Alg. és számelm. 4 (tan.) **1. feladatsor** *2024. február 13-14.*

Gyűrűk, testek, kvaterniók

1. *Gyöktelenítsük az alábbi törtek nevezőjét:*

$$\frac{1}{1+\sqrt[3]{3}}, \qquad \frac{3+2\sqrt[3]{3}}{2+\sqrt[3]{2}}, \qquad \frac{1}{1+\sqrt[5]{5}}\,.$$

Megoldás. Az első két esetben használjuk az $a^3+b^3=(a+b)(a^2-ab+b^2)$ azonosságot, a harmadik esetben pedig az $a^5+b^5=(a+5)(a^4-a^3b+a^2b^2-ab^3+b^4)$ azonosságot, hogy a törtet bővítve eltűnjön a gyök a nevezőből:

$$\frac{1}{1+\sqrt[3]{3}}=\frac{1}{1+\sqrt[3]{3}}\cdot\frac{1-\sqrt[3]{3}+\sqrt[3]{9}}{1-\sqrt[3]{3}+\sqrt[3]{9}}=\frac{1-\sqrt[3]{3}+\sqrt[3]{9}}{1+3}=\frac{1-\sqrt[3]{3}+\sqrt[3]{9}}{4}$$

$$\frac{3+2\sqrt[3]{3}}{2+\sqrt[3]{2}}=\frac{3+2\sqrt[3]{3}}{2+\sqrt[3]{2}}\cdot\frac{4-2\sqrt[3]{2}+\sqrt[3]{4}}{4-2\sqrt[3]{2}+\sqrt[3]{4}}=\frac{20+2\sqrt[3]{2}-\sqrt[3]{4}}{8+2}=\frac{20+2\sqrt[3]{2}-\sqrt[3]{4}}{10}$$

$$\frac{1}{1+\sqrt[5]{5}}=\frac{1}{1+\sqrt[5]{5}}\cdot\frac{1-\sqrt[5]{5}+\sqrt[5]{25}-\sqrt[5]{125}+\sqrt[5]{625}}{1-\sqrt[5]{5}+\sqrt[5]{25}-\sqrt[5]{125}+\sqrt[5]{625}}=\frac{1-\sqrt[5]{5}+\sqrt[5]{25}-\sqrt[5]{125}+\sqrt[5]{625}}{6}$$

Emlékeztető: $a^n-b^n=(a-b)(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1})$ minden n-re teljesül. Páratlan kitevőkre, azaz az $n=2k+1$ esetben pedig $a^{2k+1}+b^{2k+1}=(a+b)(a^{2k}-a^{2k-1}b+\cdots-ab^{2k-1}+b^{2k})$ igaz.

2. *a) Igazoljuk, hogy az x^3-6x+1 polinom irreducibilis $\mathbb{Q}$ fölött.*
b) Mutassuk meg, hogy a polinomnak van egy α valós gyöke, amelyre $2<\alpha<3$.
c) Igazoljuk azt is, hogy csak egy ilyen α gyök van.
d) „Alfátlanítsuk” az $\dfrac{1}{1+\alpha}$ tört nevezőjét.

