Bevezetés a számításelméletbe I.
Zárthelyi feladatok — pontozási útmutató
2015. november 26.

Általános alapelvek.

A pontozási útmutató célja, hogy a javítók a dolgozatokat egységesen értékeljék. Ezért az útmutató minden feladat (legalább egy lehetséges) megoldásának főbb gondolatait és az ezekhez rendelt részpontszámokat közli. Az útmutatónak *nem célja* a feladatok teljes értékű megoldásának részletes leírása; a leírt lépések egy maximális pontszámot érő megoldás vázlatának tekinthetők.

Az útmutatóban feltüntetett részpontszámok csak akkor járnak a megoldónak, ha a kapcsolódó gondolat egy áttekinthető, világosan leírt és megindokolt megoldás egy lépéseként szerepel a dolgozatban. Így például az anyagban szereplő ismeretek, definíciók, tételek puszta leírása azok alkalmazása nélkül nem ér pontot (még akkor sem, ha egyébként valamelyik leírt tény a megoldásban valóban szerephez jut). Annak mérlegelése, hogy az útmutatóban feltüntetett pontszám a fentiek figyelembevételével a megoldónak (részben vagy egészében) jár-e, teljes mértékben a javító hatásköre.

Részpontszám jár minden olyan ötletért, részmegoldásért, amelyből a dolgozatban leírt gondolatmenet alkalmas kiegészítésével a feladat hibátlan megoldása volna kapható. Az útmutatóban szereplő részpontszámok szükség esetén tovább is oszthatók. Az útmutatóban leírttól eltérő jó megoldás természetesen maximális pontot ér.

Minden feladat 10 pontot ér. A vizsgajegybe a dolgozat pontszáma számít bele, így a dolgozatokra osztályzatot nem adunk.

1. Határozzuk meg az alábbi A mátrix inverzének bal felső sarkában álló elemét.

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 1 \\ 2 & 2 & 1 \end{pmatrix}$$

* * * * *

Az A^{-1} mátrix első oszlopát (a definíció, vagy az A^{-1} meghatározására tanult eljárás szerint) az $A \cdot \underline{x} = \underline{e}_1$ lineáris egyenletrendszer megoldásával kaphatjuk (ahol $\underline{e}_1$ az egységmátrix első oszlopát jelöli). (2 pont)

Azonban ebből a lineáris egyenletrendszerből is csak x_1-et, vagyis az $\underline{x}$ megoldás első koordinátáját kérdezi a feladat. (2 pont)

Az $\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 2 & 3 & 1 & 0 \\ 2 & 2 & 1 & 0 \end{array}\right)$ kibővített együtthatómátrixú $A \cdot \underline{x} = \underline{e}_1$ lineáris egyenletrendszerben a harmadik sorból az elsőt levonva az $\left(\begin{array}{ccc|c} 1 & 2 & 1 & 1 \\ 2 & 3 & 1 & 0 \\ 1 & 0 & 0 & -1 \end{array}\right)$ alakot kapjuk. (3 pont)

Ennek utolsó sora mutatja, hogy x_1 értéke, vagyis az A^{-1} bal felső sarkában álló elem (-1). (3 pont)

Természetesen nem hiba, csak fölösleges akár az $A \cdot \underline{x} = \underline{e}_1$ megoldására, akár az A^{-1} meghatározására vonatkozó teljes Gauss-eliminációt elvégezni és abból kiolvasni a keresett értéket. Aki ezt megteszi, az eredményül az $A^{-1} = \begin{pmatrix} -1 & 0 & 1 \\ 0 & 1 & -1 \\ 2 & -2 & 1 \end{pmatrix}$ mátrixot (illetve $A \cdot \underline{x} = \underline{e}_1$ esetében ennek első oszlopát) kapja.

Ha egy megoldó így jár el, akkor minden, a megoldás menetét érdemben nem befolyásoló számolási hiba darabonként 1 pont levonást jelent (akkor is, ha a szóban forgó számolási hiba a végeredményként kapott bal felső elemet egyébként nem érinti).

2. A 6×10-es A mátrixra $\mathrm{r}(A) = 3$. Igaz-e mindig, hogy A-nak elhagyható egy sora és egy oszlopa úgy, hogy a kapott 5×9-es B mátrixra $\mathrm{r}(B) = 3$ teljesüljön?

