Az ortogonális csoport vektorinvariánsai a 2 karakterisztikájú esetben

Diplomamunka

Készítette: Frenkel Péter
Témavezető: Domokos Mátyás

Budapest, 2002

0.1. Bevezetés

Az ortogonális csoport és más klasszikus csoportok vektorinvariánsairól Hermann Weyl kimerítő tárgyalást adott híres [11] könyvében, melynek első kiadása 1939-ben jelent meg. Az eredmények egy része már Weyl 1924-es [10] cikkében szerepelt. Az egységes tárgyalásmód – mely Capelli, Weitzenböck és mások módszereit is felhasználja – és az eredmények jelentős része Weyl sajátja, bár például az ortogonális csoportra vonatkozó úgynevezett „első alaptételt” E. Study már 1897-ben bebizonyította [8].

Weyl könyve csak a nullkarakterisztikájú esettel foglalkozik. C. De Concini és C. Procesi 1976-ban megjelent [1] cikkükben kiterjesztették az eredményeket más testekre is. Az ortogonális és a speciális ortogonális csoport esetében a kiterjesztés csak 2-től különböző karakterisztikájú testek esetén működött. David R. Richman 1989-es [7] cikkében 2 karakterisztikájú végtelen test felett is leírta az „ortogonális csoport” vektorinvariánsait abban az esetben, ha a csoportot az $A^T A = I$ egyenlettel definiáljuk. De a 2 karakterisztikájú esetben nem ezt szokás ortogonális csoportnak nevezni. Domokos Mátyás, S. G. Kuzmin és A. N. Zubkov megjelenés alatt álló [2] cikkükben – egy másik invariánselméleti probléma vizsgálatának melléktermékeként – rámutattak, hogy ha a (speciális) ortogonális csoportot egy 2 karakterisztikájú, algebrailag zárt test felett a szokásos módon, egy nem-elfajuló kvadratikus alak invarianciájával definiáljuk, akkor az invariáns polinomok az eddig említett esetektől gyökeresen elütő módon viselkednek (legalábbis a cikkben vizsgált $SO(4)$ csoport esetén).

Ebben a dolgozatban a 2 karakterisztikájú esetre koncentrálva vizsgáljuk az ortogonális csoport vektorinvariánsait. Az első fejezetben magát a csoportot definiáljuk, és bebizonyítjuk néhány fontos tulajdonságát. A második fejezetben definiáljuk az invariánsokat, és olyan tételeket bizonyítunk, amelyek az invariáns polinomok algebrájának szerkezetéről adnak információt. A hangsúly itt azokon az ellenpéldákon van, amelyek a 2 karakterisztikájú esetet az összes többitől eltérővé teszik. A 3.1 alfejezetben definiáljuk és jellemezzük a nullkúpot, és ebből további következtetést vonunk le az invariáns polinomok algebrájára vonatkozólag. A harmadik fejezet további részében a klasszikus algebrai geometria néhány egyszerű eszközét bevetve leírjuk az invariáns racionális kifejezések testét, és a dimenzióhoz képest kevés számú vektorváltozó esetén az invariáns polinomok algebráját is. A harmadik fejezet eredményei olyan jellegűek, mint a 2-től különböző karakterisztika esetén megszokottak.

A diplomamunkában saját eredmények a 2.2, 2.3, 2.6, 3.3 és 3.4 alfejezetek eredményei. A többi állításnál vagy kiderül a szövegből, hogy kitől származik, vagy olyan ismert tényről van szó, amelyről nehéz volna megállapítani, hogy ki bizonyította először.

Köszönöm témavezetőmnek, Domokos Mátyásnak az érdekes témát és a diplomamunka írása során nyújtott rengeteg segítséget.

1. Az ortogonális csoport

Az $O(n)$ ortogonális csoportot a valós test fölött az $A^TA = I$ egyenlettel definiáljuk. Ez – tetszőleges k test felett tekintve is – azt fejezi ki, hogy A, mint a k^n tér lineáris transzformációja, invariánsan hagyja a „standard" nem-elfajuló bilineáris függvényt (skalárszorzatot). Ha char $k \neq 2$, akkor ez egyenértékű azzal, hogy A invariánsan hagyja a „standard" kvadratikus alakot (a koordináták négyzetösszegét). Ha viszont char $k = 2$, akkor A-nak ez a két tulajdonsága már nem egyenértékű. Továbbá a koordináták négyzetösszege teljes négyzetté alakítható és emiatt – az alábbi 1.1.3 definíció értelmében – elfajuló, ezért nem a négyzetösszeget fogjuk standard kvadratikus alaknak nevezni.

Az alábbiakban egy tetszőlegesen rögzített nem-elfajuló kvadratikus alak invarianciájával definiáljuk az ortogonális csoportot, és tisztázzuk néhány alaptulajdonságát. Az 1.2 és 1.3 alfejezetekben többé-kevésbé Donald E. Taylor [9] könyvét követjük.

Ha nem mondunk mást, akkor egy 2 karakterisztikájú k alaptest felett dolgozunk; V mindig egy k feletti n dimenziós vektorteret jelöl. A második és harmadik fejezetben, az invariánselméleti vizsgálódások során mindig feltesszük majd, hogy k végtelen, sőt a harmadik fejezetben azt is, hogy algebrailag zárt. Most még nincs szükségünk ilyen feltevésre.

1.1. Kvadratikus alakok

1.1.1. Állítás. *Ebben az állításban a k alaptest tetszőleges lehet.*

A $q : V \to k$ függvényre vonatkozó alábbi feltételek ekvivalensek:

(i) Van olyan $\{\cdot,\cdot\}$ bilineáris függvény V-n, amelynek q a diagonalizáltja: $q(v) = \{v, v\}$ minden $v \in V$ esetén.

(ii) A q függvény a koordináták homogén másodfokú polinomjaként írható fel tetszőleges V-n felvett lineáris koordinátarendszer esetén.

(iii) A q függvény a koordináták homogén másodfokú polinomjaként írható fel egy alkalmas V-n felvett lineáris koordinátarendszer esetén.

A közismert (és nagyon egyszerű) bizonyítást nem részletezzük. Ha az állításban szereplő ekvivalens feltételek teljesülnek, akkor q-t kvadratikus alaknak nevezzük.

1.1.2. Állítás. *A k alaptest most is tetszőleges lehet. Legyen $q : V \to k$ egy kvadratikus alak. Ekkor*

$$\beta(v, w) = q(v + w) - q(v) - q(w) \tag{1}$$

egy β szimmetrikus bilineáris függvényt definiál V-n. (Ezt q polarizáltjának nevezzük.)

Ha char $k = 2$, *akkor β nem csak szimmetrikus, hanem alternáló: $\beta(v, v) = 0$ minden $v \in V$ vektorra.*

Bizonyítás. Legyen q a $\{\cdot,\cdot\}$ bilineáris függvény diagonalizáltja. Ekkor

$$\beta(v, w) = \{v + w, v + w\} - \{v, v\} - \{w, w\} = \{v, w\} + \{w, v\},$$

amiből az állítás nyilvánvalóan következik. □

A továbbiakban β mindig az éppen szóban forgó q kvadratikus alak polarizáltját fogja jelölni.

1.1.3. Definíció. *A k alaptest most is tetszőleges lehet. A $q : V \to k$ kvadratikus alakot nem-elfajulónak mondjuk, ha abból, hogy $q(v) = 0$ és minden w-re $\beta(v, w) = 0$, következik, hogy $v = 0$. Ekkor a (V, q) párt ortogonális geometriának nevezzük.*

Ha char $k \neq 2$, akkor q pontosan akkor elfajuló, ha β az. Ha viszont char $k = 2$, akkor előfordulhat, hogy β elfajuló, de q nem.

1.1.4. Állítás. *Tegyük fel, hogy a 2 karakterisztikájú k test algebrailag zárt. Legyen q egy kvadratikus alak V-n. Ekkor léteznek $\varrho, \sigma \geq 0$ egészek úgy, hogy $2\varrho + \sigma = n = \dim V$, és egy $(x_1, \ldots, x_\varrho, y_1, \ldots, y_\varrho, z_1, \ldots, z_\sigma)$ lineáris koordinátarendszer, amellyel*

$$q = \sum_{i=1}^{\varrho} x_i y_i \quad \text{vagy} \quad q = \sum_{i=1}^{\varrho} x_i y_i + z_1^2.$$

Bizonyítás. Mivel β alternáló, ezért van olyan $(X_1, \ldots, X_\varrho, Y_1, \ldots, Y_\varrho, Z_1, \ldots, Z_\sigma)$ koordinátarendszer, amellyel

$$\beta\left(v^{(1)}, v^{(2)}\right) = \sum_{i=1}^{\varrho} \left(X_i^{(1)} Y_i^{(2)} + Y_i^{(1)} X_i^{(2)}\right).$$

(Itt és minden hasonló esetben $X_i^{(1)}$ a $v^{(1)}$ vektor X_i koordinátáját jelenti stb.)

