

Név:

Összpontszám:

Algebra és számelmélet

2. zárthelyi megoldása

(2019. 11. 30.)

1. Feladat. (4 pont)

Igazak-e a következő állítások. Válaszait röviden indokolja.

(A) Ha $n > 2$ egész, akkor $\varphi(n)$ páros.

(M) **Igaz.** A függvény gyenge multiplikatívítása miatt, ha $n = \prod p_i^{k_i}$ (p_i prím), akkor a $\varphi(n) = \prod (p_i^{k_i} - p_i^{k_i-1})$ szorzatban csak akkor nincs páros tényező, ha $n = 2$, de ezt kizártuk.

(B) Ha egy $\mathbb{C}$ fölötti polinom irreducibilis, akkor nincs gyöke.

(M) **Hamis.** A komplex számtest fölötti irreducibilis polinomok az elsőfokúak, ezeknek pedig nyilván van gyökük.

(C) Az $x^3 + \bar{1}$ polinom irreducibilis a $\mathbb{Z}_3[x]$ polinmgűrűben.

(M) **Hamis,** ugyanis $x^3 + \bar{1} = (x + \bar{1})^3$ a $\mathbb{Z}_3[x]$ polinmgűrűben.

(D) Az $(x^2 + \bar{1})u \equiv \bar{1} \pmod{m}$ kongruencia nem oldható meg a $\mathbb{Z}_2[x]$ polinmgűrűben, ahol $m = x^3 + x^2 + \bar{1}$

(M) **Hamis,** ugyanis ln. k. o. $(x^2 + \bar{1}, x^3 + x^2 + \bar{1}) = \bar{1}$.

2. Feladat. (4 pont)

Határozza meg az $x^6 - 27$ és az $x^4 + 4$ polinomok irreducibilis fölbontását mind a valós, mind a komplex számtest fölött.

(M) Tudjuk, hogy egyrészt $27 = (\sqrt{3})^3$, másrészt a 6. egységgyökök a ± 1 , és $\pm \frac{1}{2} \pm \frac{\sqrt{3}}{2}i$ komplex számok. A $\sqrt[6]{27}$ 3értékei:

$$\pm\sqrt{3}, \quad \pm\frac{\sqrt{3}}{3} \pm \frac{3i}{2}.$$

Ezek alapján egyrészt az $\mathbb{R}$ fölötti fölbontás:

$$x^6 - 27 = (x - \sqrt{3})(x + \sqrt{3})(x^2 + \sqrt{3}x - 3)(x^2 - \sqrt{3}x - 3),$$

míg a $\mathbb{C}$ fölötti

$$(x - \sqrt{3})(x + \sqrt{3})(x - (\frac{\sqrt{3}}{2} + \frac{3i}{2}))(x - (\frac{\sqrt{3}}{2} - \frac{3i}{2}))(x - (-\frac{\sqrt{3}}{2} + \frac{3i}{2}))(x + (\frac{\sqrt{3}}{2} + \frac{3i}{2}))$$

Egyrészt $x^4 + 4 = (x^2 + 2i)(x^2 - 2i)$, másrészt $2i = (\pm(1 + i))^2$ és $-2i = (\pm(1 - i))^2$. Ezeket használva

$$x^4 + 4 = (x - (1 + i))(x - (1 - i))(x - (-1 + i))(x - (-1 - i)) = (x^2 + 2x + 2)(x^2 - 2x + 2)$$

a komplex, ill. valós számtest fölötti fölbontás.

3. Feladat. (4 pont)

Határozza meg az alábbi elemeket: A $\mathbb{Z}_2[x]/(x^3 + x + 1)$ véges testben az $\bar{x}^{-1}$, és az $\bar{x}^{2^{-1}}$ elemeket.

(M) Az $\bar{x}$ multiplikatív inverze $\overline{x^2 + ax + b}$ alakú, ahol $a, b \in \{0, 1\}$.

$$\bar{1} = \overline{\bar{x}x^2 + ax + b} = \overline{ax^2 + (b+1)x + 1}$$

amiből $a = 0$, $b = 1$, és így $\bar{x}^{-1} = \overline{x^2 + 1}$. Ezt fölhasználva: $\overline{x^2}^{-1} = \overline{x^2 + x + 1}$.

4. Feladat. (4 pont)

Adjon meg a $\mathbb{Z}_7$ test fölött két olyan különböző polinomot, amelyek ugyanazt a polinomfüggvényt adják meg. Indokolja meg választását.

(M) Az Euler-Fermat tétel alapján, például az x és x^7 polinomok ilyenek.

5. Feladat. (4 pont)

Adja meg egy 4 elemű test művelet táblázatát.

(M) A $\mathbb{Z}_2[x]/(x^2 + x + 1)$ test 4 elemű, művelet táblái (a fölülvonásokat az egyszerűség kedvéért elhagytuk):

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x