Kombinatorikus Nullhelytételek

BSc Szakdolgozat

Írta: Mezei Tamás Róbert

Matematika BSc, matematikus szakirány

Témavezető

Kós Géza, egyetemi adjunktus
Analízis Tanszék

Eötvös Loránd Tudományegyetem
Természettudományi Kar
2011

Köszönetnyilvánítás

Ez úton is szeretnék köszönetet mondani témavezetőmnek, Kós Gézának, aki sok érdekes problémával ismertetett meg, segített a dolgozat témavezetésének és fő irányának a kialakításában, és ezekkel, valamint számos tanácsával hozzájárult a dolgozatom létrejöttéhez.

Köszönetet mondok mindazoknak a tanároknak, akik a képzés 3 éve alatt lelkiismeretes munkájukkal teret adtak matematikai tudásom bővítéséhez.

Tartalomjegyzék

1. fejezet

Bevezető

1.1. Előszó

A szakdolgozat célja az Alon-féle kombinatorikus nullhelytétel[1] valamint kiterjesztéseinek bizonyításainak és alkalmazásainak bemutatása. A dolgozat felépítése a következő.

- Az **1. fejezetben** bevezetünk néhány jelölést a változók nagy számára való tekintettel, és belátunk néhány egyszerű tételt, amikre a dolgozat egy részében támaszkodni fogunk.
- A **2. fejezetben** belátjuk Alon kombinatorikus nullhelytételét, és bemutatunk néhány alternatív bizonyítási módszert.
- A **3. fejezetben** számelméleti problémakörök eredményein keresztül ismertetjük a kombinatorikus nullhelytétel néhány alkalmazását, nyilvánvalóvá téve a tétel fontosságát.
- A **4. fejezet** a kombinatorikus nullhelytétel kiterjesztéséről szól, ennek bemutatjuk egy-egy alkalmazását is.
- Egy másik irányban terjeszti ki a kombinatorikus nullhelytételt az **5. fejezet**. Itt fognak értelmet nyerni a **2. fejezetben** bemutatott bizonyítási módszerek, mivel a kiterjesztett tételeket egy már korábban látott gondolatmenet mentén fogjuk belátni, ami által a bizonyítások is érthetőbbek lesznek.
- Végül néhány saját eredményemet tárgyalom a **6. fejezetben**. Ebben a **4.** és **5. fejezet** főbb tételeinek (közös) kiterjesztéseit adom meg.

1.2. Jelölések

A tételekben általában n-változós polinomokkal kell dolgozni, így érdemes bevezetni néhány konvenciót a jelölésre. A terek dimenziója általában n pozitív egész lesz, $\mathbb{F}$ alatt mindig egy testet értünk, $S_1, \dots, S_n$ pedig $\mathbb{F}$ nem üres részhalmazai lesznek. A valós számok testét $\mathbb{R}$-rel, a nemnegatív egész számok halmazát pedig $\mathbb{N}$-nel jelöljük.

A rendezett n-eseket félkövér betűvel jelöljük, például $\mathbf{s} \in \mathbb{F}^n$, de ha az i-ik koordinátájáról beszélünk, azt normális vastagságú betűvel írva, s_i-vel jelöljük, azaz $\mathbf{s} = (s_1, \dots, s_n)$. Így például az $f(x_1, \dots, x_n)$

[1] Gyakran nullhelytétel helyett Nullstellensatznak nevezik, nem csak német, hanem angol irodalomban is, az eredeti, Hilbert-féle Nullstellensatz hagyománya okán.

polinom helyett általában $f(\mathbf{x})$-et írunk, és hasonlóan $\mathbb{F}[x_1,\ldots,x_n]=\mathbb{F}[\mathbf{x}]$. Gyakran szükségünk van arra, hogy elhagyjunk egy koordinátát a rendezett n-esből, így az $(s_1,\ldots,s_{i-1},s_{i+1},\ldots,s_n)$ rendezett $n-1$-est $\mathbf{s}_{-i}$-vel jelöljük.

Ha adott néhány sorvektor egy A mátrixba rendezve, akkor $\mathbf{a}_{i.}$-tal jelöljük az $i.$ vektort, ennek a $j.$ koordinátáját pedig a_{ij} jelöli. Ha a hangsúly inkább a vektorok megindexelésén, és kevésbé a megszámozásán van, akkor általában $\mathbf{w}_\lambda$-t írunk, ahol $\lambda\in\Lambda$ indexhalmaznak. Ha egy számot írunk félkövéren, akkor az azt jelenti, hogy minden koordinátában az az érték szerepel, tehát az origót jelölése $\mathbf{0}=(0,\ldots,0)\in\mathbb{F}^n$.

A két szám közötti relációkat értelmezzük n dimenziós vektorokra is, úgy, hogy $\mathbf{u}$ *rel* $\mathbf{w}$ pontosan akkor, ha minden i koordinátában u_i *rel* w_i. Ehhez hasonlóan értelmezzük n dimenziós vektorok között a kétváltozós alapműveleteket, azaz $\mathbf{u}$ *op* $\mathbf{w}=(u_1$ *op* $w_1,\ldots,u_n$ *op* $w_n)$. A hatványozás értelmezése pedig $\mathbf{x}^\mathbf{u}=x_1^{u_1}\cdot\ldots\cdot x_n^{u_n}$. Tehát például $(\mathbf{x}-\mathbf{s})^\mathbf{u}=(x_1-s_1)^{u_1}\cdot\ldots\cdot(x_n-s_n)^{u_n}$.

Többször felhasználjuk egy $f\in\mathbb{F}[\mathbf{x}]$ polinom $\mathbf{s}\in\mathbb{F}^n$ vektor körüli felbontását, azaz f-nek a következő alakban való felírhatóságát: $f(\mathbf{x})=\sum_{\mathbf{u}\in\mathbb{N}^n} f_\mathbf{u}(\mathbf{s})(\mathbf{x}-\mathbf{s})^\mathbf{u}$. Speciálisan, $f(\mathbf{x})=\sum_{\mathbf{u}\in\mathbb{N}^n} f_\mathbf{u}(\mathbf{0})\mathbf{x}^\mathbf{u}$, ilyenkor a $c_\mathbf{u}=f_\mathbf{u}(\mathbf{0})$ jelölést fogjuk használni. Könnyen lehet látni, hogy $f_\mathbf{u}(\mathbf{s})$ egyértelműen meghatározott f, $\mathbf{u}$ és $\mathbf{s}$ által, hiszen $\sum_{\mathbf{u}\in\mathbb{N}^n} f_\mathbf{u}(\mathbf{s})\mathbf{x}^\mathbf{u}=f(\mathbf{x}+\mathbf{s})$.

A többváltozós polinomokra sokszor fogunk úgy tekinteni, mintha csak egyik változójuktól függnének, így érdemes bevezetni a $\deg_{x_i}(f)$ jelölést ($f\in\mathbb{F}[\mathbf{x}]$) az f polinom x_i változóban vett fokára.

$\mathrm{Sym}(k)$-val a $1,\ldots,k$ számok összes permutációinak a csoportját jelöljük. A $\chi(A)$ függvény definíció szerint az A elemein 1-et vegyen fel, és mindenhol máshol 0-t.

1.3. Néhány tétel polinomok maradékos osztásáról és ideáljairól

A teljesség kedvéért most pontosan leírunk és bebizonyítunk néhány, a dolgozatban felhasználandó elemi állítást. A következőekben R-ről feltesszük, hogy kommutatív és egységelemes.

1.1. Definíció. Legyen $f\in R[\mathbf{x}]$ polinom. Az f polinom nem 0 együtthatós monomjai kitevő vektorainak a halmazát $\mathrm{Supp}(f)$-fel fogjuk jelölni, azaz

$$\mathrm{Supp}(f)=\left\{\ \mathbf{u}\in\mathbb{N}^n\ \mid \text{az } \mathbf{x}^\mathbf{u} \text{ monom együtthatója } f\text{-ben nem } 0\ \right\}.$$

$\mathrm{Supp}(f)$ elemein a $\geq$ reláció természetes módon ad egy részbenrendezési struktúrát, tehát ha azt mondjuk, hogy $\mathrm{Supp}(f)$-ben $\mathbf{t}$ maximális, akkor azt úgy értjük, hogy nincs olyan $\mathbf{u}\in\mathrm{Supp}(f)$, amire $\mathbf{u}\geq\mathbf{t}$ és $\mathbf{u}\neq\mathbf{t}$. Ha azt mondjuk, hogy $\mathbf{x}^\mathbf{t}$ maximális fokú monom f-ben, akkor azt úgy értjük, hogy $\mathbf{t}$ maximális a $\mathrm{Supp}(f)$ halmazban, és $\deg(\mathbf{x}^\mathbf{t})=\sum t_i=\deg(f)$.

1.2. Definíció (Többváltozós polinomok közötti maradékos osztás)**.** Legyen $f\in\mathbb{F}[\mathbf{x}]$ és $g_\lambda\in\mathbb{F}[\mathbf{x}]$ minden $\lambda\in\Lambda$ esetén. Tegyük fel, hogy a g_λ-nak csak egy $\deg(g_\lambda)$ fokú monomja van, legyen az $\mathbf{x}^{\mathbf{w}_\lambda}$, és tegyük fel, hogy ennek az együtthatója 1. Az algoritmus a h_λ hányadosokat, illetve az r maradékot fogja előállítani.

1. Inicializálunk, legyen $r = f$ és $h_\lambda = 0$.
2. Válasszuk ki r-nek egy $\deg(r)$ fokú monomját, legyen az $\mathbf{x}^{\mathbf{u}}$, és legyen az együtthatója a.
3. Keressünk egy λ-t, amire g_λ-nak a legnagyobb monomja, $\mathbf{x}^{\mathbf{w}_\lambda}$, osztja $\mathbf{x}^{\mathbf{u}}$-t, azaz $\mathbf{w}_\lambda \leq \mathbf{u}$.
   - Amennyiben nincs ilyen λ, akkor véget ér az algoritmus.
   - Ha találtunk egy ilyet, akkor legyen $h'_\lambda := h_\lambda + a\frac{\mathbf{x}^{\mathbf{u}}}{\mathbf{x}^{\mathbf{w}_i}}$ és $r' := r - a\frac{\mathbf{x}^{\mathbf{u}}}{\mathbf{x}^{\mathbf{w}_\lambda}} g_\lambda$.
4. Legyen $h_\lambda = h'_\lambda$ és $r = r'$, és ugorjunk a 2. lépéshez.

A fenti formában az algoritmus futása nem egyértelmű, de ennek ellenére sok esetben egyértelmű maradékot szolgáltat.

Az $\langle \mathbf{x}^{\mathbf{u}} \mid \forall \lambda \in \Lambda\ \mathbf{u} \not\geq \mathbf{w}_\lambda \rangle$ vektorteret fogjuk az osztási maradékok vektorterének hívni, az maradékos osztással kapott maradék ennek a vektortérnek eleme lesz, továbbá világos az is, hogy minden eleme például önmaga osztási maradéka.

1.3. Állítás. *A fenti algoritmus véges, valamint az r és a h_λ polinomok elemei az $R[\mathbf{x}]$ polinomgyűrűnek, és teljesítik az $f - \sum_{\lambda\in\Lambda} h_\lambda g_\lambda = r$ egyenlőséget. Továbbá minden λ-ra $\deg(h_\lambda) \leq \deg(f) - \deg(g_\lambda)$, és $\mathrm{Supp}(r)$ nem tartalmaz olyan $\mathbf{u}$ kitevőt, amire $\mathbf{u} \geq \mathbf{w}_\lambda$.*

Bizonyítás. Világos, hogy r foka nem nőhet az algoritmus futása során, és ha nem csökken, akkor a maximális fokú $\mathbf{u} \in \mathrm{Supp}(r)$ vektorok száma fog csökkenni, mivel megköveteltük a g_λ polinomokról, hogy csak egy maximális fokú monomjuk legyen. Ez tehát biztosítja, hogy az algoritmus csak véges sok lépést tegyen. Viszont amíg létezik $\mathbf{u} \in \mathrm{Supp}(r)$, hogy $\mathbf{u} \geq \mathbf{w}_\lambda$ valamely λ-ra, addig az algoritmus nem fog leállni.

Továbbá a futás elején teljesül az $f = r + \sum_{\lambda\in\Lambda} h_\lambda g_\lambda$ egyenlőség, és ezt a későbbiekben sem rontjuk el. A h_λ polinomok fokára vonatkozó egyenlőtlenséget pedig igazolja a következő:

$$\deg\left(a\frac{\mathbf{x}^{\mathbf{u}}}{\mathbf{x}^{\mathbf{w}_\lambda}}\right) = \deg\left(\mathbf{x}^{\mathbf{u}}\right) - \deg\left(\mathbf{x}^{\mathbf{w}_\lambda}\right) = \deg\left(\mathbf{x}^{\mathbf{u}}\right) - \deg(g_\lambda) \leq \deg(f) - \deg(g_\lambda).$$

□

1.4. Állítás. *Tekintsük a g_λ polinomokkal való maradékos osztást. Legyen $V = \langle \mathbf{x}^{\mathbf{u}} \mid \forall \lambda \in \Lambda\ \mathbf{u} \not\geq \mathbf{w}_\lambda \rangle$ az osztási maradékok vektortere. Ekkor*

a) $\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\big(g_\lambda \mid \lambda \in \Lambda\big) \leq \dim_{\mathbb{F}} V$, *és*

b) *ha* $\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\big(g_\lambda \mid \lambda \in \Lambda\big) = \dim_{\mathbb{F}} V$ *(és a dimenziók végesek), akkor a maradékos osztás során keletkező r maradék egyértelmű.*

Bizonyítás. Tegyük fel, hogy az $(\alpha_1 r_1 + \mathfrak{I}) + \ldots + (\alpha_k r_k + \mathfrak{I})$ lineáris kombináció nem egyenlő $0 + \mathfrak{I}$, ekkor speciálisan $\alpha_1 r_1 + \ldots + \alpha_k r_k$ sem egyenlő a 0 polinommal, ami igazolja az **a)** részt. Legyen most $r_1, \ldots, r_k$ bázisa V-nek. Ezek lineárisan függetlenek, azaz minden $\alpha_1, \ldots, \alpha_k \in \mathbb{F}$ számra $\alpha_1 r_1 + \ldots + \alpha_k r_k \neq 0$ ha $\prod_{i=1}^k \alpha_i \neq 0$. A maradékos osztás miatt tudjuk, hogy $\alpha_1 r_1 + \ldots + \alpha_k r_k + \mathfrak{I}$ alakban előáll $\mathbb{F}[\mathbf{x}]/\mathfrak{I}$ minden eleme. A dimenzióra tett feltevések miatt tehát $\alpha_1 r_1 + \ldots + \alpha_k r_k + \mathfrak{I} \neq 0 + \mathfrak{I}$ ha $\prod_{i=1}^k \alpha_i \neq 0$. Tegyük fel tehát, hogy r és r' két különböző osztási maradéka f-nek. Másképpen fogalmazva $r - r' \neq 0$, miközben $r - r' + \mathfrak{I} = (f - r') - (f - r) + \mathfrak{I} = 0 + \mathfrak{I}$. Ez az előzőek fényében ellentmondás, tehát igazoltuk a **b)** részt. □

1.5. Definíció (Ideálok relatív prímsége)**.** Az a $\mathfrak{A}, \mathfrak{B} \trianglelefteq R$ ideálok relatív prímek R-ben pontosan akkor, ha komplexus összegük kiadja az egész ideált, azaz $\mathfrak{A} + \mathfrak{B} = R$. Mivel R egységelemes, ezzel ekvivalens, hogy $1 \in \mathfrak{A} + \mathfrak{B}$.

1.6. Definíció (Radikál)**.** Az $\mathfrak{A} \trianglelefteq R$ ideál radikálja:

$$\mathrm{Rad}(\mathfrak{A}) = \{x \in R \mid \exists n \in \mathbb{N} \quad x^n \in \mathfrak{A}\} \supseteq \mathfrak{A}.$$

1.7. Állítás. *Egy $\mathfrak{A} \trianglelefteq R$ ideál radikálja, $\mathrm{Rad}(\mathfrak{A}) \trianglelefteq R$ is ideál.*

Bizonyítás. Világos, hogy egy tetszőleges $r \in R$ és $x \in \mathrm{Rad}(\mathfrak{A})$ elem esetén $(rx)^n = r^n x^n \in \mathfrak{A}$, csak azt kell látni még, hogy a radikál zárt az összeadás műveletére. Legyen $x, y \in \mathrm{Rad}(\mathfrak{A})$ és $x^n \in \mathfrak{A}$ valamint $y^k \in \mathfrak{A}$. Ekkor $(x+y)^{n+k} \in \mathfrak{A}$, mivel kommutatív egységelemes gyűrűben igaz a binomiális tétel. □

1.8. Állítás. *Legyen $\mathfrak{A}, \mathfrak{B} \trianglelefteq R$.*

a) *Ha $\mathfrak{A} \subseteq \mathfrak{B}$, akkor $\mathrm{Rad}(\mathfrak{A}) \subseteq \mathrm{Rad}(\mathfrak{B})$.*

b) $\mathrm{Rad}(\mathfrak{A}+\mathfrak{B}) = \mathrm{Rad}(\mathrm{Rad}(\mathfrak{A})+\mathrm{Rad}(\mathfrak{B}))$.

c) $\mathrm{Rad}(\mathfrak{A}) = R$ *akkor és csak akkor, ha* $\mathfrak{A} = R$.

Bizonyítás. Az **a)** rész triviális, továbbá következik belőle a **b)** rész $\mathrm{Rad}(\mathfrak{A}+\mathfrak{B}) \subseteq \mathrm{Rad}(\mathrm{Rad}(\mathfrak{A})+\mathrm{Rad}(\mathfrak{B}))$ iránya. A másik irány igazolásához legyen $z^l = x+y \in \mathrm{Rad}(\mathfrak{A})+\mathrm{Rad}(\mathfrak{B})$, és $x^n \in \mathfrak{A}$ valamint $y^k \in \mathfrak{B}$. Ekkor $z^{l(n+k)} = (z^l)^{n+k} = (x+y)^{n+k} \in \mathfrak{A}+\mathfrak{B}$. A **c)** részt igazolja, hogy $1 \in \mathrm{Rad}(\mathfrak{A}) \Leftrightarrow 1 \in \mathfrak{A}$. □

1.9. Állítás. *Ha $\mathfrak{A}, \mathfrak{B} \trianglelefteq R$ és $\mathrm{Rad}(\mathfrak{A})$ és $\mathrm{Rad}(\mathfrak{B})$ relatív prímek, akkor $\mathfrak{A}$ és $\mathfrak{B}$ is relatív prímek.*

Bizonyítás. Az előző állítást használva $\mathrm{Rad}(\mathfrak{A}+\mathfrak{B}) = \mathrm{Rad}(\mathrm{Rad}(\mathfrak{A})+\mathrm{Rad}(\mathfrak{B})) = \mathrm{Rad}(R) = R$, tehát $\mathfrak{A}+\mathfrak{B} = R$. □

1.10. Tétel (Kínai maradéktétel)**.** *Legyenek $\mathfrak{I}_1, \ldots, \mathfrak{I}_n \trianglelefteq R$ páronként relatív prím ideálok, és $\mathfrak{I} = \bigcap_{i=1}^n \mathfrak{I}_i$. Ekkor $R/\mathfrak{I} \cong \bigoplus_{i=1}^n R/\mathfrak{I}_i$.*

Bizonyítás. Definiáljuk a $\varphi : R/\mathfrak{I} \to \bigoplus_{i=1}^n R/\mathfrak{I}_i$ gyűrűhomomorfizmust a következőképpen:

$$\varphi(a+\mathfrak{I}) = (a+\mathfrak{I}_1, \ldots, a+\mathfrak{I}_n).$$

Ez jól definiált, mivel $a+\mathfrak{I} = b+\mathfrak{I} \Leftrightarrow b-a \in \mathfrak{I} \Leftrightarrow$ minden i-re $b-a \in \mathfrak{I}_i$. Ezzel igazoltuk az injektivitást is.

A szürjektivitást igazolja, ha találunk egy olyan elemet $R/\mathfrak{I}$-ben, aminek a képe $(1+\mathfrak{I}_1, 0+\mathfrak{I}_2, \ldots, 0+\mathfrak{I}_n)$, ez a szimmetria miatt elég. A relatív prímség miatt $i \geq 2$ esetén létezik $a_i \in \mathfrak{I}_1$ és $b_i \in \mathfrak{I}_i$, hogy $a_i + b_i = 1$. Legyen $x = \prod_{i=2}^n b_i$. Ekkor $x+\mathfrak{I}_1 = \prod_{i=2}^n (1-a_i)+\mathfrak{I}_1 = 1+\mathfrak{I}_1$, és $x \in \mathfrak{I}_2, \ldots, \mathfrak{I}_n$, így az $x+\mathfrak{I} \in R/\mathfrak{I}$ elem képe valóban megfelelő alakú lesz. □

2. fejezet

Az Alon-féle kombinatorikus nullhelytétel és bizonyításai

2.1. A kombinatorikus nullhelytétel

2.1. Tétel (Kombinatorikus nullhelytétel vagy kombinatorikus Nullstellensatz [1]). *Legyen $\mathbb{F}$ tetszőleges test, n pozitív egész, $\mathbf{x} = (x_1, \ldots, x_n)$, azaz n darab változónak a vektora, és $f \in \mathbb{F}[\mathbf{x}]$ polinom. Legyenek továbbá az $S_1, \ldots, S_n \subseteq \mathbb{F}$ halmazok végesek és nem üresek, és definiáljuk a $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$ polinomokat. Amennyiben f minden $\mathbf{s} \in S_1 \times \ldots \times S_n$ pontban nullát vesz fel (azaz $f(\mathbf{s}) = 0$), akkor léteznek $h_1, \ldots, h_n \in \mathbb{F}[\mathbf{x}]$ polinomok, melyekkel teljesül az*

$$f = \sum_{i=1}^{n} h_i g_i$$

egyenlőség, miközben $\deg(h_i) \leq \deg(f) - \deg(g_i)$.

