4. Vandermonde-mátrixok

Most rátérünk az olimpiai feladatban szereplő rács vizsgálatára. Rögzítsünk (a_i, b_i) egész számpárokat $(1 \le i \le k)$, ahol a_i és b_i relatív prímek. Adott $n > 0$ esetén legyen M_n az az egész elemű, k sorból és $n+1$ oszlopból álló mátrix, amelyben az i-edik sor j-edik eleme $a_i^{n-j+1} b_i^{j-1}$ és A_n az M_n oszlopai által generált csoport.

4.1. Az M_n determinánsosztóinak meghatározása. Fölhasználjuk az egész együtthatós többváltozós polinomok számelméletét. Az alábbiak a [3] könyv második és harmadik fejezetéből megérthetők, különös tekintettel a 3.4. szakaszra.

4.1. tétel. *A $\mathbb{Z}[x_1, \dots, x_n]$ polinomjai között igaz a számelmélet alaptétele, azaz minden nullától és egységtől különböző polinom sorrendtől és egységszerestől eltekintve egyértelműen bontható irreducibilisek szorzatára. A prím és irreducibilis polinomok ugyanazok, és csak ± 1 egység. A $\mathbb{Z}$-beli prímszámok prímek $\mathbb{Z}[x_1, \dots, x_n]$-ben is.*

Egy polinom akkor *primitív,* ha együtthatóinak közös osztója csak egység lehet. Egy elsőfokú polinom nem feltétlenül irreducibilis, például $\mathbb{Z}[x]$-ben $2x$ nem az, hiszen a $2 \cdot x$ fölbontásban egyik tényező sem egység. Ha azonban primitív is, akkor már irreducibilis lesz, és egyben prímtulajdonságú. Ez akkor is igaz, ha az együtthatói nem egész számok, hanem egész együtthatós, akár többváltozós polinomok.

4.2. következmény. *A $\mathbb{Z}[x_1, \dots, x_n]$-beli $x_i x_j - x_k x_\ell$ polinom irreducibilis abban az esetben, ha i, j, k, ℓ páronként különböző. Két ilyen polinom különböző négyelemű indexhalmazok esetében biztosan nem egymás egységszerese.*

4.3. lemma. *Legyen a $k \times k$-as K mátrixban az i-edik sor j-edik eleme $x_i^{k-j} y_i^{j-1}$. Ekkor* $\det(K) = \prod_{1 \le i < j \le k} (x_i y_j - y_i x_j)$.

Bizonyítás. Képzeljük először azt, hogy x_i és y_i változók, így a determináns elemei $\mathbb{Z}[x_1, \dots, x_k, y_1, \dots, y_k]$-beli polinomok. Emeljünk ki a determináns i-edik sorából x_i^{k-1}-et mindegyik i-re (ez megtehető, mert $x_i \neq 0$). Az eredmény egy Vandermonde-determináns lesz az y_i/x_i generátorokkal, melynek értéke $\prod_{1 \le i < j \le k} \big((y_j/x_j) - (y_i/x_i)\big)$. A nevezőkkel szorozva az állítást kapjuk.

Így azonosságot kaptunk. Ha az x_i és y_i helyébe bármilyen számokat (sőt polinomokat, akár mod p maradékosztályokat) helyettesítünk, az egyenlőség e helyettesítés után is érvényben fog maradni. (Még akkor is, ha valamelyik x_i helyébe nullát írunk.) □

4.4. állítás. *Ha $n+1 \ge k$, akkor az M_n mátrix k-adik determinánsosztója*

$$\Delta = \prod_{1 \le i < j \le k} (a_i b_j - b_i a_j) = \det(M_{k-1}),$$

az n értékétől függetlenül. (Ha $k = 1$, akkor $\Delta = 1$, mint üres szorzat).

Bizonyítás. Legyen Δ_k az M_n mátrix k-adik determinánsosztója. Azt fogjuk megmutatni, hogy a Δ és Δ_k számok egymás osztói.

A $\Delta_k \mid \Delta$ bizonyításához legyenek x_i és y_i változók $(1 \le i \le n-k+1)$. Egészítsük ki az M_n mátrixot úgy, hogy az utolsó k sora maradjon az, ami eredetileg volt, az első $n-k+1$ sorában pedig az i-edik sor j-edik eleme legyen $x_i^{n-j+1} y_i^{j-1}$. A kapott négyzetes mátrix determinánsát a 4.3. lemma segítségével számíthatjuk ki. Az így adódó szorzatot bontsuk három részre: $P_1 P_2 P_3$, ahol

$$P_1 = \prod_{1 \le i < j \le n-k+1} (x_i y_j - y_i x_j). \tag{1}$$

$$P_2 = \prod (x_i b_j - y_i a_j), \quad \text{ahol} \quad 1 \le i \le n-k+1 \quad \text{és} \quad 1 \le j \le k. \tag{2}$$

$$P_3 = \prod_{1 \le i < j \le k} (a_i b_j - b_i a_j) = \Delta. \tag{3}$$

A Laplace-kifejtés (2.1. tétel) miatt a determináns $P_1 P_2 P_3$ értéke fölírható az M_n mátrix $k \times k$-as aldeterminánsainak olyan lineáris kombinációjaként, amelynek együtthatói $R = \mathbb{Z}[x_1, \dots, x_{n-k+1}, y_1, \dots, y_{n-k+1}]$-ből valók. Ezért R-ben a Δ_k szám osztója a $P_1 P_2 P_3 = P_1 P_2 \Delta$ szorzatnak.