Egy ilyen koordinátarendszerben

$$q = \sum_{i=1}^{\varrho} \left(a_i X_i^2 + X_i Y_i + b_i Y_i^2\right) + \sum_{j=1}^{\sigma} c_j Z_j^2$$

alkalmas a_i, b_i, c_j skalárokkal. Mivel k algebrailag zárt, így vannak olyan $x_i, y_i \in kX_i + kY_i$ lineáris funkcionálok, amelyekkel $a_i X_i^2 + X_i Y_i + b_i Y_i^2 = x_i y_i$. Mivel char $k = 2$, ezért x_i és y_i lineárisan függetlenek. Ha minden c_j nulla, akkor $(x_1, y_1, \ldots, x_\varrho, y_\varrho)$-t egészítsük ki V^* bázisává tetszőleges módon. Ha nem minden c_j nulla, akkor legyen $z_1 = \sum_{j=1}^{\sigma} \sqrt{c_j} Z_j$, és $(x_1, y_1, \ldots, x_\varrho, y_\varrho, z_1)$-et egészítsük ki V^* bázisává tetszőleges módon. Az így kapott koordinátarendszer megfelelő lesz. $\square$

1.1.5. Megjegyzés. *A q kvadratikus alak egyértelműen meghatározza az*

$$\{x_1 = \cdots = x_\varrho = y_1 = \cdots = y_\varrho = 0\}$$

alteret (és így ϱ-t és σ-t is). Valóban, a fenti altér éppen

$$\ker \beta \stackrel{\text{def}}{=} \{v \in V : \beta(v, w) = 0 \textit{ minden } w \in V \textit{ vektorra}\}.$$

Továbbá, q azt is meghatározza, hogy szerepel-e a z_1^2 tag (pontosan akkor szerepel, ha q nem tűnik el azonosan $\ker \beta$*-n).*

Könnyen látható, hogy a fenti 1.1.4 állításban szereplő alakú q pontosan akkor nem-elfajuló, ha vagy $n = 2\varrho$, vagy $n = 2\varrho + 1$ és q-ban szerepel a z_1^2 tag.

1.2. Az ortogonális csoport

Legyen V az oszlopvektorok k^n tere. Itt a koordinátákat $x_1, \dots, x_\nu, y_1, \dots, y_\nu$ fogja jelölni, ha $n = 2\nu$ páros, és $x_1, \dots, x_\nu, y_1, \dots, y_\nu, z$ fogja jelölni, ha $n = 2\nu + 1$ páratlan.

A teret ellátjuk a

$$q = \sum_{i=1}^{\nu} x_i y_i, \qquad \text{illetve} \qquad q = \sum_{i=1}^{\nu} x_i y_i + z^2 \tag{2}$$

standard nem-elfajuló kvadratikus alakkal. (Ez a k feletti n dimenziós standard ortogonális geometria; algebrailag zárt k felett izometrikus izomorfizmustól eltekintve csak ez van.) A q kvadratikus alak polarizáltja mindkét esetben

$$\beta\left(v^{(1)}, v^{(2)}\right) = \sum_{i=1}^{\nu} \left(x_i^{(1)} y_i^{(2)} + y_i^{(1)} x_i^{(2)}\right).$$

A β alternáló bilineáris függvény mátrixa

$$J = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix}, \qquad \text{illetve} \qquad J \oplus 0 = \begin{pmatrix} 0 & I & \\ I & 0 & \\ & & 0 \end{pmatrix},$$

ahol I a $\nu \times \nu$ méretű egységmátrix. A páros dimenziós esetben β-t standard szimplektikus formának nevezzük.

Az alábbiakban $\mathfrak{gl}(V)$ jelöli a $V \to V$ lineáris transzformációk (asszociatív) algebráját. Ha $V = k^n$, akkor $\mathfrak{gl}(n)$-et írunk.

1.2.1. Definíció. *Ebben a definícióban a k alaptest tetszőleges lehet.*

Legyen (V, q) egy ortogonális geometria. Az $A \in \mathfrak{gl}(V)$ transzformáció ortogonális, ha invariánsan hagyja q-t:

$$O(V) = O(V, q) = \{A \in \mathfrak{gl}(V) : q(Av) = q(v) \text{ minden } v \in V \text{ vektorra}\}.$$

A 2 karakterisztikájú, standard esetben az $O(n)$ jelölést használjuk.

1.2.2. Definíció. *A k alaptest most is tetszőleges lehet.*

Legyen (V, β) egy szimplektikus geometria, azaz egy nem-elfajuló, alternáló bilineáris függvénnyel ellátott vektortér. Az $A \in \mathfrak{gl}(V)$ transzformáció szimplektikus, ha invariánsan hagyja β-t:

$$Sp(V) = Sp(V, \beta) = \{A \in \mathfrak{gl}(V) : \beta(Av, Aw) = \beta(v, w) \text{ minden } v, w \in V \text{ vektorpárra}\}.$$

A 2 karakterisztikájú, standard esetben az $Sp(2\nu)$ jelölést használjuk:

$$Sp(2\nu) = \{A \in \mathfrak{gl}(2\nu) : \beta(Av, Aw) = \beta(v, w) \text{ minden } v, w \in k^n \text{ vektorpárra}\} = \\ = \left\{A \in \mathfrak{gl}(2\nu) : A^T J A = J\right\}.$$

1.2.3. Állítás. *A 2 karakterisztikájú, standard esetben $O(2\nu) \leq Sp(2\nu) \leq SL(2\nu)$. Páratlan n-re is $O(n) \leq SL(n)$.*

Ez valójában a nem-standard esetben is igaz.

Bizonyítás. Ha $A \in O(2\nu)$, akkor A invariánsan hagyja q-t, ezért β-t is, vagyis $A \in Sp(2\nu)$. Ha $A \in Sp(2\nu)$, akkor $A^T J A = J$, ahonnan $(\det A)^2 = 1$, azaz $\det A = 1$.

Ha $A \in O(2\nu + 1)$, akkor A invariánsan hagyja q-t, ezért β-t is. Tehát $\ker \beta$, azaz a z-tengely A-invariáns. A z-tengelyen q injektív, ezért a z-tengely minden vektora fix. Vagyis A utolsó oszlopa $(0, \dots, 0, 1)^T$. A $V/\ker \beta = k^{2\nu}$ faktortéren A szimplektikusan hat, tehát A bal felső sarka $\in Sp(2\nu)$. Ebből az állítás következik. $\square$

1.2.4. Állítás. *Tegyük fel, hogy a k 2 karakterisztikájú test tökéletes, azaz k minden elemének van négyzetgyöke k-ban. Ha $A \in O(2\nu + 1)$, akkor jelölje $\bar{A} \in Sp(2\nu)$ az A által a $k^{2\nu+1}/\ker \beta = k^{2\nu}$ faktortéren indukált szimplektikus transzformációt. Ekkor $\phi : O(2\nu + 1) \to Sp(2\nu)$, $A \mapsto \bar{A}$ csoportizomorfizmus.*

Bizonyítás. Nyilvánvaló, hogy ϕ homomorfizmus.

Legyen
$$S = \{v \in k^{2\nu+1} : q(v) = 0\}.$$
Mivel $\ker \beta$ a z-tengely és k tökéletes, ezért q minden $\ker \beta$ szerinti mellékosztályt bijektíven képez k-ra. Így a
$$v \mapsto \bar{v} = v + \ker \beta$$
természetes leképezés S-re való megszorítása egy $\pi : S \to k^{2\nu}$ bijekció. Ha $A \in O(2\nu + 1)$ és $\bar{A} = I$, akkor A identikusan hat S-en és $\ker \beta$-n, tehát $A = I$. Ezzel beláttuk, hogy ϕ injektív.

