

Név: Unger Tamás István
FTD1Y3

Összpontszám:

Algebra és számelmélet

Vizsgadolgozat

(2018. 12. 21.)

Tudnivalók. Az első két feladatnál minden választ röviden indokolni kell, a többinél csak válaszolni kell a kérdésekre. A feladatok megoldásához semmiféle segédeszköz (függvénytábla, számológép, mobiltelefon és más hasonló eszköz) nem használható. Ilyen eszközök használata esetén a dolgozat automatikusan (javítás nélkül) 0 pontos, és nincs javítási/pótlási lehetőség.

1. Feladat. (3·4 pont) Igazak-e az alábbi állítások (válaszát röviden indokolja).

(a) Tetszőleges z primitív századik egységgyök esetén $z^{50} = -1$.

Legyen z tetszőleges primitív századik egységgyök. Ekkor:

$$z = \cos \frac{2k\pi}{100} + i \sin \frac{2k\pi}{100}, \text{ ahol } \gcd(k, 100) = 1. \text{ Vizsgáljuk } z^{50} \text{-et.}$$

$$z^{50} = \cos \frac{2 \cdot 50 \cdot 2k\pi}{100} + i \sin \frac{2 \cdot 50 \cdot 2k\pi}{100} = \cos 2k\pi + i \sin 2k\pi. \text{ Vizsgáljuk most a valós és képzetes részeket.}$$
$$\cos 2k\pi = \begin{cases} -1 & \text{ha } k \text{ páratlan} \\ 1 & \text{ha } k \text{ páros} \end{cases}; \sin 2k\pi = 0 \quad \forall k \text{-ra.}$$

Így az állítás igaz. $\square$

$\gcd(k, 100) \neq 1 \Rightarrow k$ nem lehet páros, mert $\gcd(k, 100) = 1$ szükséges k -ra.

(b) Létezik olyan integritástartomány, amelyben pontosan hat egység van.

Az állítás igaz. Így hát adhatunk illene egy példát. $\mathbb{Z}_7$ jó példa.

Mivel 7 prím $\Rightarrow \mathbb{Z}_7$ nem csak integritástartomány, hanem test is.

Egységelem: $\bar{1}$, $\mathbb{Z}_7$ egységei: $\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}$. Ez pontosan 6 darab. $\square$

Ök mind az egységelem
okai (invertálható elemek).

(c) Létezik 2018-adfokú irreducibilis polinom $\mathbb{R}$ fölött

Mutassuk meg, hogy az állítás igaz. Legyen f egy polinom, $\deg f = 2018$.

Tudjuk, hogy f gyökei a komplex síkban így következhet el, hogy ha $z \in \mathbb{C}$ gyöke f -nek $(x-z) \mid f$, akkor z konjugáltja ($\bar{z}$) is gyöke f -nek $(x-\bar{z}) \mid f$. Így tehát a valós komplex gyökök mindig párosan sokan vannak, előfordulhat tehát, hogy f -nek nincsen $\mathbb{R}$ felett gyöke $\Rightarrow f$ irreducibilis $\mathbb{R}$ felett. De persze

nem szükséges ez. $\square$

2. Feladat. (4 · 4 pont) Adjon példát és röviden indokolja meg, hogy a példája miért rendelkezik a kívánt tulajdonsággal.

(a) Adja meg az összes nem izomorf 4 elemű csoportot.

Két ilyen négyelemű csoport van. Az egyik az ún. ciklus csoport, ilyen például: $(\mathbb{Z}_4; +)$. Művelettáblája:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

A másik ilyen az úgynevezett Klein-csoport, erre példa

lesz a (d) feladattal összeadótáblája. Itt nem ismétlem

meg azt. Minden más 4-elemű csoport ezzel izomorf. $\square$

(b) Adjon meg két olyan különböző a, b természetes számot, amelyekre $\varphi(a) = \varphi(b) = 36$.

Először is $a = 37$, mert a prím, ezért $\varphi(a) = \varphi(37) = a - 1 = 37 - 1 = 36$.

Legyen $b = p_1 p_2$, p_1 és p_2 prímszám. Ekkor:

$$\varphi(b) = b \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) = p_1 p_2 \left(1 - \frac{1}{p_2} - \frac{1}{p_1} + \frac{1}{p_1 p_2}\right) = p_1 p_2 \left(\frac{p_1 p_2 - p_1 - p_2 + 1}{p_1 p_2}\right) =$$

$$= p_1 p_2 - p_1 - p_2 + 1 = (p_1 - 1)(p_2 - 1). \text{ Legyen } p_1 = 3 \text{ és } p_2 = 19. \text{ Ekkor } \varphi(p_1 p_2) = 36, b = 57. \quad \square$$

(c) Adjon példát olyan $f \in \mathbb{R}[x]$ hatodfokú polinomra, amelyre $f / \ln. k. o. (f, f') = x^4 - 1$.

Erre szeretnék hét lépés megoldást mutatni, de külön lapra.

(d) Adja meg a négyelemű test művelettábláit.

Ilyen négyelemű test: $\mathbb{Z}_2 / (X^2 + X + 1)$ faktorgyűrű.

