1. Bevezetés

Ez a cikk nem könnyű olvasmány. Meg szeretnénk mutatni, hogy a mélyebb matematikai háttér hogyan segíthet egy probléma elemzésében. Ehhez képet kell adnunk magáról a háttérről, ami nem egyszerű, mert ezek a fogalmak és tételek matematikai érettséget igényelnek, tipikusan az egyetemi tananyagban szerepelnek. Egy olimpiai feladat jó alkalmat kínál az első randevúra, még ha a komolyabb ismerkedés későbbre marad is. A 2017-es Matematikai Diákolimpia hatodik feladata a következő volt.

1.1. feladat. *Egy egész számokból álló (x, y) rendezett párt primitív rácspontnak nevezünk, ha x és y legnagyobb közös osztója 1. Ha adott primitív rácspontok egy véges S halmaza, bizonyítsuk be, hogy van olyan n pozitív egész, és vannak olyan $z_0, z_1, \ldots, z_n$ egészek, hogy minden (x, y) S-beli pontra teljesül*

$$z_0x^n + z_1x^{n-1}y + z_2x^{n-2}y^2 + \ldots + z_{n-1}xy^{n-1} + z_ny^n = 1.$$

A sokféle lehetséges megközelítés egyike a következő. Legyenek az S halmaz elemei az $(a_1, b_1), \ldots, (a_k, b_k)$ párok. Tekintsük a következő oszlopvektorokat:

$$\mathbf{v}_j = \begin{bmatrix} a_1^j b_1^{n-j} \\ \ldots \\ a_k^j b_k^{n-j} \end{bmatrix} \qquad j = 0, \ldots, n.$$

A kérdés az, hogy előáll-e a konstans 1 oszlopvektor a $\mathbf{v}_0, \ldots, \mathbf{v}_n$ vektorok egész együtthatós lineáris kombinációjaként. (Az n számot mi választhatjuk.)

Fölmerülnek további kérdések is. Mely n számok lesznek jók? Miért pont a konstans 1 vektor szerepel a jobb oldalon? Meg tudjuk-e határozni, hogy általában mely vektorok állnak elő ilyen lineáris kombinációként? Előfordulhat-e, hogy az összes egész koordinátájú vektor előáll? Az egész vektorok hány százaléka áll így elő?

Ezek a lineáris kombinációk egy *rácsot* alkotnak. Az alábbiakban algebrai és geometriai módszerekkel is vizsgáljuk majd a hasonló rácsokat, és megválaszoljuk a fenti kérdéseket. Speciálisan a feladat állítását is belátjuk.

A rácsokat rengeteg helyen alkalmazzák a matematikában. A legsűrűbb faültetés feladata háromszögráccsal oldható meg. Minkowski rácsgeometriai tételének egy számelméleti alkalmazását mi is fölidézzük a 6. szakaszban. Ugyancsak rácsokat használ a Lenstra–Lenstra–Lovász algoritmus (lásd [5]) polinomok szorzatra bontására. A sík rácsairól Erdős Pál és Surányi János [1] könyvében olvashatunk bevezetőt.

Köszönetet mondunk *Gróf Andreának* és *Moussong Gábornak* értékes tanácsaikért.

2. Az előismeretek összefoglalása

Számelméletből Freud Róbert és Gyarmati Edit [3] tankönyvét érdemes tanulmányozni. Feltételezzük, hogy az Olvasó tud bánni kongruenciákkal, ismeri a mod m számolás fogalmát, az Euler–Fermat-tételt, és azt a tényt, hogy egész számok legnagyobb közös osztója fölírható e számok egész együtthatós lineáris kombinációjaként.

2.1. Lineáris algebra. Ismertnek tételezzük föl Freud Róbert [2] tankönyvének első fejezetei alapján a valós számok fölötti vektorok, mátrixok és determinánsok alaptulajdonságait (lineáris függetlenség, rang, bázis, előjeles aldeterminánsok, kifejtés és ferde kifejtés, mátrixműveletek, az inverz mátrix képlete, Vandermonde-determináns). A determinánsokra vonatkozó eredmények akkor is érvényesek, ha a determináns elemei nem számok, hanem például polinomok, hiszen minden számolás ugyanaz, és polinomokból törteket is képezhetünk. Ha p prímszám, akkor mod p számolva is érvényben maradnak a determinánsról tanult állítások.

Most determinánsok Laplace-kifejtését, és a Cauchy–Binet formulákat idézzük föl. A bizonyítások elolvashatók Kiss Emil honlapján[1]. (Ugyanebben a dokumentumban mátrixok invertálására is található egy gyors, eliminációs eljárás.) Legyen M egy $k \times n$-es mátrix. Az M egy $r \times r$-es aldeterminánsán azt értjük, hogy kiválasztunk r sort és oszlopot, és vesszük az ezek metszéspontjaiban álló elemek alkotta mátrix determinánsát. Ha a sorok, illetve oszlopok indexei $I = \{i_1, \ldots, i_r\}$ és $J = \{j_1, \ldots, j_r\}$, akkor a kapott aldeterminánsjele $M_{I,J}$, a hozzá tartozó előjel $\mathrm{sg}(I, J) = (-1)^{i_1+\ldots+i_r+j_1+\ldots+j_r}$.