Tegyük föl indirekt, hogy van olyan p prímszám, melynek Δ_k-beli kitevője nagyobb, mint a Δ-beli kitevője. Mivel R-ben igaz a számelmélet alaptétele, és p ebben is prímszám (4.1. tétel), ezért $p \mid P_1 P_2$. Tehát vagy $p \mid x_i y_j - y_i x_j$, vagy $p \mid x_i b_j - y_i a_j$ alkalmas i, j-re. Ez azonban lehetetlen, mert a_j és b_j relatív prímek, és így mindkét polinom primitív. Tehát tényleg $\Delta_k \mid \Delta$.

A fordított oszthatósághoz azt kell igazolnunk, hogy Δ osztója $\det(K)$-nak, ha K az M_n egy tetszőleges $k \times k$-as részmátrixa. Vegyünk föl u_i, v_i változókat $(1 \le i \le k)$, és írjuk föl az M_n mátrixot, valamint a Δ és $\det(K)$ számokat is a_i helyett u_i-vel és b_i helyett v_i-vel (azaz képzeljünk az a_i és b_i számok helyébe változókat). Nyilván elegendő az oszthatóságot ebben az esetben igazolni.

Rögzített $i<j$ mellett legyen $d=u_iv_j-v_iu_j$, és írjuk föl $\det(K)$ Laplace-kifejtését (2.1. tétel) arra az esetre, amikor a soroknak a kételemű $\{i,j\}$ indexhalmazát vesszük. Azt kapjuk, hogy $\det(K)$ előáll az i-edik és j-edik sorból képzett kétszer kettes aldeterminánsok lineáris kombinációjaként. Ezek a kétszer kettes aldeterminánsok mind oszthatók d-vel: ha a két oszlopindex $s<t$, akkor

$$\begin{vmatrix} u_i^{n-s+1}v_i^{s-1} & u_i^{n-t+1}v_i^{t-1} \\ u_j^{n-s+1}v_j^{s-1} & u_j^{n-t+1}v_j^{t-1} \end{vmatrix} = v_i^{s-1}u_i^{n-t+1}v_j^{s-1}u_j^{n-t+1} \begin{vmatrix} u_i^{t-s} & v_i^{t-s} \\ u_j^{t-s} & v_j^{t-s} \end{vmatrix},$$

és az $a-b \mid a^{t-s}-b^{t-s}$ szabály miatt $u_iv_j-v_iu_j \mid (u_iv_j)^{t-s}-(v_iu_j)^{t-s}$. Így $d \mid \det(K)$.

Beláttuk tehát, hogy $\det(K)$ osztható az $u_iv_j-v_iu_j$ mindegyikével. Ezek a polinomok azonban páronként relatív prímek a 4.2. következmény miatt. A számelmélet alaptétele miatt e polinomok szorzata, ami Δ, szintén osztója $\det(K)$-nak. □

4.5. feladat. *Számítsuk ki M_n összes determinánsosztóját.*

Útmutatás. Az a_i és a b_i relatív prímek, ezért $\Delta_1=1$. Ha $2\le r\le \min(k,n+1)$, akkor vegyük $\{1,\dots,k\}$ egy r elemű S részhalmazát, és álljon az M mátrix az M_n ennek megfelelő soraiból. A 4.4. lemma miatt az M mátrix $r\times r$-es aldeterminánsainak legnagyobb közös osztója azon $a_ib_j-b_ia_j$ számok Δ_S szorzata, amelyekre $i,j\in S$ és $i<j$. Az összes $r\times r$-es aldeterminánsa legnagyobb közös osztója tehát ezeknek a Δ_S számoknak a legnagyobb közös osztója. Így Δ_r sem függ az n választásától. □

4.2. Redukció prímhatvány modulusra. Egy vektort hívjunk s-sel oszthatónak, ha mindegyik komponense osztható s-sel. Az s-sel osztható vektorok halmazát jelölje $s\mathbb{Z}^k$. Azt mondjuk, hogy egy A csoport tartalmazza a $\mathbf{v}$ vektort mod s, ha $\mathbf{v}$ fölírható egy s-sel osztható és egy A-beli vektor összegeként, azaz $\mathbf{v}\in s\mathbb{Z}^k+A$.

4.6. lemma. *Legyen $A\subseteq\mathbb{Z}^k$ egy csoport, $\mathbf{v}\in\mathbb{Z}^k$ és s, t relatív prím egészek. Ha A tartalmazza $\mathbf{v}$-t* mod s *és* mod t*, akkor tartalmazza* mod st *is.*

Bizonyítás. Legyen $v=su+g=tw+h$, ahol $g,h\in A$ és $u,w\in\mathbb{Z}^k$. Mivel $(s,t)=1$, van olyan $e,f\in\mathbb{Z}$, hogy $se+tf=1$. Ekkor $v=sev+tfv=se(tw+h)+tf(su+g)=st(ew+fu)+(seh+tfg)\in st\mathbb{Z}^k+A$. □

Ha A indexe $\mathbb{Z}^k$-ban Δ, akkor a 3.5. feladat szerint minden Δ-val osztható vektor eleme A-nak. Ha tehát be akarjuk látni, hogy $\mathbf{v}\in A$, akkor elegendő megmutatni, hogy a Δ index minden q prímhatvány-osztója esetén $\mathbf{v}$ benne van A-ban mod q.