2.2. *Megjegyzés.* Ha $f \in R[\mathbf{x}]$, ahol R az $\mathbb{F}$ test egy részgyűrűje, akkor a h_i polinomokról is feltehető, hogy elemei $R[\mathbf{x}]$-nek.

A kombinatorikus nullhelytétel ezen kimondását gyakran szokás erős alaknak nevezni, megkülönböztetve az alkalmazásokban legtöbbször felhasznált ún. gyenge formájától, amit majd a következő alfejezetben el nem tűnési tétel néven le fogunk vezetni a 2.1 tételből.

A 2.1 tétel –melyre ezen dolgozatnak a nagy része is épül– bizonyításához (mint látni fogjuk) csakis elemi állításokat kell használni test feletti polinomokról. Jól mutatja ezt, ha a 2.1 tétel egyváltozós speciális esetét tekintjük: ekkor a tétel azt állítja, hogy az f test fölötti $\deg(f)$ fokú polinomnak legfeljebb $\deg(f)$ zérushelye van. Először ezt az egyszerű tényt fogjuk általánosítani a tétel bizonyításához.

2.3. Lemma ([1]). *Legyen $\mathbb{F}$ tetszőleges test, és $P \in \mathbb{F}[\mathbf{x}]$ egy n-változós polinom. Tegyük fel, hogy P, mint x_i polinomja legfeljebb t_i (nem-negatív egész) fokú ($1 \leq i \leq n$), és ekkor legyenek $S_i \subseteq \mathbb{F}$, melyekre $|S_i| \geq t_i + 1$. Amennyiben $P(\mathbf{s}) = 0$ minden $\mathbf{s} \in S_1 \times \ldots \times S_n$ pontban, akkor $P \equiv 0$.*

Bizonyítás. Az állítást n-re vett indukcióval bizonyítjuk. Az $n = 1$ esetben a lemma állítása ekvivalens azzal, hogy egy t_1 fokú polinomnak legfeljebb t_1 gyöke van, ez egy jól ismert algebrai állítás. Most tegyük fel, hogy a lemmát már igazoltuk az $n-1$ esetben. Írjuk fel a $P = P(\mathbf{x})$ polinomot, mint x_n polinomját, ekkor

$$P = \sum_{i=0}^{t_n} P_i(\mathbf{x}_{-n}) x_n^i$$

ahol P_i minden i-re egy olyan polinom, mely az x_j változóban legfeljebb t_j fokú minden $j<n$-re, és $\deg_{x_n}(P_i)=0$. Amennyiben rögzítjük az $\mathbf{s}_{-n}\in S_1\times\ldots\times S_{n-1}$ rendezett $n-1$-est és behelyettesítjük P-be az $\mathbf{x}_{-n}$ helyére, akkor egy $\mathbb{F}[x_n]$ gyűrűbeli polinomot kapunk, melybe bármelyik $s_n\in S_n$ értéket helyettesítjük be, eltűnik. Így a már igazolt $n=1$ eset miatt ez az azonosan 0 polinom lesz, vagyis az összes együtthatója 0, azaz $P_i(\mathbf{s}_{-n})=0$. Mivel ez teljesül minden $\mathbf{s}_{-n}\in S_1\times\ldots\times S_{n-1}$ elemre, az indukciós feltevés következtében $P_i\equiv 0$. Vagyis $P\equiv 0$, amivel beláttuk a lemmát. □

A 2.1 tétel bizonyítása. Legyen $t_i:=|S_i|-1$ minden i-re. Osszuk el f-et maradékosan a g_i polinomokkal (1.2 definíció). Az 1.3 tétel miatt az osztás során keletkező hányadosok, azaz a h_i polinomok, teljesíteni fogják a fokukra vonatkozó feltételeket, a maradékra pedig $r=f-\sum_{i=1}^n h_ig_i$, és $\deg_{x_i}(r)\le t_i$. Vegyük észre, hogy minden $\mathbf{s}\in S_1\times\ldots\times S_n$ esetén $r(\mathbf{s})=0$. Alkalmazhatjuk tehát r-re a 2.3 lemmát, vagyis $r\equiv 0$, tehát $f=\sum_{i=1}^n h_ig_i$. Az 1.3 állításból következik a 2.2 megjegyzés is. □

2.4. *Megjegyzés.* Könnyen látható, hogy $\mathbb{F}$-ről csak azt használtuk ki a lemmában és a tételben is, hogy egy integritási tartomány, így ilyen gyűrűk feletti halmazokra és polinomokra is igaz a 2.1 tétel, de ez persze következik azon jól ismert algebrai tételből is, hogy az integritási tartomány beágyazható a hányadostestébe.

2.2. Bizonyítás kommutatív algebrai eszközökkel

A kiterjesztett nullhelytételeket többek között absztrakt algebrai eszközökkel fogjuk bizonyítani, így érdemes végiggondolni, hogy hogyan bizonyíthatjuk be ilyen módszerrel a nullhelytétel előbb bemutatott, legegyszerűbb formáját. Ennek a bizonyításnak nagy előnye, hogy nincs szüksége speciális, a 2.3 lemmához hasonló állításokra, ugyanis az érvelés lényege bizonyos faktorgyűrűk dimenziójának a leszámlálása.

A 2.1 tétel bizonyítása. Definiáljuk a következő ideálokat:

$$\mathfrak{I}(\mathbf{s})=\Big\{f\in\mathbb{F}[\mathbf{x}]\;\Big|\;f(\mathbf{s})=0\Big\}\ \text{ és }\ \mathfrak{I}=\bigcap_{\mathbf{s}\in S_1\times\ldots\times S_n}\mathfrak{I}(\mathbf{s}).$$

$\mathfrak{I}(\mathbf{s})$ nyilván ideál, hiszen egy elemét egy akármilyen polinommal megszorozva $\mathbf{s}$ továbbra is gyöke marad. Azért ilyen módon konstruáltuk meg az $\mathfrak{I}$ ideált, mert így pontosan azokat a polinomokat tartalmazza, melyek minden $\mathbf{s}$ pontban eltűnnek.

Vegyük észre, hogy $\mathfrak{I}(\mathbf{s})=\big(x_1-s_1,\ldots,x_n-s_n\big)$, mivel a jobb oldal nyilván része a bal oldalnak, valamint a jobboldalon egy maximális ideál szerepel, és a bal oldalnak nem eleme 1. Ennek következtében az $\mathfrak{I}(\mathbf{s})$ ideálok páronként relatív prímek (a különböző s_i-hez tartozó generátorelemek különbsége nem 0 és eleme $\mathbb{F}$-nek), és $\dim_{\mathbb{F}}\left(\mathbb{F}[\mathbf{x}]/\mathfrak{I}(\mathbf{s})\right)=1$ minden $\mathbf{s}\in S_1\times\ldots\times S_n$-re. Alkalmazhatjuk az 1.10, vagyis a kínai-maradéktételt:

$$\mathbb{F}[\mathbf{x}]/\mathfrak{I}\cong\bigoplus_{\mathbf{s}\in S_1\times\ldots\times S_n}\mathbb{F}[\mathbf{x}]/\mathfrak{I}(\mathbf{s}),$$

amiből a dimenziók számára a $\dim_{\mathbb{F}}\mathbb{F}[\mathbf{x}]/\mathfrak{I}=\sum_{\mathbf{s}\in S_1\times\ldots\times S_n}\dim_{\mathbb{F}}\mathbb{F}[\mathbf{x}]/\mathfrak{I}(\mathbf{s})=\prod_{i=1}^n|S_i|$ egyenlőséget kapjuk.

Tekintsünk először az f polinomot az $\mathbb{F}[\mathbf{x}]$ polinomgyűrű egy tetszőleges elemének, és osszuk el a g_i polinomokkal maradékosan. Ekkor az 1.3 állítás miatt $\deg(h_i)\le\deg(f)-\deg(g_i)$, és az r maradékra $\deg_{x_i}r<|S_i|$, tehát a maradékok vektorterének a dimenziója $\prod_{i=1}^n|S_i|$. Ekkor az 1.4 állítás **a)** része miatt $\dim_{\mathbb{F}}\mathbb{F}[\mathbf{x}]/(g_1,\ldots,g_n)\le\prod_{i=1}^n|S_i|$. Továbbá könnyen ellenőrizhetően $g_i\in\mathfrak{I}$, emiatt $(g_1,\ldots,g_n)\subseteq\mathfrak{I}$ egy altér, tehát ez csak úgy lehet, ha $\dim_{\mathbb{F}}\mathbb{F}[\mathbf{x}]/(g_1,\ldots,g_n)=\prod_{i=1}^n|S_i|$, és emiatt $(g_1,\ldots,g_n)=\mathfrak{I}$.

A feltétel szerint $f\in\mathfrak{I}=(g_1,\ldots,g_n)$, és az osztási maradék egyértelmű az 1.4 állítás **b)** része miatt, tehát $r\equiv 0$. □

2.3. El nem tűnési tételek/kritériumok

Ebben a fejezetben feltesszük, hogy $\mathbb{F}$ tetszőleges test, és $f \in \mathbb{F}[\mathbf{x}]$ polinom. A 2.1 tétel igazi ereje a belőle levezethető el nem tűnési kritériumban jelenik meg. Ezek elégséges feltételt adnak arra, hogy az f polinom mikor nem azonosan 0 az $S_1 \times \ldots \times S_n$ halmazon.

2.5. Tétel (Kombinatorikus nullhelytétel, el nem tűnési változat [1]). *Tegyük fel, hogy* $\deg(f) = \sum_{i=1}^{n} t_i$, *ahol* t_i *nemnegatív egészek, és a* $\prod_{i=1}^{n} x_i^{t_i}$ *monom együtthatója* f*-ben nem* 0 *(vagy másképpen fogalmazva,* $\prod_{i=1}^{n} x_i^{t_i}$ *maximális fokú tagja* f*-nek). Ekkor, ha* $S_i \subseteq \mathbb{F}$ *és* $|S_i| \geq t_i + 1$ *minden* $1 \leq i \leq n$*-re, akkor létezik* $\mathbf{s} \in S_1 \times \ldots \times S_n$, *amire* $f(\mathbf{s}) \neq 0$.

Bizonyítás. Tegyük fel, hogy f mégis azonosan 0 az $S_1 \times \ldots \times S_n$ halmazon. Legyen $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$, ekkor a 2.1 tétel miatt léteznek $h_1, \ldots, h_n \in \mathbb{F}[\mathbf{x}]$ polinomok, melyekkel

$$f = \sum_{i=1}^{n} h_i g_i, \text{ és minden } j\text{-re } \deg(h_j) \leq \left(\sum_{i=1}^{n} t_i\right) - \deg(g_j) = \left(\sum_{i=1,\, i \neq j}^{n} t_i\right) - 1$$

Így h_j kifejtésében a skatulya elv miatt minden monom valamelyik $i \neq j$-re legfeljebb $x_i^{t_i - 1}$-gyel osztható. Tehát $\prod_{i=1}^{n} x_i^{t_i}$ együtthatója a jobboldalon 0 lesz, de ez ellentmond az f-re tett feltevésünknek. □

Ez az egyik leghasznosabb következménye a 2.1 tételnek, számtalan alkalmazással rendelkezik (lásd [1], [2], [6], [8]). Ennek a következő, egy kicsit általánosabb alakját is be lehet látni ([5]).

2.6. Következmény ([5]). *Tegyük fel, hogy* $\deg(f) = \sum_{i}^{n} t_i$, *ahol* t_i *nemnegatív egészek, és a* $\prod_{i=1}^{n} x_i^{t_i}$ *monom együtthatója* f*-ben nem* 0. *Ha* $S_i \subseteq \mathbb{F}$ *és* $r_i = |S_i| - t_i \geq 1$ *minden* $1 \leq i \leq n$*-re, és léteznek olyan* $D_i \subseteq S_i$ *halmazok, hogy* $D_1 \times \ldots \times D_n$ *tartalmazza az összes olyan pontot, ahol* f *nem* 0, *akkor* $|D_i| \geq r_i$ *minden* $1 \leq i \leq n$ *esetén.*

Bizonyítás. Tegyük fel, hogy valamely j-re $|D_j| < r_j$. Legyen $l_j(x_j) = \prod_{d \in D_j}(x_j - d)$. Mivel $f l_j$-nek $x_1^{t_1} \ldots x_{j-1}^{t_{j-1}} x_j^{t_j + |D_j|} x_j^{t_j} \ldots x_n^{t_n}$ maximális fokú tagja, és $t_j + |D_j| < |S_j|$ (ez az indirekt feltevés), valamint $i \neq j$-re $t_i < |S_i|$, ezért alkalmazható a 2.5 lemma, vagyis létezik $\mathbf{s} \in S_1 \times \ldots \times S_n$, hogy $(f l_j)(\mathbf{s}) \neq 0$. Azonban, ha $s_j \in D_j$, akkor l_j vesz fel 0 értéket, egyébként pedig $\mathbf{s} \notin D_1 \times \ldots \times D_n$, ekkor f kénytelen 0 értéket felvenni, így ez összességében ellentmondás. □

2.4. További bizonyítások az el nem tűnési tételre

A későbbi fejezetekben a 2.5 tétel számos általánosítását fogjuk tekinteni, így érdemes többféle bizonyítást is kidolgozni, hogy minél több fény vetüljön a lényegre. A következő bizonyítások tehát mind a 2.5 tétel bizonyításai, azonban nem használnak fel semmilyen eddig szerepelt tételt vagy lemmát.

2.4.1. Bizonyítás osztott differenciákkal

Ebben a részben végig valós test felett dolgozunk, mivel a következő bizonyítás használ egy középértéktételt az osztott differenciákról. Az 5. fejezetben az osztott differenciákat egy másféle úton felépítve viszont működőképessé tesszük a bizonyítást véges karakterisztikájú testekre is.

2.7. Definíció. Legyen $f \in \mathbb{F}[\mathbf{x}]$, és S_i egy nem üres halmaz. Legyen ekkor $f[S_i]_{x_i}$ az f-nek, mint x_i polinomjának, S_i halmaz elemei szerint vett osztott differenciája. Ez jól-definiált, mivel az osztott differencia nem függ az osztópontok sorrendjétől. Amennyiben f egyváltozós polinom, akkor nem feltétlenül jelöljük a változót.

2.8. Állítás. *Az $f[A]_{x_1} \in \mathbb{F}[\mathbf{x}_{-1}]$ polinom előáll az $f|_{x_1=a} \in \mathbb{F}[\mathbf{x}_{-1}]$ polinomok ($a \in A$), f-től független együtthatóval vett lineáris kombinációjaként.*

Bizonyítás. Az osztott differenciák definícióját felírva $f[a]_{x_1} = f|_{x_1=a}$ ($a \in A$), és ha A legalább kételemű és $a', a'' \in A$, akkor

$$f[A]_{x_1} = \frac{1}{a'-a''} f[A \setminus \{a''\}]_{x_1} - \frac{1}{a'-a''} f[A \setminus \{a'\}]_{x_1}.$$

Mivel lineáris kombinációk kompozíciója is lineáris kombináció, és $\frac{1}{a'-a''}$ független f-től, ezzel beláttuk az állítást. □

A 2.5 tétel bizonyítása az $\mathbb{F} = \mathbb{R}$ esetben. Az S_i halmazokból néhány elemet elhagyva feltehetjük, hogy $|S_i| = t_i + 1$ legyen. Tekintsük az $f[S_1]_{x_1} \dots [S_n]_{x_n}$ osztott differenciát. Mivel f egy valós polinom, ezért az osztott differenciákra vonatkozó középértéktétel szerint létezik $\xi_n \in [\min S_n, \max S_n]$, hogy

$$f[S_1]_{x_1} \dots [S_n]_{x_n} = \frac{1}{t_n!} \partial_{x_n}^{t_n} \left(f[S_1]_{x_1} \dots [S_{n-1}]_{x_{n-1}} \right) (\xi_n)$$

Innen indukcióval világos, hogy létezik $\xi \in [\min S_1, \max S_1] \times \dots \times [\min S_n, \max S_n]$, amire

$$f[S_1]_{x_1} \dots [S_n]_{x_n} = \partial_{x_1}^{t_1} \dots \partial_{x_n}^{t_n} f(\xi) \tag{2.1}$$

Mivel $\mathbf{x}^{\mathbf{t}}$ maximális fokú monom f-ben, a jobboldalon $\mathbf{x}^{\mathbf{t}}$ együtthatója áll, amiről viszont feltettük, hogy nem 0. A bal oldal pedig $f(\mathbf{s})$ ($\mathbf{s} \in S_1 \times \dots \times S_n$) alakú elemek lineáris kombinációja, így nem lehet mindegyik 0. □

2.4.2. Bizonyítás indukcióval

Bizonyítás. ([12]) Indukcióval bizonyítjuk $\sum_{i=1}^n t_i$ értéke szerint. Ha $\sum_{i=1}^n t_i = 0$, akkor $t_i = 0$ és így f nem függ $\mathbf{x}$-től, viszont $\mathbf{x}^{\mathbf{0}}$ együtthatója nem 0, tehát $f \equiv c \neq 0$, vagyis ekkor igaz az állítás.

Legyen most $\sum_{i=1}^n t_i > 0$, feltehetjük, hogy $t_1 > 0$. Legyen $a \in S_1$ és osszuk el f-et maradékosan $(x_1 - a)$-val:

$$f = g \cdot (x_1 - a) + h, \text{ ahol } \deg_{x_1}(h) = 0 \text{ így } h \text{ csak } \mathbf{x}_{-1}\text{-től függ.}$$

Ha valamilyen $\mathbf{s} \in S_1 \times \dots \times S_n$ vektorra $h(\mathbf{s}) \neq 0$, akkor $f(a, \mathbf{s}_{-1}) = h(a, \mathbf{s}_{-1}) = h(\mathbf{s}) \neq 0$, mivel x_1-től nem függ h. Egyébként pedig alkalmazzuk az indukciós feltevést g-re, aminek a maradékos osztás tulajdonságai miatt $\mathbf{x}^{(t_1-1, t_2, \dots, t_n)}$ maximális fokú monomja, így van egy $\mathbf{s} \in (S_1 \setminus \{a\}) \times S_2 \times \dots \times S_n$ pont, amire $g(\mathbf{s}) \neq 0$. Mivel $s_1 \neq a$, ezért $f(\mathbf{s}) = g(\mathbf{s})(s_1 - a) + h(\mathbf{s}) = g(\mathbf{s})(s_1 - a) \neq 0$. □

3. fejezet

Alkalmazások

Ebben a fejezetben a kombinatorikus nullhelytétel néhány, főként számelméleti alkalmazását mutatjuk be. Meg kell még említenünk, hogy a kombinatorikus nullhelytétel számos gráfelméleti alkalmazással is rendelkezik, jó áttekintés található Alon munkájában [1].

3.1. Kockafedések

A következő tétel Alon és Füredi cikkében található ([3]), számos kiterjesztésével együtt. A tétel igaz marad akkor is, ha az egységkocka csúcsai helyett valamilyen téglába eső rácspontok halmazát vesszük, ezt majd a 4. fejezetben látni fogjuk.

3.1. Tétel ([3]). *Tegyük fel, hogy $H_1, H_2, \ldots, H_m$ hipersíkok $\mathbb{R}^n$-ben, és nem mennek át a $\mathbf{0} \in \mathbb{R}^n$ ponton, de lefedik az n dimenziós egységkocka többi csúcsát, azaz a $\{0,1\}^n \setminus \{\mathbf{0}\}$ halmaz pontjait. Ekkor $m \geq n$, és n darab hipersík elegendő is.*

Bizonyítás. ([1]) Tegyük fel indirekten, hogy $m < n$. Legyen $(\mathbf{a}_{i.}, \mathbf{x}) = b_i$ a H_i hipersíkot megadó egyenlet ($\mathbf{a}_{i.} \in \mathbb{R}^n$, $b_i \in \mathbb{R}$ és $(.,.)$ a skaláris szorzatot jelöli). Mivel $\mathbf{0} \notin H_i$, ezért $b_i \neq 0$. Legyen

$$f(\mathbf{x}) = \prod_{i=1}^{m} ((\mathbf{a}_{i.}, \mathbf{x}) - b_i) \quad \text{valamint} \quad P(\mathbf{x}) = \prod_{i=1}^{n} (1 - x_i) \quad \text{és} \quad F(\mathbf{x}) = f(\mathbf{x}) - f(\mathbf{0})P(\mathbf{x}).$$

Legyen $S_i = \{0, 1\}$ minden $1 \leq i \leq n$-re, ekkor $F(\mathbf{s}) = 0$ minden $\mathbf{s} \in S_1 \times \ldots \times S_n$-re, hisz $P(\mathbf{0}) = 1$, valamint $P(\mathbf{x}) \neq 0 \Leftrightarrow \mathbf{x} = \mathbf{0}$, vagyis $F(\mathbf{0}) = 0$, egyéb $\mathbf{s}$ esetén pedig $F(\mathbf{s}) = f(\mathbf{s})$. Vegyük észre, hogy $f(\mathbf{0}) \neq 0$, mivel egyenlőségből az következne, hogy $\mathbf{0}$ rajta van valamelyik hipersíkon. Kihasználva az indirekt feltevést, és hogy $f(\mathbf{0}) \neq 0$, $\deg(f) = m < n = \deg(f(\mathbf{0})P)$, így $\deg(F) = n$, és a legnagyobb fokú tag kitevői ugyanazok, mint P-ben. Mivel a legnagyobb fokú tag itt nyilván $\prod_{i=1}^{n} x_i$, így alkalmazva a 2.5 tételt a valós számok $\mathbb{R}$ testére, miközben $t_i = 1$ minden i-re, azt kapjuk, hogy létezik $\mathbf{s} \in S_1 \times \ldots \times S_n$, hogy $F(\mathbf{s}) \neq 0$. Ez ellentmondás, tehát mégis $m \geq n$.