2.1. tétel. *Legyen M egy $k \times k$-as mátrix. Rögzítsük az r elemű $I \subseteq \{1, 2, \ldots, k\}$ halmazt tetszőlegesen, és jelölje I' az I komplementumát az $\{1, 2, \ldots, k\}$ halmazra nézve. Ekkor az M determinánsának* Laplace-féle kifejtése *(ahol az összegzés az oszlopok r elemű J részhalmazaira terjed ki, tehát $\binom{k}{r}$ tag van):*

$$\det(M) = \sum_J \mathrm{sg}(I, J) M_{I,J} M_{I',J'}.$$

[1] ewkiss.web.elte.hu/wp/wordpress/wp-content/uploads/2014/11/inv_CB_Laplace.pdf.

2.2. tétel. *Legyen az M mátrix $m \times k$-as, az N pedig $k \times n$-es (hogy összeszorozhatóak legyenek) és $K = MN$. Rögzítsük az r elemű $I \subseteq \{1, 2, \ldots, m\}$ és $J \subseteq \{1, 2, \ldots, n\}$ részhalmazokat. Ekkor a* Cauchy–Binet-formula *a következő* ($|S|$ *az S elemszáma*) :

$$K_{I,J} = \sum_{S \subseteq \{1,2,\ldots,k\},\ |S|=r} M_{I,S} N_{S,J}.$$

2.2. Mátrix normálalakja. A [4] könyv 7.4.5. lemmáját ismertetjük. Legyen M egész elemű mátrix, melynek k sora és n oszlopa van, azaz $M \in \mathbb{Z}^{k \times n}$. A következő lépéseket engedjük meg.

(1) Egy oszlopból egy másik oszlop egész számszorosának levonása.
(2) Két oszlop cseréje.
(3) Egy sorból egy másik sor egész számszorosának levonása.
(4) Két sor cseréje.

2.3. tétel. *A fenti négyféle átalakítás alkalmas sorozatával M a következő* normálalakra *hozható. A mátrix főátlójában álló $s_1, s_2, \ldots, s_k$ számok sorban egymás osztói (lehetséges, hogy egy idő után mindegyik nulla), és a mátrix többi eleme nulla. Az s_i számok előjel erejéig egyértelműen meg vannak határozva, és föltehető, hogy $s_i \geq 0$.*

Ha $n < k$, akkor legyen $s_{n+1} = \ldots = s_k = 0$, azaz a főátlót kiegészítjük nulla elemekkel. A bizonyítás ki is található, maradékos osztással kell kombinálni a Gauss-eliminációt, és arra törekedni, hogy a mátrix bal fölső sarkába kerülő szám az összes többinek osztója legyen. Az egyértelműségi állítást most bebizonyítjuk.

2.4. definíció. Az M mátrix m-edik *determinánsosztója* az $m \times m$ méretű aldeterminánsainak a legnagyobb (nemnegatív) közös osztója, jele Δ_m. Legyen $\Delta_0 = 1$. (Nyilván M (determináns)rangja a legnagyobb olyan r, melyre $\Delta_r \neq 0$.)

2.5. lemma. *Ha $m \leq \ell$, akkor $\Delta_m \mid \Delta_\ell$.*

Bizonyítás. A Laplace-kifejtés (2.1. tétel) miatt mindegyik $\ell \times \ell$ méretű aldeterminánsa előáll $m \times m$-es aldeterminánsok egész együtthatós lineáris kombinációjaként. □

2.6. lemma. *A* 2.3. *tételbeli átalakítások a determinánsosztókon nem változtatnak.*

Bizonyítás. A cserére vonatkozó állítás nyilvánvaló. Adjuk az i-edik sor t-szeresét a j-edik sorhoz, az így módosított mátrixot jelölje M'. Csak azok az $m \times m$-es aldeterminánsok változhatnak meg, amelyeken a j-edik sor áthalad, de az i-edik sor nem. Legyen N ilyen aldeterminánsa M-nek, N' a módosított M' mátrix megfelelő aldeterminánsa, K pedig az a determináns, amit N-ből úgy kapunk, hogy a j-edik sorába beírjuk az M mátrix i-edik sorának a megfelelő oszlopokba eső részét.