Megoldás. a) Tudjuk, hogy egy racionális harmadfokú polinom pontosan akkor irreducibilis $\mathbb{Q}$ fölött, ha nincs gyöke. A racionális gyökteszt alapján viszont ennek a polinomnak – jelöljük a továbbiakban $f(x)$-szel – csak olyan a/b egyszerűsített alakú racionális gyöke lehetne, amelyre $a,b=\pm1$. (A racionális gyökteszt alapján az egyszerűsített formában fölírt törtek közül csak azok lehetnek gyökei a polinomnak, amelyeknél a nevező osztója a főegyütthatónak, a számláló pedig a konstans tagnak.) Ugyanakkor ±1 egyike sem gyöke a polinomnak.
b) $f(2)=2^3-6\cdot2+1=-3$, ugyanakkor $f(3)=3^3-6\cdot3+1=10$. Tehát a $(2,3)$ intervallum két végpontján ellentétes előjelű értéket vesz föl a polinomfüggvény, ezért a Bolzano-tétel alapján valahol az intervallum belsejében a nullát is fölveszi értékül, azaz a $(2,3)$ intervallumban van egy α gyök. (Az előzőek szerint, persze, ez nem racionális.)
c) Számoljuk ki az $f(x)$ polinom deriváltját: $f'(x)=3x^2-6$. Könnyen látható, hogy minden $x\in[2,3]$ értékre $6=f'(2)<f'(x)<f'(3)=21$, vagyis a derivált polinom az egész intervallumon pozitív. Ez azt jelenti, hogy az f-hez tartozó polinomfüggvény a $[2,3]$ intervallumon szigorúan monoton növő, így maximum egy gyöke lehet neki.
d) Osszuk el maradékosan az $f(x)$ polinomot a $g(x)=1+x$ polinommal. Azt kapjuk, hogy $f(x)=x^3-6x+1=(x^2-x-5)(x+1)+6$. Mivel α gyöke az $f(x)$-nek, ezért $f(\alpha)=0=(\alpha^2-\alpha-5)(\alpha+1)+6$, vagyis $(\alpha+1)(\alpha^2-\alpha-5)=-6$. Ez tehát azt jelenti, hogy a megadott törtet az $\alpha^2-6\alpha+1$ kifejezéssel érdemes bővíteni, hiszen a nevezővel szorozva így egy α nélküli konstanst kapunk:

$$\frac{1}{1+\alpha}=\frac{1}{1+\alpha}\cdot\frac{\alpha^2-6\alpha+1}{\alpha^2-6\alpha+1}=\frac{\alpha^2-6\alpha+1}{-6}$$

Megjegyzés: Úgy tűnik, szerencsénk volt, hogy az α-nak egy elsőfokú kifejezése szerepelt a nevezőben, így a maradékos osztásnál konstans polinomot kaptunk maradékul, s a tört bővítése után nem maradt α a nevezőben. Persze, az eljárást esetleg többször megismételve magasabb fokú kifejezésekkel is el tudnánk bánni (hiszen egy-egy ilyen maradékos osztással fokozatosan csökkenthetjük a nevezőben levő kifejezés fokát). De azt, hogy valójában hogyan is kell „osztani” egy tetszőleges α-kifejezéssel (és miért), ha tudjuk, hogy α gyöke egy racionális együtthatós polinomnak, majd a későbbiekben, a testbővítések elméleténél fogjuk igazán megérteni.

3. *Írjuk föl az $1 + 2i + 3j + 4k$ kvaternió inverzét.*

Megoldás. Ha $h = 1 + 2i + 3j + 4k$, akkor $h^{-1} = \frac{1}{h \cdot \bar{h}} \cdot \bar{h} = \frac{1}{30} \cdot (1 - 2i - 3j - 4k)$.