A szürjektivitás bizonyításához legyen $\tilde{A} \in Sp(2\nu)$ tetszőleges. Ha $v \in S$ és $w \in \ker \beta$, akkor legyen
$$A(v + w) = \pi^{-1}\left(\tilde{A}\pi(v)\right) + w.$$
Világos, hogy $A(au) = aA(u)$ minden $u \in k^{2\nu+1}$ és $a \in k$ esetén. Továbbá $q(Au) = q(u)$, hiszen
$$q(v + w) = q(v) + \beta(v, w) + q(w) = q(w),$$
ha $v \in S$ és $w \in \ker \beta$. Az A leképezés linearitásának igazolásához még azt kell ellenőrizni, hogy $v^{(1)}, v^{(2)} \in S$ esetén
$$A\left(v^{(1)} + v^{(2)}\right) = Av^{(1)} + Av^{(2)}.$$
Az világos, hogy
$$A\left(v^{(1)} + v^{(2)}\right) = Av^{(1)} + Av^{(2)} + w$$
alkalmas ($v^{(1)}$-től és $v^{(2)}$-től függő) $w \in \ker \beta$-val. Mindkét oldalra q-t alkalmazva azt kapjuk, hogy
$$\beta\left(v^{(1)}, v^{(2)}\right) = \beta\left(Av^{(1)}, Av^{(2)}\right) + q(w).$$
Másrészt
$$\beta\left(Av^{(1)}, Av^{(2)}\right) = \beta\left(\pi^{-1}\left(\tilde{A}\pi\left(v^{(1)}\right)\right), \pi^{-1}\left(\tilde{A}\pi\left(v^{(2)}\right)\right)\right) = \beta\left(v^{(1)}, v^{(2)}\right).$$

Ezért $q(w) = 0$, ahonnan $w = 0$. Ezzel beláttuk, hogy A lineáris, tehát $A \in O(2\nu + 1)$. Világos, hogy $\bar{A} = \tilde{A}$. $\square$

1.2.5. Megjegyzés. *Ez a konstrukció valójában a nem-standard esetben is működik; a bizonyítás szinte szó szerint átvihető. Lényeges viszont az a feltétel, hogy k tökéletes.*

1.2.6. Megjegyzés. *A fenti ϕ csoportizomorfizmus reguláris leképezés (algebro-geometriai értelemben), de ϕ^{-1} nem az (feltéve, hogy $\nu \geq 1$ és k végtelen).*

1.3. Tükrözések

1.3.1. Definíció. *Ebben a definícióban (V, q) tetszőleges k test feletti ortogonális geometria lehet.*

Tetszőleges $v \in V$ esetén legyen $v^\perp = \{w \in V : \beta(v, w) = 0\}$. Tetszőleges $H \subseteq V$ esetén legyen $H^\perp = \bigcap_{v \in H} v^\perp$.

A $v \in V$, $v \neq 0$ vektor szinguláris, ha $q(v) = 0$. Egy altér totálisan szinguláris, ha minden vektora szinguláris (vagy nulla). Egy egydimenziós altér szinguláris, ha totálisan szinguláris.

Ha $q(v) \neq 0$, akkor a

$$T_v w = w - \frac{\beta(w, v)}{q(v)} v$$

képlettel definiált T_v transzformációt a v által meghatározott tükrözésnek nevezzük. Könnyen ellenőrizhető, hogy T_v valójában csak a kv egydimenziós altértől függ, ortogonális, fixpontjainak halmaza $v^\perp$, és $T_v^2 = I$. Nyilvánvaló, hogy $T_v = I$ akkor és csak akkor áll fenn, ha $v \in \ker \beta$.

Az alábbiakban célunk annak bizonyítása, hogy $O(n)$-et generálják a tükrözések. Először a páratlan dimenziós esetet intézzük el, az 1.2.4 állításban szereplő ϕ csoportizomorfizmus segítségével. Ehhez feltesszük, hogy k tökéletes.

Ha $x \in V = k^{2\nu+1}$, akkor legyen $\bar{x}$ az x képe $\bar{V} = V/\ker \beta = k^{2\nu}$-ben. A T_v tükrözésnek a

$$\bar{T}_v : \bar{w} \mapsto \bar{w} - \frac{1}{q(v)} \beta(\bar{w}, \bar{v}) \bar{v}$$

$Sp(2\nu)$-beli transzformáció felel meg. Rögzített $\bar{v}$ mellett az itt szereplő $\frac{1}{q(v)}$ tetszőleges nullától különböző skalár lehet. Ezért elegendő a következő állítást igazolni:

1.3.2. Állítás. *Az*

$$F_{v,a} : k^{2\nu} \to k^{2\nu}, \quad w \mapsto w + a\beta(w, v)v \qquad \left(v \in k^{2\nu}, a \in k\right)$$

szimplektikus transzformációk (az úgynevezett szimplektikus transzvekciók) generálják az $Sp(2\nu)$ csoportot. Sőt, $Sp(2\nu)$ minden eleme előáll 4ν szimplektikus transzvekció szorzataként.

Bizonyítás. Az identikus leképezés is transzvekció, ezért elég azt belátni, hogy $Sp(2\nu)$ minden eleme előáll *legfeljebb* 4ν ilyen szorzataként. Legyen $\mathcal{F}$ a szimplektikus transzvekciók halmaza. Először azt mutatjuk meg, hogy bármely nullától különböző vektor átvihető bármelyik másikba legfeljebb két szimplektikus transzvekció egymásutánjával. Ha $u_1, u_2 \neq 0$ és $\beta(u_1, u_2) \neq 0$, akkor a

$$v = u_1 - u_2, \qquad a = \frac{1}{\beta(u_1, u_2)}$$

választással $F_{v,a} u_1 = u_2$. Ha viszont $\beta(u_1, u_2) = 0$, akkor válasszunk egy olyan w-t, amellyel $\beta(u_1, w) \neq 0$ és $\beta(u_2, w) \neq 0$ (van ilyen w, hiszen csak két valódi alteret zárunk ki). Ekkor $w \in \mathcal{F} u_1$ és $u_2 \in \mathcal{F} w$, tehát $u_2 \in \mathcal{F}\mathcal{F} u_1$.

Most megmutatjuk, hogy bármely, a $\beta(u, v) = 1$ egyenletet kielégítő rendezett vektorpár (úgynevezett hiperbolikus pár) átvihető bármely másikba legfeljebb négy szimplektikus transzvekció egymásutánjával. Evégett legyenek (u_1, v_1) és (u_2, v_2) hiperbolikus párok. Az előzőek miatt feltehetjük, hogy $u_1 = u_2 = u$, de ekkor legfeljebb két transzvekcióval kell boldogulnunk. Ha $\beta(v_1, v_2) \neq 0$, akkor a

$$v = v_1 - v_2, \qquad a = \frac{1}{\beta(v_1, v_2)}$$

választással $F_{v,a} u = u$ és $F_{v,a} v_1 = v_2$, készen vagyunk. Ha viszont $\beta(v_1, v_2) = 0$, akkor $(u, u + v_1)$ olyan hiperbolikus pár, amelyre már $\beta(u, u + v_1) = \beta(v_2, u + v_1) = 1$, ezért (u, v_1) és (u, v_2) bármelyikébe átvihető szimplektikus transzvekcióval.

Ezután az állítást ν szerinti teljes indukcióval bizonyítjuk. A $\nu = 0$ esetben nincs mit bizonyítani. Tegyük fel, hogy az állítás igaz $(\nu - 1)$-re. Legyen $A \in Sp(2\nu)$ teszőleges. Legyen u, illetve v az x_ν illetve y_ν irányú standard bázisvektor. Az (u, v) pár hiperbolikus. Van olyan T, amely legfeljebb négy szimplektikus transzvekció szorzata és amellyel $TAu = u$, $\;TAv = v$. Tehát TA identikus az $L = ku \oplus kv$ altéren, és invariánsan hagyja az $L^\perp = k^{2(\nu-1)}$ alteret. Az indukciós feltevés szerint

$$(TA)\,|_{L^\perp} = T'_1 \cdots T'_{4(\nu-1)}\ ,$$

ahol mindegyik $T'_i \in Sp(2(\nu-1))$ szimplektikus transzvekció. Legyen $T_i = T'_i \oplus I \in Sp(2\nu)$. Ekkor T_i szimplektikus transzvekció, és $A = T^{-1} T_1 \cdots T_{4(\nu-1)}$. □

1.3.3. Következmény. *Ha k tökéletes, akkor a tükrözések generálják $O(2\nu+1)$-et. Sőt, $O(2\nu+1)$ minden eleme előáll 4ν tükrözés szorzataként.*

Rátérünk a páros dimenziós esetre. Az ortogonális geometriát definiáló q kvadratikus alak polarizáltja, β itt nem-elfajuló, ezért az identitás nem tükrözés (szemben a páratlan dimenziós esettel). Ki fog derülni, hogy nem is áll elő páratlan számú tükrözés szorzataként (ld. az 1.3.7 következményt).