Elemek: $\bar{0}, \bar{1}, \bar{X}, \overline{X+1}$

mind $\mathbb{Z}_2$ felett, tehát test is.

A művelettáblák:

+	$\bar{0}$	$\bar{1}$	$\bar{X}$	$\overline{X+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{X}$	$\overline{X+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{X+1}$	$\bar{X}$
$\bar{X}$	$\bar{X}$	$\overline{X+1}$	$\bar{0}$	$\bar{1}$
$\overline{X+1}$	$\overline{X+1}$	$\bar{X}$	$\bar{1}$	$\bar{0}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{X}$	$\overline{X+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{X}$	$\overline{X+1}$
$\bar{X}$	$\bar{0}$	$\bar{X}$	$\overline{X+1}$	$\bar{1}$
$\overline{X+1}$	$\bar{0}$	$\overline{X+1}$	$\bar{1}$	$\bar{X}$

$\uparrow$

$(X^2 + 1) : (X^2 + X + 1) = \bar{1}$
 $-(X^2 + X + 1)$
 $\hline \bar{X}$

ez egy ún. Klein-csoport,
 itt a példa (a) - hoz...

$X^2 : (X^2 + X + 1) = \bar{1}$
 $-(X^2 + X + 1)$
 $\hline \bar{X+1}$

$(X^2 + X) : (X^2 + X + 1) = \bar{1}$
 $-(X^2 + X + 1)$
 $\hline \bar{1}$

12
3. Feladat. (4 · 3 pont) Egészítse ki a definíciókat, ill. tételkimondásokat.

(a) A $F[x]/(f)$ maradékosztály-gyűrű akkor és csak akkor test, ha f irreducibilis F fölött.

(b) Azt mondjuk, hogy az $f \in F[x]$ polinomnak az $\alpha \in F$ elem gyöke, ha $(x - \alpha)^k | f$, de $(x - \alpha)^{k+1} \nmid f$.

(c) A G csoportot ciklikus csoportnak nevezzük, ha valamely $a \in G$ -re $[a] = G$.

(d) Tetszőleges $n \in \mathbb{N}$ és $u, z \in \mathbb{C}$ esetén azt mondjuk, hogy az u n -edik gyöke z -nek, ha $u^n = z$.

10
4. Feladat. (10 pont) Egészítse ki a következő tétel bizonyítását.

Tétel. Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre $p \nmid a_n, p \nmid a_{n-1}, \dots, p \nmid a_1, p \parallel a_0$, akkor f irreducibilis a racionális számok teste felett.

Bizonyítás. Tegyük fel, hogy $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ olyan polinom, amelyhez létezik a tétel feltételeit kielégítő p prímszám, de f mégsem irreducibilis $\mathbb{Q}$ felett. Ekkor a Gauss-lemma (következménye) szerint léteznek olyan $g, h \in \mathbb{Z}[x]$ polinomok, amelyekre $f = gh$ és $0 < \deg g, \deg h < n$. Legyen $g = b_k x^k + \dots + b_1 x + b_0$ és $h = c_\ell x^\ell + \dots + c_1 x + c_0$.

Írjuk fel az $f = gh$ egyenlőséget együtthatónként. A konstans tagokat összehasonlítva kapjuk, hogy $a_0 = b_0 c_0$, erről pedig tudjuk, hogy osztható p -vel. Mivel p prím, ebből következik, hogy $p | b_0$ vagy $p | c_0$. A két oszthatóság közül csak az egyik teljesülhet, mert $p \nmid a_0$. Az általánosság megszorítása nélkül feltehetjük, hogy $p | c_0$ és $p \nmid b_0$.

Az első-, másod-, ..., $(\ell - 1)$ -edfokú tagokat vizsgálva igazolható, hogy $p | c_1, \dots, p | c_{\ell-1}$.

Nézzük most az ℓ -edfokú tagokat az $f = gh$ egyenlőségben: $a_\ell = \dots$ Tudjuk, hogy $p | a_\ell$, hiszen A jobb oldalon a $b_0 c_\ell$ tag kivételével minden tagról láttuk már, hogy p -vel osztható. Tehát $p | b_0 c_\ell$, amiből p prímtulajdonságát és a $p \nmid b_0$ feltevést használva következik, hogy $p | c_\ell$.

Végül az n -edfokú tagokat összehasonlítva kapjuk, hogy $a_n = b_k c_\ell$, ahol a jobb oldalról már tudjuk, hogy p -vel osztható, mert $p | c_\ell$. Ez pedig ellentmond annak a feltevésnek, hogy $p \nmid a_n$.

Megoldási idő 90 perc

$$\sum_{i=0}^k b_i c_{\ell-i+1}$$

$$\sum_{i=0}^{\ell} b_i c_{\ell-i}$$

ezt tesszük fel
az elején, és
 $\deg h < n$,
 $\ell < n$.

2. feladat, (c) része.

1. megoldás.