4. *Oldjuk meg $\mathbb{H}$-ban az $x^2 = 1$, illetve az $x^2 = -1$ egyenletet.*

Megoldás. Az $x^2 = 1$ egyenletnek nyilván megoldása a ± 1. Megmutatjuk, hogy más megoldás nincs. Ha ugyanis $h^2 = 1$, azaz $h^2 - 1 = 0$, akkor $h^2 - 1^2 = (h-1)(h+1) = 0$ miatt az egyik tényező 0, és így $h = 1$ vagy $h = -1$. – Az $x^2 = -1$ egyenletnek már nemcsak két megoldása lesz, hiszen kapásból tudunk hat különböző megoldást: $\pm i$, $\pm j$ és $\pm k$ mind megoldások lesznek. Ez azért meglepő, mert azt tanultuk korábban, hogy test fölött egy polinomnak legföljebb fokszámnyi gyöke van. A probléma abban van, hogy $\mathbb{H}$ nem test, mert nem kommutatív. És ez most számít: $h^2 = -1$, azaz $h^2 + 1 = 0$ esetén ugyanis most nem mondhatjuk, hogy $h^2 - i^2 = (h - i)(h + i) = 0$, ugyanis egyáltalán nem biztos, hogy $hi = ih$, hiszen az i nem mindennel fölcserélhető (pl. $ij \neq ji$)! Vegyük észre, hogy az előző esetben azért nem volt semmi baj, mert az i helyén az 1 állt, és az 1 bizony minden $h \in \mathbb{H}$-val fölcserélhető! – Ha már találtunk 6 megoldást, találjuk meg az összeset! Mutassuk meg, hogy pontosan azok a h kvaterniók lesznek megoldásai az $x^2 = -1$ egyenletnek, amelyekre h tisztán képzetes (vagyis a valós része 0, azaz $\bar{h} = -h$), és melyeknek a normája $N(h) = h\bar{h} = 1$. Az világos, hogy az előbbi két feltételnek eleget tevő kvaterniók gyökei lesznek az egyenletnek, hiszen ez esetben $h^2 = h \cdot (-\bar{h}) = -N(h) = -1$. Megfordítva, ha $h^2 = -1$, akkor mindkét oldal normáját véve azt kapjuk, hogy $N(h^2) = N(-1) = 1$. Ebből $N(h^2) = N(h)^2$ és $N(h) \geq 0$ miatt $N(h) = 1$ adódik. (Itt használtuk az $N(h^2) = N(h)^2$ összefüggést: ez következik pl. a következő feladat b) részéből.) Továbbá: $h = 1 \cdot h = N(h) \cdot h = N(\bar{h})h = \bar{h} \cdot h \cdot h = \bar{h} \cdot h^2 = -\bar{h}$, tehát h valóban tisztán képzetes. – A megoldások tehát megegyeznek az i, j, k elemek által kifeszített háromdimenziós valós altér egységgömbjének a pontjaival: ezek azok az $a + bi + cj + dk$ alakú kvaterniók, melyekre $a = 0$ és $b^2 + c^2 + d^2 = 1$.

5. *a) Teljesül-e a kvaterniók körében a $\overline{qr} = \overline{q} \cdot \overline{r}$ azonosság?*
b) Ellenőrizzük, hogy $q, r \in \mathbb{H}$ esetén $\overline{qr} = \overline{r} \cdot \overline{q}$, majd ennek segítségével vezessük le, hogy $N(qr) = N(q)N(r)$.
c) Mutassunk rá mindenfajta számolás nélkül, hogy ha két egész szám felírható négy négyzetszám összegeként, akkor a szorzatuk is.
d) Bontsuk fel az $(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + v^2)$ kifejezést két (lényegesen) különböző módon is négy kifejezés négyzetének összegére.

Megoldás. a) Nem teljesül: $q = i$, $r = j$ esetén $q \cdot r = i \cdot j = k$, tehát $\overline{qr} = \overline{k} = -k$. Ugyanakkor $\overline{q} = -i$, $\overline{r} = -j$, így $\overline{q} \cdot \overline{r} = (-i) \cdot (-j) = ij = k$.
b) Legyen $q = a + bi + cj + dk$ és $r = a' + b'i + c'j + d'k$. Ekkor $\overline{q} = a - bi - cj - dk$, és $\overline{r} = a' - b'i - c'j - d'k$, továbbá:

$$\begin{aligned}
qr &= (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')i + (ac' + ca' - bd' + db')j + (ad' + da' + bc' - cb')k \\
\overline{qr} &= (aa' - bb' - cc' - dd') - (ab' + ba' + cd' - dc')i - (ac' + ca' - bd' + db')j - (ad' + da' + bc' - cb')k \\
\overline{r}\overline{q} &= (a'a - b'b - c'c - d'd) + (a'(-b) + (-b')a + (-c')(-d) - (-d')(-c))i + \\
&\quad + ((a')(-c) + (-c')a - (-b')(-d) + (-d')(-b))j + (a'(-d) + (-d')a + (-b')(-c) - (-c')(-b))k
\end{aligned}$$