Az alfejezet hátralevő részében foglaltak a következő általánosabb feltételek mellett is érvényesek: k teszőleges test, V a k feletti véges dimenziós vektortér, és q olyan kvadratikus alak V-n, melynek β polarizáltja nem-elfajuló.

Az általánosabb szituációban is $O(V)$ jelöli a q-t megtartó transzformációk csoportját.

1.3.4. Lemma. *Ha $A \in O(V)$ és r pozitív egész, akkor*

$$\ker(I-A)^r = (\operatorname{im}(I-A)^r)^{\perp}.$$

Bizonyítás. Tetszőleges u, v vektorokra $\beta((I-A)u, v) = \beta(Au, (A-I)v)$. Ebből indukcióval

$$\beta\left((I-A)^r u, v\right) = \beta\left(A^r u, (A-I)^r v\right).$$

Ha tehát $v \in \ker(I-A)^r$, akkor $\beta\left((I-A)^r u, v\right)$ is nulla. Ezzel beláttuk, hogy

$$\ker(I-A)^r \leq (\operatorname{im}(I-A)^r)^{\perp}.$$

E két altér azonos dimenziójú, tehát megegyeznek. □

1.3.5. Állítás. *Ha $A \in O(V)$ fixponthalmaza 1 kodimenziós altér, akkor A tükrözés.*

Bizonyítás. Az $\operatorname{im}(I-A)$ képtér egydimenziós, legyen egy nullától különböző vektora v. Ekkor

$$Aw = w + \lambda(w)v$$

egy λ lineáris funkcionállal. Mivel β nem-elfajuló, így

$$Aw = w + \beta(w, u)v$$

egy rögzített $u \neq 0$ vektorral. Ebből $\ker(I-A) = u^{\perp}$, a lemma $r = 1$ esetéből $u = av$ alkalmas $a \neq 0$ skalárral. Tehát

$$Aw = w + a\beta(w, v)v.$$

Mivel A ortogonális, minden w-re

$$q(w) = q(w) + a\beta(w, v)^2 + a^2\beta(w, v)^2 q(v),$$

ahonnan $a = -\frac{1}{q(v)}$, $A = T_v$. □

A továbbiakban az A lineáris leképezés rangját $\operatorname{rk} A$ fogja jelölni.

1.3.6. Állítás. *Legyen $0 \neq v \in V$ nem-szinguláris és $A \in O(V)$ tetszőleges.*

(i) Ha $v \in \operatorname{im}(I-A)$, $\quad v = (I-A)u$, akkor

$$\operatorname{im}(I - T_v A) = \operatorname{im}(I-A) \cap u^{\perp}.$$

(ii) Ha $v \notin \operatorname{im}(I-A)$, akkor

$$\operatorname{im}(I - T_v A) = \operatorname{im}(I-A) \oplus kv.$$

Bizonyítás. (i) Könnyen látható, hogy $q(v) = \beta(u, v)$. Ezért $T_v u = u - v = Au$. Így $u \in \ker(I - T_v A)$, ahonnan az 1.3.4 lemma alapján $\mathrm{im}(I - T_v A) \leq u^\perp$.

Vegyük észre, hogy

$$I - T_v A = (I - T_v)A + (I - A).$$

Emiatt egyrészt

$$\mathrm{im}(I - T_v A) \leq \mathrm{im}(I - A),$$

hiszen $\mathrm{im}(I - T_v) = kv \leq \mathrm{im}(I - A)$, másrészt viszont

$$\mathrm{rk}(I - T_v A) \geq \mathrm{rk}(I - A) \ - 1.$$

Tehát

$$\mathrm{im}(I - T_v A) \leq \mathrm{im}(I - A) \cap u^\perp,$$

és a két oldal azonos dimenziójú, hiszen $u \notin \ker(I - A)$ miatt $u^\perp \not\geq \mathrm{im}(I - A)$.

(ii) Vegyük észre, hogy $w \in \ker(I - T_v A)$ pontosan akkor, ha $T_v w = Aw$, azaz, ha

$$(I - A)w = \frac{\beta(w, v)}{q(v)} v.$$

A $v \notin \mathrm{im}(I - A)$ esetben ez azzal ekvivalens, hogy $w \in \ker(I - A) \cap v^\perp$. Tehát

$$\ker(I - T_v A) = \ker(I - A) \cap v^\perp.$$

Ebből az 1.3.4 lemma alapján következik az állítás. □

1.3.7. Következmény. *(i) Legyen $T \in O(V)$ tükrözés és $A \in O(V)$ teszőleges. Ekkor*

$$\mathrm{rk}(I - TA) = \mathrm{rk}(I - A) \ \pm 1.$$

(ii) Ha $A \in O(V)$ előáll r tükrözés szorzataként, akkor $\mathrm{rk}(I - A) \equiv r \mod 2$.

Tehát I nem áll elő páratlan sok tükrözés szorzataként.

1.3.8. Tétel. *Ha k algebrailag zárt, akkor a tükrözések generálják $O(V)$-t. Sőt, $O(V)$ minden eleme előáll legfeljebb $2n - 1$ tükrözés szorzataként.*

Az algebrai zártság helyett valójában elég feltenni, hogy k nem a kételemű test. Sőt a kételemű test felett is igaz az állítás „majdnem minden” ortogonális geometriára. Az általános bizonyítás – mely ráadásul $(2n - 1)$-nél lényegesen jobb becslést (a kételeműtől különböző test esetén n-et) ad, viszont az alábbi bizonyításnál jóval hosszadalmasabb – megtalálható a [9] könyvben.

Bizonyítás. Legyen $e^{(1)}, \ldots, e^{(n)}$ olyan bázis, mely nem-szinguláris vektorokból áll, s amelyre $L = \left\langle e^{(1)}, \ldots, e^{(n-1)} \right\rangle^{\perp}$ sem szinguláris. Ilyen van: ha char $k \neq 2$, akkor bármely β-ortogonális bázis megfelel; ha pedig char $k = 2$, akkor legyen a és b két egymástól és nullától különböző skalár, és az 1.1.4 állítás által biztosított $(x_1, \ldots, x_\nu, y_1, \ldots, y_\nu)$ koordinátarendszerben legyenek $e^{(2i-1)}$ koordinátái

$$x_i = a, \quad y_i = b, \qquad x_j = y_j = 0 \quad (j \neq i),$$

$e^{(2i)}$ koordinátái pedig

$$x_i = b, \quad y_i = a, \qquad x_j = y_j = 0 \quad (j \neq i).$$

Elég belátni, hogy ha $A \in O(V)$, és r a legkisebb index, amelyre $Ae^{(r)} \neq e^{(r)}$, akkor van olyan T, amely legfeljebb két tükrözés szorzata, sőt $r = n$ esetén tükrözés, és amellyel TA-ra már $TAe^{(i)} = e^{(i)}$ minden $i \leq r$-re (ami persze azzal ekvivalens, hogy $Te^{(i)} = e^{(i)}$ minden $i < r$-re, és $TAe^{(r)} = e^{(r)}$).

Legyen $c = q\left(e^{(r)}\right) = q\left(Ae^{(r)}\right)$ és $W = \left\langle e^{(1)}, \ldots, e^{(r-1)} \right\rangle^{\perp}$. Ekkor $0 \neq e^{(r)} - Ae^{(r)} \in W$, hiszen A invariánsan hagyja β-t.

Az $r = n$ esetben a $0 \neq e^{(r)} - Ae^{(r)} \in W = L$ vektor nem szinguláris, így $T = T_{e^{(r)} - Ae^{(r)}}$ megfelelő. Tegyük fel, hogy $r < n$. Jelölje $\tilde{W}$ az $e^{(r)} + W = Ae^{(r)} + W$ affin teret. Elég olyan $u \in \tilde{W}$ vektort találni, melyre $q(u) = c$, továbbá $q\left(u - e^{(r)}\right)$ és $q\left(u - Ae^{(r)}\right)$ egyike sem nulla. Ekkor ugyanis $T = T_{u-e^{(r)}} T_{u-Ae^{(r)}}$ megfelelő lesz.

Azt állítjuk, hogy a $\tilde{W}$ affin térben a

$$Q = \left\{ u \in \tilde{W} : q(u) = c \right\}$$

másodrendű algebrai hiperfelület irreducibilis, és az

$$S_1 = \left\{ u \in \tilde{W} : q\left(u - e^{(r)}\right) = 0 \right\}, \quad S_2 = \left\{ u \in \tilde{W} : q\left(u - Ae^{(r)}\right) = 0 \right\}$$

hiperfelületek egyike sem fedi le, így együtt sem fedik le, ami a fenti tulajdonságú u létezését bizonyítja.