4.3. Az olimpiai feladat megoldása. Ha $d_{ij}=a_ib_j-b_ia_j=0$ valamilyen $i\ne j$ esetén, akkor, mivel a_i és b_i, valamint a_j és b_j relatív prímek, csak az lehetséges, hogy (a_i,b_i) és (a_j,b_j) egyenlők vagy ellentettek. Az első esetben (a_j,b_j) elhagyható. A második esetben szintén, ha az n kitevőt párosnak választjuk (erre majd ügyelünk). Ezért a továbbiakban föltesszük, hogy d_{ij} soha nem nulla, és azt is, hogy $n\ge k-1$. Az M_n által generált A_n ekkor rács, hiszen a k-adik determinánsosztó a 4.4. állításban definiált Δ szám, ami nem nulla. Az A_n indexe tehát Δ, az n-től függetlenül.

4.7. lemma. *Legyen $q=p^m$, ahol p prím és $m\ge 1$. Tegyük föl, hogy az n szám osztható $2\varphi(q)$-val, és nagyobb vagy egyenlő, mint $2m$ és $k-1$. Ekkor A_n tartalmazza a konstans 1 vektort* mod q.

Bizonyítás. Ha $p\nmid a_i$, akkor az Euler–Fermat-tétel és $\varphi(q)\mid(n/2)$ miatt $a_i^{n/2}\equiv 1\ (q)$. Ha $p\mid a_i$, akkor $n/2\ge m$ miatt $a_i^{n/2}\equiv 0\ (q)$. Ugyanez igaz a b_i számokra is. Vegyük M_n első, középső és utolsó oszlopát (van középső, mert n páros). Mindegyikben csak 1 és 0 szerepelhet mod q, és a középső oszlop a két szélső szorzata mod q. Egy sor két szélső eleme nem lehet egyszerre nulla, mert a_i és b_i relatív prímek. Ezért a két szélső oszlop összegéből a középsőt kivonva konstans 1-et kapunk mod q. □

Az előző szakasz eredményeivel kombinálva, ha n elég nagy, és $2\varphi(q)\mid n$ teljesül Δ minden q prímhatvány-osztójára, akkor a konstans 1 vektor A_n-ben van.

4.8. feladat. *Igazoljuk, hogy A_n és A_m vektorait komponensenként összeszorozva A_{n+m}-beli vektorokat kapunk, így az A_n rácsok periodikusan ismétlődnek ($n\ge k-1$).*

Útmutatás. Ha a konstans 1 vektor A_m-ben van, akkor $A_n\subseteq A_{n+m}$. Mivel az indexük ugyanaz a Δ szám, meg is egyeznek. □

4.4. Az A_n rács vektorai. Most is föltesszük, hogy $d_{ij}=a_ib_j-b_ia_j\ne 0$ (amikor $i\ne j$). Ha $n\ge k-1$, akkor A_n indexe $\Delta=\prod_{1\le i<j\le k} d_{ij}$, így A_n a $\mathbb{Z}^k$ vektorainak Δ-ad részét tartalmazza (ez pontos értelmet kap, ha egy nagy gömb vektorait tekintjük).

4.9. feladat. *Mutassuk meg, hogy ha $k\ge 4$, akkor $A_n\ne\mathbb{Z}^k$, mert M_n-nek van két* mod 2 *egyenlő sora. Általánosítsuk ezt 2 helyett általános prím modulusra.*

Útmutatás. Ha p prím, akkor a $t = a_i/b_i$ osztás $p \nmid b_i$ esetén elvégezhető mod p, azaz van olyan t egész, hogy $tb_i \equiv a_i$ (p). Ha $p \mid b_i$, akkor $p \nmid a_i$, mert a_i és b_i relatív prímek, ilyenkor legyen $t = a_i/b_i$ a ∞ szimbólum. Ez tehát t-re $p+1$ lehetőség mod p.

Ha a_j/b_j is t mod p, akkor $p \mid a_ib_j - b_ia_j$. Mivel $p \mid a_i$ és $p \mid b_i$ egyszerre nem lehetséges, az a_j/a_i és b_j/b_i törtek egyike biztosan értelmes mod p, és ha mindkettő az, akkor ugyanaz az s értékük mod p, ha pedig valamelyik nem értelmes, akkor a számlálója és nevezője is nulla mod p. Így mindig $sa_i \equiv a_j$ (p) és $sb_i \equiv b_j$ (p). Ezért az M_n mátrix j-edik sora az i-edik sor s^n-szerese mod p. Ugyanez tehát A_n vektorainak megfelelő koordinátáira is igaz, vagyis ha $k > p+1$, akkor $A_n \neq \mathbb{Z}^k$. (A mod p vett M_n mátrix rangja a különböző mod p vett a_i/b_i törtek száma, hiszen ha r olyan sort vesszünk, melyekre a_i/b_i páronként különböznek mod p, akkor ennek a részmátrixnak az r-edik determinánsosztója nem osztható p-vel a 4.5. feladat miatt.) □

Ha $i \neq j$, akkor $d_{ij} = a_ib_j - b_ia_j$ a legnagyobb modulus, melyre nézve a_j/a_i és b_j/b_i egyenlő. Az az s_{ij} szorzó, melyre $s_{ij}a_i \equiv a_j$ (d_{ij}) és $s_{ij}b_i \equiv b_j$ (d_{ij}) az $s_{ij} = e_ia_j + f_ib_j$ képlettel kapható, ahol $e_ia_i + f_ib_i = 1$ (van ilyen e_i, f_i, mert a_i és b_i relatív prímek). Legyen $1 \leq i \leq k$ esetén $s_{ii} = 1$.