* * * * *

Első megoldás. $\mathrm{r}(A) = 3$-ból az oszloprang definíciója szerint következik, hogy A-nak kiválasztható 3 lineárisan független oszlopa. (1 pont)
Hagyjunk el A-ból egy ettől a háromtól különböző oszlopot, a kapott 6×9-es mátrix legyen C. (1 pont)
Ekkor C-ben továbbra is megtalálható ugyanaz a 3 lineárisan független oszlop. (1 pont)
Ennél több viszont nyilván nem, különben A-ban is kiválasztható lenne 3-nál több lineárisan független oszlop, ellentmondásban $\mathrm{r}(A) = 3$-mal. (1 pont)
Így $\mathrm{r}(C) = 3$ (az oszloprang definíciója szerint). (1 pont)
Ezért a sorrang definíciója szerint C-nek kiválasztható 3 lineárisan független sora. (1 pont)
Hagyjunk el C-ből egy ettől a háromtól különböző sort, a kapott 5×9-es mátrix legyen B. (1 pont)
A fenti gondolatmenettel analóg módon következik, hogy $\mathrm{r}(B) = 3$: B-nek továbbra is kiválasztható 3 lineárisan független sora, de annál több $\mathrm{r}(C) = 3$ miatt nem. (1 pont)
Mivel B az A-ból egy oszlop, majd egy sor elhagyásával keletkezett és $\mathrm{r}(B) = 3$, az állítás igaz. (2 pont)

Második megoldás. A determinánsrang definíciója szerint A-nak kiválasztható 3 sora és 3 oszlopa úgy, hogy az ezek kereszteződéseiben kialakuló 3×3-as M részmátrixra $\det M \neq 0$. (2 pont)
Hagyjuk most el A-nak egy olyan sorát és egy olyan oszlopát, amelyek az M négyzetes részmátrix kiválasztásában nem játszottak szerepet, a kapott 5×9-es mátrix legyen B. (2 pont)
Most M nyilván a B-nek is nemnulla determinánsú, 3×3-as részmátrixa. (2 pont)
De 3×3-asnál nagyobb, nemnulla determinánsú, négyzetes részmátrix nyilván nem választható ki B-ből, hiszen ugyanez A-ból is kiválasztható volna, ellentmondásban $\mathrm{r}(A) = 3$-mal. (2 pont)
Mindezekből $\mathrm{r}(B) = 3$, vagyis az állítás igaz. (2 pont)

3. A 6×10-es A mátrixra $\mathrm{r}(A) = 3$. Mutassuk meg, hogy léteznek olyan $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_7 \in \mathbb{R}^{10}$ vektorok, amelyekre $\underline{v}_1, \underline{v}_2, \ldots, \underline{v}_7$ lineárisan független rendszert alkot és $A \cdot \underline{v}_1 = \underline{0}$, $A \cdot \underline{v}_2 = \underline{0}$, …, $A \cdot \underline{v}_7 = \underline{0}$ teljesül.

* * * * *

Legyen $f : \mathbb{R}^{10} \to \mathbb{R}^6$ az $\underline{x} \mapsto A \cdot \underline{x}$ lineáris leképezés (amelyre tehát $[f] = A$). (1 pont)
A tanultak szerint $\mathrm{Im}\, f$ az A oszlopainak (mint $\mathbb{R}^6$-beli vektoroknak) a generált altere. (1 pont)
A szintén az anyagban szerepelt tétel szerint $\mathrm{r}(A)$ az A oszlopai generált alterének a dimenziója. (1 pont)
Mindezekből tehát $\dim \mathrm{Im}\, f = \mathrm{r}(A) = 3$. (1 pont)
Ebből és a dimeziótételből $\dim \mathrm{Ker}\, f = 7$ következik. (1 pont)
Legyen ezért $\underline{v}_1, \ldots, \underline{v}_7$ a $\mathrm{Ker}\, f$ egy bázisa. (2 pont)
Ekkor $\underline{v}_1, \ldots, \underline{v}_7$ lineárisan független (hiszen bázis) (1 pont)
és $A \cdot \underline{v}_1 = f(\underline{v}_1) = \underline{0}, \ldots, A \cdot \underline{v}_7 = f(\underline{v}_7) = \underline{0}$ következik a $\mathrm{Ker}\, f$ definíciójából. (2 pont)

4. Az $f : \mathbb{R}^3 \to \mathbb{R}^3$ lineáris transzformáció $B = \{\underline{b}_1 = (1; 1; 0),\ \underline{b}_2 = (2; 0; 3),\ \underline{b}_3 = (0; 1; -2)\}$ bázis szerinti mátrixa az alábbi. Az $\mathbb{R}^3$ melyik elemét rendeli f a $2\underline{b}_1 - \underline{b}_2 + 3\underline{b}_3$ vektorhoz?

