{aligned}
$$

Egy végtelen faktortest

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

$$
\begin{aligned}
\overline{2 - x}^{-1} = \overline{u} &\iff \overline{2 - x} \cdot \overline{u} = \overline{1} \\
&\iff (2 - x)\, u \equiv 1 \pmod{x^3 - 7} \\
&\iff \exists v \in \mathbb{Q}[x] : (2 - x)\, u = 1 + \left(x^3 - 7\right) v \\
&\iff u \equiv x^2 + 2x + 4 \pmod{x^3 - 7} \\
&\iff \overline{u} = \overline{x^2 + 2x + 4}
\end{aligned}
$$

Egy végtelen faktortest

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

$$\begin{aligned}
\overline{2 - x}^{-1} = \overline{u} &\iff \overline{2 - x} \cdot \overline{u} = \overline{1} \\
&\iff (2 - x)\, u \equiv 1 \pmod{x^3 - 7} \\
&\iff \exists v \in \mathbb{Q}[x] : (2 - x)\, u = 1 + \left(x^3 - 7\right) v \\
&\iff u \equiv x^2 + 2x + 4 \pmod{x^3 - 7} \\
&\iff \overline{u} = \overline{x^2 + 2x + 4}
\end{aligned}$$

Tehát $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$.

Gyöktelenítés

Menjünk le alfába:

$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Gyöktelenítés

Menjünk le alfába:

$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki:

Gyöktelenítés

Menjünk le alfába:

$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki: $\alpha = \sqrt[3]{7}$!
(Vagy

Gyöktelenítés

Menjünk le alfába:

$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki: $\alpha = \sqrt[3]{7}$!
(Vagy $\alpha = \sqrt[3]{7}\,\mathrm{cis}\,\frac{\pm 2\pi}{3}$.)

Gyöktelenítés

Menjünk le alfába:

$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki: $\alpha = \sqrt[3]{7}$! (Vagy $\alpha = \sqrt[3]{7}\,\mathrm{cis}\,\frac{\pm 2\pi}{3}$.) Tehát K tekinthető számtestnek is:

$$K = \left\{ a\sqrt[3]{49} + b\sqrt[3]{7} + c \colon a, b, c \in \mathbb{Q} \right\}.$$

Gyöktelenítés

Menjünk le alfába:

$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki: $\alpha = \sqrt[3]{7}$! (Vagy $\alpha = \sqrt[3]{7}\,\mathrm{cis}\,\frac{\pm 2\pi}{3}$.) Tehát K tekinthető számtestnek is:

$$K = \left\{ a\sqrt[3]{49} + b\sqrt[3]{7} + c \colon a, b, c \in \mathbb{Q} \right\}.$$

Az előbb kiszámoltuk, hogy $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$, ami azt jelenti, hogy $(2 - \alpha)^{-1} = \alpha^2 + 2\alpha + 4$,

Gyöktelenítés

Menjünk le alfába:

$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki: $\alpha = \sqrt[3]{7}$! (Vagy $\alpha = \sqrt[3]{7}\,\mathrm{cis}\,\frac{\pm 2\pi}{3}$.) Tehát K tekinthető számtestnek is:

$$K = \left\{ a\sqrt[3]{49} + b\sqrt[3]{7} + c \colon a, b, c \in \mathbb{Q} \right\}.$$

Az előbb kiszámoltuk, hogy $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$, ami azt jelenti, hogy $(2 - \alpha)^{-1} = \alpha^2 + 2\alpha + 4$, azaz

$$\frac{1}{2 - \sqrt[3]{7}} = \sqrt[3]{49} + 2\sqrt[3]{7} + 4.$$

Gyöktelenítés

Menjünk le alfába:

$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki: $\alpha = \sqrt[3]{7}$! (Vagy $\alpha = \sqrt[3]{7}\,\mathrm{cis}\,\frac{\pm 2\pi}{3}$.) Tehát K tekinthető számtestnek is:

$$K = \left\{ a\sqrt[3]{49} + b\sqrt[3]{7} + c \colon a, b, c \in \mathbb{Q} \right\}.$$

Az előbb kiszámoltuk, hogy $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$, ami azt jelenti, hogy $(2 - \alpha)^{-1} = \alpha^2 + 2\alpha + 4$, azaz

$$\frac{1}{2 - \sqrt[3]{7}} = \sqrt[3]{49} + 2\sqrt[3]{7} + 4.$$

Ezzel a módszerrel (lényegében az euklideszi algoritmussal) lehet bonyolult nevezőket gyöktelenníteni.