4.10. feladat. *Nyilván* $\mathbf{s}_j = [s_{j1}, \ldots, s_{jk}]^T \in A_1$ *és* $\mathbf{d}_j = [d_{j1}, \ldots, d_{jk}]^T \in A_1$. *Készítsünk egy olyan bázist* A_n*-ben az* $\mathbf{s}_j$ *és* $\mathbf{d}_j$ *komponensenkénti szorzásával a* 4.8. *feladat alapján, ahol a vektorok háromszögmátrixot alkotnak* $(n \geq k-1)$.

Útmutatás. Legyen $1 \leq j \leq k$. A $\mathbf{d}_j$ vektor j-edik koordinátája nulla, ezért a j-edik bázisvektor elkészítéséhez tekintsük a $\mathbf{d}_1, \ldots, \mathbf{d}_{j-1}$ (komponensenkénti) szorzatát. Ennek az első $j-1$ koordinátája nulla. Ahhoz, hogy A_n-be jussunk, szorozzunk még $\mathbf{s}_j^{n-j+1}$-nel. A főátlóban álló elemek szorzata Δ, mert $s_{jj} = 1$ és a főátló j-edik eleme $d_{1,j} \cdot \ldots \cdot d_{j-1,j}$. Így a vektoraink függetlenek, és az általuk generált rács indexe Δ. De A_n indexe is Δ, ezért bázist kaptunk. □

Ha az előző feladatban kapott háromszögmátrix K, akkor $\mathbf{v} = [c_1, \ldots, c_k]^T$ pontosan akkor van A_n-ben, ha a $K[x_1, \ldots, x_n]^T = \mathbf{v}$ lineáris egyenletrendszer (egyértelmű) megoldása egész x_i számokból áll. Ezt az egyenletrendszert föntről lefelé haladva könnyű megoldani. A K inverzével szorozva $[x_1, \ldots, x_n]^T = K^{-1}\mathbf{v} \in \mathbb{Z}^k$. Ez k oszthatósági feltétel, ahol a bal oldalon mindig Δ áll, mert ΔK^{-1} egész elemű. Az első ezek közül automatikusan teljesül, mert K első sorának első eleme 1.

4.11. példa. Legyenek a megadott párok $(1,1)$, $(1,3)$ és $(1,-1)$. Ekkor $n \geq 2$ esetén az összes A_n egyenlő, $d_{12} = 2$, $d_{13} = -2$, $d_{23} = -4$, $\Delta = 16$, mindegyik $s_{ij} = 1$, és $[c_1, c_2, c_3]^T$ pontosan akkor van A_n-ben, ha $16 \mid -8c_1 + 8c_2$ és $16 \mid -4c_1 + 2c_2 + 2c_3$.

5. Ortogonális rácsok

Zárásként belátjuk Peter McMullen egy gyönyörű tételét. Mostantól kicsit nagyobb tudást föltételezünk lineáris algebrából (például euklideszi tér, ortogonális kiegészítő altér). Legyenek $\mathbf{v}_1, \ldots, \mathbf{v}_r \in \mathbb{R}^k$ lineárisan független vektorok és V az általuk generált altér. Ebben $\mathbf{v}_1, \ldots, \mathbf{v}_r$ egész együtthatós lineáris kombinációi egy r rangú B rácsot alkotnak. Ez tehát nem az egész $\mathbb{R}^k$-nak rácsa, hanem csak a V altérnek.

5.1. állítás. *Jelölje* L *a* $[\mathbf{v}_1, \ldots, \mathbf{v}_r]$ *mátrix* $r \times r$*-es aldeterminánsainak négyzetösszegét* $(r \geq 1)$. *Ekkor a* B *rács alap-parallelotópjának térfogata* $\sqrt{L}$.

Bizonyítás. Föltehető, hogy $r < k$. Legyen $\mathbf{v}_{r+1}, \ldots, \mathbf{v}_k$ ortonormált bázis a $\mathbf{v}_1, \ldots, \mathbf{v}_r$ által generált V altér $V^\perp$ ortogonális kiegészítő alterében (ezek egy „kockát” feszítenek ki), és $M = [\mathbf{v}_1, \ldots, \mathbf{v}_k]$. Geometriai megfontolásokból kapjuk, hogy $\det(M)$ abszolút értéke a $\mathbf{v}_1, \ldots, \mathbf{v}_r$ által generált rács alap-parallelotópjának d térfogata.

Az M^TM mátrix két diagonális blokkból áll, és a többi eleme nulla. A második blokk a $(k-r) \times (k-r)$-es egységmátrix. Az első, $r \times r$-es blokkot jelölje N. Ekkor $d^2 = \det(M^TM) = \det(N)$. Alkalmazzuk a Cauchy–Binet-formulát (2.2. tétel) az M^TM szorzatra és az első r sorra/oszlopra. Ekkor $d^2 = L$ adódik. □

Ha B rács $\mathbb{Z}^k$-ban és V altér $\mathbb{R}^k$-ban, akkor V-be B-nek kevés vektora is eshet. Például az $y = \sqrt{2}x$ egyenes nem tartalmaz egész koordinátájú pontot az origón kívül. Nevezzük V-t *racionális altérnek,* ha generálható racionális koordinátájú vektorokkal. Racionális vektorok egy családja pontosan akkor független $\mathbb{Q}$ fölött, ha $\mathbb{R}$ fölött az. Ha a V racionális altér r-dimenziós, akkor $V \cap \mathbb{Q}^k$ ortogonális komplementerének dimenziója $\mathbb{Q}^k$-ban $k-r$, és így az $\mathbb{R}^k$-ban vett ortogonális kiegészítő is racionális altér. Továbbá $\mathbb{Z}^k \cap V$-ben van r független vektor, hiszen egy racionális vektort alkalmas nem nulla egésszel megszorozva egész vektort kapunk. Ezért $\mathbb{Z}^k \cap V$ rács V-ben.