Mivel Q másodrendű hiperfelület, így irreducibilitásának igazolásához elég megmutatni, hogy nem áll elő két ($\tilde{W}$-beli) hipersík uniójaként. Azt állítjuk, hogy nincs olyan 1 kodimenziós $H < W$ altér, melyre

$$e^{(r)} \in \tilde{H} \stackrel{\text{def}}{=} e^{(r)} + H \subseteq Q$$

állna. Tegyük fel indirekt módon, hogy H ilyen. Ekkor $H \leq \left\langle e^{(r)} \right\rangle^{\perp} \cap W$, ahol a dimenziók egyezése miatt egyenlőség áll. Továbbá H totálisan szinguláris. Ez lehetetlen, mert $H \geq L$.

Az S_1 felület nem fedi le Q-t. Valóban, legyen $w \in W$ úgy, hogy $\beta\left(e^{(r)}, w\right) \neq 0$ és $q(w) \neq 0$. (Van ilyen, hiszen W-ből csak két algebrai felületet zártunk ki.) Ekkor $T_w e^{(r)} \in Q \backslash S_1$.

Ugyanígy látható be, hogy $S_2 \not\supseteq Q$. $\square$

A standard $V = k^{2\nu}$, $q = \sum_{i=1}^{\nu} x_i y_i$ esetben a tételből könnyen adódik az

1.3.9. Következmény. *Ha k algebrailag zárt, akkor $O(2\nu)$-t generálják az*

$$\hat{A} = \begin{pmatrix} A & \\ & A^{-T} \end{pmatrix} \qquad (A \in GL(\nu))$$

alakú elemei és az $x_1 \leftrightarrow y_1$ tükrözés. (Itt A^{-T} az A mátrix inverzének transzponáltját jelöli.)

Az algebrai zártság helyett valójában elég feltenni, hogy k minden elemének van négyzetgyöke k-ban.

Bizonyítás. Vegyük észre, hogy ha $v \in k^{2\nu}$, éspedig $v = \begin{pmatrix} x \\ y \end{pmatrix}$, ahol $x, y \in k^{\nu}$, akkor $q(v) = \langle x, y \rangle$, ahol $\langle \cdot, \cdot \rangle$ a standard skalárszorzat a k^{ν} téren. Ezért $\hat{A}$ valóban ortogonális:

$$q\left(\hat{A}v\right) = \left\langle Ax, A^{-T}y \right\rangle = \langle x, y \rangle = q(v).$$

Az $x_1 \leftrightarrow y_1$ involúció valóban tükrözés, mégpedig az

$$x_1 = y_1 = 1, \qquad x_i = y_i = 0 \quad (i \neq 1)$$

koordinátájú vektor által meghatározott tükrözés. Azt állítjuk, hogy tetszőleges T_v tükrözés megkapható ebből úgy, hogy egy alkalmas $\hat{A}$-pal konjugáljuk. (Ha ezt belátjuk, akkor az előző tétel miatt készen vagyunk.) A v vektort alkalmas skalárszorosával helyettesítve feltehetjük, hogy $q(v) = 1$ (itt kihasználjuk, hogy k minden elemének van négyzetgyöke k-ban). Állításunk azzal ekvivalens, hogy ha W egy ν dimenziós vektortér és $x \in W$, $y \in W^*$ úgy, hogy $yx = 1$, akkor van olyan bázis W-ben, melynek első vektora x, a duális bázis első vektora pedig y. Ez viszont nyilvánvaló: x-hez vegyük hozzá a $\ker y$ 1 kodimenziós altér egy tetszőleges bázisát. □

1.3.10. Definíció. *Az A ortogonális transzformációt speciálisnak nevezzük, ha páros sok tükrözés szorzata. Az ilyenek csoportját $SO(V) = SO(V, q)$, illetve $SO(n)$ jelöli.*

Ezt a definíciót tetszőleges k test feletti ortogonális geometria esetén alkalmazhatjuk. Ha $\operatorname{char} k \neq 2$, akkor visszakapjuk a megszokott $SO(V) = O(V) \cap SL(V)$ definíciót. Ha viszont $\operatorname{char} k = 2$, akkor – mint láttuk – $O(V) \leq SL(V)$.

Legyen k 2 karakterisztikájú. Ha k tökéletes, akkor $SO(2\nu + 1) = O(2\nu + 1)$ adódik az 1.3.3 következményből, mert I is tükrözés. Másrészt $|O(2\nu) : SO(2\nu)| = 2$ adódik az 1.3.8 tételből és abból, hogy I nem áll elő páratlan számú tükrözés szorzataként.

1.4. Algebro-geometriai megjegyzések

Ebben az alfejezetben feltesszük, hogy a 2 karakterisztikájú k alaptest algebrailag zárt. Az állítások 2-től különböző karakterisztika esetén is igazak, a bizonyítások triviális módosításokkal átvihetők.

A topológiai kifejezéseket a Zariski-féle értelemben használjuk.

1.4.1. Állítás. *A k^n vektortéren értelmezett kvadratikus alakok vektorterében a nem-elfajuló kvadratikus alakok nyílt halmazt alkotnak.*

Bizonyítás. Legyen először n páros. Az a leképezés, mely minden kvadratikus alakhoz a polarizáltját rendeli, lineáris. Továbbá egy kvadratikus alak pontosan akkor nem-elfajuló, ha a polarizáltja nem-elfajuló. Ezért elég belátni, hogy az alternáló bilineáris függvények vektorterében a nem-elfajulók nyílt halmazt alkotnak. Ez nyilvánvaló, hiszen egy bilineáris függvény pontosan akkor elfajuló, ha mátrixának determinánsa nulla.

Legyen most $n = 2\nu + 1$ páratlan. Jelölje U a nem-elfajuló kvadratikus alakok halmazát. Az 1.1.4 állítás következtében a nem-elfajuló kvadratikus alakok egyformák: vagy mindegyikük belső pontja U-nak, vagy egyikük sem. Ezért elég belátni, hogy U tartalmaz egy nem-üres nyílt halmazt.

Legyen q egy kvadratikus alak. Legyen q polarizáltjának mátrixa

$$\beta = \begin{pmatrix} A & v \\ v^T & 0 \end{pmatrix},$$

ahol $A \in k^{2\nu\times 2\nu}$ persze alternáló. Tegyük fel, hogy $\det A \neq 0$. Ekkor a $\ker\beta$ altér egydimenziós, és egy nullától különböző vektora $\begin{pmatrix} A^{-1}v \\ 1 \end{pmatrix}$, ezért q pontosan akkor nem-elfajuló, ha $q\begin{pmatrix} A^{-1}v \\ 1 \end{pmatrix} \neq 0$. Ezzel beláttuk, hogy U tartalmazza a

$$\left\{ q :\ \det A \neq 0,\ q\begin{pmatrix} A^{-1}v \\ 1 \end{pmatrix} \neq 0 \right\}$$

halmazt. Ez nyílt, hiszen $\det A$ és $q\begin{pmatrix} A^{-1}v \\ 1 \end{pmatrix}$ egyaránt racionális függvényei q-nak; továbbá nem üres, hiszen tartalmazza a standard nem-elfajuló kvadratikus alakot. □

1.4.2. Állítás. *Az $O(n)$ ortogonális csoport algebrai (azaz algebrai egyenletekkel definiálható) részhalmaz a $\mathfrak{gl}(n)$ térben.*

Bizonyítás. Tekintsük a $\mathfrak{gl}(n)$ félcsoport természetes jobboldali hatását a kvadratikus alakok vektorterén: $q^A(v) = q(Av)$. A hatás polinomiális, ezért $O(n)$, mint a standard nem-elfajuló kvadratikus alak stabilizátora, algebrai részhalmaz. □

Könnyen látható, hogy ha a G mátrixcsoport algebrai részhalmaz a $\mathfrak{gl}(n)$ térben, akkor G-nek (mint affin algebrai halmaznak) az irreducibilis komponensei diszjunktak. Ezért mindegy, hogy irreducibilis komponensekről vagy összefüggő komponensekről beszélünk. A komponensek (mint algebrai varietások) izomorfak. Az egységelemet tartalmazó komponens (röviden egységkomponens) egy véges indexű normálosztó. A komponensek épp az egységkomponens szerinti mellékosztályok.