Az is világos, hogy n sík elegendő: $\mathbf{a}_{i.} = \mathbf{e}_{i.}$ és $b_i = 1$ választással (ahol $\mathbf{e}_{i.}$ a $\mathbb{R}^n$ standard bázisának i. eleme) pontosan azokat a pontokat fedjük le, amiknek legalább az egyik koordinátája 1. □

3.2. A Chevalley-Warning tétel

3.2. Tétel (Chevalley-Warning tétel). *Legyen p prím és $\mathbb{F}_p$ a p elemű test. Legyenek $P_1, \ldots, P_m \in \mathbb{F}_p[\mathbf{x}]$ polinomok. Ha $\sum_{i=1}^{m} \deg(P_i) < n$ és létezik egy $\mathbf{c} \in \mathbb{F}_p^n$ közös gyöke a polinomoknak (azaz $P_i(\mathbf{c}) = 0$ minden $1 \leq i \leq m$-re), akkor létezik egy másik közös gyök is.*

Bizonyítás. Tegyük fel, hogy nem igaz az állítás, és legyen

$$q(\mathbf{x})=\prod_{i=1}^{m}(1-P_i(\mathbf{x})^{p-1}),\quad r(\mathbf{x})=\delta\prod_{j=1}^{n}\prod_{c\in\mathbb{F}_p,c\neq c_j}(x_j-c)\quad\text{ahol}\quad\delta=\prod_{j=1}^{n}\prod_{c\in\mathbb{F}_p,c\neq c_j}(c_j-c)^{-1},\text{ és}$$

$$f(\mathbf{x})=q(\mathbf{x})-r(\mathbf{x}).$$

Legyen $S_i=\mathbb{F}_p$ $(1\le i\le n)$, és vegyük észre, hogy minden $\mathbf{s}\in S_1\times\ldots\times S_n$ vektorra $f(\mathbf{s})=0$. Ha $\mathbf{s}=\mathbf{c}$, akkor $q(\mathbf{s})=r(\mathbf{s})=1$. Ha pedig valamely i-re $s_i\neq c_i$, akkor az indirekt feltevés szerint valamely j-re $1-P_j(\mathbf{s})^{p-1}=0$ (P_j-nek nem gyöke $\mathbf{s}$), így $q(\mathbf{s})=0$, és $r(\mathbf{s})=0$ is teljesül, hiszen osztható (x_i-s_i)-vel. Mivel $\delta\neq 0$ és $\deg(q)=\sum_{i=1}^{m}((p-1)\deg(P_i))<(p-1)n=\deg(r)$, ezért f-ben $\prod_{j=1}^{n}\prod_{c\in\mathbb{F}_p,c\neq c_j}x_j=$ $=\prod_{j=1}^{n}x_j^{p-1}$ együtthatója $-\delta\neq 0$. Tehát $t_i=p-1$ választással alkalmazhatjuk a 2.5 tételt, azaz létezik olyan $\mathbf{s}\in S_1\times\ldots\times S_n$, amire $f(\mathbf{s})\neq 0$, ez ellentmondás. □

3.3. *Megjegyzés.* A tétel könnyen igazolható bármilyen véges test felett is, hisz $\mathbb{F}_{p^\alpha}$ testben $1=x^{p^\alpha-1}$ és $x\neq 0$ ekvivalensek, vagyis a bizonyításban mindenhol írhatunk p helyére p^α-t.

3.2.1. Az Erdős-Ginzburg-Ziv tétel

3.4. Tétel. *Legyen $k\ge 1$, és $a_1,\ldots,a_{2k-1}\in\mathbb{Z}$ nem feltétlen különböző egészek. Ekkor kiválasztható k darab elem ezek közül, hogy $a_{i_1}+\ldots+a_{i_n}\equiv 0\ (mod\ k)$.*

Könnyű belátni, hogy a tétel állítása visszavezethető $k=p$ prím esetre. Ez az eset viszont egyszerű következménye a Chevalley-Warning tételnek.

3.5. Állítás. *Legyen p prím, és $a_1,\ldots,a_{2p-1}\in\mathbb{F}_p$. Ekkor van közöttük p darab, melyek összege 0.*

Bizonyítás. Legyenek $f_1,f_2\in\mathbb{F}_p[x_1,\ldots,x_{2p-1}]$ a következő polinomok:

$$f_1=\sum_{i=1}^{2p-1}x_i^{p-1}\qquad f_2=\sum_{i=1}^{2p-1}a_ix_i^{p-1}.$$

Mivel $f_1(\mathbf{0})=f_2(\mathbf{0})=0$, és $\deg(f_1)+\deg(f_2)=2p-2<2p-1$, így a 3.2 tétel miatt van még egy közös gyökük, legyen az $(c_1,\ldots,c_{2n-1})$. Vegyük észre, hogy f_1 és f_2 értéke csak attól függ, hogy mely c_i értéke 0-e vagy sem, hiszen $c_i^{p-1}=\chi(c_i\neq 0)$. így legyen $C=\{i\mid c_i\neq 0\}$. Az f_1 polinom miatt $p\,|\,|C|$, de mivel nem lehet mindegyik $c_i=0$ (nem azonos a $\mathbf{0}$ közös gyökkel), ezért $p=|C|$. Ekkor persze

$$f_2(\mathbf{c})=\sum_{i=1}^{2p-1}a_ic_i^{p-1}=\sum_{i\in C}a_i=0$$

tehát beláttuk az állítást. □

3.3. A Cauchy-Davenport tétel és egyéb számelméleti tételek

3.6. Tétel (Caucy-Davenport tétel)**.** *Legyen p prím, és $A,B\subseteq Z_p$ nem üres részhalmazok. Ekkor*

$$|A+B|\ge\min\{p,|A|+|B|-1\}.$$

Bizonyítás. ([1]) Ha $|A|+|B|>p$, akkor minden $g\in Z_p$ esetén az A és $g-B$ halmazok metszete nem üres, tehát $A+B=Z_p$. Így elég azt az esetet tekinteni, amikor $|A|+|B|\le p$, ekkor indirekt módon tegyük fel, hogy $|A+B|\le|A|+|B|-2$. Legyen $C\subseteq Z_p$ olyan, hogy $A+B\subseteq C$ és $|C|=|A|+|B|-2$. Legyen

$$f(x,y)=\prod_{c\in C}(x+y-c),\text{ ekkor persze }f(a,b)=0\ \text{ minden }a\in A,\ b\in B\text{ esetén.}$$

Mivel $\deg(f)=|C|=|A|-1+|B|-1$, így alkalmazva a 2.5 tételt $n=2$-re $\mathbb{F}_p$ testtel, miközben $t_1=|A|-1$, $t_2=|B|-1$ és $S_1=A$, $S_2=B$, ellentmondást kapunk, amennyiben $x^{|A|-1}y^{|B|-1}$ együtthatója nem 0. Ezt a monomot az f polinomban a zárójeleket kibontva $\binom{|A|-1+|B|-1}{|A|-1}$-féleképpen kaphatjuk meg, így ennyi az együtthatója. Mivel $|A|+|B|-2<p$, a binomiális együttható faktoriálisos kiszámításában nem szerepel sehol sem a 0 tényezőként, így tehát Z_p felett is teljesül, hogy $\binom{|A|-1+|B|-1}{|A|-1}\neq 0$. Tehát létezik $a\in A$ és $b\in B$, hogy $f(a,b)\neq 0$, ez ellentmondás. □

A következő két rész mindegyikében szükségünk lesz a következő lemmára.

3.7. Lemma. *Legyen p prím és $\varepsilon_1,\ldots,\varepsilon_m\in\mathbb{C}$ mindegyike $q=p^\alpha$-adik egységgyök. Ha $\sum_{i=1}^m \varepsilon_i=0$, akkor p osztja az m számot.*

Bizonyítás. Legyen ε primitív q-adik egységgyök, ekkor léteznek α_i egész számok, hogy $\varepsilon_i=\varepsilon^{\alpha_i}$. Legyen $R(x)=\sum_{i=1}^m x^{\alpha_i}$ polinom, ennek gyöke ε. Ekkor $\mathbb{Z}[x]$ gyűrűben osztható lesz ε minimálpolinomjával, azaz a q. körosztási polinommal, $\Phi_q(x)$-szel. Ekkor $x=1$-et helyettesítve $R(1)=m$ és $\Phi_q(1)=p$, tehát $\mathbb{Z}$-ben p osztja m-et. □

3.3.1. Korlátozott összegek (Restricted sums)

3.8. Definíció. Legyen $\mathbb{F}$ test, $\mathbf{x}\in\mathbb{F}^n$, és $h\in\mathbb{F}[\mathbf{x}]$. Az $A_1,\ldots,A_k\subseteq\mathbb{F}$ halmazok h polinom által korlátozott összegén a következő halmazt értjük:

$$\oplus_h\sum_{i=1}^n A_i=\left\{a_1+\ldots+a_n \;\middle|\; \mathbf{a}\in A_1\times\ldots\times A_n \text{ minden } i\text{-re, és } h(\mathbf{a})\neq 0\right\}$$

A korlátozott összegekre levezethető a kombinatorikus nullhelytételből egy általánosabb tétel, aminek a Cauchy-Davenport tétel is speciális esete. Érdemes megjegyezni, hogy ez a tétel korábbi, mint a kombinatorikus nullhelytétel. Alon eredetileg ezt a tételt látta be közvetlenül, és csak később emelte ki a bizonyításból a kombinatorikus nullhelytételt. Ezt szokás "polinom lemmának/módszernek" is nevezni, emiatt a kombinatorikus nullhelytételt is illetik ezzel a névvel.

3.9. Tétel ([1])**.** *Tegyünk fel mindent úgy, ahogy az előző definícióban szerepel. Legyen $t_i=|A_i|-1$ és $m=(\sum_{i=1}^n t_i)-\deg(h)$. Ha a*

$$h(\mathbf{x})(x_1+\ldots+x_n)^m\in\mathbb{F}[\mathbf{x}] \tag{3.1}$$

polinomban a $\prod_{i=1}^n x_i^{t_i}$ együtthatója nem 0, akkor $|\oplus_h\sum_{i=1}^n A_i|\geq m+1$ (és ekkor $p>m$).

Bizonyítás. Tegyük fel, hogy az állítás nem igaz, és legyenek $c_1,\ldots,c_m$ nem feltétlenül különböző elemek, amikre $\oplus_h\sum_{i=1}^n A_i\subseteq\bigcup_{i=1}^n\{c_i\}$. Legyen $f\in\mathbb{F}[\mathbf{x}]$ a következő polinom:

$$f(\mathbf{x})=h(\mathbf{x})\prod_{i=1}^m(x_1+\ldots+x_n-c_i).$$

Vegyük észre, hogy minden $\mathbf{a}\in A_1\times\ldots\times A_n$ esetén $f(\mathbf{a})=0$, hiszen ha $h(\mathbf{a})\neq 0$, akkor létezik j, hogy $a_1+\ldots+a_n=c_j$. Az f polinom foka legfeljebb akkora, mint a (3.1) alatt szereplőé, és ezért a maximális fokú $\prod_{i=1}^n x_i^{t_i}$ monom együtthatója bennük megegyezik, vagyis f-ben sem 0. Legyen tehát $S_i=A_i$, és ekkor f-re alkalmazva a 2.5 tételt megkapjuk, hogy létezik $\mathbf{a}\in A_1\times\ldots\times A_n$, hogy $f(\mathbf{a})\neq 0$, ez ellentmondás. □

Vegyük észre, hogy ha $n=2$ és $h\equiv 1$, akkor $m=|A_1|+|A_2|-2$, és így "visszakapjuk" a Caucy-Davenport tételt (a bizonyítás lényegében változatlan). A tétel egyszerű alkalmazásaként kapjuk például a következő tételt.

3.10. Tétel ([1]). *Legyen p prím és $A, B \subseteq F_p$ nem-üres részhalmazok. Ekkor*

$$\{a+b \mid a \in A,\ b \in B \text{ és } ab \neq 1\} \geq \min\{p, |A|+|B|-3\}.$$

Bizonyítás. Feltehetjük, hogy $|A| \geq 2$ és $|B| \geq 2$, mivel egyébként az állítás semmitmondó. Ha $p = \min\{p,\ |A|+|B|-3\}$, akkor hagyjuk el A és B néhány elemét úgy, hogy $|A|+|B|-3 = p$ legyen, ekkor elegendő a lecsökkentett halmazokra belátni a tételt, hiszen visszatéve az elhagyott elemeket, a korlátozott összeg mérete csak nőhet. Ha $|A|+|B|-3 \leq p$, akkor alkalmazzuk a 3.9 tételt, legyenek $n=2$, $h(x,y) = xy-1$, $A_1 = A$, $A_2 = B$, és ekkor $m = |A|+|B|-4$. Az $(x+y)^{|A|+|B|-4}(xy-1)$ polinomban az $x^{|A|-1}y^{|B|-1}$ együtthatója $\binom{|A|+|B|-4}{|A|-2}$, ami nem 0, hiszen $|A|+|B|-4 < p$, $|A|-2 < p$, és $|B|-2 < p$ (kisebbek a karakterisztikánál). □

3.3.2. Az Erdős-Heilbronn sejtés

3.11. Definíció. A fejezetben lényegében a következő halmaz számosságát fogjuk becsülni, így bevezetünk egy jelölést:

$$A \dot{+} B = \{a+b \mid a \in A,\ b \in B \text{ és } a \neq b\}$$

3.12. Tétel (Erdős-Heilbronn sejtés). *Legyen p prím és $A \subseteq Z_p$, és legyen $C = A \dot{+} A$. Ekkor*

$$|A \dot{+} A| \geq \min\{p, 2|A|-3\}$$

Bizonyítás. A $p=2$ eset triviális, és azt is nyilván feltehetjük, hogy $|A| = k \geq 2$. Mivel $A \subseteq A'$ miatt $A \dot{+} A \subseteq A' \dot{+} A'$, ezért ha $p = \min\{p,\ 2|A|-3\}$, akkor feltehető, hogy $2k-3 = p$. Ha $2k-3 \leq p$, akkor alkalmazzuk a 3.9 tételt, legyenek $n=2$, $h(x,y) = x-y$, $A_1 = A$, $A_2 = A \setminus \{a\}$, ahol $a \in A$ tetszőleges elem. Nyilvánvaló, hogy $A \dot{+} A = A_1 \dot{+} A_2$. Tehát $m = 2k-4$, és az $(x+y)^{2k-4}(x-y)$ polinomban az $x^{k-1}y^{k-2}$ együtthatója

$$\binom{2k-4}{k-2} - \binom{2k-4}{k-1} = \frac{(k-1)(2k-4)! - (k-2)(2k-4)!}{(k-1)!\,(k-2)!} = \frac{(2k-4)!}{(k-1)!\,(k-2)!}$$

Ez nem 0, mivel $2k-4 < p$. □

Az állítás minden Abel-csoportban is igaz ([8]), ha p helyére a nem 0 elemek rendjének a minimumát írjuk (ez lehet ∞ is). Az előző tételnél egy kicsit általánosabb tételt fogunk belátni, amivel a Z_{p^α} csoportokra is igazoljuk az Erdős-Heilbronn sejtést. Ehhez a G csoportot a $\mathbb{C}$ komplex számok multiplikatív csoportjába fogjuk beágyazni.

3.13. Tétel ([8]). *Legyen p prím, $q = p^\alpha$, $A, B \subseteq \mathbb{F}_q$ nemüres részhalmazok, és legyen $C = A \dot{+} B$. Ekkor*

$$|A \dot{+} B| \geq \min\{p, |A|+|B|-3\}$$

Bizonyítás. Feltehetjük, hogy $|A| = k \leq 2$ és $|B| = l \leq 2$. Mivel $A \subseteq A'$ és $B \subseteq B'$ maga után vonja, hogy $|A' \dot{+} B'| \geq |A \dot{+} B|$, ezért feltehető, hogy $k+l-3 \leq p$.

Legyen $\varepsilon = e^{\frac{2\pi i}{q}}$, és generálja a G csoportot g. Ekkor az ε által a komplex számok $\mathbb{C}^*$ multiplikatív csoportjában generált csoport izomorf lesz G-vel, így definiáljuk a $\varphi : G \hookrightarrow \mathbb{C}^*$ beágyazást a $\varphi(kg) = \varepsilon^k$ hozzárendeléssel. Definiáljuk a következő halmazokat:

$$\tilde{A} = \{\varphi(a) \mid a \in A\},\ \tilde{B} = \{\varphi(b)^{-1} \mid b \in B\},\ \tilde{C} = \{\varphi(c) \mid c \in C\}$$

Vegyük észre, hogy $a \in A$, $b \in B$, és $c \in C$ elemekre

$$a = b \Longleftrightarrow \varphi(a)\varphi(b)^{-1} - 1 = 0, \quad \text{és} \quad a+b = c \Longleftrightarrow \varphi(a) - \varphi(c)\varphi(b)^{-1} = 0 \tag{3.2}$$

Tehát ha $\tilde{a} \in \tilde{A}$ és $\tilde{b} \in \tilde{B}$ akkor $\tilde{a}\tilde{b} - 1 = 0$ vagy létezik $\tilde{c} \in \tilde{C}$, hogy $\tilde{a} - \tilde{c}\tilde{b} = 0$. Tegyük fel indirekt, hogy $|C| = |\tilde{C}| \leq k+l-4$, és legyen $|\tilde{D}| = k+l-4$ úgy, hogy $\tilde{C} \subseteq \tilde{D} \subseteq \varphi(G)$. Legyen $f \in \mathbb{C}[x,y]$ és

$$f(x,y) = (xy-1) \prod_{\tilde{d} \in \tilde{D}} (x - \tilde{d}y),$$

ekkor $f(\tilde{a}, \tilde{b}) = 0$ minden $\tilde{a} \in \tilde{A}$ és $\tilde{b} \in \tilde{B}$ elemre. Legyen $S_1 = \tilde{A}$, $S_2 = \tilde{B}$, $t_1 = k-1$, $t_2 = l-1$, ekkor az ellentmondáshoz már elég csak azt belátni, hogy $f(x,y)$-ban $x^{k-1}y^{l-1}$ együtthatója nem 0. Ennek az együtthatónak az értéke

$$\sum_{\tilde{E} \subseteq \tilde{D}, |\tilde{E}| = k-2} (-1)^k \prod_{\tilde{e} \in \tilde{E}} \tilde{e}$$

azaz $\binom{k+l-4}{k-2}$ darab q-adik egységgyök összege, hisz $\tilde{e} \in \tilde{E} \subseteq \varphi(G)$. Ekkor a 3.7 lemma miatt készen vagyunk, hiszen $k+l-4 < p$. □

3.4. A Snevily-sejtés

A kombinatorikus nullhelytétellel most egy másik nehéz problémát vizsgálunk.

3.14. Sejtés. *Legyen G véges, páratlan rendű csoport. Ekkor G bármely két k elemű $A = \{a_1, \ldots, a_k\}$ és $B = \{b_1, \ldots, b_k\}$ részhalmazához létezik az $\{1, \ldots, k\}$ elemek egy $\pi \in \mathrm{Sym}(k)$ permutációja, hogy az $a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$ elemek páronként különbözőek.*

A Snevily-sejtést prímrendű ciklikus csoportokra Alon látta be [2] a 2.5 tétel segítségével. Ezt a bizonyítást továbbfejlesztve látták be Károlyi et al. [6], hogy az állítás minden ciklikus csoportra is igaz. A bizonyítás további módosításával Arshovski nemrégiben igazolta a tételt Abel-csoportokra [4].

A páratlan rend szükséges feltétel, hiszen ha $2 \big| |G|$, akkor lesz egy másodrendű $g \in G$, és ekkor $a_1 = b_1 = 0$ és $a_2 = b_2 = g$ esetén nem lehet megfelelő permutációt találni. A tételt először prímrendű ciklikus csoportokra látjuk be Alon bizonyítását [2] követve.

3.4.1. A Z_p illetve a $(Z_p)^\alpha$ esete

Vegyük észre, hogy a 3.14 tétel $G = Z_p$ és $k = p$ páratlan prím esetben triviális, hisz $2a_i$ különböző elemek lesznek Z_p-ben páratlan p esetén (hisz egy elem rendje nem lehet páros). Így a $G = Z_p$ esetben a következő tételből már következik a 3.14 tétel állítása páratlan prímrendű ciklikus csoportokra.

3.15. Tétel ([2])**.** *Legyen $G = Z_p$ prímrendű ciklikus csoport, és $k < p$ pozitív egész. Legyen továbbá $a_1, \ldots, a_k$ a G csoport k darab nem feltétlen különböző eleme, és B pedig k elemű részhalmaza G-nek. Ekkor létezik az $\{1, \ldots, k\}$ elemek egy $\pi \in \mathrm{Sym}(k)$ permutációja, hogy az $a_1 + b_{\pi(1)}, \ldots, a_k + b_{\pi(k)}$ elemek páronként különbözőek.*

A 3.15 és további tételek bizonyításához szükségünk lesz a következő lemmára.