5.2. definíció. Egy B csoport $\mathbf{v}$ elemének B-beli *magassága* a legnagyobb olyan egész, amivel $\mathbf{v}$ eloszthető úgy, hogy B-ben maradjunk. Ha $B = \mathbb{Z}^k$, akkor ez a $\mathbf{v}$ komponenseinek legnagyobb közös osztója. Tehát $\mathbf{v}$ akkor primitív, ha magassága $\mathbb{Z}^k$-ban 1. A B részcsoport *tiszta* $\mathbb{Z}^k$-ban, ha a vektorok magassága ugyanaz B-ben, mint $\mathbb{Z}^k$-ban. (Ez a 3.9. következmény (2) pontjában szereplő feltétel.)

5.3. lemma. *Ha* V *racionális altér* $\mathbb{R}^k$*-ban, akkor* $V \cap \mathbb{Z}^k$ *tiszta részrácsa* $\mathbb{Z}^k$*-nak.*

Bizonyítás. Valóban, ha $\mathbf{v} \in \mathbb{Z}^k$ és $m\mathbf{v} \in V \cap \mathbb{Z}^k$, akkor $\mathbf{v} \in V$ (hiszen V zárt az $1/m$ számmal való szorzásra), és így $\mathbf{v} \in V \cap \mathbb{Z}^k$. □

5.4. tétel (McMullen, [4]). *Legyen V racionális altér $\mathbb{R}^k$-ban. Ha $A_1 = V \cap \mathbb{Z}^k$ és $A_2 = V^\perp \cap \mathbb{Z}^k$, akkor A_1 és A_2 alap-parallelotópjának térfogata megegyezik.*

Bizonyítás. Legyen $\dim(V) = r$ és $0 < r < k$ (az $r = 0$ és $r = k$ esetben $\{\mathbf{0}\}$ térfogatát 1-nek tekintve igaz az állítás). Vegyük A_1-nek egy $\mathbf{b}_1, \ldots, \mathbf{b}_r$ és A_2-nek egy $\mathbf{b}_{r+1}, \ldots, \mathbf{b}_k$ bázisát. Ezek együtt bázist alkotnak $\mathbb{R}^k$-ban, hiszen $A_1 \perp A_2$ (de $\mathbb{Z}^k$-ban általában nem). Az 5.3. lemma és a 3.9. következmény miatt a $[\mathbf{b}_1, \ldots, \mathbf{b}_r]$ mátrix r-edik determinánsosztója 1. Az analóg állítás érvényes A_2 esetében is.

Tekintsük a $[\mathbf{b}_1, \ldots, \mathbf{b}_k]$ mátrix első r oszlopa szerinti $e_1 f_1 g_1 + \ldots + e_m f_m g_m$ Laplace-kifejtését, ahol f_i az első r oszlophoz, g_i az utolsó $k - r$ oszlophoz tartozó aldeterminánsok, e_i a megfelelő előjelek, és $m = \binom{k}{r}$. Legyen $\mathbf{w}_1 = [e_1 f_1, \ldots, e_m f_m]$ és $\mathbf{w}_2 = [g_1, \ldots, g_m]$. Ekkor $\mathbf{w}_1$ és $\mathbf{w}_2$ skaláris szorzata a $[\mathbf{b}_1, \ldots, \mathbf{b}_k]$ mátrix d determinánsa (aminek abszolút értéke a $\mathbf{b}_1, \ldots, \mathbf{b}_k$ által generált rács alap-parallelotópjának térfogata, azaz indexe).

Jelölje d_1 és d_2 az A_1, illetve A_2 rácsok alap-parallelotópjának térfogatát. Az 5.1. állítás miatt d_1^2 a $\mathbf{w}_1$ vektor komponenseinek négyzetösszege, hiszen a négyzetre emelés után az előjelek már nem számítanak, és ugyanez áll d_2-re és $\mathbf{w}_2$-re is. Mivel e két rács ortogonális, $d_1 d_2 = |d|$. Ez azt jelenti, hogy a $\mathbf{w}_1$ és $\mathbf{w}_2$ vektorokra fölírt Cauchy-egyenlőtlenségben egyenlőség áll. Ezért $\mathbf{w}_1$ és $\mathbf{w}_2$ egymás skalárszorosai. Ez a skalár szükségképpen racionális szám, azaz alkalmas m_1 és m_2 nem nulla egészekre $m_1 \mathbf{w}_1 = m_2 \mathbf{w}_2$. De a $[\mathbf{b}_1, \ldots, \mathbf{b}_r]$ mátrix r-edik determinánsosztója 1, ezért $\mathbf{w}_1$ (és hasonlóan $\mathbf{w}_2$ is) primitív vektorok. Tehát $\mathbf{w}_1 = \pm \mathbf{w}_2$, és így $d_1 = d_2$. □

6. Appendix: Vetítések és alkalmazásaik

Az alábbi feladatokban a mátrixok normálalakja helyett geometriai módszerekkel igazolunk korábbi állításokat. Szó lesz egy számelméleti alkalmazásról is. Fő eszközünk a vetítés. Ha az e_1 és e_2 egyenesek az origóban metszik egymást, akkor az e_1-re való e_2 irányú vetítés az a leképezés, amely a sík minden P pontjához az e_1 egyenes azon Q pontját rendeli, melyre PQ párhuzamos e_2-vel.

