1	2-8	9-12	13-	Σ

NÉV _____ **NEPTUNKÓD** _____

Bevezetés az algebrába 1 **3. vizsga – elmélet** **2021-01-15**

Az írásbeli dolgozat első felében tesztkérdésekre kell válaszolni, melyekre összesen 20 pont kapható. A második részében definíciók és tételek precíz megfogalmazását kérjük. Az utolsó részben bizonyításokat, vagy azok egyes részeit kell tömören, de világosan leírni. A válaszokat írjuk a kérdéshez tartozó üres dobozba! Kidolgozási idő 60 perc. Semmilyen segédeszköz nem használható!

1. Mindegyik állításról állapítsuk meg, hogy igaz vagy hamis (I|H)! *(6 pont)*

a) Ha $\{ r_1, \dots, r_m \}$ teljes maradékrendszer modulo m, akkor $\{ -r_1, \dots, -r_m \}$ is teljes maradékrendszer. I

b) Minden legalább harmadfokú valós polinomnak van valós gyöke H

c) Ha $n \in \mathbb{N}^+$ páratlan, akkor $2^{n-1} \equiv 1 \pmod{n}$. H

d) Ha $\mathbf{v}_1, \dots, \mathbf{v}_k$ lineárisan összefüggők, akkor $\dim \operatorname{span}(\mathbf{v}_1, \dots, \mathbf{v}_k) < k$. I

e) Minden $A \in \mathbb{R}^{m \times n}$-re és $\mathbf{b} \in \mathbb{R}^m$-re megoldható az $A^T A\mathbf{x} = A^T\mathbf{b}$ egyenletrendszer. I

f) Ha BB^T és $B^T B$ is léteznek, akkor B négyzetes mátrix. H

2. Adjuk meg azt a legkisebb $c \in \mathbb{N}^+$ számot, amelyre a $18x + 60y = c$ diofantoszi egyenlet megoldható! *(2 pont)*

6

3. Írjuk fel a $z = a + bi = r(\cos\varphi + i\sin\varphi)$ (ahol $a, b, r, \varphi \in \mathbb{R}$, $r > 0$) komplex szám reciprokát, $(1/z)$-t algebrai és trigonometrikus alakban. *(2 pont)*

$1/z = \dfrac{a}{a^2+b^2} - i\dfrac{b}{a^2+b^2} =$
$\frac{1}{r}(\cos(-\varphi) + i\sin(-\varphi))$.

4. Adjunk meg egy olyan $f(x) \in \mathbb{Z}[x]$ polinomot, amely $\mathbb{Q}[x]$-ben irreducibilis, de $\mathbb{Z}[x]$-ben nem! *(2 pont)*

Pl. $f(x) = 2x + 4$

5. Legyen $A \in \mathbb{R}^{m \times n}$, és L az A redukált lépcsős alakja. Az alábbi állítások közül melyikből következik, hogy az $A\mathbf{x} = \mathbf{0}$ n-változós homogén egyenletrendszernek csak egyetlen megoldása van? *(2 pont)*
(A) L-nek m nemnulla sora van.
(B) L-nek m nemnulla oszlopa van.
(C) L-nek n nemnulla sora van.
(D) L-nek n nemnulla oszlopa van.

C

6. Legyen $f : \mathbb{Z}_2^2 \to \mathbb{Z}_2^2$ lineáris transzformáció, amelyre $f(1,0) = (1,1)$. Hány lehetséges értéke van $f(1,1)$-nek? *(2 pont)*

4

7. Adjuk meg az $\mathcal{U} = \{(x,y,z) \mid x + y + z = 0\} \leq \mathbb{R}^3$ altér merőlegesének egy bázisát! *(2 pont)*

$\{(1,1,1)\}$

8. Ha $A \in \mathbb{R}^{3\times 5}$, és $\dim \mathcal{N}(A) = 3$, akkor mi az $A^T A$ mátrix mérete (azaz hányszor hányas) és rangja? *(2 pont)*

$A^T A \in \mathbb{R}^{5\times 5}$,
$r(A^T A) = r(A) = 5 - 3 = 2$.

9. Definiáljuk egy nemnulla komplex szám (multiplikatív) rendjét! Adjunk meg egy negyedrendű és egy végtelen rendű komplex számot! *(3 pont)*

Egy z szám rendje a legkisebb $k \in \mathbb{N}^+$, amelyre $z^k = 1$. Ha nincs ilyen k, akkor a rend végtelen.
Pl. Az i szám rendje 4, a 2 rendje végtelen.