3.16. Lemma. *A $d_{\mathbf{c}}(\mathbf{x}) = \prod_{1 \leq j < i \leq k} (x_i - x_j) \prod_{1 \leq j < i \leq k} (c_i x_i - c_j x_j)$ polinom foka legfeljebb $k(k-1)$, és a $\prod_{i=1}^k x_i^{k-1}$ együtthatója benne $(-1)^{\binom{k}{2}} \mathrm{Per} V(c_1, \ldots, c_k)$.*

Bizonyítás. A polinom foka legfeljebb a $j < i$ párok számának kétszerese, azaz $2\binom{k}{2} = k(k-1)$. Jól ismert tény a Vandermonde-determinánsról, hogy

$$\prod_{1 \leq j < i \leq k} (x_i - x_j) = \mathrm{Det} V(x_1, \ldots, x_k) = \mathrm{Det} \begin{bmatrix} 1 & \ldots & 1 \\ x_1 & \ldots & x_k \\ \vdots & \vdots & \vdots \\ x_1^{k-1} & \ldots & x_k^{k-1} \end{bmatrix} = \sum_{\pi \in \mathrm{Sym}(k)} \mathrm{sgn}(\pi) \prod_{i=1}^k x_i^{\pi(i)-1} \quad (3.3)$$

Hasonlóan kapjuk, hogy

$$\prod_{1\le j<i\le k}(c_ix_i-c_jx_j)=\sum_{\sigma\in\mathrm{Sym}(k)}\mathrm{sgn}(\sigma)\prod_{i=1}^{k}(c_ix_i)^{\sigma(i)-1}=\sum_{\pi\in\mathrm{Sym}(k)}(-1)^{\binom{k}{2}}\mathrm{sgn}(\pi)\prod_{i=1}^{k}(c_ix_i)^{k-\pi(i)} \tag{3.4}$$

hiszen ha $\sigma(i)=k+1-\pi(i)$ minden i-re, akkor $\sigma\in\mathrm{Sym}(k)$, és ha π befutja $\mathrm{Sym}(k)$-t, akkor σ is. Továbbá ha $\mathrm{sgn}(\pi)=(-1)^{N(\pi)}$, akkor $\mathrm{sgn}(\sigma)=(-1)^{\binom{k}{2}-N(\pi)}$, hiszen az inverziók száma az ellentétére változik. A (3.3) és (3.4) egyenleteket szorzatából a $\prod_{i=1}^{k}x_i^{k-1}$ tagokon kívül mindent elhagyva kapjuk, hogy

$$\sum_{\pi\in\mathrm{Sym}(k)}(-1)^{\binom{k}{2}}\prod_{i=1}^{k}c_i^{k-\pi(i)}x_i^{k-1}=(-1)^{\binom{k}{2}}\sum_{\pi\in\mathrm{Sym}(k)}\left(\prod_{j=1}^{k}c_j^{k-\pi(j)}\right)\left(\prod_{i=1}^{k}x_i^{k-1}\right)=$$

$$=(-1)^{\binom{k}{2}}\mathrm{Per}V(\mathbf{c})\prod_{i=1}^{k}x_i^{k-1}$$

□

A 3.15 tétel bizonyítása. Legyen $\mathbf{x}=(x_1,\dots,x_k)$, és az $f\in\mathbb{F}_p[\mathbf{x}]$ polinom a következő:

$$f(\mathbf{x})=\left(\prod_{1\le j<i\le k}(x_i-x_j)\right)\left(\prod_{1\le j<i\le k}^{k}(a_i+x_i-(a_j+x_j))\right)$$

Az f polinom foka és a $\prod_{i=1}^{k}x_i^{k-1}$ monomjának az együtthatója nyilván megegyezik a 3.16 lemmában tárgyalt $d_{\mathbf{1}}$ polinoméval (azaz legyen $\mathbf{c}=\mathbf{1}$). Ekkor $(-1)^{\binom{k}{2}}\mathrm{Per}V(\mathbf{1})=(-1)^{\binom{k}{2}}k!\neq 0$, mivel $\mathrm{char}\,\mathbb{F}_p>k$. Tehát az f polinomra alkalmazhatjuk a 2.5 tételt $S_i=B$ és $t_i=k-1$ $(1\le i\le k)$ helyettesítéssel, így létezik $\mathbf{b}\in B^k$, hogy $f(\mathbf{b})=\left(\prod_{1\le i<j\le k}(b_j-b_i)\right)\left(\prod_{1\le i<j\le k}^{k}(a_j+b_j-(a_i+b_i))\right)\neq 0$ Az első tényező miatt a b_i elemek a B halmaz elemeinek egy permutációját adják, a második tényező miatt pedig az a_i+b_i párok mind különbözőek lesznek. □

3.17. Állítás. *Az előző bizonyítás igazolja $G=(Z_p)^{\alpha}$ esetén is a tételt.*

Bizonyítás. Persze, mivel a 2.5 tételt alkalmazhattuk volna az $\mathbb{F}_{p^\alpha}$ testre is, hisz annak az additív csoportja $(Z_p)^{\alpha}$. Ezen kívül az $\mathbb{F}_p$ testről csak azt használtuk ki, hogy a karakterisztikája p, tehát minden következtetésünk érvényben marad, például $(-1)^{\binom{k}{2}}k!$ továbbra sem egyenlő 0. □

3.4.2. Páratlan rendű ciklikus csoportok

3.18. Tétel ([6]). *Legyen G páratlan rendű ciklikus csoport. Legyen továbbá $A=\{a_1,\dots,a_k\}$ és $B=\{b_1,\dots,b_k\}$ a G csoport két k elemű részhalmaza. Ekkor létezik az $\{1,\dots,k\}$ elemek egy $\pi\in\mathrm{Sym}(k)$ permutációja, hogy az $a_1+b_{\pi(1)},\dots,a_k+b_{\pi(k)}$ elemek páronként különbözőek.*

A 3.4.1 alfejezetben (és a dolgozat nagy részében) a Z_p csoportra az $\mathbb{F}_p$ test additív csoportjaként tekintünk. Azonban egy test lényegében 2 csoportból épül fel, vagyis megpróbálhatjuk kihasználni a multiplikatív csoportjának a tulajdonságait is.

Bizonyítás. Tegyük fel, hogy $|G|=n$, és legyen $\mathbb{F}_{2^{\phi(n)}}$ a test, ami felett dolgozunk, ahol ϕ az Euler-féle függvény. $\mathbb{F}_{2^{\phi(n)}}$ multiplikatív csoportja egy $2^{\phi(n)}-1$ rendű ciklikus csoport, legyen g_1 a generátora. Mivel n osztja a $2^{\phi(n)}-1$ számot, ezért van értelme a $g=g_1^{\frac{2^{\phi(n)}-1}{n}}$ elemről beszélni. Ennek a rendje a multiplikatív csoportban nyilván n, tehát g a G csoporttal izomorf részcsoportját generálja az $\mathbb{F}_{2^{\phi(n)}}$ multiplikatív csoportjának. Feltehetjük tehát, hogy G csoport bele van ágyazva a testbe, innentől kezdve multiplikatíve

tekintünk rá. Legyen $S_i = B$, $t_i = k-1$, és tekintsük a $d_{(a_1,\dots,a_k)}$ polinomot. Mivel $\operatorname{char} \mathbb{F}_{2^{\phi(n)}} = 2$, ezért a 3.16 lemmában szereplő együttható értéke

$$(-1)^{\binom{k}{2}}\mathrm{Per}V(a_1,\dots,a_k) = (-1)^{\binom{k}{2}}\mathrm{Det}V(a_1,\dots,a_k) = (-1)^{\binom{k}{2}} \prod_{1\le j<i\le k} (a_i - a_j) \neq 0$$

Az előző tételhez hasonlóan alkalmazhatjuk a 2.5 tételt, így létezik egy $\mathbf{b}$ vektor, hogy $d_{\mathbf{c}}(\mathbf{b}) \neq 0$. Az első tényező miatt $b_i \neq b_j$, a második tényező miatt pedig $a_i b_i \neq a_j b_j$. □

A komplex számok testének multiplikatív csoportját használva belátjuk a 3.15 tételt kicsit általánosabb csoportokra is.

3.19. Tétel ([6]). *Legyen p prím, $G = Z_{p^\alpha}$ ciklikus csoport, és $k < p$ pozitív egész. Legyen továbbá $a_1, \dots, a_k$ a G csoport k darab nem feltétlen különböző eleme, és B pedig k elemű részhalmaza G-nek. Ekkor létezik az $\{1,\dots,k\}$ elemek egy $\pi \in \mathrm{Sym}(k)$ permutációja, hogy az $a_1 + b_{\pi(1)}, \dots, a_k + b_{\pi(k)}$ elemek páronként különbözőek.*

Bizonyítás. Legyen $q = p^\alpha$, és ε egy q-adik primitív egységgyök $\mathbb{C}$-ben. Ekkor ε generál a $\mathbb{C}^*$ csoportban egy G-vel izomorf részcsoportot, elég erre belátni az állítást. Legyen $S_i = B$, $t_i = k-1$, és tekintsük a $d_{(a_1,\dots,a_k)}$ polinomot. Ahogy az előző tételben is, már csak annyit kell belátnunk, hogy $\mathrm{Per}V(a_1,\dots,a_k) \neq 0$. Kifejtve $\mathrm{Per}V(a_1,\dots,a_k) = \sum_{\pi\in\mathrm{Sym}(k)} \prod_{i=1}^k a_i^{\pi(i)-1} \neq 0$, azonban a $\prod_{i=1}^k a_i^{\pi(i)-1} \neq 0$ tagok a szummából mind q-adik egységgyökök, és $k!$ darab tagja van a szummának. Mivel p nem osztja $k!$-t, így a 3.7 lemma miatt $\mathrm{Per}V(a_1,\dots,a_k)$ nem lehet 0. □

4. fejezet

Kombinatorikus nullhelytétel többszörös gyökökkel és kivételes pontokkal

4.1. Definíció. Az $f \in \mathbb{F}[\mathbf{x}]$ polinomnak t-szeres gyöke van az $\mathbf{s}$ pontban, ha $f_{\mathbf{u}}(\mathbf{s}) = 0$ minden olyan $\mathbf{u} \in \mathbb{N}^n$, melyre $\sum_{i=1}^{n} u_i < t$.

4.2. Definíció. Legyen $T(n,t)$ az $\{1,\ldots,n\}$ halmaz fölötti összes t hosszú, nem-csökkenő sorozat halmaza. Ha $\tau \in T(n,t)$, akkor jelölje $\tau(i)$ a τ sorozat i-ik elemét, és ha j megjelenik a τ sorozatban, akkor azt $j \in \tau$-val jelöljük.

A következőekben kiterjesztjük a kombinatorikus nullhelytételt arra az esetre, amikor nem csak azt tudjuk az f polinomról, hogy bizonyos helyeken 0-t vesz fel, hanem azt is, hogy a 0 legalább t-szeres gyöke egy halmazon. Ennek következményeként belátunk egy "kilyukasztott" nullhelytételt is (vagyis egy kivételes pontban megengedjük, hogy ne legyen t-szeres gyöke), amivel a 3.1 tétel egy általánosítását is megkapjuk.

4.1. Kombinatorikus nullhelytétel többszörös gyökökkel

4.3. Tétel (Kombinatorikus nullhelytétel többszörös gyökökkel [5])**.** *Legyen $\mathbb{F}$ tetszőleges test, n és t pozitív egész, $\mathbf{x} = (x_1,\ldots,x_n)$ a változók vektora, és $f \in \mathbb{F}[\mathbf{x}]$ polinom. Legyenek továbbá $S_1,\ldots,S_n \subseteq \mathbb{F}$ halmazok nem üresek, és definiáljuk a $g_i(x_i) = \prod_{s\in S_i}(x_i - s)$ polinomokat. Amennyiben f-nek minden $\mathbf{s} \in S_1 \times \ldots \times S_n$ pontban legalább t-szeres gyöke van, akkor léteznek a $h_\tau \in \mathbb{F}[\mathbf{x}]$ polinomok, melyekre $\deg(h_\tau) \le \deg(f) - \sum_{i=1}^{t} \deg(g_{\tau(i)})$, továbbá kielégítik a következő egyenlőséget:*

$$f = \sum_{\tau\in T(n,t)} h_\tau \prod_{i=1}^{t} g_\tau(i).$$

Bizonyítás. ([5]) Indukcióval látjuk be n és t értékére. Ha $t = 1$, akkor pont 2.1 tételt, vagyis az eredeti kombinatorikus Nullstellensatz állítását kapjuk vissza. Ha $n = 1$, akkor minden $s \in S_1$-re $(x_1 - s)^t$ osztja f-et, tehát $(g_1)^t$ is, vagyis $f = g_1(x_1)^t h(x_1)$.

Rögzítsük n-et és t-t, és tegyük fel, hogy az állítást már beláttuk minden $k \le n$ és $r < t$ illetve minden $k < n$ és $r \le t$ esetén. Meg fogjuk mutatni, hogy írhatjuk f-et a következő alakban:

$$f = g_n(x_n)P + \sum_{\tau\in T(n-1,t)} h_\tau \prod_{i=1}^{t} g_{\tau(i)}, \tag{4.1}$$

ahol $\deg(P) \le \deg(f) - \deg(g_n)$ és $\deg(h_\tau) \le \deg(f) - \sum_{i=1}^{t} \deg(g_{\tau(i)})$.

Ha $|S_n| = 0$, akkor persze kész vagyunk, így legyen $\alpha \in S_n$ és $f = (x_n - \alpha)P_\alpha + Q_\alpha$, ahol $P_\alpha \in \mathbb{F}[\mathbf{x}]$ és $Q_\alpha \in \mathbb{F}[\mathbf{x}_{-n}]$. A Q_α polinomnak t-szeres gyöke van az $S_1 \times \ldots \times S_{n-1}$ halmaz minden elemén (lásd a 4.1 definíciót), így az indukciós feltétel miatt

$$Q_\alpha = \sum_{\tau \in T(n-1,t)} l_\tau \prod_{i=1}^{t} g_{\tau(i)},$$

ahol $\deg l_\tau \le \deg(Q_\alpha) - \sum_{i=1}^{t} \deg(g_{\tau(i)}) \le \deg(f) - \sum_{i=1}^{t} \deg(g_{\tau(i)})$. Ha $|S_n| = 1$ volt, akkor f-et a megfelelő alakra hoztuk.

Ha van egy további $\beta \in S_n$ is, akkor $P_\alpha = (x_n - \beta)P_\beta + Q_\beta$, ahol $P_\beta \in \mathbb{F}[\mathbf{x}]$ és $Q_\beta \in \mathbb{F}[\mathbf{x}_{-n}]$, továbbá a Q_β polinomnak t-szeres gyöke van az $S_1 \times \ldots \times S_{n-1}$ halmaz minden elemén, így az indukciós feltétel miatt

$$Q_\beta = \sum_{\tau \in T(n-1,t)} m_\tau \prod_{i=1}^{t} g_{\tau(i)},$$

ahol $\deg m_\tau \le \deg(Q_\beta) - \sum_{i=1}^{t} \deg(g_{\tau(i)}) \le \deg(f) - 1 - \sum_{i=1}^{t} \deg(g_{\tau(i)})$. Az előzőeket behelyettesítve P_α helyére azt kapjuk, hogy

$$f = (x_n - \alpha)(x_n - \beta)P_\beta + \sum_{\tau \in T(n-1,t)} \left[\Big((x_n - \alpha)m_\tau + l_\tau \Big) \prod_{i=1}^{t} g_{\tau(i)} \right]$$

ahol $(x_n - \alpha)m_\tau + l_\tau \le \deg(f) - \sum_{i=1}^{t} \deg(g_{\tau(i)})$.

Ezt az átalakítást folytatva S_n maradék elemeire, pont a (4.1) alakot kapjuk. A $g_n(x_n)P$ polinomnak t-szeres gyöke van az $S_1 \times \ldots \times S_n$ halmazon, így ugyanezen a halmazon P-nek legalább $t-1$-szeres gyöke van, így indukcióval

$$P = \sum_{\tau \in T(n,t-1)} o_\tau \prod_{i=1}^{t} g_{\tau(i)},$$

ahol $\deg(o_\tau) \le \deg(P) - \sum_{i=1}^{t-1} g_{\tau(i)}$, tehát

$$f = \left(\sum_{\tau \in T(n,t-1)} o_\tau \prod_{i=1}^{t-1} g_{\tau(i)} \right) g_n + \sum_{\tau \in T(n-1,t)} h_\tau \prod_{i=1}^{t} g_{\tau(i)},$$

ezzel pedig beláttuk az állítást. □

Az Alon-féle kombinatorikus nullhelytételhez hasonlóan, a 4.3 tételhez is tartozik egy el nem tűnési kritérium.

4.4. Következmény ([5]). *Legyen $\mathbb{F}$ test, $\mathbf{x}=(x_1,\ldots,x_n)$, $f \in \mathbb{F}[\mathbf{x}]$, és tegyük fel, hogy $\prod_{i=1}^{n} x_i^{t_i}$ maximális fokú tagja f-nek, továbbá $S_i \subseteq \mathbb{F}$ nem üres részhalmazok. Ha bármely α_i nemnegatív egészekre, melyekre $\sum_{j=1}^{n} \alpha_j = t$, teljesül, hogy $t_j < \alpha_j |S_j|$, akkor létezik $\mathbf{s} \in S_1 \times \ldots \times S_n$, ahol f-nek legfeljebb $t-1$-szeres gyöke van.*

Bizonyítás. Tegyük fel, hogy f-nek az $S_1 \times \ldots \times S_n$ halmaz minden elemén legalább t-szeres gyöke van. Ekkor a 4.3 tétel miatt léteznek $h_\tau \in \mathbb{F}[\mathbf{x}]$ polinomok, hogy $\deg h_\tau \le \deg(f) - \sum_{i=1}^{t} \deg(g_{\tau(i)})$, és

$$f = \sum_{\tau \in T(n,t)} g_{\tau(1)} \cdot \ldots \cdot g_{\tau(n)} h_\tau.$$

Az egyenlet jobb oldalán egy maximális fokú monomhoz létezik τ, hogy $\prod_{i=1}^{t} x_{\tau(i)}^{|S_{\tau(i)}|}$ osztja őt. Így létezik egy τ, hogy $t_j \ge \sum_{j \in \tau} |S_j|$. Legyen α_j az a szám, hogy j hányszor szerepel τ-ban. Ekkor $\sum_{j=1}^{t} \alpha_j = t$, és $t_j \ge \alpha_j |S_j|$ minden j-re, ez ellentmondás. □

4.2. Kombinatorikus nullhelytétel kivételes pontokkal

Tegyük fel, hogy az $S_1 \times \ldots \times S_n$ halmaz néhány pontjában nem tudjuk garantálni, hogy f-nek ott legalább t-szeres gyöke van. Ekkor a 4.3 tétel ugyan gyengébb következménnyel, de viszonylag hasonló alakban továbbra is érvényben marad.

4.5. Tétel ([5])**.**

a) *Legyen $\mathbb{F}$ test, $\mathbf{x} = (x_1, \ldots, x_n)$, és $f \in \mathbb{F}[\mathbf{x}]$. Legyenek $S_1, \ldots, S_n \subseteq \mathbb{F}$ véges nem üres halmazok, továbbá $D_i \subset S_i$. Legyen $g_i(x_i) = \prod_{s \in S_i}(x_i - s)$ és $l_i(x_i) = \prod_{d \in D_i}(x_i - d)$. Ha f-nek t-szeres gyöke van az $S_1 \times \ldots \times S_n \setminus D_1 \times \ldots \times D_n$ halmazon, a $D_1 \times \ldots \times D_n$ halmazon pedig pedig legalább egy pontban legfeljebb $t-1$-szeres gyöke van, akkor léteznek $h_\tau \in \mathbb{F}[\mathbf{x}]$ polinomok, melyekre $\deg(h_\tau) \leq \deg(f) - \sum_{i=1}^{t} \deg(g_{\tau(i)})$, és létezik egy $0 \not\equiv h \in \mathbb{F}[\mathbf{x}]$ polinom, melyre $\deg(h) \leq \deg(f) - \sum_{i=1}^{t}(\deg(g_{\tau(i)}) - \deg(l_{\tau(i)}))$, úgy, hogy*

$$f = \sum_{\tau \in T(n,t)} h_\tau \prod_{i=1}^{t} g_{\tau(i)} + h \prod_{i=1}^{n} \frac{g_i}{l_i}. \tag{4.2}$$

b) *Továbbá, ha létezik $\mathbf{d} \in D_1 \times \ldots \times D_n$, hogy $f(\mathbf{d}) \neq 0$, akkor*

$$\deg(f) \geq (t-1) \max_j (|S_j| - |D_j|) + \sum_{i=1}^{n} (|S_i| - |D_i|).$$

Bizonyítás. Először az **a)** részt látjuk be. Legyen $\mathfrak{I}(n,t)$ a $\left\{ \prod_{i=1}^{t} g_{\tau(i)} \;\middle|\; \tau \in T(n,t) \right\}$ halmaz által generált ideál. Az f polinomot írhatjuk a következő alakban:

$$f = r + \sum_{\tau \in T(n,t)} g_{\tau(1)} \cdot \ldots \cdot g_{\tau(n)} h_\tau,$$

ahol az r polinom $\mathbb{F}[\mathbf{x}]$-en belül ugyanabban az $\mathfrak{I}(n,t)$ szerinti ekvivalenciaosztályban van, mint f, továbbá r-ben minden olyan $\prod_{i=1}^{n} x_i^{t_i}$ monomnak az együtthatója 0, melyre létezik egy $\tau \in T(n,t)$, hogy $t_j \geq \geq \sum_{j=1}^{t} |S_{\tau(j)}|$ minden j-re (ha mégis lenne ilyen monom, akkor azt el tudnánk tüntetni $\mathfrak{I}(n,t)$-nek a τ-hoz tartozó generátorelemének a többszörösének a kivonásával).