Az utóbbi két sor összehasonlításából azt kapjuk, hogy $\overline{qr} = \overline{r}\overline{q}$, vagyis a szorzat konjugáltja a konjugáltak szorzata, de fordított sorrendben. (Ehhez hasonló a szabályunk a mátrixszorzat transzponálására is.) Ebből viszont könnyen kapjuk a második összefüggést: $N(qr) = (qr) \cdot \overline{(qr)} = (qr)(\overline{r}\overline{q}) = q(r\overline{r})\overline{q} = q\overline{q}N(r) = N(q)N(r)$. Itt használtuk azt, hogy $N(r)$ valós szám, tehát minden kvaternióval fölcserélhető. (*Megjegyzés:* Érdemes elgondolkozni, hogy lehetne-e a szorzattartást valamivel egyszerűbb számolással kihozni.)
c) Ha egy m egész szám négy négzetszám összege, azaz pl. $m = a^2 + b^2 + c^2 + d^2$, akkor $m = N(q)$, ahol $q = a + bi + cj + dk$, azaz m a normája egy „egész” kvaterniónak, azaz olyan h-nak, melynek az együtthatói egész számok. De két egész kvaternió szorzata is egész kvaternió lesz, és annak a normája épp a normáik szorzatával egyenlő, tehát ha pl. $m = N(q)$ és $n = N(r)$, akkor $nm = N(q)N(r) = N(qr)$, és így $N(q)N(r)$ is előáll négy négyzetszám összegeként.
d) Vegyük észre hogy itt két kvaterniónorma van összeszorozva, ami egyenlő a megfelelő kvaterniók szorzatának a normájával:

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + v^2) = N(q)N(r) = N(qr)$$

A hozzájuk tartozó kvaterniók azonban nem egyértelműek: pl. az $(a^2+b^2+c^2+d^2)$ kifejezés a $\pm a\pm bi\pm cj\pm dk$ kvaterniók bármelyikének a normájaként is megkapható (ez 16 lehetőség, csak az egyik tényezőnél). Ha tehát választunk két különböző q_1 és q_2 kvaterniót a lehetségesek közül, akkor egy rögzített r kvaternióval kombinálva két különböző négyzetösszeget kaphatunk. Pl. $q_1 = a + bi + cj + dk$ és $q_2 = -a + bi + cj + dk$, valamint $r = x + yi + zj + vk$ esetén:

$$q_1 r = (ax - by - cz - dv) + (ay + bx + cv - dz)i + (az + cx - bv + dy)j + (av + dx + bz - cy)k$$
$$q_2 r = (-ax - by - cz - dv) + (-ay + bx + cv - dz)i + (-az + cx - bv + dy)j + (-av + dx + bz - cy)k$$

és ezért a keresett két előállítás:

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + v^2) = N(q_1)N(r) = N(q_1 r) =$$
$$= (ax - by - cz - dv)^2 + (ay + bx + cv - dz)^2 + (az + cx - bv + dy)^2 + (av + dx + bz - cy)^2$$
$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + v^2) = N(q_2)N(r) = N(q_2 r) =$$
$$= (-ax - by - cz - dv)^2 + (-ay + bx + cv - dz)^2 + (-az + cx - bv + dy)^2 + (-av + dx + bz - cy)^2$$

6. *Legyen* $\mathbb{E} = \left\{ \dfrac{a + b\sqrt{3}\cdot i}{2} \mid a, b \in \mathbb{Z},\ a \equiv b \pmod 2 \right\}$*. Ellenőrizzük, hogy* $\mathbb{E}$ *a komplex számok testének egységelemes részgyűrűje (Euler-egészek). Keressük meg* $\mathbb{E}$*-ben az összes egységet.*

Megoldás. Nyilván $1 = \frac{2+0\sqrt{3}}{2} \in \mathbb{E}$, tehát $\mathbb{E}$-ben benne van az egységelem. Azt nyilván könnyű megmutatni, hogy $\mathbb{E}$ zárt az összeadásra és a kivonásra, úgyhogy egyedül azon kell egy kicsit elgondolkoznunk, hogy miért lesz zárt a szorzásra. De ehhez elegendő észrevennünk, hogy az $\mathbb{E}$ elemei pontosan az $a + b\omega$ típusú komplex számok, ahol $a, b \in \mathbb{Z}$ és $\omega = \cos(2\pi/3) + i\sin(2\pi/3)$ az egyik primitív egységgyök, továbbá hogy $\omega^2 = -1 - \omega$. Ekkor ugyanis:

$$a + b\omega \cdot c + d\omega = ac + bd\omega^2 + (ad + bc)\omega = (ac - bd) + (ad + bc - bd)\omega.$$

Ez azt jelenti, hogy $\mathbb{E}$ zárt a szorzásra is, tehát részgyűrű.
Az $a + b\omega$ alakból azt kapjuk, hogy $\mathbb{E}$ elemei egy háromszögrács pontjai a síkon, és a komplex norma multiplikativitása (azaz $N(zw) = N(z)N(w)$) miatt azt kapjuk, hogy csak az 1 normájú ilyen számok lesznek egységek. Ezek: ± 1, $\pm\omega$, $\pm\omega^2 = \mp(1 + \omega)$.