1.4.3. Állítás. *Az $O(n)$ csoport egységkomponense $SO(n)$.*

Bizonyítás. Legyen

$$U = \left\{ \left(v^{(1)}, \dots, v^{(2n-2)}\right) \in k^{n\times(2n-2)} : q\left(v^{(1)}\right) \cdots q\left(v^{(2n-2)}\right) \neq 0 \right\}.$$

Az U halmaz nyílt, ezért irreducibilis. Tekintsük a

$$\varphi : U \to O(n), \qquad \varphi\left(v^{(1)}, \dots, v^{(2n-2)}\right) = T_{v^{(1)}} \cdots T_{v^{(2n-2)}}$$

racionális leképezést. Az $SO(n) = \varphi(U)$ kép is irreducibilis, és tartalmazza az egységelemet. Ezért $SO(n)$ része az egységkomponensnek. Másrészt $SO(n)$ legfeljebb 2 indexű részcsoport $O(n)$-ben, így az egységkomponensben is, ezért sűrű az egységkomponensben (ellenkező esetben az $SO(n)$ lezárása és az $O(n)\backslash SO(n)$ lezárása külön-külön nem, de együtt lefedné az egységkomponenst, holott az irreducibilis). Mivel azonban $SO(n)$ az U affin nyílt halmaz racionális képe az (irreducibilis) egységkomponensben, ezért csak úgy lehet sűrű, ha tartalmazza az egységkomponens egy nem-üres nyílt részhalmazát. (Itt használjuk a később bizonyítandó 3.2.6 általános algebro-geometriai segédtételt. Ha ezt el akarjuk kerülni, hivatkozhatunk a szintén később bizonyítandó 2.1.4 megjegyzésre is, amely szerint $SO(2\nu)$ algebrai, továbbá arra, hogy $SO(2\nu+1) = O(2\nu+1)$.) Mivel $SO(n)$ részcsoport, meg kell egyeznie az egységkomponenssel. □

Az alábbi állításban felhasználjuk az affin algebrai halmazok dimenziójának fogalmát és a következő alapvető tényt: ha X és Y affin terek, és egy $X \to Y$ polinomiális leképezésnél Y egy nem-üres nyílt részhalmaza pontjainak azonos dimenziójú az őképe, akkor ez a közös dimenzió $\dim X - \dim Y$. (Egy ennél jóval általánosabb állítás: [4], 11.13 korollárium és az azt kiegészítő megjegyzés.)

1.4.4. Állítás. *Az $O(n)$ és $SO(n)$ csoportok dimenziója $\binom{n}{2}$.*

Bizonyítás. Elegendő $O(n)$-nel foglalkozni. Tekintsük ismét az $X = \mathfrak{gl}(n)$ félcsoport jobboldali hatását a kvadratikus alakok $\binom{n+1}{2}$ dimenziós Y terén. Az 1.1.4 állítás miatt a $GL(n) \subset \mathfrak{gl}(n)$ általános lineáris csoport hatása tranzitív a nem-elfajuló kvadratikus alakok nyílt halmazán. Az

$$X \to Y, \qquad A \mapsto q_0^A$$

leképezésre (ahol q_0 a standard nem-elfajuló kvadratikus alakot jelöli) alkalmazható a fent idézett állítás, hiszen bármely nem-elfajuló kvadratikus alak ősképe egy $O(n)$ szerinti jobboldali mellékosztály $GL(n)$-ben. Ezért az $O(n)$ stabilizátor dimenziója

$$\dim O(n) = \dim X - \dim Y = n^2 - \binom{n+1}{2} = \binom{n}{2}.$$

□

2. Invariánsok

Legyen k egyelőre tetszőleges végtelen test. Jelölje

$$R = R_{n\times m, p\times n} = k\left[v^{(1)}, \ldots, v^{(m)}, \xi_{(1)}, \ldots, \xi_{(p)}\right],$$

illetve

$$K = K_{n\times m, p\times n} = k\left(v^{(1)}, \ldots, v^{(m)}, \xi_{(1)}, \ldots, \xi_{(p)}\right)$$

a $v^{(1)}, \ldots, v^{(m)}$ n-dimenziós határozatlan vektorok (oszlopvektorok) és $\xi_{(1)}, \ldots, \xi_{(p)}$ n-dimenziós határozatlan kovektorok (sorvektorok) koordinátáitól, mint határozatlanoktól függő polinomok, illetve racionális kifejezések algebráját, illetve testét. (Ha csak $n \times m$ áll az indexben, akkor $p = 0$ értendő. Az alábbi 2.0.5 tételtől kezdve mindvégig erre az esetre fogunk szorítkozni.) Azt mondjuk, hogy az $f \in K$ racionális kifejezés invariáns a $G \le GL(n)$ csoporttal szemben, ha

$$f\left(Av^{(1)}, \ldots, Av^{(m)}, \xi_{(1)}A^{-1}, \ldots, \xi_{(p)}A^{-1}\right) = f\left(v^{(1)}, \ldots, v^{(m)}, \xi_{(1)}, \ldots, \xi_{(p)}\right)$$

teljesül minden $A \in G$ esetén. Az ilyen f racionális kifejezések testét jelölje K^G. Legyen $R^G = K^G \cap R$ a G-invariáns polinomok algebrája.

A vektorinvariánsok elméletének elsődleges célkitűzése az, hogy az R^G algebrát generáljuk véges sok (minél egyszerűbb) „alapinvariánssal" (egy ilyen generátorrendszert megadó tételt „első alaptételnek" szokás nevezni), és meghatározzuk az ezekre teljesülő algebrai összefüggések ideálját („második alaptétel"). A nullkarakterisztikájú esetben Hermann Weyl ezt megtette a $G = GL(n)$, $SL(n)$, $O(n)$, $SO(n)$, $Sp(2\nu)$ klasszikus csoportok mindegyikére (lásd Weyl híres [11] könyvét). Az első alaptétel mindegyik esetben úgy szól, hogy az $R^G_{n\times m,p\times n}$ algebrát generálják bizonyos legfeljebb n-edfokú ($GL(n)$, $O(n)$, $Sp(2\nu)$ esetén pontosan másodfokú) invariánsok, melyek mindegyike az $(m+p)$ (ko)vektorváltozó közül legfeljebb n-től ($GL(n)$, $O(n)$, $Sp(2\nu)$ esetén legfeljebb kettőtől) függ. Például, az ortogonális csoportra vonatkozó első alaptétel – amelyet E. Study [8] már 1897-ben bebizonyított – a következő. (Mivel $R^{O(n)}_{n\times m,p\times n}$ nyilvánvaló módon azonosítható $R^{O(n)}_{n\times(m+p)}$-nel, ezért elég a $p = 0$ esettel foglalkozni.)

2.0.5. Tétel. *Az ortogonális csoporttal szemben invariáns polinomok $R^{O(n)}_{n\times m}$ algebráját generálják a*

$$\left\langle v^{(i)}, v^{(j)}\right\rangle \qquad (1 \le i \le j \le m)$$

skalárszorzatok.

Ezzel teljesen analóg a szimplektikus csoportra vonatkozó első alaptétel. Emlékeztetjük az olvasót, hogy az $Sp(2\nu)$ szimplektikus csoportot minden test felett az $A^TJA = J$ egyenlettel definiáljuk, ahol $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$. Ez azt fejezi ki, hogy A invariánsan hagyja a

$$\beta(u, v) = u^TJv \qquad (u, v \in k^{2\nu})$$

standard szimplektikus formát.

2.0.6. Tétel. *A szimplektikus csoporttal szemben invariáns polinomok $R_{2\nu\times m}^{Sp(2\nu)}$ algebráját generálják a*

$$\beta\left(v^{(i)}, v^{(j)}\right) \qquad (1 \leq i < j \leq m)$$

szimplektikus szorzatok.

C. De Concini és C. Procesi 1976-ban megjelent [1] dolgozatukban megmutatták, hogy ezek az eredmények szórul szóra átvihetők $GL(n)$, $SL(n)$, $Sp(2\nu)$ esetén minden (végtelen) testre, $O(n)$ és $SO(n)$ esetén pedig minden 2-től különböző karakterisztikájú (végtelen) testre.

Az alábbiakban egy végtelen, 2 karakterisztikájú k alaptest felett vizsgáljuk az ortogonális csoport vektorinvariánsait (kovektorokkal nem foglalkozunk).