10. Definiáljuk egy A $n \times n$-es mátrix determinánsának az a_{ij} elemhez tartozó előjeles aldeterminánsát, A_{ij}-t, és írjuk fel a determinánsok sorokra vonatkozó kifejtési tételét. *(3 pont)*

$A_{ij} = (-1)^{i+j} D_{ij}$, ahol D_{ij} annak a mátrixnak a determinánsa, amelyet úgy kapunk, hogy A-ból elhagyjuk az i. sort és a j. oszlopot.
$|A| = \sum\limits_{j=1}^{n} a_{ij} A_{ij}$.

11. Mondjuk ki a számelmélet alaptételét $\mathbb{Z}$-ben! *(2 pont)*

Minden egész szám, ami $\neq 0, \pm 1$, sorrendtől és egységszeresektől (előjelektől) eltekintve egyértelműen felírható felbonthatatlan egészek szorzataként.

12. Definiáljuk egy mátrix inverzét! Mi a feltétele annak, hogy egy test fölötti négyzetes háromszögmátrix invertálható legyen? *(2 pont)*

A inverze B, ha $AB = I$ és $BA = I$.
Egy háromszögmátrix pontosan akkor invertálható, ha a diagonális elemei nem nullák.

13. Mondjuk ki és bizonyítsuk be az Euler–Fermat-tételt! *(5 pont)*

Tétel: Ha $m \in \mathbb{N}^+$, $a \in Z$, $(a, m) = 1$, akkor $a^{\varphi(m)} \equiv 1 \pmod{m}$.
Biz.: Legyen $\{ r_1, \ldots, r_{\varphi(m)} \}$ redukált maradékrendszer modulo m.
Mivel $(a, m) = 1$, $\{ ar_1, \ldots, ar_{\varphi(m)} \}$ is redukált maradékrendszer, és így valamilyen sorrendben az $r_1, \ldots r_{\varphi(m)}$ számokkal kongruensek az elemei. $\Rightarrow$
$r_1 \cdots r_{\varphi(m)} \equiv ar_1 \cdots ar_{\varphi(m)} \equiv a^{\varphi(m)} r_1 \cdots r_{\varphi(m)} \pmod{m}$
$r_1 \ldots r_{\varphi(m)}$ relatív prím m-hez, ezért egyszerűsíthetjük vele a kongruenciát. $\Rightarrow$
$1 \equiv a^{\varphi(m)} \pmod{m}$.

14. Az alábbi tétel három ekvivalens állítást sorol fel arra, hogy egy vektortér két alterének direkt összege.
a) Mondjuk ki a direkt összeg definícióját (azaz az (i) állítás jelentését)
b) Az $\mathcal{U} = \operatorname{span}((1, -1, 0), (1, 0, -1))$ és $\mathcal{W} = \operatorname{span}((1, 0, 0), (0, 0, 1))$ alterekre $\mathcal{V} := \mathbb{R}^3 \neq \mathcal{U} \oplus \mathcal{W}$. Példákkal mutassuk meg, hogy az (i), (ii) és (iii) állítás egyike sem teljesül erre a két altérre! *(5 pont)*

a) $\mathcal{V} = \mathcal{U} \oplus \mathcal{W}$, ha $\mathcal{V} = \mathcal{U} + \mathcal{W}$ és $\mathcal{U} \cap \mathcal{W} = 0$.
b) (i): $\mathbf{0} \neq (1, 0, -1) = (1, 0, 0) - (0, 0, 1) \in \mathcal{U} \cap \mathcal{W}$
(ii): $(1, 0, -1) = (1, 0, -1) + \mathbf{0} = \mathbf{0} + ((1, 0, 0) - (0, 0, 1))$ kétféle felírás $\mathbf{u} + \mathbf{w}$ alakban.
(iii): Az $\mathcal{U}$ és $\mathcal{W}$ megadott generátorrendszere független, mert kételemű, és egyik vektor sem skalárszorosa a másiknak. Tehát ezek bázist adnak $\mathcal{U}$-ben, illetve $\mathcal{W}$-ben, de az uniójuk 4-elemű, így nem lehet bázis a háromdimenziós $\mathbb{R}^3$-ben.

Tétel: Az $\mathcal{U}, \mathcal{W} \leq \mathcal{V}$ alterekre ekvivalens:

(i) $\mathcal{V} = \mathcal{U} \oplus \mathcal{W}$.

(ii) $\forall\ \mathbf{v} \in \mathcal{V}$ egyértelműen írható $\mathbf{v} = \mathbf{u} + \mathbf{w}$ $(\mathbf{u} \in \mathcal{U},\ \mathbf{w} \in \mathcal{W})$ alakban.

(iii) Ha $\mathcal{B}$ az $\mathcal{U}$-nak, $\mathcal{C}$ a $\mathcal{W}$-nek bázisa, akkor $\mathcal{B} \dot{\cup} \mathcal{C}$ bázisa $\mathcal{V}$-nek.