3.43. Tétel.

Akkor és csak akkor létezik q-elemű test, ha q prímhatvány.

Véges testek

3.43. Tétel.

Akkor és csak akkor létezik q-elemű test, ha q prímhatvány.

Bizonyítás helyett.

Bármely p prímszám és n pozitív egész szám esetén létezik n-edfokú irreducibilis polinom $\mathbb{Z}_p$ felett (messze nem triviális!).

Véges testek

3.43. Tétel.

Akkor és csak akkor létezik q-elemű test, ha q prímhatvány.

Bizonyítás helyett.

Bármely p prímszám és n pozitív egész szám esetén létezik n-edfokú irreducibilis polinom $\mathbb{Z}_p$ felett (messze nem triviális!).

Ha $f \in \mathbb{Z}_p[x]$ egy ilyen polinom, akkor $T[x] / (f)$ egy p^n-elemű test.

Véges testek

3.43. Tétel.

Akkor és csak akkor létezik q-elemű test, ha q prímhatvány.

Bizonyítás helyett.

Bármely p prímszám és n pozitív egész szám esetén létezik n-edfokú irreducibilis polinom $\mathbb{Z}_p$ felett (messze nem triviális!).

Ha $f \in \mathbb{Z}_p[x]$ egy ilyen polinom, akkor $T[x] / (f)$ egy p^n-elemű test.

Ha K egy q-elemű test, akkor tartalmaz prím elemszámú résztestet (közel sem triviális!).

Véges testek

3.43. Tétel.

Akkor és csak akkor létezik q-elemű test, ha q prímhatvány.

Bizonyítás helyett.

Bármely p prímszám és n pozitív egész szám esetén létezik n-edfokú irreducibilis polinom $\mathbb{Z}_p$ felett (messze nem triviális!).

Ha $f \in \mathbb{Z}_p[x]$ egy ilyen polinom, akkor $T[x] / (f)$ egy p^n-elemű test.

Ha K egy q-elemű test, akkor tartalmaz prím elemszámú résztestet (közel sem triviális!).

Ha T egy p-elemű részteste K-nak, akkor K vektorteret alkot T felett.

Véges testek

3.43. Tétel.

Akkor és csak akkor létezik q-elemű test, ha q prímhatvány.

Bizonyítás helyett.

Bármely p prímszám és n pozitív egész szám esetén létezik n-edfokú irreducibilis polinom $\mathbb{Z}_p$ felett (messze nem triviális!).

Ha $f \in \mathbb{Z}_p[x]$ egy ilyen polinom, akkor $T[x] / (f)$ egy p^n-elemű test.

Ha K egy q-elemű test, akkor tartalmaz prím elemszámú résztestet (közel sem triviális!).

Ha T egy p-elemű részteste K-nak, akkor K vektorteret alkot T felett.

Ha ez a vektortér n-dimenziós, akkor $K \cong T^n$, ezért $|K| = p^n$. □

Véges testek

3.43. Tétel.

Akkor és csak akkor létezik q-elemű test, ha q prímhatvány.

Bizonyítás helyett.

Bármely p prímszám és n pozitív egész szám esetén létezik n-edfokú irreducibilis polinom $\mathbb{Z}_p$ felett (messze nem triviális!).

Ha $f \in \mathbb{Z}_p[x]$ egy ilyen polinom, akkor $T[x] / (f)$ egy p^n-elemű test.

Ha K egy q-elemű test, akkor tartalmaz prím elemszámú résztestet (közel sem triviális!).

Ha T egy p-elemű részteste K-nak, akkor K vektorteret alkot T felett.

Ha ez a vektortér n-dimenziós, akkor $K \cong T^n$, ezért $|K| = p^n$. □

A q-elemű testet (mely izomorfia erejéig egyértelműen meghatározott), Galois tiszteletére $\mathrm{GF}(q)$ jelöli (Galois Field).

Véges testek

Példa.

- kételemű test:

Véges testek

Példa.

- kételemű test: $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test:

Véges testek

Példa.