A feltétel szerint minden i-re az $f l_i^t$ polinomnak az $S_1 \times \ldots \times S_n$ halmaz minden pontjában legalább t-szeres gyöke van, és ezért az $r l_i^t$ polinomnak is. Alkalmazva rá a 4.3 tételt, léteznek p_τ polinomok, melyekkel

$$r l_i^t = \sum_{\tau \in T(n,t)} g_{\tau(1)} \cdot \ldots \cdot g_{\tau(n)} p_\tau. \tag{4.3}$$

Azonban $r l_i^t$-nek nincsen olyan $\prod_{j=1}^{n} x_j^{t_j}$ monomja, amihez létezne olyan $\tau \in T(n,t)$, hogy $i \notin \tau$ és $t_j \geq \geq \sum_{j \in \tau} |S_j|$ minden j-re. Ezért léteznek o_τ polinomok, hogy

$$r l_i^t = g_i(x_i) \sum_{\tau \in T(n,t-1)} g_{\tau(1)} \cdot \ldots \cdot g_{\tau(t-1)} o_\tau,$$

amiből következik, hogy g_i osztja $r l_i^t$-t minden i-re. Mivel l_i osztja g_i-t és $(g_i/l_i, l_i) = 1$, ezért g_i/l_i osztja r-et. Így írhatjuk f-et a következő alakban

$$f = \sum_{\tau \in T(n,t)} g_{\tau(1)} \cdot \ldots \cdot g_{\tau(t)} h_\tau + h \prod_{i=1}^{n} \frac{g_i}{li},$$

ahol $h \prod_{i=1}^{n} \frac{g_i}{li} = r \not\equiv 0$, mivel $f \notin \mathfrak{I}(n,t)$ a feltételek szerint, tehát $h \not\equiv 0$.

A **b)** rész bizonyításánál feltehetjük, hogy $\max_j(|S_j|-|D_j|)=|S_1|-|D_1|$, és ekkor a (4.3) egyenlőség szerint az $i=1$ esetben $\mathbf{x}_{-1}=\mathbf{d}_{-1}$ helyettesítéssel $\prod_{i=2}^n \frac{g_i}{l_i}(d_i)=c\neq 0$, és így

$$(rl_i^t)(x_1,\mathbf{d}_{-1})=h(x_1,\mathbf{d}_{-1})\left(\frac{g_1}{l_1}(x_1)\right)\cdot c\cdot l_1^t(x_1)=g_1^t(x_1)p_1(x_1,\mathbf{d}_{-1}),$$

ahol $p_1=p_\tau$, ahol τ a csak 1-eseket tart tartalmazó $\tau\in T(n,t)$. Ebből következik, hogy $\left(\frac{g_1}{l_1}\right)^{t-1}$ osztja $h(x_1,\mathbf{d}_{-1})$-et. Mivel $f(\mathbf{d})\neq 0$, ezért $h(\mathbf{d})\frac{g_1}{l_1}(d_1)\neq 0$, és így $h(\mathbf{d})\neq 0$, tehát $h(x_1,\mathbf{d}_{-1})\not\equiv 0$. Ezeket felhasználva

$$\deg(f)\geq\deg(r)=\deg\left(h\prod_{i=1}^n\frac{g_i}{li}\right)\geq\deg(h)+\sum_{i=1}^n(|S_i|-|D_i|)\geq\deg\left(\left(\frac{g_1}{l_1}\right)^{t-1}\right)+\sum_{i=1}^n(|S_i|-|D_i|)\geq$$

$$\geq(t-1)(|S_1|-|D_1)+\sum_{i=1}^n(|S_i|-|D_i|)\,.$$

□

Az előző tételnek egy bizonyos értelemben vett megfordítása a következő tétel.

4.6. Következmény. *Legyen $\mathbb{F}$ test, $\mathbf{x}=(x_1,\ldots,x_n)$ és $f\in\mathbb{F}[\mathbf{x}]$, és tegyük fel, hogy $D_1\times\ldots\times D_n$ tartalmazza az összes olyan pontját $S_1\times\ldots\times S_n$-nek, ahol f nem tűnik el, és $D_i\subseteq S_i$ minden i-re. Ha létezik egy $\mathbf{d}\in D_1\times\ldots\times D_n$ pont, ahol $f(\mathbf{d})\neq 0$, akkor létezik $\mathbf{t}\in\mathbb{N}^n$, hogy $|S_i|-1\geq t_i\geq|S_i|-|D_i|$ és f-ben az $\mathbf{x^t}$ monom együtthatója nem 0.*

Bizonyítás. A 4.5 tétel miatt f-et felírhatjuk a (4.2) alakban, azaz $f=\sum_{i=1}^t g_ih_i+r$, ahol $r=h\prod_{i=1}^n\frac{g_i}{l_i}$ és $h\not\equiv 0$. Ezért $\deg_{x_i}r\geq|S_i|-|D_i|$, továbbá $\deg_{x_i}(h)<|D_i|$ miatt $\deg_{x_i}r<|S_i|$. Mivel a szummában szereplő tagok x_i-ben vett fokai mind nagyobb vagy egyenlőek mint $|S_i|$, ezért az r polinom monomjainak együtthatói változatlanul jelennek meg f-ben. □

4.7. Következmény ([3, 5])**.** *Legyen $\mathbb{F}$ test, $\mathbf{x}=(x_1,\ldots,x_n)$, $f\in\mathbb{F}[\mathbf{x}]$, és $S_1,\ldots,S_n\subseteq\mathbb{F}$ véges nem üres részhalmazai. Ha létezik egy $\mathbf{s}\in S_1\times\ldots\times S_n$ pont, hogy $f(\mathbf{s})\neq 0$, akkor létezik legalább*

$$\min_{\substack{\forall i\ 0<y_i\leq|S_i|\\ \sum_{i=1}^n y_i\geq\sum_{i=1}^n|S_i|-\deg(f)}}\prod_{i=1}^n y_i$$

pontja $S_1\times\ldots\times S_n$-nek, hogy ott f nem 0.

Bizonyítás. A változók számára vett indukcióval bizonyítunk. Ha $n=1$, akkor az $|S_1|\leq\deg(f)$ esetben a minimum 1, ha pedig $|S_1|>\deg(f)$, akkor a minimum $|S_1|-\deg(f)$ lesz, és ez a becslés nyilván igaz.

Legyen D_n azon részhalmaza S_n-nek, amelyek azon $d\in\mathbb{F}$ elemeket tartalmazzák, melyekre $f(\mathbf{x}_{-n},d)\not\equiv 0$. Mivel van egy pont $S_1\times\ldots\times S_n$-ben, ahol f nem 0-t vesz fel, ezért D_n nem üres. Legyen $\mathbf{s}\in S_1\times\ldots\times S_{n-1}$ és $d\in D_n$, ekkor a 4.5 tétel miatt

$$f(\mathbf{s},d)=\sum_{i=1}^t g_i(s_i)h_i(\mathbf{s},d)+h(\mathbf{s},d)\left(\prod_{i=1}^{n-1}\frac{g_i}{l_i}(s_i)\right)\frac{g_n}{l_n}(d)=h(\mathbf{s},d)\left(\prod_{i=1}^{n-1}\frac{g_i}{l_i}(s_i)\right)\frac{g_n}{l_n}(d),$$

vagyis létezik egy $p\in\mathbb{F}[\mathbf{x}_{-n}]$ polinom, amire $\deg(p)\leq\deg(f)-(|S_n|-|D_n|)$, és $p(\mathbf{s})=f(\mathbf{s},d)$ minden $\mathbf{s}\in S_1\times\ldots\times S_{n-1}$ esetén.

Ekkor indukció miatt létezik legalább $\min\prod_{i=1}^{n-1}y_i$ darab pont $S_1\times\ldots\times S_{n-1}$-ben, amiken p nem 0 értéket vesz fel, ahol a minimumot olyan y_i-k fölött vesszük, melyekre $0<y_i\leq|S_i|$ és $\sum_{i=1}^{n-1}y_i\geq\sum_{i=1}^{n-1}|S_i|-$ $-deg(p)$. Tehát létezik $|D_n|\min\prod_{i=1}^{n-1}y_i$ pont az $S_1\times\ldots\times S_n$ halmazban, ahol f nem tűnik el, és persze $0<|D_n|\leq|S_n|$, továbbá $\sum_{i=1}^{n-1}y_i+|D_n|\geq\sum_{i=1}^{n-1}|S_i|-deg(p)+|D_n|\geq\sum_{i=1}^{n-1}|S_i|-(\deg(f)-(|S_n|-|D_n|))+$ $+|D_n|=\sum_{i=1}^n|S_i|-\deg(f)$, ezzel beláttuk az állítást n-re is. □

4.3. Alkalmazások

A 3.1 tétel általánosítása a következő tétel.

4.8. Tétel ([5]). *Legyen $\mathbb{F}$ test, és legyen adva az $\mathbb{F}$ feletti n dimenziós affin térben m darab hipersík, melyeket az $(\mathbf{a}_{j\cdot}, \mathbf{x}) = b_j$ egyenletek határoznak meg. Legyenek $S_i \subseteq \mathbb{F}$ és $D_i \subset S_i$ nem üres részhalmazok minden $1 \leq i \leq n$ esetén. Ekkor ha minden $\mathbf{s} \in S_1 \times \ldots \times S_n \setminus D_1 \times \ldots \times D_n$ pont rajta van t darab hipersíkon, és van egy $\mathbf{d} \in D_1 \times \ldots \times D_n$, ami egyetlen hipersíkon sincs rajta, akkor*

$$m \geq (t-1) \max_j (|S_j| - |D_j|) + \sum_{i=1}^{n} (|S_i| - |D_i|) .$$

Bizonyítás. Legyen $f = \prod_{j=1}^{m} ((\mathbf{a}_{i\cdot}, \mathbf{x}) - b_i)$. Ekkor f-nek t-szeres gyöke van $S_1 \times \ldots \times S_n \setminus D_1 \times \ldots \times D_n$ pontjaiban, és nincs gyöke $D_1 \times \ldots \times D_n$ egy pontjában. Alkalmazva a 4.5 tételt, pontosan az állítást kapjuk, hiszen $\deg(f) = m$. □

A 4.8 tételnek a $t = 1$ esetben a következő tétel bizonyos értelemben megfordítása.

4.9. Tétel ([5]). *Legyenek $S_1, \ldots, S_n \subseteq \mathbb{F}$ véges nem üres részhalmazai. Ha adott m hipersík az n dimenziós $\mathbb{F}$ feletti affin térben, melyek nem fedik le a $S_1 \times \ldots \times S_n$ összes pontját, akkor legalább $\min_Y \prod_{i=1}^{n} y_i$ pontját nem fedik, ahol*

$$Y = \left\{ \mathbf{y} \in \mathbb{F}^n \mid 0 < y_i \leq |S_i| \text{ minden } i\text{-re, és } \sum_{i=1}^{n} y_i \geq \sum_{i=1}^{n} |S_i| - m \right\}.$$

Bizonyítás. Vegyük ugyanazt az f polinomot, mint az előző tételben, és alkalmazzuk a 4.7 tételt. □

4.10. *Megjegyzés.* Ha $\mathbb{F} = \mathbb{R}$ és $S_i = \{0,1\}$ és $D_i = \{0\}$, akkor azt kapjuk, hogy m darab hipersík (ahol $m < n$) legalább 2^{n-m} pontját nem fedi le a $\{0,1\}^n$ hiperkocka csúcsainak, hiszen a 3.1 tétel miatt lesz egy pont, ami nincs lefedve.

5. fejezet

Kombinatorikus nullhelytétel multihalmazokra és gyűrűkre

5.1. Definíció. Legyen $S \subseteq R$ halmaz, m pedig egy $R \to \mathbb{N}$ multiplicitásfüggvény, azaz jelölje $m(s)$ az $s \in S$ elem multiplicitását. Azt mondjuk, hogy $(S, m) \subseteq R$ egy multihalmaz akkor és csak akkor, ha egy $s \in R$ elemre $m(s) > 0 \Leftrightarrow s \in S$. A multihalmaz mérete legyen $d(S) = \sum_{s \in S} m(s)$.
Ez a definíció lényegében azt jelenti, hogy egy multihalmazt egy alaphalmaz és egy hozzácsatolt multiplicitásfüggvény határoz meg, vagyis az (S, m) párban szereplő S-re továbbra is halmazként gondolunk.

5.2. Definíció. Legyenek $(S_1, m_1), \ldots, (S_n, m_n)$ multihalmazok, azaz egy $s \in S_i$ elem multiplicitását $m_i(s)$ jelöli. A $\mathbf{s} \in S_1 \times \ldots \times S_n$ ponthoz tartozó multiplicitás vektor ekkor legyen $m(\mathbf{s}) = (m_1(s_1), \ldots, m_n(s_n))$.

5.3. Definíció. Legyen $\mathbf{s} \in S_1 \times \ldots \times S_n$ és $\mathbf{w} \in \mathbb{N}^n$. Ekkor legyen $I(\mathbf{s}, \mathbf{w})$ azon polinomok ideálja, melyek $\mathbf{s}$ körüli felbontásában, azaz az $f = \sum_{\mathbf{u}} f_{\mathbf{u}}(\mathbf{s})(\mathbf{x} - \mathbf{s})^{\mathbf{u}}$ alakjában, $\mathbf{u} < \mathbf{w}$ esetén $f_{\mathbf{u}}(\mathbf{s}) = 0$.

Ebben a fejezetben kiterjesztjük a kombinatorikus nullhelytételt multihalmazokra, illetve arra az esetre, amikor lehetnek kivételes pontok is a multihalmazok szorzatában, ehhez a már bemutatott kommutatív algebrai eszközöket fogjuk használni. Ezen kívül az el nem tűnési tételt kiterjesztjük nem csak test, hanem gyűrű feletti polinomgyűrűkre is. Észrevehetjük, hogy már korábban tárgyalt eredményeket kapunk, ha minden halmazbeli elem multiplicitását 1-nek választjuk (azaz ha a multiplicitás függvényekről megfeledkezünk).

5.1. Kombinatorikus nullhelytétel multihalmazokra

5.4. Tétel (Kombinatorikus nullhelytétel multihalmazokra [10])**.** *Legyen $\mathbb{F}$ test, n pozitív egész, $\mathbf{x} = (x_1, \ldots, x_n)$ a változók vektora, $f \in \mathbb{F}[\mathbf{x}]$ polinom. Legyenek továbbá $(S_1, m_1), \ldots, (S_n, m_n) \subseteq \mathbb{F}$ véges nem üres multihalmazok, és definiáljuk a $g_i(x_i) = \prod_{s \in S_i} (x_i - s)^{m_i(s)}$ polinomokat. Amennyiben $f \in \mathfrak{I}(\mathbf{s}, m(\mathbf{s}))$ minden $\mathbf{s} \in S_1 \times \ldots \times S_n$ pontra, akkor léteznek $h_1, \ldots, h_n \in \mathbb{F}[\mathbf{x}]$ polinomok, melyekkel teljesül az*

$$f = \sum_{i=1}^{n} h_i g_i$$

egyenlőség, miközben $\deg(h_i) \leq \deg(f) - \deg(g_i) = \deg(f) - d(S_i)$.

Bizonyítás. ([10]) A bizonyítás a 2.2 részben tárgyalt bizonyításnak a kiterjesztése lesz. Vegyük észre, hogy $\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\mathfrak{I}(\mathbf{s},\mathbf{w}) = \prod_{i=1}^{n} w_i$, mivel az $\left\{(\mathbf{x}-\mathbf{s})^{\mathbf{u}} \mid \mathbf{u} < \mathbf{w}\right\}$ alakú monomok által reprezentált ekvivalenciaosztályok bázisát adják az $\mathbb{F}[\mathbf{x}]/\mathfrak{I}(\mathbf{s},\mathbf{w})$ térnek. Legyen

$$\mathfrak{I} = \bigcap_{\mathbf{s}\in S_1\times\ldots\times S_n} \mathfrak{I}\left(\mathbf{s}, m(\mathbf{s})\right).$$

Az $\mathfrak{I}(\mathbf{s}, m(\mathbf{s}))$ ideál radikálja az $\left(x_1 - s_1, \ldots, x_n - s_n\right)$ maximális ideál, így a metszetben szereplő ideálok páronként relatív prímek, vagyis alkalmazhatjuk a kínai maradéktételt:

$$\mathbb{F}[\mathbf{x}]/\mathfrak{I} \cong \bigoplus_{\mathbf{s}\in S_1\times\ldots\times S_n} \mathbb{F}[\mathbf{x}]/\mathfrak{I}(\mathbf{s}, m(\mathbf{s})),$$

tehát $\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\mathfrak{I} = \sum_{\mathbf{s}\in S_1\times\ldots\times S_n} \prod_{i=1}^{n} m_i(s_i) = \left(\sum_{s_1\in S_1} m_1(s_1)\right)\cdot\ldots\cdot\left(\sum_{s_n\in S_n} m_n(s_n)\right) = \prod_{i=1}^{n} d(S_i)$.

Tekintsünk először az f polinomot az $\mathbb{F}[\mathbf{x}]$ polinomgyűrű egy tetszőleges elemének, és osszuk el a g_i polinomokkal maradékosan. Ekkor az 1.3 állítás miatt $\deg(h_i) \le \deg(f) - \deg(g_i)$, és az r maradékra $\deg_{x_i} r < d(S_i)$, tehát a maradékok vektorterének a dimenziója $\prod_{i=1}^{n} d(S_i)$. Ekkor az 1.4 állítás **a)** része miatt $\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/(g_1,\ldots,g_n) \le \prod_{i=1}^{n} d(S_i)$. Továbbá $g_i \in \mathfrak{I}$, tehát $(g_1,\ldots,g_n) \subseteq \mathfrak{I}$ egy altér, így ez csak úgy lehet, ha $\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/(g_1,\ldots,g_n) = \prod_{i=1}^{n} d(S_i)$, és emiatt $(g_1,\ldots,g_n) = \mathfrak{I}$.

A feltétel szerint $f \in \mathfrak{I} = (g_1,\ldots,g_n)$, és az osztási maradék egyértelmű az 1.4 állítás **b)** része miatt, tehát $r \equiv 0$. □

5.5. Tétel (Kombinatorikus nullhelytétel multihalmazokra, kivételes pontokkal [10])**.**

a) *Legyen $\mathbb{F}$ tetszőleges test, n pozitív egész, $\mathbf{x} = (x_1,\ldots,x_n)$ a változók vektora, és $f \in \mathbb{F}[\mathbf{x}]$ polinom. Legyenek továbbá $S_1,\ldots,S_n \subseteq \mathbb{F}$ véges nem üres multihalmazok, továbbá $D_i \subseteq S_i$, és ha $s_i \in D_i$, akkor s_i-nek a D_i-ben is $m_i(s_i)$ a multiplicitása. Definiáljuk a $g_i(x_i) = \prod_{s\in S_i}(x_i - s)^{m_i(s)}$ és $l_i(x_i) = \prod_{s_i\in D_i}(x_i - s_i)^{m_i(s_i)}$ polinomokat. Amennyiben $f \in \mathfrak{I}\left(\mathbf{s}, m(\mathbf{s})\right)$ minden $\mathbf{s} \in S_1\times\ldots\times S_n \setminus D_1\times\ldots\times D_n$ pontra, akkor léteznek $h, h_1,\ldots,h_n \in \mathbb{F}[\mathbf{x}]$ polinomok, melyekkel teljesül az*

$$f = \sum_{i=1}^{n} h_i g_i + h \prod_{i=1}^{n} \frac{g_i}{l_i}$$

egyenlőség, miközben $\deg(h_i) \le \deg(f) - \deg(g_i) = \deg(f) - d(S_i)$, és $\deg(h) \le \deg(f) - \sum_{i=1}^{n} \deg\left(\frac{g_i}{l_i}\right)$.

b) *Továbbá, ha létezik $\mathbf{s}^* \in D_1\times\ldots\times D_n$, hogy $f \notin \mathfrak{I}(\mathbf{s}^*, m(\mathbf{s}^*))$, akkor $\deg(f) \ge \sum_{i=1}^{n}(d(S_i) - d(D_i))$.*

Bizonyítás. Az előző tétel bizonyítását fogjuk módosítani. A feltétel szerint f eleme a következő ideálnak:

$$\mathfrak{I}' = \bigcap_{\mathbf{s}\in S_1\times\ldots\times S_n\setminus D_1\times\ldots\times D_n} \mathfrak{I}\left(\mathbf{s}, m(\mathbf{s})\right).$$

Az összemetszett ideálok radikáljainak relatív prímsége miatt pedig

$$\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\mathfrak{I}' = \sum_{\mathbf{s}\in S_1\times\ldots\times S_n\setminus D_1\times\ldots\times D_n} \prod_{i=1}^{n} m_i(s_i).$$

Vegyük észre, hogy $\prod_{i=1}^{n} \frac{g_i}{l_i} \in \mathfrak{I}'$, így $(g_1,\ldots,g_n,\prod_{i=1}^{n} \frac{g_i}{l_i}) \subseteq \mathfrak{I}'$. Osszuk el először f-et maradékosan a $g_1,\ldots,g_n$ polinomokkal, ekkor az $\mathbf{x}^{\mathbf{u}}$ $(0 \le \mathbf{u} < (d(S_1),\ldots,d(S_n)))$ monomok által generált vektortér egy elemét kapjuk maradékként. Osszuk el ezt a maradékot még $\prod_{i=1}^{n} \frac{g_i}{l_i}$-vel is. Könnyű látni, hogy az így kapott maradék azon $\mathbf{x}^{\mathbf{u}}$ monomok által generált vektortérbe esik, ahol a kitevőre $0 \le \mathbf{u} < (d(S_1),\ldots,d(S_n))$,

úgy, hogy közben $\mathbf{u} \geq (d(S_1)-d(D_1),\dots,d(S_n)-d(D_n))$ ne teljesüljön. Világos, hogy ennek a térnek a dimenziója

$$\sum_{\mathbf{s}\in S_1\times\ldots\times S_n}\prod_{i=1}^{n} m_i(s_i) - \prod_{i=1}^{n}\sum_{s_i\in D_i} m_i(s_i) = \sum_{\mathbf{s}\in S_1\times\ldots\times S_n}\prod_{i=1}^{n} m_i(s_i) - \sum_{\mathbf{s}\in D_1\times\ldots\times D_n}\prod_{i=1}^{n} m_i(s_i),$$

vagyis $(g_1,\dots,g_n,\prod_{i=1}^{n}\frac{g_i}{l_i})=\mathfrak{J}'$, és f a maradékot egyértelműen meghatározza, így az csakis 0 lehet. Ezzel beláttuk a tétel **a)** részét.