7. *a) Legyen* $\mathbb{K} = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\}$ *Igazoljuk, hogy* $\mathbb{R} \leq \mathbb{C}^{2\times 2}$.
b) Számítsuk ki $\mathbb{K}$ *elemeinek determinánsát és inverzét is (ha van).*
c) Igazoljuk, hogy $\mathbb{K}$ *olyan ferdetest, ami nem test.*

Megoldás. a) Ahhoz, hogy igazoljuk, $\mathbb{K}$ részgyűrű, igazolnunk kell a műveletekre (összeadásra, kivonásra, szorzásra) való zártságot (a halmaz nyilván nem üres, hiszen pl. tartalmazza a nullamátrixot). Az összeadásra való zártságot pl. az alábbi számolás igazolja:

$$\begin{pmatrix} z_1 & w_1 \\ -\bar{w}_1 & \bar{z}_1 \end{pmatrix} + \begin{pmatrix} z_2 & w_2 \\ -\bar{w}_2 & \bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1 + z_2 & w_1 + w_2 \\ -\bar{w}_1 - \bar{w}_2 & \bar{z}_1 + \bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1 + z_2 & w_1 + w_2 \\ -\overline{(w_1 + w_2)} & \overline{z_1 + z_2} \end{pmatrix}.$$

Itt tehát a z-nek és w-nek megfelelő általános elem $z_1 + z_2$, illetve $w_1 + w_2$. A kivonás hasonlóan egyszerű.
A szorzásra való zártságot az alábbi számolás mutatja:

$$\begin{pmatrix} z_1 & w_1 \\ -\bar{w}_1 & \bar{z}_1 \end{pmatrix} \cdot \begin{pmatrix} z_2 & w_2 \\ -\bar{w}_2 & \bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1 z_2 - w_1 \bar{w}_2 & z_1 w_2 + w_1 \bar{z}_2 \\ -\bar{w}_1 z_2 - \bar{z}_1 \bar{w}_2 & -\bar{w}_1 w_2 + \bar{z}_1 \bar{z}_2 \end{pmatrix} = \begin{pmatrix} z_1 z_2 - w_1 \bar{w}_2 & z_1 w_2 + w_1 \bar{z}_2 \\ -\overline{(z_1 w_2 + w_1 \bar{z}_2)} & \overline{z_1 z_2 - w_1 \bar{w}_2} \end{pmatrix}$$

Itt is olyan alakú mátrixot kapunk, mint amilyen $\mathbb{K}$ általános eleme.
b) $\det \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} = |z|^2 + |w|^2$, ami tehát azt jelenti, hogy a determináns csak akkor nulla, ha $z = w = 0$, azaz a nullamátrixon kívül minden elemnek van inverze. Az inverz mátrix képlete alapján nem nulla mátrix esetén:

$$\begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix}^{-1} = \frac{1}{|z|^2 + |w|^2} \begin{pmatrix} \bar{z} & -\bar{w} \\ w & z \end{pmatrix} \in \mathbb{K}$$

c) Az előző részben láttuk, hogy minden nem nulla $\mathbb{K}$-beli mátrix invertálható, és az inverze is $\mathbb{K}$-ban van. Mivel az a) rész alapján $\mathbb{K}$ részgyűrű is, ezért $\mathbb{K}$ valóban ferdetest, ami nem kommutatív. Ez utóbbit pl. az a $A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ és a $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ mátrixok mutatják: $AB = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$, míg $BA = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$. A szorzás tehát nem kommutatív.