Ha U és W alterek, és $\mathbb{R}^k$ minden eleme egyértelműen fölírható egy U-beli és egy W-beli vektor összegeként, akkor azt mondjuk, hogy $\mathbb{R}^k$ a V és W alterek *direkt összege,* jele $\mathbb{R}^k = U \oplus V$. Az egyértelműség feltétele, hogy $U \cap W$ csak a nullvektorból álljon. A bázisok nyelvén ez azt jelenti, hogy van olyan $\mathbf{b}_1, \ldots, \mathbf{b}_r$ bázis U-ban, és $\mathbf{b}_{r+1}, \ldots, \mathbf{b}_k$ bázis W-ben, hogy ezek együtt bázist alkotnak $\mathbb{R}^k$-ban. Hasonlóan értelmezzük azt is, amikor $\mathbb{Z}^k$ az A és B csoportok direkt összege, azaz $\mathbb{Z}^k = A \oplus B$.

Ha $\mathbf{v} = \mathbf{u} + \mathbf{w}$, ahol $\mathbf{u} \in U$ és $\mathbf{w} \in W$, akkor az a leképezés, amely $\mathbf{v}$-hez $\mathbf{u}$-t rendeli, az $\mathbb{R}^k$-nak az U-ra való *vetítése a W irányban.* Ha $\mathbf{v} = \lambda_1 \mathbf{b}_1 + \ldots + \lambda_k \mathbf{b}_k$, akkor $\mathbf{u} = \lambda_1 \mathbf{b}_1 + \ldots + \lambda_r \mathbf{b}_r$, vagyis a vetítés „kinullázza" az utolsó $k - r$ koordinátát.

6.1. feladat. *Legyen $\mathbb{R}^k = U \oplus W$, ahol U egy $\mathbb{R}$ fölött r-dimenziós racionális altér. Igazoljuk, hogy W pontosan akkor racionális altér, ha $\mathbb{Q}^k$-nak az U-ra vett W irányú vetületében nincs r-nél több $\mathbb{Q}$ fölött független vektor.*

Útmutatás. Legyen $\mathbf{b}_1, \ldots, \mathbf{b}_r$ racionális bázis U-ban és $\mathbf{b}_{r+1}, \ldots, \mathbf{b}_s$ maximális számú, $\mathbb{R}$ fölött független racionális vektor W-ben. Ha $s < k$, akkor van olyan $\mathbf{v} \in \mathbb{Q}^k$, ami $\mathbb{R}$ fölött független $\mathbf{b}_1, \ldots, \mathbf{b}_s$-től. Ekkor $\mathbf{v}$ vetülete független $\mathbb{Q}$ fölött $\mathbf{b}_1, \ldots, \mathbf{b}_r$-től. □

6.2. feladat. *Igazoljuk, hogy ha $\mathbf{v}_1, \ldots, \mathbf{v}_{k+1} \in \mathbb{R}^k$ független $\mathbb{Q}$ fölött, akkor az általuk generált csoport nem diszkrét, ezért nem is rács.*

Útmutatás. Föltehető (k szerinti indukcióval), hogy $\mathbf{v}_1, \ldots, \mathbf{v}_k$ független $\mathbb{R}$ fölött, legyen B az általuk generált rács és P az általuk kifeszített parallelotóp. Tekintsük az $n\mathbf{v}_{k+1}$ vektorokat (n egész), és mindegyiket toljuk vissza P-be a B megfelelő elemével. A kapott pontok mind különbözők $\mathbf{v}_1, \ldots, \mathbf{v}_{k+1} \in \mathbb{R}^k$ függetlensége miatt. □

6.3. feladat. *Igazoljuk, hogy minden irracionális szám egész többszöröseinek törtrészei* sűrűn *helyezkednek el $[0, 1]$-ben (azaz minden rész-intervallumban van törtrész).*

Útmutatás. Az előző feladat $\mathbf{v}_1 = 1$ és $\mathbf{v}_2 = \alpha$ esetén azt adja, hogy $[0, 1]$-ben végtelen sok ilyen törtrész van. Ezért minden $\varepsilon > 0$-ra lesz kettő ε-nál közelebb egymáshoz. A megfelelő egész szorzókat kivonva olyan törtrészt kapunk, ami a nullához van ε-nál közelebb. Minden ε hosszú intervallumba beleesik ennek valamelyik többese. □

Sokkal erősebb állítás is igazolható Minkowski rácsokról szóló tétele segítségével: ha α irracionális, akkor van végtelen sok olyan r/s tört, melyek bármelyike α-tól kevesebb, mint $1/(2s^2)$-tel tér el (lásd [2], 8.2. szakasz). Kronecker approximációs tétele arra ad feltételt, hogy $\mathbf{v}_{k+1}$ egész többesei P-ben alkossanak sűrű halmazt.

6.4. feladat. *Tegyük föl, hogy U racionális altér és C a $\mathbb{Z}^k$-nak az U-ra vett W irányú vetülete. Mutassuk meg, hogy C pontosan akkor rács U-ban, ha W is racionális altér.*

Útmutatás. Ha W racionális altér, $\mathbf{b}_1, \ldots, \mathbf{b}_r$ racionális bázis U-ban és $\mathbf{b}_{r+1}, \ldots, \mathbf{b}_k$ racionális bázis W-ben, akkor írjuk föl ezekkel $\mathbb{Z}^k$ egy bázisát. Ha az együtthatók közös nevezője N, akkor minden $\mathbf{v} \in \mathbb{Z}^k$ vektor U-ra eső vetületének N-szerese benne van a $\mathbf{b}_1, \ldots, \mathbf{b}_r$ generálta csoportban. Így C diszkrét, és nyilván $\mathbb{R}$ fölött generálja az U alteret. Megfordítás: 6.1. és 6.2. □

6.5. feladat. *Mutassuk meg a normálalak használata nélkül, hogy a* 3.9. *következményben* (2)*-ből következik* (1).