A K sorait átrendezhetjük úgy, hogy M egy $m \times m$-es aldeterminánsát kapjuk. Ez maximum előjelváltással jár, tehát ha Δ jelöli az M mátrix m-edik determinánsosztóját, akkor $\Delta \mid \det(N), \det(K)$. Ezért $\Delta \mid \det(N') = \det(N) + t \det(K)$. Beláttuk tehát, hogy az M' mátrix m-edik Δ' determinánsosztója többese Δ-nak. Mivel az átalakítást visszafelé végezve ugyanolyan típusú átalakítást kapunk (a j-edik sorhoz az i-edik sor $-t$-szeresét kell adni ahhoz, hogy M'-ből M-et kapjuk), ezért $\Delta = \Delta'$. □

Egy normálalakú mátrix m-edik determinánsosztója nyilvánvalóan $s_1 s_2 \ldots s_m$. Így $s_m = \Delta_m / \Delta_{m-1}$, ahol Δ_m az eredeti M mátrix m-edik determinánsosztója. Ez a képlet működik, amíg $\Delta_{m-1} \neq 0$. Ha r a legnagyobb, melyre $\Delta_r \neq 0$ (azaz M rangja r), akkor a képlet szerint $s_{r+1} = 0$, és így $i > r$ esetén is $s_i = 0$, hiszen $s_{r+1} \mid s_i$.

3. Rácsok bázisa és indexe

3.1. Két példa. A kockás papíron látható „rács” az egész koordinátájú pontok A halmaza a síkon. Az origóból a rácspontokba mutató vektorok *csoportot* alkotnak. Ez azt jelenti, hogy bármely két rácsvektor összege és különbsége is benne van a rácsban. A rács *diszkrét* is: korlátos területre csak véges sok rácspont esik. A $\mathbf{b}_1 = (0, 1)$ és $\mathbf{b}_2 = (1, 0)$ vektorok *bázist* alkotnak: mindegyik rácsvektor egyértelműen előáll $z_1 \mathbf{b}_1 + z_2 \mathbf{b}_2$ alakban, ahol z_i egész számok (azaz a bázisvektorok egész együtthatós *lineáris kombinációjaként*). Bázist alkotnak a $\mathbf{c}_1 = (1, 1)$ és $\mathbf{c}_2 = (0, 1)$ vektorok is.

Forgassuk el az A rácsot az origó körül 45 fokkal, és nyújtsuk $\sqrt{2}$-szörösére. Ez is egy egész pontokból álló B rács (azaz B *részrácsa* A-nak), azokból a pontokból áll, melyeknek vagy mindkét koordinátája páros, vagy mindkét koordinátája páratlan. B is zárt az összeadásra és a kivonásra, azaz *részcsoport* A-ban. Ha B minden eleméhez hozzáadjuk a $\mathbf{v} = (0, 1)$ vektort (az így eltolt halmazt jelölje $\mathbf{v} + B$, ez egy *mellékosztály* A-ban B szerint), akkor az A-ra vett komplementer halmazt kapjuk, azokat a pontokat, melyeknek egyik koordinátája páros, a másik páratlan. Ha $\mathbf{w} \in B$, akkor $\mathbf{w} + B = B$, tehát B maga is mellékosztály. Az A rács tehát két B szerinti mellékosztály diszjunkt uniója. Azt fogjuk mondani, hogy B *indexe* A-ban 2. A B rácsban bázist alkot $\mathbf{d}_1 = (1, 1)$ és $\mathbf{d}_2 = (1, -1)$, de $\mathbf{e}_1 = (1, 1)$ és $\mathbf{e}_2 = (0, 2)$ is.

Vizsgáljuk meg, hogy e két rácsból hány rácspont esik egy adott területre, mondjuk a $(0, 0)$, $(0, n)$, $(n, 0)$, (n, n) csúcsú négyzetbe. E négyzetet azon (α_1, α_2) pontok halmazának képzeljük, melyekre $0 \leq \alpha_1, \alpha_2 < n$ (azaz a négy

csúcsból pontosan egyet tartalmaz). Az ide eső rácspontok száma tehát n^2, ami pontosan a négyzet területe. Ez nem is meglepő, hiszen a nagy négyzetet kiparkettázhatjuk n^2 egységnégyzettel (ezeket is úgy képzeljük, hogy a határuknak csak a bal és az alsó része tartozik hozzájuk). Minden ilyen kis négyzetben pontosan egy rácspont van.

A parkettázást elvégezhetjük a $\mathbf{c}_1$ és $\mathbf{c}_2$ vektorok által kifeszített P paralelogramma eltoltjaival is. Ennek a csúcsai $(0,0)$, $(1,1)$, $(0,1)$ és $(1,2)$. Ismét úgy tekintjük, hogy P az $\alpha_1\mathbf{c}_1+\alpha_2\mathbf{c}_2$ pontok halmaza, ahol $0\le\alpha_1,\alpha_2<1$. A P eltoltjai is hézagmentesen lefedik a síkot, és mindegyik eltolt pontosan egy rácspontot tartalmaz. A nagy négyzetből néhol kilógnak azok az eltoltak, amik a határhoz közel vannak, de könnyű látni, hogy a kilógó kis paralelogrammák száma elhanyagolható a többiéhez képest. Azoknak az eltoltaknak a száma, amelyek teljesen a nagy négyzetbe esnek, n^2-tel osztva 1-hez tart, ha n tart a végtelenhez. Ebből következik, hogy a kis paralelogramma területe 1 (ami persze nyilvánvaló, hiszen alapja és magassága is 1).