A **b)** rész bizonyításához tegyük fel indirekt, hogy $h\equiv 0$, és ekkor $f\in(g_1,\dots,g_n)=\mathfrak{J}\subseteq I(\mathbf{s}^*,m(\mathbf{s}^*))$, ami ellentmondás, tehát $\deg(h)\geq 0$. □

5.2. El nem tűnési kritérium testekre

5.6. Tétel ([5]). *Tegyük fel, hogy* $\deg(f)=\sum_i^n t_i$, *ahol* t_i *nemnegatív egészek, és a* $\prod_{i=1}^{n} x_i^{t_i}$ *monom együtthatója* f*-ben nem* 0. *Ekkor, ha* $(S_1,m_1),\dots,(S_n,m_n)$ *nem üres multihalmazai* $\mathbb{F}$*-nek, és a méretükre teljesül, hogy* $d(S_i)>t_i$ *minden* $1\leq i\leq n$*-re, akkor létezik* $\mathbf{s}\in S_1\times\ldots\times S_n$ *és* $0\leq\mathbf{u}<m(\mathbf{s})$, *amire* $f_{\mathbf{u}}(\mathbf{s})\neq 0$.

Bizonyítás. Tegyük fel, hogy f mégis eleme az 5.4 tételben definiált $\mathfrak{I}$ ideálnak. Ekkor a tétel miatt felírható $f=\sum_{i=1}^{n} h_i g_i$ alakban. A bal oldalon $\mathbf{x}^{\mathbf{t}}$ együtthatója nem 0. A jobb oldalon pedig $\deg(h_i g_i)\leq$ $\leq\deg(f)$, és ebben minden maximális fokú monom osztható $x_i^{d(S_i)}$-vel, így ellentmondásra jutottunk. □

5.2.1. Bizonyítás osztott differenciákkal

Az 5.6 tételt a 2.5 tételhez hasonlóan, osztott differenciák segítségével is be lehet látni. Azonban a karakterisztikánál nagyobb rendű deriváltak definiálásakor adódó problémák kikerülése végett közvetlenebb módon számoljuk ki egy polinom főegyütthatóját.

Legyen $\mathbf{S}=S_1\times\ldots\times S_n$, és $d(\mathbf{S})=(d(S_1),\dots,d(S_n))$. Az 5.4 tétel miatt tudjuk, hogy r egyértelmű, ha $f-r\in(g_1,\dots,g_n)$ és $\deg_{x_i} r<d(S_i)$ minden i-re. Ezt $r=(f \mod g_1,\dots,g_n)$-nel jelöljük majd.

5.7. Definíció. Legyen $f\in\mathbb{F}[\mathbf{x}]$ polinom, és vegyük az $(f \mod g_1,\dots,g_n)$ polinom $\mathbf{x}^{d(\mathbf{S})-\mathbf{1}}=$ $=x_1^{d(S_1)-1}\cdot\ldots\cdot x_n^{d(S_n)-1}$ monomjának együtthatóját, ezt $f[\mathbf{S}]$-sel fogjuk jelölni.

5.8. Lemma ([10]). *Legyen* $\mathbf{x}\in\mathbb{F}^n$ *és* $f\in\mathbb{F}[\mathbf{x}]$, *és* $d(\mathbf{S})-\mathbf{1}=\mathbf{t}$.

a) *Ha minden* S_i *multihalmazban egyetlen* a_i *elem van* t_i+1 *multiplicitással, akkor* $f[\mathbf{S}]=$ $=f_{\mathbf{t}}((a_1,\dots,a_n))$.

b) *Tegyük fel, hogy az* S_i *multihalmazban van két különböző elem,* a *és* b. *Legyen* $S_i'=S_i\setminus\{a\}$ *és* $S_i''=S_i\setminus\{b\}$ *(azaz eggyel csökkentettük a kivont elem multiplicitását), és* $\mathbf{S}'=S_1\times\ldots\times S_{i-1}\times S_i'\times$ $\times S_{i+1}\times\ldots\times S_n$ *és* $\mathbf{S}''=S_1\times\ldots\times S_{i-1}\times S_i''\times S_{i+1}\times\ldots\times S_n$. *Ekkor*

$$f[\mathbf{S}]=\frac{f[\mathbf{S}']-f[\mathbf{S}'']}{b-a}.$$

Bizonyítás. Az **a)** rész bizonyításához vegyük észre, hogy

$$\big(f(\mathbf{x}) \mod (x_1-a_1)^{t_1+1},\dots,(x_n-a_n)^{t_n+1}\big)=\sum_{\mathbf{u}\leq\mathbf{t}} f_{\mathbf{u}}(\mathbf{a})(\mathbf{x}-\mathbf{a})^{\mathbf{u}}.$$

A bal oldalon $\mathbf{x}^{\mathbf{t}}$ együtthatója definíció szerint $f[\mathbf{S}]$, a jobb oldalon pedig $f_{\mathbf{t}}(\mathbf{a})$.

A **b)** rész bizonyításánál a definíciókat beírva

$$(x_i-a)\left(f(\mathbf{x}) \mod g_1(x_1),\dots,g_{i-1}(x_{i-1}),\frac{g_i(x_i)}{x_i-a},g_{i+1}(x_{i+1}),\dots,g_n(x_n)\right)-$$

$$-(x_i-b)\left(f(\mathbf{x}) \mod g_1(x_1),\dots,g_{i-1}(x_{i-1}),\frac{g_i(x_i)}{x_i-b},g_{i+1}(x_{i+1}),\dots,g_n(x_n)\right)=$$

$$=\Big((x_i-a)f(\mathbf{x}) \mod g_1(x_1),\dots,g_n(x_n)\Big)-\Big((x_i-b)f(\mathbf{x}) \mod g_1(x_1),\dots,g_n(x_n)\Big)=$$

$$=\Big((b-a)f(\mathbf{x}) \mod g_1(x_1),\dots,g_n(x_n)\Big).$$

Innen világos, hogy az egyenlőség elején $\mathbf{x^t}$ együtthatója $f[\mathbf{S}']-f[\mathbf{S}'']$, a végén pedig $(b-a)f[\mathbf{S}]$. □

5.9. Állítás. *Legyen $f\in\mathbb{F}[\mathbf{x}]$. Ha $\mathbf{t}$ maximális $\mathrm{Supp}(f)$-ben, akkor $f_\mathbf{t}=f_\mathbf{t}(\mathbf{s})$ nem függ $\mathbf{s}$-től, tehát speciálisan $f_\mathbf{t}=f_\mathbf{t}(\mathbf{0})$ is teljesül.*

Bizonyítás. Annyit kell csak látni, hogy $\mathbf{x^t}$ együtthatója $f_\mathbf{t}(\mathbf{s})$ kell legyen ilyenkor f-ben. Ez pedig világos, hiszen az $f=\sum_\mathbf{u} f_\mathbf{u}(\mathbf{s})(\mathbf{x}-\mathbf{s})^\mathbf{u}$ felbontásban csak $\mathbf{u}\geq\mathbf{t}$ esetén lesz $(\mathbf{x}-\mathbf{s})^\mathbf{u}$ kibontásában $\mathbf{x^t}$ alakú monom. □

Emiatt az állítás miatt értelmezhető a következő tétel. Ennek egyszerű következménye lesz az 5.6 tétel, de már önmagában is érdekes.

5.10. Tétel ([10])**.** *Legyen $d(\mathbf{S})=\mathbf{t}+1$, és $F\subset\mathbb{F}[\mathbf{x}]$ azon polinomok halmaza, melyekre minden $\mathbf{u}\geq\mathbf{t}$, $\mathbf{u}\neq\mathbf{t}$ esetén $\mathbf{x^u}$ együtthatója az f polinomban 0, de $\mathbf{x^t}$ együtthatója nem 0.*

a) *Ekkor léteznek $\alpha_\mathbf{u}^{(\mathbf{s})}\in\mathbb{F}$ konstansok, hogy minden $f\in F$ polinomra*

$$f_\mathbf{t}=\sum_{\mathbf{s}\in\mathbf{S}}\sum_{\mathbf{u}<m(\mathbf{s})}\alpha_\mathbf{u}^{(\mathbf{s})}f_\mathbf{u}(\mathbf{s}). \tag{5.1}$$

b) *Az $(S_1,m_1),\dots,(S_n,m_n)$ multihalmazok, az $\mathbf{s}\in\mathbf{S}$ pont, és az $\mathbf{u}$ (és $\mathbf{t}$) vektor együtt egyértelműen meghatározzák az $\alpha_\mathbf{u}^{(\mathbf{s})}$ konstansot.*

c) *Minden $\mathbf{s}\in\mathbf{S}$ pontra $\mathbf{u}=m(\mathbf{s})-\mathbf{1}$ esetén $\alpha_\mathbf{u}^{(\mathbf{s})}\neq 0$.*

Bizonyítás. **a)** Definíció szerint $f_\mathbf{t}=f[\mathbf{S}]$. A jobb oldalra alkalmazzuk az 5.8 lemma **b)** részét addig, amíg már csak olyan $f[\mathbf{M}]$ alakú elemek vannak, ahol $\mathbf{M}=M_1\times\ldots\times M_n$ és minden i-re M_i egyelemű, mely elem u_i multiplicitására $u_i+1\leq m_i(a_i)$. Az 5.8 lemma **a)** része miatt $f[M]=f_\mathbf{u}(\mathbf{a})$. Az együtthatókat pedig $\mathbf{S}$ elemeinek koordinátáiból kaptuk, így azok nem függnek f-től.

b) Tegyük fel, hogy az $\left(\alpha_\mathbf{u}^{(\mathbf{s})}\right)$ és az $\left(\alpha'^{(\mathbf{s})}_\mathbf{u}\right)$ számok is kielégítik az **a)** részben szereplő egyenletet minden $f\in F$ esetén. Legyen $\delta_\mathbf{u}^{(\mathbf{s})}=\alpha_\mathbf{u}^{(\mathbf{s})}-\alpha'^{(\mathbf{s})}_\mathbf{u}$, ekkor

$$\sum_{\mathbf{s}\in\mathbf{S}}\sum_{\mathbf{u}<m(\mathbf{s})}\delta_\mathbf{u}^{(\mathbf{s})}f_\mathbf{u}(\mathbf{s})=0, \tag{5.2}$$

minden $f\in F$ polinomra. Válasszunk a $\geq$ rendezésre maximális $\mathbf{u}$ vektort úgy, hogy $\delta_\mathbf{u}(\mathbf{s})\neq 0$. A következő polinomra (mely eleme F-nek) felírva az 5.2 egyenletet, annak a bal oldalán az egyetlen nem 0 elem $\delta_\mathbf{u}(\mathbf{s})f_\mathbf{u}(\mathbf{s})$ lesz:

$$f(\mathbf{x})=\prod_{i=1}^{n}\left((x_i-s_i)^{u_i}\prod_{s\in S_i\setminus\{s_i\}}(x_i-s)^{m_i(s)}\right).$$

c) Alkalmazzuk megint az $f[\mathbf{S}]$ osztott differenciára rekurzívan a 5.8 lemmát. Világos, hogy ha minden i-re $M_i=\{s_i\}$ és benne s_i multiplicitása $m_i(s_i)$, akkor csak egy féle képpen juthatunk el az $f[M_1\times\ldots\times M_n]=$ $=f_{m(\mathbf{s})-\mathbf{1}}(\mathbf{s})$ osztott differenciáig, és az együtthatója emiatt nem 0 lesz. □

5.11. Tétel. *Legyen $\mathbb{F}$ test, $f \in \mathbb{F}[\mathbf{x}]$ polinom. Legyen $\mathbf{t}$ maximális a $\mathrm{Supp}(f)$ halmazban. Ha minden $1 \le i \le n$ esetén (S_i, m_i) véges multihalmaz $\mathbb{F}$-ben, és a mérete, $d(S_i) > t_i$, akkor létezik egy $\mathbf{s} = (s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$ pont és egy $\mathbf{u}$ kitevő vektor, melyre $u_i < m_i(s_i)$ minden i-re, melyekre $f_{\mathbf{u}}(\mathbf{s}) \neq 0$.*

Bizonyítás. Ha $d(S_i) > t_i + 1$ valamely i-re, akkor csökkentsük S_i-ben egy elem multiplicitását (vagy dobjuk ki a halmazból), így feltehetjük, hogy $d(\mathbf{S}) = \mathbf{t} + \mathbf{1}$. Alkalmazhatjuk az 5.10 tételt. Az (5.1) egyenlet bal oldalán szereplő $f_{\mathbf{t}}$-ről feltettük, hogy nem 0 (lásd az 5.9 tételt). A jobb oldalon tehát kell legyen egy $\mathbf{s}$ és $\mathbf{u}$, hogy $f_{\mathbf{u}}(\mathbf{s}) \neq 0$. □

5.3. El nem tűnési kritérium gyűrűkre

Az ebben a fejezetben tárgyalt tétel bizonyításához nem használjuk fel az 5.4 tételt, helyette a 2.4.2 részben bemutatott bizonyítási módszert alkalmazzuk, azaz közvetlenül fogjuk belátni a tételt.

5.12. Tétel ([9])**.** *Legyen R kommutatív gyűrű, $f \in R[\mathbf{x}]$ polinom. Legyen $\mathbf{t}$ maximális a $\mathrm{Supp}(f)$ halmazban. Legyenek továbbá minden $1 \le i \le n$ esetén (S_i, m_i) multihalmazok R-ben úgy, hogy a méretükre $d(S_i) > t_i$, továbbá minden i-re és minden $s_1, s_2 \in S_i$ esetén $s_1 \neq s_2 \Rightarrow s_1 - s_2$ nem nullosztó R-ben. Ekkor létezik $\mathbf{s} = (s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$ és egy $\mathbf{u}$ kitevő, hogy $u_i < m_i(s_i)$ minden i-re, melyekkel $f_{\mathbf{u}}(\mathbf{s}) \neq 0$.*

Bizonyítás. Indukcióval bizonyítjuk $\sum_{i=1}^{n} t_i$ értékére. Ha $\sum_{i=1}^{n} t_i = 0$, akkor $t_i = 0$ és így f nem függ $\mathbf{x}$-től, viszont $\mathbf{x}^{\mathbf{0}}$ együtthatója nem 0, tehát $f \equiv c \neq 0$, vagyis ekkor igaz az állítás.

Legyen most $\sum_{i=1}^{n} t_i > 0$, feltehetjük, hogy $t_1 > 0$. Legyen $s \in S_1$ egy pozitív multiplicitású elem, és osszuk el f-et maradékosan $(x_1 - s)$-sel:

$$f = g \cdot (x_1 - s) + h, \text{ ahol } \deg_{x_1}(h) = 0 \text{ így } h \text{ csak } \mathbf{x}_{-1}\text{-től függ.}$$

Írjuk fel g és f polinomok $\mathbf{s}$ körüli felbontását:

$$g(\mathbf{x}) = \sum_{\mathbf{u} \in \mathbb{N}^n} (g_{\mathbf{u}}(\mathbf{s})(\mathbf{x} - \mathbf{s})^{\mathbf{u}}) \text{ amivel } f(\mathbf{x}) = \sum_{\mathbf{u} \in \mathbb{N}^n} (g_{\mathbf{u}}(\mathbf{s})(x_1 - s)(\mathbf{x} - \mathbf{s})^{\mathbf{u}}) + \sum_{\mathbf{u} \in \{0\} \times \mathbb{N}^{n-1}} (h_{\mathbf{u}}(\mathbf{s})(\mathbf{x} - \mathbf{s})^{\mathbf{u}}) \quad (5.3)$$

és vegyük észre, hogy ha $s_1 = s$, akkor a két szummát átírhatjuk úgy, hogy $\mathbf{u}$ diszjunkt halmazok fölött fusson, tehát

$$f(\mathbf{x}) = \sum_{\mathbf{u} \in (\mathbb{N} \setminus \{0\}) \times \mathbb{N}^{n-1}} \left(g_{(u_1 - 1, u_2, \ldots, u_n)}(\mathbf{s})(\mathbf{x} - \mathbf{s})^{\mathbf{u}}\right) + \sum_{\mathbf{u} \in \{0\} \times \mathbb{N}^{n-1}} (h_{\mathbf{u}}(\mathbf{s})(\mathbf{x} - \mathbf{s})^{\mathbf{u}}) \quad (5.4)$$

Írjuk fel h $\mathbf{s}' \in S_2 \times \ldots \times S_n$ körüli felbontását:

$$h(\mathbf{x}_{-1}) = \sum_{\mathbf{w} \in \mathbb{N}^{n-1}} (h_{\mathbf{w}}(\mathbf{s}')(\mathbf{x}_{-1} - \mathbf{s}')^{\mathbf{w}})$$

Amennyiben létezik $\mathbf{s}'$ és $\mathbf{w} < \mathbf{t}_{-1}$, hogy $h_{\mathbf{w}}(\mathbf{s}') \neq 0$, akkor fejezzük ki f-et $\mathbf{s} = (s, \mathbf{s}') \in S_1 \times \ldots \times S_n$ szerint. Az f polinomnak az (5.4) felírásából látszik, hogy $(\mathbf{x} - \mathbf{s})^{(0, \mathbf{w})}$ együtthatója $h_{\mathbf{w}}(\mathbf{s}')$ lesz, és mivel $t_1 > 0$, ezért $(0, \mathbf{w}) < \mathbf{t}$, vagyis ebben esetben igazoltuk az állítást.

Most tegyük fel, hogy a (5.4) egyenlet jobboldalán a második szummában minden s és minden $\mathbf{u} < \mathbf{t}$ esetén a $(\mathbf{x} - \mathbf{s})^{\mathbf{u}}$ tag együtthatója 0. A maradékos osztás tulajdonságai miatt

$$\mathrm{Supp}(g) \subseteq \left\{ (u_1 - k, u_2, \ldots, u_n) \in \mathbb{N}^n \;\middle|\; \mathbf{u} \in \mathrm{Supp}(f),\ 1 \le k \le u_1 \right\} \text{ és } (t_1 - 1, t_2, \ldots, t_n) \in \mathrm{Supp}(g),$$

tehát $(t_1-1,t_2,\dots,t_n)$ maximális lesz $\mathrm{Supp}(g)$-ben. Így alkalmazhatjuk az eggyel kisebb indukciós esetet g-re az S_1 multihalmazban $m_1(s)$-et eggyel csökkentve, valamint $S_2,\dots,S_n$ multihalmazokat változatlanul hagyva. Így kapjuk, hogy létezik olyan $s\in S_1\times\ldots\times S_n$ és $w<(t_1-1,t_2,\dots,t_n)$, hogy $g_{\mathbf{w}}(s)\neq 0$.

Ha $s_1=s$, akkor az (5.4) egyenlet alapján $(\mathbf{x}-\mathbf{s})^{(w_1+1,w_2,\dots,w_n)}$ együtthatója $g_{\mathbf{w}}(\mathbf{s})\neq 0$, és mivel $(w_1+1,w_2,\dots,w_n)<\mathbf{t}$, ezért ebben az esetben is igaz az állítás.

Ha $s_1\neq s$, akkor az (5.3) egyenletet továbbírva:

$$f(\mathbf{x})=\sum_{\mathbf{u}\in\mathbb{N}^n}\left((s_1-a)g_{\mathbf{u}}(\mathbf{s})(\mathbf{x}-\mathbf{s})^{\mathbf{u}}+g_{\mathbf{u}}(\mathbf{s})(x_1-s_1)(\mathbf{x}-\mathbf{s})^{\mathbf{u}}\right)+\sum_{\substack{\mathbf{u}\in\{0\}\times\mathbb{N}^{n-1}\\ \neg(\mathbf{u}<\mathbf{t})}}\left(h_{\mathbf{u}}(\mathbf{s})(\mathbf{x}-\mathbf{s})^{\mathbf{u}}\right)$$

Tehát

$$f(\mathbf{x})=\sum_{\mathbf{u}\in\mathbb{N}^n}\left[\left((s_1-a)g_{\mathbf{u}}(\mathbf{s})+\chi_{(u_1\geq 1)}\cdot g_{(u_1-1,u_2,\dots,u_n)}(\mathbf{s})\right)(\mathbf{x}-\mathbf{s})^{\mathbf{u}}\right]+\sum_{\substack{\mathbf{u}\in\{0\}\times\mathbb{N}^{n-1}\\ \neg(\mathbf{u}<\mathbf{t})}}\left(h_{\mathbf{u}}(\mathbf{s})(\mathbf{x}-\mathbf{s})^{\mathbf{u}}\right)$$

Feltehetjük, hogy w-t a minimálisnak választottuk. Ekkor $\mathbf{w}<\mathbf{t}$, és $(\mathbf{x}-\mathbf{s})^{\mathbf{w}}$ együtthatója $(s_1-a)g_{\mathbf{w}}(\mathbf{s})+$ $+\chi_{(w_1\geq 1)}\cdot g_{(w_1-1,w_2,\dots,w_n)}(\mathbf{s})$, azonban $(w_1-1,u_2,\dots,u_n)<\mathbf{w}$, így $g_{(w_1-1,w_2,\dots,w_n)}(\mathbf{s})=0$, tehát az együttható egész egyszerűen $(s_1-a)g_{\mathbf{w}}(\mathbf{s})\neq 0$, mivel $g_{\mathbf{w}}(\mathbf{s})\neq 0$ és s_1-a pedig nem nullosztó R-ben, így ezzel az esettel a bizonyítás teljes lett. □

5.13. *Megjegyzés.* Ha $\sum_{i=1}^n t_i=\deg(f)$ akkor persze $\mathbf{t}$ maximális lesz $\mathrm{Supp}(f)$-ben.