$$[f]_B = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

* * * * *

Első megoldás. A $\underline{v} = 2\underline{b}_1 - \underline{b}_2 + 3\underline{b}_3$ jelöléssel nyilván $[\underline{v}]_B = \begin{pmatrix} 2 \\ -1 \\ 3 \end{pmatrix}$. (2 pont)

Az $[f]_B$ definíciójából következik, hogy $[f(\underline{v})]_B = [f]_B \cdot [\underline{v}]_B$. (2 pont)

Elvégezve a szorzást: $[f(\underline{v})]_B = \begin{pmatrix} 1 \\ 5 \\ 2 \end{pmatrix}$. (1 pont)

A koordinátavektor definíciója szerint tehát $f(\underline{v}) = \underline{b}_1 + 5\underline{b}_2 + 2\underline{b}_3$. (3 pont)
Ebbe helyettesítve a $\underline{b}_1$, $\underline{b}_2$, $\underline{b}_3$ megadott értékeit: $f(\underline{v}) = (11; 3; 11)$. (2 pont)

Ha egy megoldó csak az $[f]_B \cdot (2;-1;3)^T$ szorzást végzi el és a kapott $(1;5;2)$-t hiszi végeredménynek, az (a fentiek szerint) megkaphatja a szorzásért járó 1 pontot; továbbá (esetleg részben) még a $[\underline{v}]_B$ felírásáért járó 2 pontot is, ha a megoldásból (például – de nem feltétlen – a $[\underline{v}]_B$ jelölés használata révén) kiderül, hogy a megoldó értve használta a koordinátavektor fogalmát. Ha azonban a megoldás csak ennyire szorítkozik, akkor 3-nál több pontot nem érhet. Igaz ez még akkor is, ha az $[f(\underline{v})]_B = [f]_B \cdot [\underline{v}]_B$ „képlet" szerepel a megoldásban, de alkalmazást nem nyer (az útmutató elején írtakkal összhangban). Ettől természetesen különbözik az az eset, ha egy megoldó eljut az $f(\underline{v}) = \underline{b}_1 + 5\underline{b}_2 + 2\underline{b}_3$ alak felírásáig, csak a $\underline{b}_1$, $\underline{b}_2$, $\underline{b}_3$ behelyettesítése marad el: ez a fentiek szerint 8 pontot érhet.

Az alábbi megoldás a fentinél jóval hosszadalmasabb, fölöslegesen sok számolást igényel. Csak azért szerepel a pontozási útmutatóban, hogy az ezt írók dolgozata egységesen értékelhető legyen.

Második megoldás.

A B bázisnak megfelelő $B = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 1 \\ 0 & 3 & -2 \end{pmatrix}$ mátrix inverze $B^{-1} = \begin{pmatrix} -3 & 4 & 2 \\ 2 & -2 & -1 \\ 3 & -3 & -2 \end{pmatrix}$, amit a tanult, Gauss-elimináción alapuló módszerrel határozhatunk meg. (2 pont)

A tanult tétel szerint $[f]_B = B^{-1} \cdot [f] \cdot B$. Ezt az összefüggést balról B-vel, jobbról B^{-1}-zel szorozva: $B \cdot [f]_B \cdot B^{-1} = [f]$. (2 pont)

Behelyettesítve B-t, $[f]_B$-t és B^{-1}-et az $[f] = \begin{pmatrix} -1 & 4 & 1 \\ 4 & -3 & -2 \\ -10 & 13 & 6 \end{pmatrix}$ mátrixot kapjuk. (2 pont)

A feladatbeli $\underline{v} = 2\underline{b}_1 - \underline{b}_2 + 3\underline{b}_3$ vektort kiszámítva: $\underline{v} = (0;5;-9)^T$. (1 pont)

$[f]$ definíciójából $f(\underline{v}) = [f] \cdot \underline{v}$. (2 pont)

A szorzást elvégezve a fentiekből $f(\underline{v}) = (11;3;11)$ (illetve ennek transzponáltja) adódik. (1 pont)

5. Adjuk meg a p paraméter értékét és az alábbi A mátrix egy sajátvektorát, ha tudjuk, hogy az 5 sajátértéke A-nak.

$$A = \begin{pmatrix} 3 & p \\ 1 & 4 \end{pmatrix}$$

* * * * *

Mivel az 5 sajátértéke A-nak, ezért a tanult tétel szerint $\det(A - 5E) = 0$, (1 pont)

vagyis $\begin{vmatrix} -2 & p \\ 1 & -1 \end{vmatrix} = 0$. (2 pont)