Ha a B ráccsal végezzük el ezt a számolást, akkor azt kapjuk, hogy a nagy négyzetben közel $n^2/2$ rácspont van, annak megfelelően, hogy a $(0,0)$, $(1,1)$ $(1,-1)$, $(2,0)$ négyzetnek és a $(0,0)$, $(1,1)$, $(0,2)$, $(1,3)$ paralelogrammának is 2 a területe. Mindkét paralelogrammába mindkét B szerinti mellékosztálynak egy-egy pontja esik. A két „alap"-paralelogramma területének hányadosa B indexe A-ban.

3.2. Alap-parallelotóp. Az eddigi példákat általánosítjuk. Az $\mathbb{R}^k$ tér P pontjait azonosítjuk az origóból a P-be vezető helyvektorral, azaz $\mathbb{R}^k$ oszlopvektoraival.

Az $\mathbb{R}^k$ összeadásra és kivonásra zárt, nem üres A részhalmazait *csoportnak* hívjuk (a csoport algebrai fogalma ennél általánosabb). Ha A minden elemének minden valós számszorosát is tartalmazza, akkor neve (valós) *altér.* Ilyen például egy origón átmenő egyenes vagy sík a térben. Az A *diszkrét,* ha $\mathbb{R}^k$ minden gömbje A-nak csak véges sok pontját tartalmazza. Az $\mathbb{R}^k$ *rácsának* az olyan diszkrét csoportokat nevezzük, melyekben van k lineárisan független vektor.

Altérre úgy kaphatunk példát, hogy veszünk $\mathbf{v}_1,\dots,\mathbf{v}_n$ vektorokat, és tekintjük az összes $\lambda_1\mathbf{v}_1+\ldots+\lambda_n\mathbf{v}_n$ alakú lineáris kombinációk halmazát, ahol λ_i tetszőleges valós számok; ez a $\mathbf{v}_1,\dots,\mathbf{v}_n$ által *generált* altér. Ha mindegyik λ_i egész szám, akkor az általuk generált csoportot kapjuk. *Ha tehát generált altérről beszélünk, akkor valós együtthatós lineáris kombinációkra gondolunk, ha generált csoportról vagy rácsról, akkor az együtthatók egészek.* Ha vektoraink függetlenek is (ekkor szükségképpen $n\le k$), akkor a kombinációk együtthatói egyértelműen meghatározottak, és az altér, illetve a csoport *bázisát* kapjuk. A bázis elemszáma az altér *dimenziója,* illetve a csoport *rangja.* Belátjuk majd, hogy minden rácsnak van bázisa.

3.1. definíció. Legyenek $\mathbf{v}_1,\dots,\mathbf{v}_k$ függetlenek. Az általuk *kifeszített P parallelotóp* az $\alpha_1\mathbf{v}_1+\ldots+\alpha_k\mathbf{v}_k$ alakú pontok halmaza, ahol $1\le i\le k$ esetén $0\le\alpha_i<1$. Ez a $\mathbf{v}_1,\dots,\mathbf{v}_k$ által generált B rács (egyik) *alap-parallelotópja.* Tehát az alap-parallelotópokat B egy-egy bázisának vektorai feszítik ki.

Magasabb dimenzióban a térfogat fogalmát intuitív módon használjuk. A parallelotópok térfogata alapszor magasság, ahol az alap „területe" az eggyel alacsonyabb dimenziós térfogatot jelenti. A k-dimenziós térfogat fogalmának fölépítése történhet determinánsok segítségével, lásd [2], 9.8. szakasz. Mindenképpen igaz a következő.

3.2. tétel. *A $\mathbf{v}_1,\dots,\mathbf{v}_k\in\mathbb{R}^k$ vektorok által kifeszített parallelotóp térfogata egyenlő a $[\mathbf{v}_1,\dots,\mathbf{v}_k]$ mátrix determinánsának abszolút értékével. (E determináns előjele a $\mathbf{v}_1,\dots,\mathbf{v}_k$ rendszer úgynevezett irányítását adja meg.)*

Legyen P a B rács egyik alap-parallelotópja. A P-nek a $\mathbf{v}\in B$ vektorokkal vett $\mathbf{v}+P$ eltoltjai hézagmentesen kitöltik az $\mathbb{R}^k$ teret. Minden ilyen $\mathbf{v}+P$ eltoltban pontosan egy eleme van B-nek: maga a $\mathbf{v}$ vektor. Ezért az előző szakaszban, a konkrét példák esetében látott gondolatmenet általában azt adja, hogy ha veszünk egy R sugarú G gömböt, akkor a G térfogata elosztva a G-be eső B-beli pontok számával a P parallelotóp térfogatához tart, midőn R tart a végtelenhez.