Egy f monom multifokán értsük az $\alpha = \left(\alpha^{(1)}, \ldots, \alpha^{(m)}\right)$ sorozatot, ha f $v^{(1)}$-ben $\alpha^{(1)}$-ed, ... , $v^{(m)}$-ben $\alpha^{(m)}$-edfokú. Egy polinom multihomogén, ha minden tagjának ugyanaz a multifoka. Egy G-invariáns polinom multihomogén komponensei is G-invariánsak (tetszőleges $G \leq GL(n)$ mellett).

Az első fejezet jelöléseivel összhangban, $n = 2\nu$ esetén $x_1^{(i)}$, ... , $x_\nu^{(i)}$, $y_1^{(i)}$, ... , $y_\nu^{(i)}$, $n = 2\nu + 1$ esetén pedig $x_1^{(i)}$, ... , $x_\nu^{(i)}$, $y_1^{(i)}$, ... , $y_\nu^{(i)}$, $z^{(i)}$ fogja jelölni a $v^{(i)}$ határozatlan vektor koordinátáit. Tehát mindvégig e határozatlanok polinomjairól beszélünk.

Használjuk $i, j, i_1, \ldots i_n \in \{1, \ldots, m\}$ esetén a

$$\begin{aligned}
Q^{(i)} = q\left(v^{(i)}\right) &= \begin{cases} x_1^{(i)}y_1^{(i)} + \cdots + x_\nu^{(i)}y_\nu^{(i)} \\ x_1^{(i)}y_1^{(i)} + \cdots + x_\nu^{(i)}y_\nu^{(i)} + {z^{(i)}}^2, \end{cases} \\
B^{(ij)} = \beta\left(v^{(i)}, v^{(j)}\right) &= x_1^{(i)}y_1^{(j)} + y_1^{(i)}x_1^{(j)} + \cdots + x_\nu^{(i)}y_\nu^{(j)} + y_\nu^{(i)}x_\nu^{(j)}, \\
D^{(i_1,\ldots,i_n)} = \det\left[v^{(i_1)}, \ldots, v^{(i_n)}\right] &
\end{aligned} \tag{3}$$

jelöléseket. Ekkor $Q^{(i)}, B^{(ij)}, D^{(i_1,\ldots,i_n)} \in R_{n\times m}^{O(n)}$ multihomogén $O(n)$-invariáns polinomok.

2.1. Determináns helyett

Az alábbiakban tetszőleges ν esetén konstruálunk olyan polinomot, amely $SO(2\nu)$-re invariáns, de $O(2\nu)$-re nem (mint a 2-től különböző karakterisztikájú esetben a determináns).

2.1.1. Lemma. *Jelöljük $SO(2\nu, \mathbb{C})$-vel a komplex test feletti, a $q = x_1y_1 + \cdots + x_\nu y_\nu$ kvadratikus alak által definiált 2ν-dimenziós ortogonális geometria speciális ortogonális csoportját, míg $SO(2\nu)$ a 2 karakterisztikájú k test feletti csoportot jelölje. Ha az $f \in \mathbb{Z}\left[v^{(1)}, \ldots, v^{(m)}\right]$ egész együtthatós, $(2\nu \times m)$-változós polinom invariáns az $SO(2\nu, \mathbb{C})$ csoporttal szemben, akkor a modulo 2 tekintett $\bar{f} \in k\left[v^{(1)}, \ldots, v^{(m)}\right]$ polinom is invariáns az $SO(2\nu)$ csoporttal szemben.*

Az $SO(2\nu)$ helyett az $O(n)$ csoportra is igaz az analóg állítás; a következő bizonyítás kézenfekvő módon átvihető.

Bizonyítás. Az, hogy f invariáns $SO(2\nu, \mathbb{C})$-vel szemben, azt jelenti, hogy bármely két tükrözés szorzatával szemben invariáns:

$$f\left(T_u T_w v^{(1)}, \ldots, T_u T_w v^{(m)}\right) = f\left(v^{(1)}, \ldots, v^{(m)}\right),$$

ha $u, w \in \mathbb{C}^{2\nu}$ és $q(u)q(w) \neq 0$. Itt mindkét oldal együtthatói az u és w vektorváltozók egész együtthatós racionális függvényeinek tekinthetők, és a megfelelő együtthatók egyenlőségének formálisan is fenn kell állnia. De akkor ezek a formális egyenlőségek k felett is fennállnak. (Lényeges, hogy a tükrözések 1.3.1 szerinti definíciójában a nevezőben szereplő $q(u)$ illetve $q(w)$ a modulo 2 redukciónál sem válik azonosan nullává.) Ez viszont azt jelenti, hogy $\bar{f}$ is invariáns bármely két tükrözés szorzatával, tehát $SO(2\nu)$-vel szemben. □

A továbbiakban a $*$ szimbólum az x és y betűk bármelyikét jelölheti.

2.1.2. Állítás. *Tekintsük a (3) által $\mathbb{Z}$ felett definiált B polinomokból képzett*

$$\sum B^{(i_1 i_2)} B^{(i_3 i_4)} \cdots B^{(i_{2\nu-1} i_{2\nu})}$$

2ν-lineáris polinomot, ahol az összegzést az $1, \ldots, 2\nu$ indexek azon $i_1, \ldots, i_{2\nu}$ permutációira terjesztjük ki, amelyekre $i_1 < i_2$, $i_3 < i_4$, $\ldots$, $i_{2\nu-1} < i_{2\nu}$ és $i_1 < i_3 < \cdots < i_{2\nu-1}$. Ha a $*_{j_1}, \ldots, *_{j_{2\nu}}$ betűk az $x_1, \ldots, x_\nu, y_1, \ldots, y_\nu$ betűknek egy permutációját alkotják, akkor a $*_{j_1}^{(1)} \cdots *_{j_{2\nu}}^{(2\nu)}$ monom együtthatója a fenti polinomban 1. Ha nem alkotnak permutációt, akkor az együttható páros.

Bizonyítás. A $B^{(i_1 i_2)} B^{(i_3 i_4)} \cdots B^{(i_{2\nu-1} i_{2\nu})}$ szorzat azoknak a $*_{j_1}^{(1)} \cdots *_{j_{2\nu}}^{(2\nu)}$ monomoknak az összege, amelyekre $j_{i_1} = j_{i_2}$, $j_{i_3} = j_{i_4}$, $\ldots$, $j_{i_{2\nu-1}} = j_{i_{2\nu}}$, és az ezen indexpárok bármelyikének megfelelő két csillag egyike x, másika y. Tehát csak olyan monomok lépnek fel, amelyekben ugyanannyi – mondjuk τ_t – darab x_t és y_t szerepel minden t-re. Egy ilyen monom együtthatója a B-szorzatok összegében $\tau_1! \ldots \tau_\nu!$, mert annyi B-szorzatban szerepel, ahányféleképpen a tényezői összepárosíthatók úgy, hogy csak $\{x_t, y_t\}$ alakú párok jöjjenek létre. Ez az együttható csak akkor páratlan, ha $\tau_1 = \cdots = \tau_\nu = 1$ (azaz ha permutációról van szó); és akkor 1. □

2.1.3. Állítás. (Domokos M., szóbeli közlés.) *Tetszőleges ν esetén létezik olyan $R_{2\nu \times 2\nu}$-beli, 2ν-lineáris polinom, amely invariáns $SO(2\nu)$-re, de $O(2\nu)$-re nem.*

Bizonyítás. Az előző állításban szereplő összegből vonjuk ki a (szintén $\mathbb{Z}$ felett képezett) $D^{(1\cdots(2\nu))}$ determinánst. A kapott polinom az állítás következtében csupa páros együtthatóval bír, tehát $2f$ alakú, ahol $f \in \mathbb{Z}\left[v^{(1)}, \ldots, v^{(m)}\right]$. Ha a $*_{j_1}, \ldots, *_{j_{2\nu}}$ betűk az $x_1, \ldots, x_\nu, y_1, \ldots, y_\nu$ betűknek egy permutációját alkotják, akkor – ismét az előző állítás miatt – a $*_{j_1}^{(1)} \cdots *_{j_{2\nu}}^{(2\nu)}$ monom együtthatója az f polinomban 0 vagy 1 aszerint, hogy a permutáció páros-e vagy páratlan. Ez a tény öröklődik a modulo 2 tekintett $\bar{f}$ polinomra is. Mivel f nyilvánvalóan invariáns $SO(2\nu, \mathbb{C})$-re, ezért a fenti 2.1.1 lemma szerint $\bar{f}$ invariáns $SO(2\nu)$-re. Másrészt $\bar{f}$ nem invariáns az $x_1 \leftrightarrow y_1$ tükrözésre, mert ez a páratlan permutációknak megfelelő monomokat a páros permutációknak megfelelőkbe viszi. □