Σ a hosszabb. Legyen $f \in \mathbb{R}[x]$, $\deg f = 6$. Adott, hogy $\frac{f}{\text{luko}(f, f')} = \frac{x^4 - 1}{\cancel{x^4 - 1}}$. Tudjuk, hogy

$\deg f' = 5$. Legyen $g = x^4 - 1$, az egyenlet jobb oldala, látjuk, hogy $\deg g = 4$.

Ezért miatt biztos, hogy $\text{luko}(f, f')$ másodfokú, azaz $\deg(\text{luko}(f, f')) = 2$.

Legyen $\text{luko}(f, f') = \alpha x^2 + \beta x + \gamma$, $\alpha \neq 0$, $\alpha, \beta, \gamma \in \mathbb{R}$. Látjuk:

$$f = (x^4 - 1) \text{luko}(f, f') \Leftrightarrow f = (x^4 - 1)(\alpha x^2 + \beta x + \gamma). \text{ Nézzük a deriváltat.}$$

A sorozatderiválás szabályát használva:

$$f' = 4x^3(\alpha x^2 + \beta x + \gamma) + (x^4 - 1)(2\alpha x + \beta). \text{ Triviális, hogy:}$$

$$\text{luko}(f, f') \mid f'.$$

Vizsgáljuk f' -t:

$$f' = \underbrace{4x^3(\alpha x^2 + \beta x + \gamma)}_{\alpha x^2 + \beta x + \gamma \mid \checkmark} + \underbrace{(x^4 - 1)(2\alpha x + \beta)}_{\text{az kell, hogy enné is igaz legyen, hogy}}$$

$$\alpha x^2 + \beta x + \gamma \mid \checkmark$$

ez minden

$$\alpha x^2 + \beta x + \gamma \mid, \text{ mert akkor}$$

$x^4 - 1$ -et bontsuk fel 12 felé.

$$\text{luko}(f, f') \mid f.$$

$$\begin{array}{r} (x^4 - 1) : (x - 1) = x^3 \\ -(x^4 + x^3) \\ \hline -x^3 - 1 \\ -(-x^3 - 1) \\ \hline 0 \end{array}$$

$$i) (x^4 - 1) : (x - 1) = x^3 + x^2 + x + 1$$

$$\begin{array}{r} (x^4 - 1) \\ -(x^4 - x^3) \\ \hline x^3 - 1 \end{array}$$

$$\begin{array}{r} x^3 - 1 \\ -(x^3 - x^2) \\ \hline x^2 - 1 \end{array}$$

$$\begin{array}{r} x^2 - 1 \\ -(x^2 - x) \\ \hline x - 1 \end{array}$$

$$\begin{array}{r} x - 1 \\ -(x - 1) \\ \hline 0 \end{array}$$

$$\begin{array}{r} x - 1 \\ -(x - 1) \\ \hline 0 \end{array}$$

$$\begin{array}{r} x - 1 \\ -(x - 1) \\ \hline 0 \end{array}$$

$$\begin{array}{r} x - 1 \\ -(x - 1) \\ \hline 0 \end{array}$$

$$\Rightarrow (x^4 - 1) = (x - 1)(x^3 + x^2 + x + 1).$$

Te tudjuk, hogy $+1$ is és -1 is gyök. Bontsuk tovább.

$$(X^3 + X^2 + X + 1) : (X + 1) = X^2 + 1$$

$$\begin{array}{r} (X^3 + X^2) \\ \hline X + 1 \\ \hline - (X + 1) \\ \hline 0 \end{array}$$

Tehát $X^4 - 1 = (X - 1)(X + 1)(X^2 + 1)$ ami egy irreducibilis felbontás $\mathbb{R}$ felett.

Kapjuk:

$$f' = 4X^3(\alpha X^2 + \beta X + \gamma) + (X - 1)(X + 1)(X^2 + 1)$$

ahol $\alpha = 1, \beta = 0, \gamma = 1$

net $X^2 + 1 > X^2 - 1$ és
 Enko zeli.

$X^2 + X - X - 1 = X^2 - 1$

$\alpha = 1$
 $\beta = 0$
 $\gamma = 1$

Tehát $\text{enko}(f, f') = X^2 + 1$, így

$$f = (X^2 + 1)(X^4 - 1) = X^6 + X^4 - X^2 - 1.$$

~~$f = (X^2 + 1)(X^4 - 1) = X^6 + X^4 - X^2 - 1$~~

2. megoldás

Tudjuk, hogy $X^4 - 1$ gyökei ugyanazok, mint f gyökei (tanult tétel), csak $X^4 - 1$ minden gyökénél multiplisitása egyszeres.

$$X^4 - 1 = (X - 1)(X + 1)(X^2 + 1). \text{ Ennek fokszáma 4. Legyen}$$

$$f = (X - 1)(X + 1)(X^2 + 1)^2 = (X^2 + X - X - 1)(X^2 + 1)(X^2 + 1) =$$

$$= (X^2 - 1)(X^2 + 1)(X^2 + 1) = (X^4 + X^2 - X^2 - 1)(X^2 + 1) =$$

$$= (X^4 - 1)(X^2 + 1) = X^6 + X^4 - X^2 - 1. \quad \checkmark$$