Legyen most A tetszőleges olyan rács, amely B-t tartalmazza. Bármely $\mathbf{v}\in B$ esetén a $\mathbf{v}$ vektorral való eltolás az A és B rácsokat önmagukba viszi. Ezért ha a P parallelotópba az A rácsnak d pontja esik (a d véges szám, hiszen A diszkrét), akkor ugyanez igaz mindegyik $\mathbf{v}+P$ eltoltra is. Emiatt ha a fenti G gömb térfogatát a G-be eső A-beli rácspontok számával osztjuk, akkor ez a hányados a P parallelotóp térfogatának $1/d$-szereséhez tart, midőn R tart a végtelenhez.

3.3. állítás. *Ha $\mathbf{u},\mathbf{w}\in A$, akkor a $\mathbf{w}+B$ halmazt (az egyik) B szerinti* mellékosztálynak *hívjuk. Az $\mathbf{u}+B$ és $\mathbf{w}+B$ mellékosztályok vagy egyenlők, vagy diszjunktak; akkor egyenlők, ha $\mathbf{u}-\mathbf{w}\in B$. Ezért A a B szerinti mellékosztályok (diszjunkt) uniója. A mellékosztályok száma a B részcsoport A-beli* indexe, *jele $|A:B|$.*

A könnyű bizonyítást az Olvasóra hagyjuk. Az általános, csoportokra vonatkozó eset bizonyítása megtalálható a [4] könyv 4.4. szakaszában.

A 3.1. definíció jelöléseit használva

$$\mathbf{u}=\gamma_1\mathbf{v}_1+\ldots+\gamma_k\mathbf{v}_k\quad\text{és}\quad\mathbf{w}=\delta_1\mathbf{v}_1+\ldots+\delta_k\mathbf{v}_k$$

akkor esnek ugyanabba a B szerinti mellékosztályba, ha $\gamma_i-\delta_i$ egészek. Ezért $\mathbf{u}+B$-nek egyetlen $\mathbf{w}$ vektora esik P-be: amikor δ_i a γ_i törtrésze. Azaz P minden B szerinti mellékosztályból pontosan egy vektort tartalmaz, és így $|A:B|=d$.

Ha A-nak is van bázisa, és így egy Q alap-parallelotópja is, akkor persze G térfogata elosztva a G-be eső A-beli pontok számával Q térfogatához tart. Ezért beláttuk az alábbi tétel második állítását azzal a föltevéssel, hogy A-ban és B-ben is van bázis.

3.4. tétel. *Minden rácsnak van bázisa. Ha B részrácsa A-nak, akkor B indexe A-ban a B és A alap-parallelotópjai térfogatának hányadosa (a kisebbik rácsban nagyobb ez a térfogat). Speciálisan A bármely két alap-parallelotópjának a térfogata egyenlő.*

Bizonyítás. A tétel első állításának bizonyításához legyen A rács és $\mathbf{v}_1, \ldots, \mathbf{v}_k$ független vektorok A-ban. Essen d darab A-beli pont a $\mathbf{v}_1, \ldots, \mathbf{v}_k$ által kifeszített P parallelotópba. Ha van ezek között egy $0 \neq \mathbf{v} = \alpha_1\mathbf{v}_1 + \ldots + \alpha_k\mathbf{v}_k$, akkor válasszunk egy olyan i indexet, amelyre $\alpha_i \neq 0$. A $\mathbf{v}_i$ helyére $\mathbf{v}$-t téve a kapott parallelotóp térfogata kisebb lesz, mint az eredetié volt, annak α_i-szeresére változik. Ezt érdemes a síkon vagy a térben elképzelni (a magasság α_i-szeresére csökken), de algebrailag is könnyű megmutatni determinánsok segítségével. Az eljárást folytatva egy olyan vektorrendszert találunk A-ban, amelyre már $d = 1$, vagyis a P-be eső egyetlen A-beli pont az origó. De akkor a $\mathbf{v}_1, \ldots, \mathbf{v}_k$ generálta B rács maga A. Valóban, A minden $\mathbf{u}$ eleme beleesik valamelyik $\mathbf{v} + P$ eltoltba, ahol $\mathbf{v} \in B$. Ebben az eltoltban az egyetlen A-beli pont az $\mathbf{u}$, ezért $\mathbf{u} = \mathbf{v} \in B$. □

3.5. feladat. *Legyen $d = |A : B|$. Igazoljuk, hogy minden $\mathbf{u} \in A$-ra $d\mathbf{u} \in B$.*

Útmutatás. Vegyünk ki mindegyik B szerinti mellékosztályból egy-egy $\mathbf{u}_i$ vektort. Ekkor $\mathbf{u}+\mathbf{u}_i$ is csupa különböző mellékosztályban van, tehát mindegyik mellékosztályba egy ilyen vektor esik. Ezért $\mathbf{u}_1+\ldots+\mathbf{u}_d$ és $(\mathbf{u}+\mathbf{u}_1)+\ldots+(\mathbf{u}+\mathbf{u}_d)$ ugyanabban a mellékosztályban vannak. Különbségük $d\mathbf{u}$. □