8. *Módosítsuk a valós függvények gyűrűjét oly módon, hogy az összeadás továbbra is pontonként történjen (vagyis $(f+g)(x) = f(x) + g(x)$, a szorzást viszont a függvények kompozíciójával definiáljuk, vagyis az $(fg)(x) = (f \circ g)(x)$ előírással. Mely gyűrűaxiómák maradnak érvényben?*

Megoldás. A pontokénti összeadásra az összeadás axiómái teljesülnek, vagyis egy kommutatív csoportot alkotnak a gyűrűelemek. Ez várható is volt, hiszen csak a szorzást változtattuk meg, s a szokásos pontonkénti függvényszorzással a függvények gyűrűt alkotnak. A szorzás asszociativitása a kompozíció asszociativitása miatt szintén teljesül, sőt még egységelemünk is van: az identitásfüggvény a kompozícióra nézve egységelemként viselkedik. Ugyanakkor az egyik disztributivitási szabály nem teljesül: legyen $f(x) = x^2$, és $g_1(x) = g_2(x) = x$. Ekkor $(f \circ (g_1 + g_2))(x) = f(2x) = 4x^2$, ugyanakkor $((f \circ g_1) + (f \circ g_2))(x) = x^2 + x^2 = 2x^2$. A két függvény tehát különbözik egymástól. A másik disztributivitás viszont ekkor is igaz: $((f_1 + f_2) \circ g)(x) = (f_1 + f_2)(g(x)) = f_1(g(x)) + f_2(g(x)) = (f_1 \circ g + f_2 \circ g)(x)$.

9. *Mutassunk példát nullosztóra a folytonos, illetve a differenciálható valós függvények gyűrűjében.*

Megoldás. Elegendő differenciálható példát adnunk. Legyen:

$$f(x) = \begin{cases} 0 & \text{ha } x \le 0 \\ x^2 & \text{ha } x \ge 0 \end{cases} \qquad \text{és} \qquad g(x) = \begin{cases} x^2 & \text{ha } x \le 0 \\ 0 & \text{ha } x \ge 0 \end{cases}$$

Ekkor mindkét függvény differenciálható (csak a nullában izgalmas egy kicsit a differenciálhatóság), egyik sem a nullafüggvény, de a szorzatuk nulla.

10. *Tekintsük az $A = \begin{bmatrix} 1 & 2 \\ 4 & 8 \end{bmatrix}$ mátrixot. Mutassuk meg, hogy azok a B valós mátrixok, melyekre $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$, alteret alkotnak $\mathbb{R}^{2\times 2}$-ben. Hány dimenziós ez az altér?*

Megoldás. Az világos, hogy ezek a mátrixok alteret alkotnak. A szokásos módon megoldva az $A\mathbf{x} = \mathbf{0}$ lineáris egyenletrendszert, azt kapjuk, hogy az ilyen B mátrixok pontosan azok, amelyek oszlopai $\begin{bmatrix} 2a \\ -a \end{bmatrix}$ alakban írhatók föl, azaz a megoldástér:

$$M = \left\{ \begin{bmatrix} 2a & 2b \\ -a & -b \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$$

Ez pedig pontosan azt mutatja, hogy $\dim M = 2$.

11. *Igazoljuk, hogy egy $0 \neq A \in T^{n\times n}$ mátrix pontosan akkor bal oldali nullosztó, ha nem invertálható. Hogyan következik ebből hasonló állítás jobb oldali nullosztókra.*

Megoldás. Invertálható A esetén az $AX = 0$ összefüggést balról szorozhatjuk az A^{-1} inverzmátrixszal, s azt kapjuk, hogy $X = 0$. Vagyis invertálható mátrix nem lehet bal oldali nullosztó. Ha viszont A nem invertálható, az azt jelenti, hogy a determinánsa 0, és ez azzal ekvivalens, hogy a mátrix redukált lépcsős alakjában nem minden oszlopban van vezéregyes. Ilyenkor tehát az $A\mathbf{x} = \mathbf{0}$ lineáris egyenletrendszernek van nem triviális megoldása: pl. $\mathbf{x}_0 \in T^n$. Legyen X az az $n \times n$-es mátrix, melynek minden oszlopa $\mathbf{x}_0$-lal egyenlő. Ekkor$X \neq 0$, és $AX = 0$. Ez azt jelenti, hogy amennyiben $A \neq 0$ nem invertálható, akkor bal oldali nullosztó. – A jobb oldali nullosztóságra vonatkozó állítás abból következik, hogy A és A^T egyszerre invertálhatók, és $XA = 0$ pontosan akkor igaz, ha $A^T X^T = 0$.