- kételemű test: $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test: $\mathrm{GF}(3) \cong \mathbb{Z}_3$
- négyelemű test:

Véges testek

Példa.

- kételemű test: $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test: $\mathrm{GF}(3) \cong \mathbb{Z}_3$
- négyelemű test: $\mathrm{GF}(4) \cong \mathbb{Z}_2[x] / \left(x^2 + x + 1\right)$
- ötelemű test:

Véges testek

Példa.

- kételemű test: $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test: $\mathrm{GF}(3) \cong \mathbb{Z}_3$
- négyelemű test: $\mathrm{GF}(4) \cong \mathbb{Z}_2[x] / \left(x^2 + x + 1\right)$
- ötelemű test: $\mathrm{GF}(5) \cong \mathbb{Z}_5$
- hatelemű test:

Véges testek

Példa.

- kételemű test: $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test: $\mathrm{GF}(3) \cong \mathbb{Z}_3$
- négyelemű test: $\mathrm{GF}(4) \cong \mathbb{Z}_2[x] / \left(x^2 + x + 1\right)$
- ötelemű test: $\mathrm{GF}(5) \cong \mathbb{Z}_5$
- hatelemű test: nincs!
- hételemű test:

Véges testek

Példa.

- kételemű test: $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test: $\mathrm{GF}(3) \cong \mathbb{Z}_3$
- négyelemű test: $\mathrm{GF}(4) \cong \mathbb{Z}_2[x] / \left(x^2 + x + 1\right)$
- ötelemű test: $\mathrm{GF}(5) \cong \mathbb{Z}_5$
- hatelemű test: nincs!
- hételemű test: $\mathrm{GF}(7) \cong \mathbb{Z}_7$
- nyolcelemű test:

Véges testek

Példa.

- kételemű test: $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test: $\mathrm{GF}(3) \cong \mathbb{Z}_3$
- négyelemű test: $\mathrm{GF}(4) \cong \mathbb{Z}_2[x] / (x^2 + x + 1)$
- ötelemű test: $\mathrm{GF}(5) \cong \mathbb{Z}_5$
- hatelemű test: nincs!
- hételemű test: $\mathrm{GF}(7) \cong \mathbb{Z}_7$
- nyolcelemű test: $\mathrm{GF}(8) \cong \mathbb{Z}_2[x] / (x^3 + x + 1) \cong \mathbb{Z}_2[x] / (x^3 + x^2 + 1)$
- kilencelemű test:

Véges testek

Példa.

- kételemű test: $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test: $\mathrm{GF}(3) \cong \mathbb{Z}_3$
- négyelemű test: $\mathrm{GF}(4) \cong \mathbb{Z}_2[x] / (x^2 + x + 1)$
- ötelemű test: $\mathrm{GF}(5) \cong \mathbb{Z}_5$
- hatelemű test: nincs!
- hételemű test: $\mathrm{GF}(7) \cong \mathbb{Z}_7$
- nyolcelemű test: $\mathrm{GF}(8) \cong \mathbb{Z}_2[x] / (x^3 + x + 1) \cong \mathbb{Z}_2[x] / (x^3 + x^2 + 1)$
- kilencelemű test: $\mathrm{GF}(9) \cong \mathbb{Z}_3[x] / (x^2 + 1) = \{a + bi : a, b \in \mathbb{Z}_3\}$
- tízelemű test:

Véges testek

Példa.

- kételemű test: $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test: $\mathrm{GF}(3) \cong \mathbb{Z}_3$
- négyelemű test: $\mathrm{GF}(4) \cong \mathbb{Z}_2[x] / (x^2 + x + 1)$
- ötelemű test: $\mathrm{GF}(5) \cong \mathbb{Z}_5$
- hatelemű test: nincs!
- hételemű test: $\mathrm{GF}(7) \cong \mathbb{Z}_7$
- nyolcelemű test: $\mathrm{GF}(8) \cong \mathbb{Z}_2[x] / (x^3 + x + 1) \cong \mathbb{Z}_2[x] / (x^3 + x^2 + 1)$
- kilencelemű test: $\mathrm{GF}(9) \cong \mathbb{Z}_3[x] / (x^2 + 1) = \{a + bi : a, b \in \mathbb{Z}_3\}$
- tízelemű test: nincs!
- ...