Útmutatás. A (2) szerint valamely független $\mathbf{b}_1, \ldots, \mathbf{b}_r \in \mathbb{Z}^k$ által generált B csoport tiszta $\mathbb{Z}^k$-ban. Legyen $\mathbf{b}_1, \ldots, \mathbf{b}_k$ racionális bázisa $\mathbb{Q}^k$-nak, W a $\mathbf{b}_1, \ldots, \mathbf{b}_r$ által generált valós altér, és U a $\mathbf{b}_{r+1}, \ldots, \mathbf{b}_k$ által generált valós altér. A 6.4. feladat miatt $\mathbb{Z}^k$-nak az U-ra vett W irányú C vetülete rács U-ban, legyenek $\mathbf{c}_{r+1}, \ldots, \mathbf{c}_k \in \mathbb{Z}^k$ olyan vektorok, melyek vetülete bázis C-ben. Ekkor minden $\mathbf{v} \in \mathbb{Z}^k$ esetén vannak olyan z_i egészek, hogy $\mathbf{v}_0 = \mathbf{v} - z_{r+1}\mathbf{c}_{r+1} - \ldots - z_k\mathbf{c}_k \in W$. Tehát $\mathbf{v}_0$ fölírható $\mathbf{b}_1, \ldots, \mathbf{b}_r$ racionális együtthatós lineáris kombinációjaként, és ezért alkalmas $m \neq 0$ egészre $m\mathbf{v}_0 \in B$. Mivel B tiszta, $\mathbf{v}_0 \in B$ és ezért $\mathbf{b}_1, \ldots, \mathbf{b}_r, \mathbf{c}_{r+1}, \ldots, \mathbf{c}_k$ bázis $\mathbb{Z}^k$-ban. □

6.6. feladat. *Legyen $B \subseteq \mathbb{Z}^k$ rács, $\mathbf{d}_1, \ldots, \mathbf{d}_k$ bázis $\mathbb{Z}^k$-ban, W a $\mathbf{d}_1, \ldots, \mathbf{d}_r$ által generált, U a $\mathbf{d}_{r+1}, \ldots, \mathbf{d}_k$ által generált valós altér. Vetítsük B-t U-ra W irányából. Igazoljuk, hogy ha $\mathbf{d}_1, \ldots, \mathbf{d}_r \in B$, akkor a vetület $B \cap U$, és $B = (B \cap W) \oplus (B \cap U)$.*

Útmutatás. A $\mathbf{v} = z_1\mathbf{d}_1 + \ldots + z_k\mathbf{d}_k$ vektor vetülete U-ra $\mathbf{u} = z_{r+1}\mathbf{d}_{r+1} + \ldots + z_k\mathbf{d}_k$. Ha $\mathbf{v} \in B$, akkor $\mathbf{d}_1, \ldots, \mathbf{d}_r \in B$ miatt $\mathbf{u} \in B$, azaz a vetület része $B \cap U$-nak. □

6.7. feladat. *Legyen $B \subseteq \mathbb{Z}^k$ rács, $\mathbf{w} \in \mathbb{Z}^k$ nem nulla vektor és C a $\mathbf{w}$-re merőleges B-beli vektorok halmaza. Vetítsük B-t merőlegesen a $\mathbf{w}$ egyenesére. Mutassuk meg, hogy van legrövidebb nem nulla vetület, és ha $\mathbf{v} \in B$ vetülete egy ilyen legrövidebb $\mathbf{w}_0$ vektor, akkor $B = A \oplus C$, ahol A a $\mathbf{v}$ egész többszöröseinek halmaza.*

Útmutatás. Az $\mathbf{u} \in B$ vektor $\mathbf{w}$-re eső vetületének hossza az $\mathbf{u} \cdot \mathbf{w} = n$ skaláris szorzat osztva $\mathbf{w}$ hosszával. Mivel n egész, ezért a vetületek között tényleg van legrövidebb. Tehát B vetülete rács a $\mathbf{w}$ egyenesén, és ezért minden vektor vetülete $\mathbf{w}_0$ egész számszorosa. Ha $\mathbf{u}$ vetülete $m\mathbf{w}_0$, akkor $\mathbf{u} - m\mathbf{v}$ merőleges $\mathbf{w}$-re, és ezért C-ben van. □

6.8. feladat. *Legyen $\mathbf{w}$ primitív vektor $\mathbb{Z}^k$-ban és C a $\mathbf{w}$-re ortogonális egész vektorok halmaza. Bizonyítsuk be, hogy $\mathbf{w}$ hossza megegyezik C alap-parallelotópjának térfogatával. (Ez McMullen tételének speciális esete.)*

Útmutatás. Mivel $\mathbf{w}$ primitív, van olyan $\mathbf{v}$ vektor, melynek $\mathbf{w}$-vel vett skaláris szorzata 1 (oldjuk meg a lineáris diofantoszi egyenletet). Az előző feladatot a $B = \mathbb{Z}^k$ rácsra alkalmazva azt kapjuk, hogy $\mathbf{v}$ és C generálják $\mathbb{Z}^k$-t, azaz C egy P alap-parallelotópja $\mathbf{v}$-vel együtt egy 1 térfogatú parallelotópot feszít ki. Ennek alapja P, magassága pedig a $\mathbf{v}$ vektor $\mathbf{w}$ irányú vetületének hossza, ami $\mathbf{w}$ hosszának reciproka. □