5.4. Alkalmazások

A következőekben kiterjesztjük a 3.1 tételt kétféleképpen is, továbbá belátjuk a Cauchy-Davenport tételt multihalmazokra.

5.14. Tétel ([10])**.** *Legyenek $(S_1,m_1),\dots,(S_n,m_n)$ az $\mathbb{F}$ test véges nem üres multihalmazai, úgy, hogy $0\in S_i$ és $m_i(0)=1$ minden i-re. Továbbá legyen adott m darab $\mathbb{F}^n$-beli hipersík. Ha minden $\mathbf{0}\neq\mathbf{s}\in\mathbf{S}$ pont legalább $\sum_{i=1}^n(m_i(s_i)-1)+1$ darab hipersíkon rajta van, és a $\mathbf{0}$ pont pedig egyetlen hipersíkra sem esik rá, akkor*

$$m\geq\sum_{i=1}^n d(S_i)-n.$$

Bizonyítás. Tegyük fel, hogy a j. hipersík egyenlete $(\mathbf{a}_{j\cdot},\mathbf{x})=b_j$. Ekkor legyen

$$f(\mathbf{x})=\prod_{j=1}^m\left((\mathbf{a}_{j\cdot},\mathbf{x})-b_j\right).$$

A feltételek miatt $f(\mathbf{0})\neq 0$, de minden más $\mathbf{s}\in\mathbf{S}$ pontban

$$f(\mathbf{x}+\mathbf{s})=\prod_{j=1}^m\left((\mathbf{a}_{j\cdot},\mathbf{x})+(\mathbf{a}_{j\cdot},\mathbf{s})-b_j\right),$$

azaz legalább $\sum_{i=1}^n(m_i(s_i)-1)+1$-szeres gyöke van $\mathbf{s}\in\mathbf{S}$-ben. Vagyis ha $\mathbf{u}<\mathbf{m}(\mathbf{s})$, akkor $\sum_{i=1}^n u_i<$ $<\sum_{i=1}^n(m_i(s_i)-1)+1$, és ekkor $f_{\mathbf{u}}(\mathbf{s})=0$, tehát $f\in\mathfrak{I}(\mathbf{s},m(\mathbf{s}))$. Így alkalmazhatjuk az 5.5 tétel **b)** részét, és így $m=\deg(f)\geq\sum_{i=1}^n(d(S_i)-d(D_i))=\sum_{i=1}^n d(S_i)-n$. □

5.15. *Megjegyzés.* Természetesen alkalmazhattuk volna az 5.5 tétel **b)** részét is $D_i=\{0\}$ és $m_i(0)=1$-re.

5.16. Tétel ([9]). *Legyen R gyűrű, és adott m darab hipersík R^n-ben az $(\mathbf{a}_j., \mathbf{x}) = b_j$ egyenletek által úgy, hogy a $\mathbf{0}$ pont kivételével lefedik a $\{0,1\}^n$ minden pontját, és a $\mathbf{0}$ egyik hipersíkon sincs rajta. Ha $\prod_{j=1}^{m} b_j \neq 0$, akkor $m \geq n$.*

Bizonyítás. Tegyük fel, hogy $m < n$. Legyen az $f \in R[\mathbf{x}]$ polinom a következő:

$$f(\mathbf{x}) = \prod_{j=1}^{m} (b_j - (\mathbf{a}_j., \mathbf{x})) - \prod_{j=1}^{n} b_j \prod_{i=1}^{n} (1 - x_i).$$

A feltételek miatt $\deg(f) = n$. Legyen $S_i = \{0,1\}$ és $m_i(0) = m_i(1) = 1$. Világos, hogy $f(\mathbf{s}) = 0$, hisz $\mathbf{s} = \mathbf{0}$ esetén ez triviális, más $\mathbf{s} \in \mathbf{S}$ esetén pedig $\mathbf{s}$ rajta van az egyik hipersíkon, és a harmadik produktum pedig nyilván 0 lesz. Viszont alkalmazva az 5.12 tételt, azt kapjuk, hogy létezik $\mathbf{s}$, hogy $f_{\mathbf{0}}(\mathbf{s}) = f(\mathbf{s}) \neq 0$, ez nyilván ellentmondás. □

5.17. Definíció. Legyen (A, m_1) és (B, m_2) két multihalmaz $\mathbb{F}_p$-ből. Legyen egy $c \in A+B$ elem multiplicitása

$$m_3(c) = \max\{m_1(a) + m_2(b) - 1 \mid a \in A, b \in B, a + b = c\},$$

így ezzel értelmezhető az $(A+B, m_3)$ multihalmaz.

5.18. Tétel (Cauchy-Davenport tétel multihalmazokra [10]). *Legyen (A, m_1) és (B, m_2) két multihalmaz $\mathbb{F}_p$-ből. Ekkor*

$$d(A+B) \geq \max\{p, d(A) + d(B) - 1\}.$$

Bizonyítás. A tételt hasonlóan fogjuk belátni, mint a 3.6 tételt. Multiplicitások csökkentésével feltehetjük, hogy $d(A) + d(B) - 1 \leq p$.

Tegyük fel indirekt módon, hogy létezik egy olyan (C, m) multihalmaz, hogy $(A+B, m_3) \subseteq (C, m)$ mint multihalmaz, azaz ha $c \in A+B$, akkor $m_3(c) \leq m(c)$, és $d(C) = d(A) - 1 + d(B) - 1 < p$. Legyen

$$f(x, y) = \prod_{c \in C} (x + y - c)^{m(c)},$$

ekkor $f \in \mathbb{F}_p[x, y]$, és a $x^{d(A)-1} y^{d(B)-1}$ monom együtthatója $\mathbb{F}_p$ felett $\binom{d(A)-1+d(B)-1}{d(A)-1} \neq 0$. Alkalmazhatjuk az 5.6 tételt (A, m_1), (B, m_2) multihalmazokra, tehát léteznek $a \in A$ és $b \in B$, illetve $k < m_1(a)$ és $l < m_2(b)$ egészek, hogy f polinom (a, b) körüli felbontásában $(x-a)^k (y-b)^l$ együtthatója nem 0.

Legyen $c' = a + b$ és $r = m(c')$, és definiálja az $f' \in \mathbb{F}_p[x, y]$ polinomot az

$$f(x, y) = f'(x, y)(x + y - c')^r$$

egyenlőség. Továbbá

$$(x + y - c')^r = \sum_{i=0}^{r} \binom{r}{i} (x - a)^i (y - b)^{r-b},$$

vagyis $f(x, y)$-nak (a, b)-ben legalább $r \geq m_1(a) + m_2(b) - 1 > k + l$-szeres gyöke van, ami ellentmondás. □

5.5. Motiváció a nullhelytétel multihalmazokra való kiterjesztéséhez

Ebben a részben megmutatjuk, hogy ha a következő sejtés igaz, akkor a Snevily-sejtés is igaz lesz minden k-ra, amely kisebb vagy egyenlő, mint G rendjének a legkisebb prímosztója.

5.19. Sejtés ([9]). *Legyen $k \leq p$ és az $a_1, \ldots, a_k$ illetve $b_1, \ldots, b_k$ tetszőleges elemek Z_p-ben. Ekkor létezik $\pi \in \mathrm{Sym}(k)$, hogy minden $1 \leq i, j \leq k$ esetén, ha $a_i + b_{\pi(i)} = a_j + b_{\pi(j)}$, akkor $a_i = a_j$ és $b_i = b_j$.*

Nagyon lényeges, hogy az 5.19 sejtésben megengedtük, hogy az elemek egybeessenek. A Snevily-sejtésről szóló fejezetben láttuk, hogy ha az 5.19 sejtésben megköveteljük, hogy a b_i elemek különbözőek legyenek, akkor az állítás igaz. Úgy tűnik, hogy a 2. fejezetben bemutatott Alon-féle kombinatorikus nullhelytételnél erősebbre van szükség ahhoz, hogy belássuk ezt a sejtést, ez motiválta, hogy multihalmazokra is kiterjesszük a tételt, hisz a sejtésben is multihalmazok szerepelnek.

A Feit-Thompson tétel szerint minden G véges páratlan rendű csoport feloldható, így ekkor létezik G-nek egy olyan kompozíciólánca is, hogy a faktorok mind prímrendű ciklikus csoportok. Mivel a G csoport elemeinek a képei a G/N faktorcsoportban már nem feltétlenül különbözőek, ezért a 3.15 tételnek egy általánosabb alakjára van szükségünk.

A csoport rendje szerinti indukcióval fogunk bizonyítani. Ha az prím, akkor a 5.19 sejtés miatt készen vagyunk. Egyébként legyen $1 \lneq N \triangleleft G$ egy maximális normálosztó, ekkor G/N egy prímrendű ciklikus csoport (G-nek létezik kompozíciólánca). Először a G/N faktorcsoportra alkalmazzuk a 5.19 sejtést. Vegyük az $a_1 + N, \ldots, a_k + N$ illetve $b_1 + N, \ldots, b_n + N$ elemeket. Mivel p osztja a G rendjét, ezért $k \leq p$ a feltevés szerint, és így a sejtés szerint létezik egy megfelelő $\pi \in \mathrm{Sym}(k)$, hogy ha a faktorcsoportban az $a_{i_1} + b_{\pi(i_1)} + N, \ldots, a_{i_l} + b_{\pi(i_l)} + N$ elemek egyenlőek, akkor $a_{i_1}, \ldots, a_{i_l} \in c + N$ illetve $b_{\pi(i_1)}, \ldots, b_{\pi(i_l)} \in d + N$, azaz egy-egy mellékosztályba esnek (tehát $a_{i_m} + b_{\pi(i_m)} \in c + d + N$). Ekkor $a_{i_1} - c, \ldots, a_{i_l} - c \in N$ páronként különbözőek illetve a $b_{\pi(i_1)} - d, \ldots, b_{\pi(i_l)} - d \in N$ is páronként különböző elemek, így N-re alkalmazhatunk indukciót (N rendjének legkisebb prímosztója persze legalább akkora, mint k). Így kapunk egy alkalmas $\sigma \in \mathrm{Sym}(i_1, \ldots, i_l)$ permutációt, hogy az $a_{i_m} + b_{\sigma\pi(i_m)}$ elemek különbözőek. Ezzel beláttuk az állítást, hiszen $a_{i_m} + b_{\sigma\pi(i_m)} \in c + d + N$, így akikkel az összeg G/N-ben sem esett egybe, azoktól továbbra is különböző marad.

6. fejezet

További kiterjesztések

Ebben a fejezetben saját eredményeimet, a kombinatorikus nullhelytétel további kiterjesztéseit mutatom be.

6.1. Definíció (Kitevők által adott ideál)**.** Legyen az $L \subseteq \mathbb{N}^n$ halmaz olyan, hogy ha $\mathbf{v} \geq \mathbf{u} \in L$, akkor $\mathbf{v} \in L$ (azaz L felszálló halmaz). Ha adott az $\mathbf{s} \in S_1 \times \ldots \times S_n$ pont és az R gyűrű, akkor legyen

$$\mathfrak{L}_R(\mathbf{s}) = \left\{ f = \sum_{\mathbf{u}} f_{\mathbf{u}}(\mathbf{s})(\mathbf{x}-\mathbf{s})^{\mathbf{u}} \;\middle|\; f_{\mathbf{u}}(\mathbf{s}) \in R,\ \mathbf{u} \notin L \Rightarrow f_{\mathbf{u}}(\mathbf{s}) = 0 \right\} \subseteq R[\mathbf{x}]$$

az L-beli kitevők által az $\mathbf{s}$ körüli felbontásra adott ideál.

6.2. Állítás. *A kitevők által adott $\mathfrak{L}_R(\mathbf{s})$ valóban ideálja az $R[\mathbf{x}]$ polinomgyűrűnek.*

Bizonyítás. Mivel R egységelemes, elég belátni, hogy bármely $f' \in R[\mathbf{x}]$ polinommal szorozva $ff' \in \mathfrak{L}_R(\mathbf{s})$. Mivel $f' = \sum_{\mathbf{v}} f'_{\mathbf{v}}(\mathbf{s})(\mathbf{x}-\mathbf{s})^{\mathbf{v}}$ alakban is írható, ezért $ff' = \sum_{\mathbf{u},\mathbf{v}} f_{\mathbf{u}}(\mathbf{s}) f'_{\mathbf{v}}(\mathbf{s})(\mathbf{x}-\mathbf{s})^{\mathbf{u}+\mathbf{v}} \in \mathfrak{L}_R(\mathbf{s})$. □

6.3. Állítás. *Legyen L felszálló halmaz. Ha $\mathbb{N}^n \setminus L$ véges (azaz L ko-véges), akkor megadható véges sok $\mathbf{w} \in W$ pont úgy, hogy $L = \{\mathbf{u} \mid \exists \mathbf{w} \in W\ \mathbf{u} \geq \mathbf{w}\}$.*

Bizonyítás. Legyen $k = |\mathbb{N}^n \setminus L|$. Vegyük a minimális elemek halmazát L-ből, ezek nyilván L-et generálják. Ha egy minimális elem valamelyik koordinátáját 1-gyel csökkentjük, akkor $\mathbb{N}^n \setminus L$-beli elemet kapunk. Minden $\mathbb{N}^n \setminus L$-beli elemet legfeljebb n féleképpen kaphatunk meg, így minimális elemből legfeljebb nk lehet. □

6.4. Tétel. *Legyen $\mathbb{F}$ egy tetszőleges test, n pozitív egész, $S_1, \ldots, S_n \subseteq \mathbb{F}$ nem-üres véges részhalmazok, és definiáljuk a $g_i(x_i) = \prod_{s \in S_i} (x_i - s)$ polinomokat. Legyen L ko-véges felszálló halmaz, és benne a W a minimális elemek halmaza, és definiáljuk az $m_{\mathbf{w}} = g_1^{w_1} \cdots g_n^{w_n}$ polinomokat minden $\mathbf{w} \in W$-re. Ha az $f \in \mathbb{F}[\mathbf{x}]$ polinom eleme az $\mathfrak{L}_{\mathbb{F}}(\mathbf{s})$ ideálnak minden $\mathbf{s} \in S_1 \times \ldots \times S_n$ pontra, akkor léteznek $h_{\mathbf{w}} \in \mathbb{F}[\mathbf{x}]$ polinomok, melyekkel teljesül az*

$$f = \sum_{\mathbf{w} \in W} h_{\mathbf{w}} m_{\mathbf{w}}$$

egyenlőség, miközben $\deg(h_{\mathbf{w}}) \leq \deg(f) - \deg(m_{\mathbf{w}})$.

Bizonyítás. Legyen $k = |\mathbb{N}^n \setminus L|$. Vegyük észre, hogy ekkor $\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\mathfrak{L}_{\mathbb{F}}(\mathbf{s}) = k$, hiszen egy $f \in \mathbb{F}[\mathbf{x}]$ polinom képe a természetes leképezéssel $\sum_{\mathbf{u} \notin L} f_{\mathbf{u}}(\mathbf{s})(\mathbf{x}-\mathbf{s})^{\mathbf{u}} + \mathfrak{L}_{\mathbb{F}}(\mathbf{s})$. Világos, hogy $\mathrm{Rad}(\mathfrak{L}_{\mathbb{F}}(\mathbf{s})) = (x_1 - s_1, \ldots, x_n - s_n)$, hiszen $(x_i - s_i)^k \in \mathfrak{L}_{\mathbb{F}}(\mathbf{s})$ minden i-re. Ebből az 1.9 állítás miatt következik, hogy páronként relatív prímek. Legyen $\mathfrak{I} = \bigcap_{\mathbf{s} \in S_1 \times \ldots \times S_n} \mathfrak{L}_{\mathbb{F}}(\mathbf{s})$, a kínai maradéktétel (1.10) miatt

$$\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\mathfrak{I} = \sum_{\mathbf{s} \in S_1 \times \ldots \times S_n} \dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\mathfrak{L}_{\mathbb{F}}(\mathbf{s}) = k|S_1| \cdot \ldots \cdot |S_n|.$$

Most vegyük az $\big(m_{\mathbf{w}} \mid \mathbf{w} \in W\big) \trianglelefteq \mathbb{F}[\mathbf{x}]$ generált ideált. Vegyük észre, hogy $m_{\mathbf{w}} \in \mathfrak{L}_{\mathbb{F}}(\mathbf{s})$ minden $\mathbf{s}$ pontban, hiszen osztható $(\mathbf{x}-\mathbf{s})^{\mathbf{w}}$-vel. Ezzel beláttuk, hogy $(m_{\mathbf{w}} \mid \mathbf{w} \in W) \subseteq \mathfrak{I}$, és emiatt $\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/(m_{\mathbf{w}} \mid \mathbf{w} \in W) \geq$ $\geq k|S_1| \cdot \ldots \cdot |S_n|$.

Legyen $P = \big\{\mathbf{u} \mid \exists \mathbf{w} \in W\, \mathbf{u} \geq (w_1|S_1|, \ldots, w_n|S_n|)\big\}$ felszálló halmaz. Tekintsük először az f polinomot $\mathbb{F}[\mathbf{x}]$ egy tetszőleges elemének, és osszuk el maradékosan az $m_{\mathbf{w}}$ polinomokkal. Legyen $V = \big\langle \mathbf{x}^{\mathbf{u}} \;\big|\; \mathbf{u} \in \mathbb{N}^n \setminus P \big\rangle$ az osztási maradékok vektortere. Az 1.3 állítás miatt $\deg(h_{\mathbf{w}}) \leq \deg(f) - \deg(g_{\mathbf{w}})$, és $r \in V$. Alkalmazva az 1.4 állítás **a)** részét, azt kapjuk, hogy

$$\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\big(m_{\mathbf{w}} \mid \mathbf{w} \in W\big) \leq \dim_{\mathbb{F}} V.$$

Vegyük észre, hogy $\dim_{\mathbb{F}} V = |\mathbb{N}^n \setminus P| = |\mathbb{N}^n \setminus L| \cdot |S_1| \cdot \ldots \cdot |S_n|$, hiszen az L halmazból például úgy kaphatjuk meg P-t, hogy először az L összes elemének a koordinátáját megszorozzuk $|S_1|$-gyel, majd a második koordinátákat $|S_2|$-vel, és így tovább egészen n-ig.

Ezzel beláttuk, hogy $\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/(m_{\mathbf{w}} \mid \mathbf{w} \in W) = k|S_1| \cdot \ldots \cdot |S_n|$ és emiatt $(m_{\mathbf{w}} \mid \mathbf{w} \in W) = \mathfrak{I}$ is teljesül, és az 1.4 állítás **b)** része miatt az r maradék egyértelmű. Feltettük, hogy $f \in \mathfrak{I} = (m_{\mathbf{w}} \mid \mathbf{w} \in W)$, így az egyértelműség miatt $r \equiv 0$. □

A 6.4 tételnek következménye a 4.3 tétel: legyen $L = \{\mathbf{u} \mid \sum_i u_i \geq t\}$, ebben a minimális elemek nyilván az olyan $\mathbf{w}$-k, melyekre $\sum_i w_i = t$. Definíció szerint $f \in \mathfrak{L}_{\mathbb{F}}(\mathbf{s})$ azt jelenti, hogy f-nek $\mathbf{s}$-ben legalább t-szeres gyöke van. A 6.4 tételből ekkor az $m_{\mathbf{w}} = g_1^{w_1} \cdot \ldots \cdot g_n^{w_n}$ (ahol $\sum_i w_i = t$) polinomokat kapjuk.

Ezzel a kiterjesztéssel azonban nem kapjuk meg az 5.4 tételt, ez motiválja a most következő részt. Láttuk, hogy a kitevőhalmazt felszálló volta miatt a minimális elemek határozzák meg. A 6.4 tételben minden $\mathbf{s}$ pontban hasonló volt az $\mathfrak{L}_{\mathbb{F}}(\mathbf{s})$ ideál struktúrája, hiszen ugyanabból az L kitevőhalmazból kaptuk őket. Ezt a hasonló struktúra fogalmat fogjuk most precízen definiálni, ehhez fel fogunk használni egyszerű hálóelméleti állításokat, ezek megtalálhatóak például [7]-ben.

6.5. Definíció. Legyen P és Q két ko-véges és felszálló, valódi részhalmaza $\mathbb{N}^n$-nek. Vegyük a minimális elemeik halmazát, ezek között pontosan n olyan lesz, melyeknek $n-1$ koordinátája 0, és egy pedig nem 0, mivel feltettük, hogy ko-végesek és komplementerük nem üres (nevezzük ezeket tengelyre eső elemeknek). A P és Q halmaz ezen elemei egyértelműen megfeleltethetőek egymásnak a szerint, hogy melyik koordinátájuk nem 0. Azt mondjuk, hogy P és Q struktúrája hasonló, ha a minimális elemeik által $\mathbb{N}^n$-ben generált hálók izomorfak, azzal a kikötéssel, hogy az előbb mutatott pontok a megadott módon felelnek meg egymásnak, és P bármely minimális elemének képe Q-beli minimális elem (nevezzük ezt kötött izomorfiának).