Ebből $(-1) \cdot (-2) - 1 \cdot p = 0$, vagyis $p = 2$. (2 pont)

Az 5-höz tartozó sajátvektorokat az $A \cdot \underline{x} = 5 \cdot \underline{x}$ (vagy az ezzel ekvivalens $(A - 5E) \cdot \underline{x} = \underline{0}$) lineáris egyenletrendszer megoldásával kereshetjük. (1 pont)

Ezt részletezve a $-2x_1 + 2x_2 = 0$, $x_1 - x_2 = 0$ egyenletrendszerre jutunk. (2 pont)

Ennek megoldása például $x_1 = x_2 = 1$, így az $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ vektor sajátvektora A-nak. (2 pont)

A $p = 2$ ismeretében természetesen nincs akadálya annak sem, hogy A minden sajátértékét és sajátvektorát meghatározzuk: az 5 sajátértékhez tartozó, a fenti megoldásban talált $(x, x)^T$ $(x \neq 0)$ sajátvektorokon kívül sajátérték még a 2 is, az ehhez tartozó sajátvektorok pedig a $(2x, -x)^T$ $(x \neq 0)$ alakú vektorok. Ezek bármelyike is elfogadható tehát jó eredményként, noha a 2 sajátérték meghatározása a megoldás szempontjából fölösleges munka. Megjegyezzük, hogy p és az 5-höz tartozó sajátvektorok meghatározása egyszerre is végezhető: $A \cdot \underline{x} = 5 \cdot \underline{x}$-ből a $-2x_1 + p \cdot x_2 = 0$, $x_1 - x_2 = 0$ egyenletrendszert kapjuk, amiből $x_1 = x_2$ behelyettesítésével a $(p-2)x_2 = 0$ egyenletet; ebből pedig $p = 2$, különben $x_2 = x_1 = 0$ adódna, így az 5 nem volna sajátérték.

6. Milyen maradékot adhat az n egész szám 142-vel osztva, ha $20n + 4$ és $72n - 12$ azonos maradékot ad 142-vel osztva?

* * * * *

A feladat szövege szerint $20n + 4 \equiv 72n - 12 \pmod{142}$, amit átrendezve az $52n \equiv 16 \pmod{142}$ lineáris kongruenciát kapjuk. (1 pont)

Mindkét oldalt 4-gyel osztva: $13n \equiv 4 \pmod{71}$, ahol a modulust $(4, 142) = 2$ miatt kellett 2-vel elosztani. (1 pont)

Mindkét oldalt 5-tel szorozva: $65n \equiv 20 \pmod{71}$, vagyis $-6n \equiv 20 \pmod{71}$. (1 pont)

Mindkét oldalt (-2)-vel osztva: $3n \equiv -10 \equiv 61 \pmod{71}$, ahol a modulus $(-2, 71) = 1$ miatt nem változott. (1 pont)

A jobb oldalhoz 71-et adva: $3n \equiv 132 \pmod{71}$, amiből 3-mal osztás után $n \equiv 44 \pmod{71}$ (és a modulus $(3, 71) = 1$ miatt nem változott). (1 pont)

Minden megtett lépés ekvivalens lépés volt – beleértve az 5-tel való szorzást is, $(5, 71) = 1$ miatt. Ezért a kapott eredmények valóban megoldásai a lineáris kongruenciának. (3 pont)

Ebből végül $n \equiv 44 \pmod{142}$ vagy $n \equiv 115 \pmod{142}$, vagyis az n egész 44 vagy 115 maradékot adhat 142-vel osztva. (2 pont)

A lépések ekvivalenciája helyett hivatkozhatunk arra is, hogy $(52, 142) = 2$ miatt két megoldás kell legyen modulo 142, vagy akár ellenőrizhetjük is a kapott eredményeket. (Viszont a három érv közül valamelyikre szükség van annak annak kizárásához, hogy a kapott eredmények között hamis gyök lehessen.) Ha egy megoldó csak azt ellenőrzi, hogy $(52, 142) = 2 \mid 16$, így a lineáris kongruenciának két megoldása van modulo 142, de ezeket kiszámolni nem tudja, az (az átrendezéssel együtt) összesen 3 pontot kapjon. Számolási hibákért 1-1 pont vonandó le, de a maradék pontszám csak akkor jár, ha a hiba miatt a feladat nem lett lényegesen könnyebb. A lineáris kongruenciának természetesen számos más, jó megoldása is van – például a fenti megoldásban szereplő 5-tel való szorzás helyett akár 6-tal, akár 7-tel szorozva is célhoz érhetünk.