6.9. feladat. *Igazoljuk, hogy a háromdimenziós térben minden egész vektor előáll két egész vektor vektoriális szorzataként.*

Útmutatás. Föltehető, hogy $\mathbf{w}$ primitív, alkalmazzuk az előző feladatot. *Második, elemi megoldás:* ha (a_1, a_2, a_3)-at akarjuk (x_1, x_2, x_3) és (y_1, y_2, y_3) vektoriális szorzataként előállítani, akkor legyen $x_3 = y_3 = \text{lnko}(a_1, a_2) = d$. Föltehető, hogy $d \neq 0$; ha $a_1x_1 + a_2x_2 = -a_3x_3$, akkor $y_1 = a_2/d + x_1$ és $y_2 = -a_1/d + x_2$ megfelelő. □

6.10. feladat. *Mutassuk meg a normálalak fölhasználása nélkül, hogy ha $B \subseteq \mathbb{Z}^k$ rács, akkor van olyan $\mathbf{c}_1, \ldots, \mathbf{c}_k$ bázisa $\mathbb{Z}^k$-nak, hogy alkalmas $s_1, s_2, \ldots, s_k$ egészekre $s_1\mathbf{c}_1, \ldots, s_k\mathbf{c}_k$ bázis B-ben.*

Útmutatás. Vegyünk egy olyan $h\mathbf{v} \in B$ vektort, melynek $\mathbb{Z}^k$-beli h magassága a lehető legkisebb. Ekkor $\mathbf{v} \in \mathbb{Z}^k$ primitív, így van olyan $\mathbf{w} \in \mathbb{Z}^k$, melynek $\mathbf{v}$-vel vett skaláris szorzata 1. Jelölje C a $\mathbf{w}$-re merőleges egész vektorok halmazát. A 6.8. feladatban használt gondolatmenet miatt $\mathbf{v}$ és C generálja $\mathbb{Z}^k$-t, és ha $\mathbf{v}$ vetülete $\mathbf{w}$ egyenesére $\mathbf{w}_0$, akkor a $\mathbb{Z}^k$ merőleges vetülete $\mathbf{w}$ egyenesére a $\mathbf{w}_0$ egész többeseiből áll.

Vetítsük a $B \subseteq \mathbb{Z}^k$ rácsot is merőlegesen $\mathbf{w}$ egyenesére, és a vetület legrövidebb vektorát jelölje $m\mathbf{w}_0$. Ha $\mathbf{u} \in B$ vetülete $m\mathbf{w}_0$, akkor a 6.7. feladat miatt B-t generálja $\mathbf{u}$ és $C \cap B$. Az $\mathbf{u}$ magassága $\mathbb{Z}^k$-ban legyen g, föltevésünk szerint $h \leq g$. Az $(1/g)\mathbf{u} \in \mathbb{Z}^k$ vektort $\mathbf{w}$ egyenesére vetítve $\mathbf{w}_0$ többszörösét kapjuk, ezért $g \mid m$. Mivel $h\mathbf{v} \in B$ vetülete $h\mathbf{w}_0$, ezért $m \mid h$. Ez csak úgy lehetséges, ha $g = h = m$.

Vagyis találtunk egy olyan $m\mathbf{v} \in B$ vektort, amelyre $\mathbf{v}$ és C generálja $\mathbb{Z}^k$-t, és $m\mathbf{v}$ és $B \cap C$ generálja B-t. Vegyünk egy bázist C-ben, és írjuk föl ebben $B \cap C$ elemeit is (ilyen átkoordinátázást használtunk a 3.11. feladatban). Az átkoordinátázás után C-ből $\mathbb{Z}^{k-1}$ lesz. Alkalmazzunk k szerinti indukciót, ekkor van olyan $\mathbf{c}_2, \ldots, \mathbf{c}_k$ bázis C-ben, hogy $s_2\mathbf{c}_2, \ldots, s_k\mathbf{c}_k \in C$ bázis $B \cap C$-ben. Legyen $\mathbf{c}_1 = \mathbf{v}$ és $s_1 = m$. □

Az alábbi feladat többszöri alkalmazásával elérhetjük az $s_1 \mid \ldots \mid s_k$ oszthatóságot.

6.11. feladat. *Tegyük föl, hogy $\mathbf{c}_1, \ldots, \mathbf{c}_k$ bázis a C rácsban és $s_1\mathbf{c}_1, \ldots, s_k\mathbf{c}_k$ bázis a $B \subseteq C$ rácsban. Legyen s az s_1 és s_2 legnagyobb közös osztója, $t = s_1s_2/s$ pedig a legkisebb közös többszörösük. Válasszunk olyan e és f egészeket, melyekre $es_1 + fs_2 = s$, legyen $\mathbf{c}_1' = (s_1/s)\mathbf{c}_1 - (s_2/s)\mathbf{c}_2$ és $\mathbf{c}_2' = f\mathbf{c}_1 + e\mathbf{c}_2$. Mutassuk meg, hogy $\mathbf{c}_1', \mathbf{c}_2', \mathbf{c}_3, \ldots, \mathbf{c}_k$ bázis C-ben és $s\mathbf{c}_1', t\mathbf{c}_2', s_3\mathbf{c}_3, \ldots, s_k\mathbf{c}_k$ bázis B-ben.*

Hivatkozások

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

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

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

[4] Peter McMullen: *Determinants of lattices induced by rational subspaces,* Bull. London Math. Soc., **16** (1984), 275–277.