3.6. feladat. *Legyenek $B \subseteq A$ részrácsai $\mathbb{Z}^k$-nak. Mutassuk meg, hogy a $|\mathbb{Z}^k : A|$ index osztja a $|\mathbb{Z}^k : B|$ indexet.*

Útmutatás. B alap-parallelotópjának mindegyik eltoltjába A-nak $|A : B|$ darab pontja esik. Ezért minden elég nagy gömbben A-nak körülbelül $|A : B|$-szer annyi pontja van, mint B-nek. Ugyanez A és $\mathbb{Z}^k$, valamint B és $\mathbb{Z}^k$ viszonylatában is elmondható. □

Ha az Olvasó e két feladat mélyebb algebrai hátterére kíváncsi, lapozza föl a [4] könyv negyedik fejezetében Lagrange tételét és a faktorcsoport fogalmát.

3.3. Részrács bázisa. A 3.1. szakaszban vizsgált mindkét példában kétféle alap-paralelogrammát láttunk. Választhatunk úgy, hogy a B rács alap-paralelogrammája kiparkettázható legyen az A rács alap-paralelogrammájának eltoltjaival: vegyük B-ben a $(0,0)$, $(1,1)$, $(0,2)$, $(1,3)$ csúcsú paralelogrammát, A-ban pedig ennek az „alsó felét”, a $(0,0)$, $(1,1)$, $(0,1)$, $(1,2)$ csúcsút. Vagyis A-ban a $\mathbf{c}_1 = (1,1)$ és $\mathbf{c}_2 = (0,1)$ bázist, B-ben a $\mathbf{c}_1$ és $2\mathbf{c}_2$ bázist tekintjük. Ebből is azonnal látszik, hogy az $|A : B|$ index 2. Igen erős tétel, a későbbiek alapja, hogy ezt általában is meg lehet tenni.

3.7. tétel. *Ha B részrácsa A-nak, akkor választhatunk olyan P és Q alap-parallelotópot A-ban, illetve B-ben, hogy P eltoltjaival Q kiparkettázható. Azaz van olyan $\mathbf{c}_1, \ldots, \mathbf{c}_k$ bázisa A-nak, hogy alkalmas $s_1, s_2, \ldots, s_k$ pozitív egészekre $s_1\mathbf{c}_1, \ldots, s_k\mathbf{c}_k$ bázis B-ben. Ekkor $|A : B| = s_1 \cdot \ldots \cdot s_k$. A két bázis úgy is választható, hogy az $s_1 \mid s_2 \mid \ldots \mid s_k$ oszthatóság is teljesüljön.*

Geometriailag világos, hogy $|A : B| = s_1 \cdot \ldots \cdot s_k$. Az algebrai bizonyításhoz vegyük észre, hogy $x_1\mathbf{c}_1 + \ldots + x_k\mathbf{c}_k$ és $y_1\mathbf{c}_1 + \ldots + y_k\mathbf{c}_k$ akkor vannak ugyanabban a mellékosztályban B szerint, ha $x_j \equiv y_j \ (s_j)$ minden j-re. Ezért mindegyik mellékosztály pontosan egyet tartalmaz azon $z_1\mathbf{c}_1 + \ldots + z_k\mathbf{c}_k$ vektorok közül, melyekre $0 \leq z_j < s_j$.

A $\mathbf{c}_i$ bázis létezését általánosabban bizonyítjuk. Láttuk, hogy B-nek van bázisa, azaz k vektorral generálható. Az általánosítás az, hogy több generátort is megengedünk, és azt sem tesszük föl, hogy van közöttük k független.

Ha A-nak vesszük egy bázisát, akkor B elemeit eleve ezek lineáris kombinációiként írhatjuk föl. Ezért nem veszítünk az általánosságból, ha az $A = \mathbb{Z}^k$ esetet tekintjük.

3.8. tétel. *Legyen $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{Z}^k$ és B az általuk generált csoport. Hozzuk normálalakra az $M = [\mathbf{v}_1, \ldots, \mathbf{v}_n]$ mátrixot a 2.3. tétel értelmében, és jelölje $s_1 \mid s_2 \mid \ldots \mid s_k$ a főátlóban szereplő számokat. Tudjuk, hogy az M mátrix r-edik determinánsosztója $s_1 \cdot \ldots \cdot s_r$. Ha M rangja r, akkor a következők teljesülnek.*

(1) *Van $\mathbb{Z}^k$-nak olyan $\mathbf{c}_1, \ldots, \mathbf{c}_k$ bázisa, hogy $s_1\mathbf{c}_1, \ldots, s_r\mathbf{c}_r$ bázis B-ben.*

(2) *Ha $r = k$, akkor B rács és $|\mathbb{Z}^k : B| = s_1 \cdot \ldots \cdot s_k$.*

Bizonyítás. Kiindulunk a B csoport $\mathbf{w}_1 = \mathbf{v}_1, \ldots, \mathbf{w}_n = \mathbf{v}_n$ generátorrendszeréből és $\mathbb{Z}^k$-nak a „szokásos” $\mathbf{b}_1 = \mathbf{e}_1, \ldots, \mathbf{b}_k = \mathbf{e}_k$ bázisából, amelyben az $\mathbf{e}_i$ vektor i-edik koordinátája 1, a többi nulla. Az M-et normálalakra hozó négyféle lépés során változtatjuk majd a $\mathbf{w}_j$ generátorrendszert és a $\mathbf{b}_i$ bázist is, úgy, hogy B ne változzon.