6.6. Állítás. *Legyen L ko-véges felszálló halmaz, és legyenek a minimális elemei az $\mathbf{u}_{i\cdot}$ $(1 \leq i \leq k)$ vektorok. Ekkor a generált háló bármely elemének j. koordinátája valamilyen i-re $\mathbf{u}_{ij}$ lesz (sőt, pontosan az ilyen alakú elemekből áll a generált háló).*

Bizonyítás. Legyen az i. tengelyre eső minimális elem $\mathbf{a}_{i\cdot}$, úgy, hogy $a_{ii} \neq 0$ de $j \neq i$ esetén $a_{ij} = 0$. Ekkor a generált háló bármely $\mathbf{b}$ elemére $(\mathbf{a}_{i\cdot} \wedge \mathbf{b})_i = b_i$ és bármely $j \neq i$-re $(\mathbf{a}_{i\cdot} \wedge \mathbf{b})_i = 0$. Világos, hogy ekkor egy fent leírt alakú elem előáll, mint $\bigvee_{i=1}^n (\mathbf{a}_{i\cdot} \wedge \mathbf{u}_{l_i\cdot})$, továbbá bármely generátor is megkapható ilyen alakban ha l_i-ket azonosnak választjuk. Ha $\bigvee_{i=1}^n (\mathbf{a}_{i\cdot} \wedge \mathbf{u}_{p_i\cdot})$ és $\bigvee_{i=1}^n (\mathbf{a}_{i\cdot} \wedge \mathbf{u}_{q_i\cdot})$ két ilyen alakú elem, akkor az uniójuk $\bigvee_{i=1}^n (\mathbf{a}_{i\cdot} \wedge (\mathbf{p}_{l_i\cdot} \vee \mathbf{q}_{l_i\cdot}))$, de ha feltesszük, hogy $p_{l_i i} \geq q_{l_i i}$, akkor $\mathbf{a}_{i\cdot} \wedge (\mathbf{p}_{l_i\cdot} \vee \mathbf{q}_{l_i\cdot}) = \mathbf{a}_{i\cdot} \wedge \mathbf{p}_{l_i\cdot}$, tehát megfelelő alakú lesz végül. A metszet műveletre való zártságot ugyanígy lehet belátni. □

6.7. Állítás. *A hasonló struktúra tulajdonság ekvivalencia reláció, és a kötött izomorfia egyértelmű.*

Bizonyítás. Ekvivalencia reláció, hiszen kötött izomorfiák kompozíciója is kötött izomorfia. Legyen az n darab tengelyre eső elem $\mathbf{a}_{i\cdot}$, úgy, hogy az i. koordináta ne legyen 0. Az izomorfiára vett képei egyértelműek azon elemeknek, melyeknek csak egyetlen koordinátájuk nem 0, hiszen n darab láncot alkotnak, melyeknek a legnagyobb eleme egy-egy, az izomorfiára kötött elem, tehát az egész lánc képe egyértelmű lesz. Most már csak azt kell észrevenni, hogy a háló bármelyik eleme felírható egyértelműen úgy, hogy az n lánc mindegyikéből választunk egy elemet, és vesszük ezeknek az unióját. A felírás létezését bizonyítja, hogy $\mathbf{b}=\bigvee_{i=1}^{n}(\mathbf{a}_{i\cdot}\wedge\mathbf{b})$. Az egyértelműség bizonyításához legyen $\mathbf{b}=\bigvee_{i=1}^{n}\mathbf{c}_{i\cdot}$ és $\mathbf{c}_{i\cdot}\leq\mathbf{a}_{i\cdot}$, ekkor $c_{ij}=0$, ha $i\neq j$, és csak $c_{ii}=b_i$ lehet. □

6.8. *Megjegyzés.* Ez az állítás tehát azt jelenti, hogy ha néhány ko-véges felszálló halmaz egy hasonló struktúra szerinti ekvivalenciaosztályba esik, akkor a minimális elemek egyértelműen felelnek meg egymásnak, és így indexelhetőek egy $\lambda\in\Lambda$ paraméterrel és a ko-véges felszálló halmazzal, úgy, hogy az azonos λ indexszel jelölt minimális elemek felelnek meg egymásnak a kötött izomorfiánál.

6.9. Állítás. *Tegyük fel, hogy adottak P és Q ko-véges felszálló halmazok $\mathbb{N}^n$-ben, és adott a P minimális elemei által generált hálóból a Q minimális elemeinek a hálójába egy φ kötött izomorfia. Ekkor a $\psi(\mathbf{b})=$ $=\mathbf{b}+\varphi(\mathbf{b})$ leképezés egy kötötten izomorf képét adja a P minimális elemei által generált hálónak.*

Bizonyítás. Azt kell belátni, hogy ψ és ψ^{-1} is rendezéstartó bijekció. Legyen $\mathbf{b}\leq\mathbf{c}$, ekkor $\psi(\mathbf{b})=\mathbf{b}+$ $+\varphi(\mathbf{b})\leq\mathbf{c}+\varphi(\mathbf{b})\leq\mathbf{c}+\varphi(\mathbf{c})=\psi(\mathbf{c})$, hiszen φ hálóizomorfizmus. Most tegyük fel, hogy $\mathbf{b}\not\leq\mathbf{c}$, azaz létezik egy i, hogy $b_i>c_i$. Ekkor $\varphi(\mathbf{b})\not\leq\varphi(\mathbf{c})$, hisz φ hálóizomorfizmus volt. Mivel φ kötött izomorfizmus szó, ezért $\varphi(\mathbf{b})_i>\varphi(\mathbf{c})_i$, mivel a tengelyekre vett vetületek egyértelműek. Tehát $\psi(\mathbf{b})_i=b_i+\varphi(\mathbf{b})_i>c_i+\varphi(\mathbf{c})_i=\psi(\mathbf{c})$, azaz $\psi(\mathbf{b})\not\leq\psi(\mathbf{c})$, ezzel beláttuk, hogy az inverz is rendezéstartó. Ugyanezzel az indoklással megkapjuk azt is, hogy ψ bijekció, mert $b\neq c$ ekvivalens azzal, hogy $b\not\leq c$ vagy $b\not\geq c$. □

6.10. *Megjegyzés.* Ennek a tételnek az volt az értelme, hogy a P minimális elemei által generált háló képe ψ-nél az $\mathbf{a}_{i\cdot}+\varphi(\mathbf{a}_{i\cdot})$ elemek által generált háló lesz. Pontosabban, a P és a Q ko-véges felszálló halmazokból csináltunk egy olyan ko-véges felszálló halmazt, aminek a struktúrája hasonló P és Q struktúrájához is.

Tegyük most fel, hogy adott az L ko-véges felszálló halmaz $\mathbb{N}^n$-ben. Ki szeretnék számolni a komplementerének az elemszámát a minimális elemeinek a függvényében. Ez azért lesz jó, mert garantálni fogja, hogy a képlet egységes legyen a hasonló struktúrájú halmazokra.

6.11. Lemma.

a) *Tegyük fel, hogy L ko-véges felszálló halmaz minimális elemei az $\mathbf{u}_{i\cdot}\in\mathbb{F}^n$, $1\leq i\leq k$ vektorok. Ekkor léteznek olyan $\alpha_{l_1,\ldots,l_n}$ számok, hogy a következő lineáris összefüggés fennáll:*

$$|\mathbb{N}^n\setminus L|=\sum_{1\leq l_1,\ldots,l_n\leq k}\alpha_{l_1,\ldots,l_n}\prod_{i=1}^{n}u_{l_i i}.$$

b) *A képlet invariáns a kötött izomorfiára.*

Bizonyítás. Az **a)** rész bizonyításához vegyük a minimális elemek által generált hálót, és tekintsük az összes olyan elemét, amelyik kisebb vagy egyenlő, mint valamelyik minimális elem, legyenek ezek a $\mathbf{v}_{i\cdot}$ $(1\leq i\leq m)$ vektorok Vegyük észre, hogy minden $\mathbf{w}\in\mathbb{N}^n\setminus L$ elemhez egyértelműen hozzárendelhető egy $\mathbf{w}\geq\mathbf{v}_{i\cdot}$ vektor, de bármely $j\neq i$ esetén $\mathbf{v}_{j\cdot}>\mathbf{w}$ vagy $\mathbf{v}_{i\cdot}\geq\mathbf{v}_{j\cdot}$. Számoljuk össze, hogy $\mathbf{v}_{i\cdot}$-hez hány elemet rendeltünk hozzá. Legyen $\mathbf{v}'_{i\cdot}$ az az elem, amit úgy kapunk, ha vesszük a hálóban a $\mathbf{v}_{i\cdot}$ elemet fedő elemek unióját, ez a legkisebb olyan elem, hogy minden j-re $v_{ij}<v'_{ij}$. Könnyű meggondolni, hogy $\mathbf{v}_{i\cdot}$-hoz pontosan azokat a $\mathbf{w}\in\mathbb{N}^n\setminus L$ elemeket rendeltük, melyekre $\mathbf{v}_{i\cdot}\leq\mathbf{w}<\mathbf{v}'_{i\cdot}$. Az ilyeneknek a száma $\prod_{j=1}^{n}(v'_{ij}-v_{ij})$.

A 6.6 állítás alapján a szorzatot kibontva kívánt alakú lineáris kombinációt kapunk. Ezeket kell tehát minden $\mathbf{v}_{i\cdot}$ elemre összeadni, ez továbbra is megfelelő alakú lineáris kombináció lesz.

A kötött izomorfia garantálja, hogy a minimális elemek minimális elembe mennek (6.7 állítás). A képlet kiszámításakor csak a háló struktúráját használtuk, az izomorfia ezt megőrzi. □

Most már ki tudunk mondani egy kiterjesztett tételt, a bizonyítás a 6.4 és az 5.4 tételéhez hasonló lesz.

6.12. Tétel. *Legyen $\mathbb{F}$ egy tetszőleges test, n pozitív egész, $S_1,\dots,S_n\subseteq\mathbb{F}$ nem-üres véges részhalmazok. Legyen minden $\mathbf{s}\in S_1,\dots,S_n$ pontra $L(\mathbf{s})$ nem-üres ko-véges felszálló halmaz, és benne a $W(\mathbf{s})$ a minimális elemek halmaza. Tegyük fel, hogy a $W(\mathbf{s})$ halmazok által generált hálók kötötten izomorfak, ekkor a minimális elemeket egyszerre indexelhetjük $\lambda\in\Lambda$-val, hiszen egyértelműen megfeleltethetőek egymásnak (legyen $\mathbf{w}_\lambda(\mathbf{s})\in W(\mathbf{s})$). Tegyük fel ezen kívül még, hogy $w_{\lambda i}(\mathbf{s})=w_{\lambda i}(s_i)$, azaz nem függ $\mathbf{s}_{-i}$-től. Definiáljuk ekkor a*

$$g_\lambda=\left(\prod_{s_1\in S_1}(x_1-s_1)^{w_{\lambda 1}(s_1)}\right)\cdots\left(\prod_{s_n\in S_n}(x_n-s_n)^{w_{\lambda n}(s_n)}\right)$$

*polinomokat. Ha az $f\in\mathbb{F}[\mathbf{x}]$ polinom eleme az $L(\mathbf{s})$ kitevőhalmazhoz tartozó $\mathfrak{L}_\mathbb{F}(\mathbf{s})$ ideálnak minden $\mathbf{s}\in\in S_1\times\ldots\times S_n$ pontra (**s** most egyszerre paraméterezi az ideálnak a kitevőhalmazát és az eltolásvektorát), akkor léteznek $h_\lambda\in\mathbb{F}[\mathbf{x}]$ polinomok, melyekkel teljesül az*

$$f=\sum_\lambda h_\lambda g_\lambda$$

egyenlőség, miközben $\deg(h_\lambda)\le\deg(f)-\deg(g_\lambda)$.

Bizonyítás. A 6.11 lemma **a)** része alapján $\dim_\mathbb{F}\mathbb{F}[\mathbf{x}]/\mathfrak{L}_\mathbb{F}(\mathbf{s})=\sum_{\lambda_1,\dots,\lambda_n\in\Lambda}\alpha_{\lambda_1,\dots,\lambda_n}\prod_{i=1}^n w_{\lambda_i i}(\mathbf{s})$, hiszen egy $f\in\mathbb{F}[\mathbf{x}]$ polinom képe a természetes leképezéssel $\sum_{\mathbf{u}\notin L(\mathbf{s})}f_\mathbf{u}(\mathbf{s})(\mathbf{x}-\mathbf{s})^\mathbf{u}+\mathfrak{L}_\mathbb{F}(\mathbf{s})$. Világos, hogy $\mathrm{Rad}(\mathfrak{L}_\mathbb{F}(\mathbf{s}))=(x_1-s_1,\dots,x_n-s_n)$, hiszen $L(\mathbf{s})$ ko-véges. Ebből az 1.9 állítás miatt következik, hogy az $\mathfrak{L}_\mathbb{F}(\mathbf{s})$ ideálok páronként relatív prímek. Legyen $\mathfrak{I}=\bigcap_{\mathbf{s}\in S_1\times\ldots\times S_n}\mathfrak{L}_\mathbb{F}(\mathbf{s})$, a kínai maradéktétel (1.10) miatt

$$\dim_\mathbb{F}\mathbb{F}[\mathbf{x}]/\mathfrak{I}=\sum_{\mathbf{s}\in S_1\times\ldots\times S_n}\dim_\mathbb{F}\mathbb{F}[\mathbf{x}]/\mathfrak{L}_\mathbb{F}(\mathbf{s})=\sum_{\mathbf{s}\in S_1\times\ldots\times S_n}\sum_{\lambda_1,\dots,\lambda_n\in\Lambda}\alpha_{\lambda_1,\dots,\lambda_n}\prod_{i=1}^n w_{\lambda_i i}(s_i)=$$

$$=\sum_{\lambda_1,\dots,\lambda_n\in\Lambda}\alpha_{\lambda_1,\dots,\lambda_n}\sum_{s_1\in S_1}\cdots\sum_{s_n\in S_n}\prod_{i=1}^n w_{\lambda_i i}(s_i)=\sum_{\lambda_1,\dots,\lambda_n\in\Lambda}\alpha_{\lambda_1,\dots,\lambda_n}\left(\sum_{s_1\in S_1}w_{\lambda_1 1}(s_1)\right)\cdots\left(\sum_{s_n\in S_n}w_{\lambda_n n}(s_n)\right)$$

Most vegyük a $(g_\lambda\mid\lambda\in\Lambda)\trianglelefteq\mathbb{F}[\mathbf{x}]$ generált ideált. Vegyük észre, hogy $g_\lambda\in\mathfrak{L}_\mathbb{F}(\mathbf{s})$ minden **s** pontban, hiszen osztható $(\mathbf{x}-\mathbf{s})^{\mathbf{w}_\lambda(\mathbf{s})}$-nel. Ezzel beláttuk, hogy $(g_\lambda\mid\lambda\in\Lambda)\subseteq\mathfrak{I}$, és emiatt

$$\dim_\mathbb{F}\mathbb{F}[\mathbf{x}]/(g_\lambda\mid\lambda\in\Lambda)\ge\sum_{\lambda_1,\dots,\lambda_n\in\Lambda}\alpha_{\lambda_1,\dots,\lambda_n}\left(\sum_{s_1\in S_1}w_{\lambda_1 1}(s_1)\right)\cdots\left(\sum_{s_n\in S_n}w_{\lambda_n n}(s_n)\right).$$

Legyen $P=\{\mathbf{u}\mid\exists\lambda\in\Lambda\,\mathbf{u}\ge(\sum_{s_1\in S_1}w_{\lambda_1 1}(s_1),\dots,\sum_{s_n\in S_n}w_{\lambda_n n}(s_n))\}$ felszálló halmaz. Tekintsük először az f polinomot $\mathbb{F}[\mathbf{x}]$ egy tetszőleges elemének, és osszuk el maradékosan a g_λ polinomokkal. Legyen $V=$ $=\left\langle\mathbf{x}^\mathbf{u}\;\middle|\;\mathbf{u}\in\mathbb{N}^n\setminus P\right\rangle$ az osztási maradékok vektortere. Az 1.3 állítás miatt $\deg(h_\lambda)\le\deg(f)-\deg(g_\lambda)$ és $r\in V$. Alkalmazva az 1.4 állítás **a)** részét, azt kapjuk, hogy

$$\dim_\mathbb{F}\mathbb{F}[\mathbf{x}]/(g_\lambda\mid\lambda\in\Lambda)\le\dim_\mathbb{F}V.$$

Vegyük észre, hogy P az összes $L(\mathbf{s})$ halmaz 6.9 állítás szerinti összege, és ilyen módon a P minimális elemei által generált háló kötötten izomorf az $L(\mathbf{s})$ minimális elemeinek hálójával, így a 6.11 lemma **b)** része miatt $\dim_\mathbb{F}V=|\mathbb{N}^n\setminus P|=\sum_{\lambda_1,\dots,\lambda_n\in\Lambda}\alpha_{\lambda_1,\dots,\lambda_n}\prod_{i=1}^n(\sum_{s_i\in S_i}w_{\lambda_i i}(s_i))$.

Ezzel beláttuk, hogy $\dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/\mathfrak{I} \leq \dim_{\mathbb{F}} \mathbb{F}[\mathbf{x}]/(g_\lambda \mid \lambda \in \Lambda) \leq \dim_{\mathbb{F}} V$, és az egyenlőtlenség két vége egyenlő, tehát az egyenlőség is teljesül. Emiatt $(g_\lambda \mid \lambda \in \Lambda) = \mathfrak{I}$, és az 1.4 állítás **b)** része miatt az r maradék egyértelmű. Feltettük, hogy $f \in \mathfrak{I} = (g_\lambda \mid \lambda \in \Lambda)$, így az egyértelműség miatt $r \equiv 0$. □

Tegyük fel, hogy $0 \neq m_i(s) \in \mathbb{N}$ minden $1 \leq i \leq n$-re és $s \in S_i$-re. Legyen $L(\mathbf{s}) = \{\mathbf{u} \mid 0 \leq \mathbf{u} < (m_1(s_1), \ldots, m_n(s_n))\}$, ekkor

$$W(\mathbf{s}) = \{(m_1(s_1),0,\ldots,0), (0, m_2(s_2),0,\ldots,0), \ldots, (0,\ldots,0,m_n(s_n))\}\,.$$

A generált hálónak még a $\mathbf{0}$ illetve az $(m_1(s_1), \ldots, m_n(s_n))$ vektorok lesznek elemei, ekkor minden $\mathbf{s}$ pontra az $L(\mathbf{s})$ halmazok struktúrája hasonló. Világos, hogy ekkor a 6.12 tétel ugyanazokat a polinomokat szolgáltatja, mint amiket az 5.4 tétel is megad.

Irodalomjegyzék

[1] Noga Alon. Combinatorial Nullstellensatz. *Combinatorics, Probability and Computing*, 1999. http://www.tau.ac.il/~nogaa/PDFS/null2.pdf.

[2] Noga Alon. Additive Latin Transversals. *Israel Journal of Mathematics*, 2000. http://www.tau.ac.il/~nogaa/PDFS/alt2.pdf.

[3] Noga Alon and Zoltán Füredi. Covering the Cube by Affine Hyperplanes. *European Journal of Combinatorics*, 1993. http://www.math.uiuc.edu/~z-furedi/PUBS/furedi_alon_cube-covering.pdf.

[4] Bodan Arsovski. A proof of Snevily's conjecture. *Israel Journal of Mathematics*, 2011. Egy egyszerűbb bizonyítás található itt: http://www.renyi.hu/~gharcos/snevily.pdf.

[5] Simeon Ball and Oriol Serra. Punctured Combinatorial Nullstellensätze. *Combinatorica*, 2009. http://www-ma4.upc.es/~simeon/puncturednullstellensatz.pdf.

[6] Samit Dasgupta, Gyula Károlyi, Oriol Serra, and Balázs Szegedy. Transversals of additive Latin squares. *Israel Journal of Mathematics*, 2000. http://bolyai.cs.elte.hu/~karolyi/snevily.pdf.

[7] Pelikán József és Gröller Ákos. Algebra jegyzet. *Előadás jegyzet*, 2000. http://www.cs.elte.hu/~pelikan/algebra.html.

[8] Gyula Károlyi. The Erdős-Heilbronn Problem in Abelian Groups. *Israel Journal of Mathematics*, 2004. http://bolyai.cs.elte.hu/~karolyi/eh.pdf.

[9] Géza Kós, Tamás Mészáros, and Lajos Rónyai. Some Extensions of Alon's Nullstellensatz. *Kézirat*, 2011. http://arxiv.org/pdf/1103.4768v1.

[10] Géza Kós and Lajos Rónyai. Alon's Nullstellensatz for Multisets. *Combinatorica*, 2010, Megjelenésre vár. http://arxiv.org/PS_cache/arxiv/pdf/1008/1008.2901v1.pdf.

[11] Michał Lasoń. A generalization of Combinatorial Nullstellensatz. *The Electronic Journal of Combinatorics*, 17, 2010. http://www.combinatorics.org/Volume_17/PDF/v17i1n32.pdf.

[12] Mateusz Michałek. A short proof of Combinatorial Nullstellensatz. *American Mathematical Monthly*, 2010. http://arxiv.org/pdf/0904.4573v1.

E-mail: tommy.mezei@gmail.com