Egy közbülső állapotban jelölje a mátrix i-edik sorának j-edik elemét n_{ij}. A kinduló állapotban nyilván $\mathbf{w}_j = n_{1j}\mathbf{b}_1 + \ldots + n_{kj}\mathbf{b}_k$. Minden lépés végrehajtása után ezzel a képlettel fogjuk definiálni az új $\mathbf{w}_j$ generátorrendszert.

Ha kicseréljük a j-edik és a j'-edik oszlopot, akkor $\mathbf{w}_j$ és $\mathbf{w}_{j'}$ helyet cserél, de B nem változik. Ha az i-edik és i'-edik sort cseréljük, de kicseréljük a $\mathbf{b}_i$ és $\mathbf{b}_{i'}$ bázisvektorokat is, akkor egyik $\mathbf{w}_j$ sem változik, és így B sem.

Ha a j'-edik oszlop t-szeresét adjuk a j-edik oszlophoz, akkor $\mathbf{w}_j$ helyén $\mathbf{w}_j + t\mathbf{w}_{j'}$ fog állni. Mivel $\mathbf{w}_j + t\mathbf{w}_{j'} \in B$, az új vektorok B-nek egy részét generálják. De ez az átalakítás megfordítható (az új j-edik oszlopból kell kivonni a j'-edik oszlop t-szeresét), ezért B most sem változik.

Végül adjuk az i'-edik sor t-szeresét az i-edik sorhoz. Az egyszerűbb tipográfia érdekében legyen $i = 1$ és $i' = 2$. Ekkor

$$\mathbf{w}_j = n_{1j}\mathbf{b}_1 + n_{2j}\mathbf{b}_2 + \ldots + n_{kj}\mathbf{b}_k = (n_{1j} + tn_{2j})\mathbf{b}_1 + n_{2j}(\mathbf{b}_2 - t\mathbf{b}_1) + \ldots + n_{kj}\mathbf{b}_k.$$

Ezért ha $\mathbf{b}_2$-t $(\mathbf{b}_2 - t\mathbf{b}_1)$-re változtatjuk, akkor $\mathbf{w}_j$ nem változik. Az Olvasóra bízzuk annak ellenőrzését, hogy az így kapott új rendszer is bázis $\mathbb{Z}^k$-ban (azaz független, és egész együtthatókkal fölírható vele $\mathbb{Z}^k$ minden vektora).

A végső állapotban, amikor M normálalakú, legyen $\mathbf{c}_i = \mathbf{b}_i$. Ekkor $\mathbf{w}_j = s_j\mathbf{c}_j$ ha $j \le k$ és $\mathbf{w}_j = \mathbf{0}$, ha $j > k$, és így az $s_j\mathbf{c}_j$ vektorok generálják B-t. A 2.6. lemma szerint menet közben nem változnak meg a determinánsosztók, és így a rang sem. Tehát az s_i számok közül az első r lesz nem nulla, és így $s_1\mathbf{c}_1, \ldots, s_r\mathbf{c}_r$ függetlenek is. □

3.9. következmény. *Legyenek $\mathbf{b}_1, \ldots, \mathbf{b}_r \in \mathbb{Z}^k$ lineárisan független vektorok ($r \ge 1$) és B az általuk generált csoport. Ekkor az alábbi állítások ekvivalensek.*

(1) *$\mathbf{b}_1, \ldots, \mathbf{b}_r$ kiegészíthető $\mathbb{Z}^k$ egy bázisává.*

(2) *Ha $m \ne 0$ egész, $\mathbf{v} \in \mathbb{Z}^k$ és $m\mathbf{v} \in B$, akkor $\mathbf{v} \in B$.*

(3) *A $[\mathbf{b}_1, \ldots, \mathbf{b}_r]$ mátrix r-edik determinánsosztója* 1.

(4) *A $[\mathbf{b}_1, \ldots, \mathbf{b}_r]$ mátrix alaptételbeli alakjában a főátló mindegyik eleme* 1.

Speciálisan $\mathbf{v} \in \mathbb{Z}^k$ pontosan akkor van benne $\mathbb{Z}^k$ egy bázisában, ha primitív, *azaz a komponenseinek a legnagyobb közös osztója* 1.

Bizonyítás. Tegyük föl, hogy létezik az (1)-ben megkövetelt $\mathbf{b}_1, \ldots, \mathbf{b}_k$ bázis. Ha $\mathbf{v} = z_1\mathbf{b}_1 + \ldots + z_k\mathbf{b}_k$, akkor $m\mathbf{v}$ pontosan akkor van B-ben, ha $z_j = 0$ minden $j > r$ indexre. De akkor $\mathbf{v} = z_1\mathbf{b}_1 + \ldots + z_r\mathbf{b}_r \in B$. Ezért (2) teljesül.

Alkalmazzuk $M = [\mathbf{b}_1, \ldots, \mathbf{b}_r]$-re az előző tételt. Ha a (2) pontban megadott feltétel teljesül, akkor $s_i\mathbf{c}_i \in B$-ből $\mathbf{c}_i \in B$, azaz $s_i = 1$ következik. Az r-edik determinánsosztó $s_1 \cdot \ldots \cdot s_r$, ami pontosan akkor 1, ha mindegyik $s_i = 1$.

Végül, ha $i \le r$ esetén $s_i = 1$, akkor nemcsak $\mathbf{b}_1, \ldots, \mathbf{b}_r$, hanem $\mathbf{c}_1, \ldots, \mathbf{c}_r$ is bázisa B-nek. Tehát $\mathbb{Z}^k$ minden eleme $\mathbf{b}_1, \ldots, \mathbf{b}_r, \mathbf{c}_{r+1}, \ldots, \mathbf{c}_k$ egész együtthatós lineáris kombinációjaként is fölírható. Ez k vektor, és ezért bázis $\mathbb{Z}^k$-ban. □

3.10. feladat. *Igazoljuk a* 3.8. *tétel segítségével, hogy ha a $B \subseteq \mathbb{Z}^k$ rácsban nincs primitív vektor, akkor van olyan $m > 1$ egész, amellyel B minden eleme osztható.*

3.11. feladat. *Mutassuk meg a normálalak fölhasználása nélkül, hogy ha $M \in \mathbb{Z}^{k\times n}$ rangja k, akkor az M oszlopai által generált rács indexe $\mathbb{Z}^k$-ban az M mátrix k-adik determinánsosztója.*

Útmutatás. Legyen B az M oszlopai által generált rács és $\mathbf{b}_1, \ldots, \mathbf{b}_k$ bázis B-ben. Minden $\mathbf{v} \in B$ fölírható $z_1\mathbf{b}_1 + \ldots + z_k\mathbf{b}_k$ alakban. Jelölje $f(\mathbf{v})$ azt az (oszlop)vektort, melynek a z_i számok a komponensei. (Az f egy úgynevezett lineáris leképezés, ami átkoordinátázza B elemeit az új bázis szerint). Nyilván $\mathbf{v} = [\mathbf{b}_1, \ldots, \mathbf{b}_k]f(\mathbf{v})$.

Az M oszlopaira f-et alkalmazva egy K mátrixot kapunk. Mutassuk meg, hogy az M mátrix k-adik Δ determinánsosztója a K mátrix k-adik D determinánsosztójának $|d|$-szerese, ahol d a $[\mathbf{b}_1, \ldots, \mathbf{b}_k]$ mátrix determinánsa (vagyis $|d| = |\mathbb{Z}^k : B|$).

K oszlopai a teljes $\mathbb{Z}^k$ rácsot generálják, mert ha $\mathbf{w} = [z_1, \ldots, z_k]^T \in \mathbb{Z}^k$, akkor $\mathbf{v} = z_1\mathbf{b}_1 + \ldots + z_k\mathbf{b}_k \in B$ fölírható M oszlopai segítségével. Ugyanez mod p is igaz minden p prímre, és ezért K-t mod p véve rangja szükségképpen k. Így van olyan $k \times k$-as aldeterminánsa, ami nem osztható p-vel, azaz $p \nmid D$. Tehát $D = 1$. □

A cikk második részében az olimpiai feladat rácsát elemezzük, bemutatjuk Peter McMullen egy tételét ortogonális rácsokról, végül feladatok segítségével lehetőséget kínálunk az Olvasónak arra, hogy néhány eddigi állításra geometriai bizonyítást adjon.

Hivatkozások

[1] Erdős Pál, Surányi János: *Válogatott fejezetek a számelméletből.* Polygon Kiadó, 1996.

[2] Freud Róbert: *Lineáris Algebra.* ELTE Eötvös Kiadó, 2014.
www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_527_LinearisAlgebra

[3] Freud Róbert, Gyarmati Edit: *Számelmélet.* Nemzeti Tankönyvkiadó, 2006.
www.tankonyvtar.hu/hu/tartalom/tamop425/2011_0001_519_Szamelmelet

[4] Kiss Emil: *Bevezetés az algebrába.* TypoTEX Kiadó, 2007.
www.tankonyvtar.hu/hu/tartalom/tamop425/2011-0001-526_kiss_emil

[5] Radnai András: *Rácselmélet alkalmazása a számelméletben,* Szakdolgozat, ELTE, 2010.
web.cs.elte.hu/blobs/diplomamunkak/bsc_mat/2010/radnai_andras.pdf