2.1.4. Megjegyzés. *Az állításból azonnal következik, hogy az $SO(2\nu)$ mátrixcsoport algebrai. Valóban, egy lineáris transzformáció pontosan akkor speciális ortogonális, ha invariánsan hagyja a q polinomot és egy tetszőlegesen rögzített $SO(2\nu)$-invariáns, de nem $O(2\nu)$-invariáns polinomot.*

2.1.5. Megjegyzés. *Bármely $R_{2\nu\times m}^{SO(2\nu)} \backslash R_{2\nu\times m}^{O(2\nu)}$-beli polinom másodfokú és egész $R_{2\nu\times m}^{O(2\nu)}$ felett, mert az $O(2\nu)\backslash SO(2\nu)$ mellékosztálynál keletkező képével vett összege és szorzata is $R_{2\nu\times m}^{O(2\nu)}$-ben van. Hasonlóan, bármely $K_{2\nu\times m}^{SO(2\nu)} \backslash K_{2\nu\times m}^{O(2\nu)}$-beli racionális kifejezés másodfokú $K_{2\nu\times m}^{O(2\nu)}$ felett. Mivel a $K_{2\nu\times m}^{SO(2\nu)} \mid K_{2\nu\times m}^{O(2\nu)}$ testbővítés nyilvánvalóan szeparábilis, azt kapjuk, hogy $m \geq 2\nu$ esetén ez a bővítés másodfokú.*

2.2. Megjegyzés a páratlan dimenziós esetről

A fejezet hátralévő részében az invariáns polinomok alacsony fokú ilyenek polinomjaként való kifejezhetőségének kérdésével foglalkozunk. A 2 karakterisztikájú test felett is érvényes 2.0.6 tétel, valamint az $O(2\nu+1)$ és $Sp(2\nu)$ közötti kapcsolat lehetőséget nyújt arra, hogy a páratlan dimenziós esetben azonnal levonjuk az alábbi következtetést:

2.2.1. Állítás. *Tegyük fel, hogy k tökéletes. Az $f \in R_{(2\nu+1)\times m}^{O(2\nu+1)}$ invariáns akkor és csak akkor fejezhető ki a $Q^{(i)}$ és $B^{(ij)}$ másodfokú invariánsok polinomjaként, ha a $z^{(1)}, \ldots, z^{(m)}$ változók mindegyike csak páros kitevővel fordul elő benne.*

Az állítás speciális eseteként adódik, hogy ha f egy tetszőleges invariáns polinom négyzete, akkor kifejezhető a Q-k és B-k polinomjaként. Ennek ellenére – legalábbis a háromdimenziós esetben – léteznek tetszőlegesen magas fokú invariáns polinomok, amelyek nem fejezhetők ki alacsonyabb fokúak polinomjaként (lásd a 2.4 alfejezetet).

Bizonyítás. A feltétel szükségessége nyilvánvaló. A megfordítás bizonyításához tegyük fel, hogy f-re teljesül a feltétel. Ha f nem függ a $z^{(1)}, \ldots, z^{(m)}$ változóktól, akkor az 1.2.4 állítás folytán invariáns $Sp(2\nu)$-re, így a 2.0.6 tétel szerint f polinomja a $B^{(ij)}$ invariánsoknak.

Tegyük fel, hogy f függ a $z^{(i)}$ változóktól. Legyen f-nek, mint ezek polinomjának az egyik legmagasabb fokú tagja

$$z^{(1)^{2\alpha_1}} \cdots z^{(m)^{2\alpha_m}} p\left(x_1^{(1)}, \ldots, x_\nu^{(1)}, y_1^{(1)}, \ldots, y_\nu^{(1)}, \ldots\ldots, x_1^{(m)}, \ldots, x_\nu^{(m)}, y_1^{(m)}, \ldots, y_\nu^{(m)}\right).$$

Tudjuk, hogy minden ortogonális mátrix utolsó oszlopa $(0, \ldots, 0, 1)^T$, bal felső sarka pedig $\in Sp(2\nu)$. Ezért f csak úgy lehet $O(2\nu+1)$-invariáns, ha p is az. Így p polinomja a $B^{(ij)}$ invariánsoknak.

Térjünk át f-ről az

$$f - Q^{(1)^{\alpha_1}} \cdots Q^{(m)^{\alpha_m}} p$$

polinomra. Ez is $O(2\nu+1)$-invariáns, a $z^{(i)}$ változók csak páros kitevőn szerepelnek, és eltűnt f kiválasztott legmagasabb fokú tagja. A keletkező új tagok pedig f-nél alacsonyabb fokúak a $z^{(i)}$ változókban. Az eljárást iterálva véges sok lépés után olyan polinomot kapunk, amely nem függ a $z^{(i)}$ változóktól. Ez a polinom kifejezhető a $Q^{(i)}$-k és $B^{(ij)}$-k polinomjaként, tehát f is. $\square$

2.3. A kétdimenziós eset

A k^2 kétdimenziós térben legyen x és y a két koordináta. A standard kvadratikus alak $q = xy$. Az

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

mátrix pontosan akkor ortogonális, ha

$$(a_{11}x + a_{12}y)(a_{21}x + a_{22}y) = xy,$$

azaz, ha $a_{11}a_{21} = a_{12}a_{22} = 0$ és $a_{11}a_{22} + a_{12}a_{21} = 1$. Ezért

$$O(2) = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} : a \in k^* \right\} \cup \left\{ \begin{pmatrix} 0 & a \\ 1/a & 0 \end{pmatrix} : a \in k^* \right\},$$

ahol az 1.3.7 állítás miatt az első tag $SO(2)$.

Ezért egy polinom pontosan akkor invariáns $SO(2)$-re, ha minden tagjában ugyanannyi x van, mint y. Ezért az $SO(2)$-invariáns polinomok algebrája generálható másodfokú elemekkel:

$$R_{2\times m}^{SO(2)} = k\left[x^{(i)}y^{(j)} : i, j = 1, \ldots, m\right].$$

Megmutatjuk, hogy az $O(2)$-invariáns polinomok algebrájával már nem ez a helyzet. Egy $SO(2)$-invariáns polinom pontosan akkor invariáns a teljes $O(2)$-re, ha $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$-re invariáns, azaz, ha

$$x^{(i_1)} \cdots x^{(i_s)} y^{(i_1)} \cdots y^{(i_s)} = Q^{(i_1)} \cdots Q^{(i_s)}$$

és

$$x^{(i_1)} \cdots x^{(i_s)} y^{(j_1)} \cdots y^{(j_s)} + y^{(i_1)} \cdots y^{(i_s)} x^{(j_1)} \cdots x^{(j_s)} \stackrel{\text{def}}{=} B^{(i_1,\ldots i_s;j_1,\ldots j_s)}$$

alakú (multihomogén) tagok k feletti lineáris kombinációja. (Vegyük észre, hogy a most bevezetett jelölés összhangban van a régebbi $B^{(ij)}$ jelöléssel.)

2.3.1. Állítás. *(i) Tegyük fel, hogy az* $i_1, \ldots, i_s, j_1, \ldots, j_s$ *indexek mind különbözőek. Ekkor* $B^{(i_1,\ldots,i_s;j_1,\ldots,j_s)}$ *nem fejezhető ki alacsonyabb fokú* $O(2)$*-invariáns polinomok polinomjaként.*

(ii) Tegyük fel, hogy az $1, \ldots, m$ *indexek mindegyike ugyanannyiszor fordul elő az* $i_1, \ldots, i_s, j_1, \ldots, j_s$ *indexek között, mint az* $i'_1, \ldots, i'_s, j'_1, \ldots, j'_s$ *indexek között. Ekkor a* $B^{(i_1,\ldots,i_s;j_1,\ldots,j_s)} + B^{(i'_1,\ldots,i'_s;j'_1,\ldots,j'_s)}$ *multihomogén* $O(2)$*-invariáns polinom kifejezhető két alacsonyabb fokú* B *szorzataként (kivéve, ha nulla).*

(iii) Tegyük fel, hogy az $i_1, \ldots, i_s, j_1, \ldots, j_s$ *indexek nem mind különbözőek. Ekkor* $B^{(i_1,\ldots,i_s;j_1,\ldots,j_s)}$ *kifejezhető alacsonyabb fokú* $O(2)$*-invariáns polinomok polinomjaként.*

Bizonyítás. (i) Legyen $B^{(i_1,\ldots,i_s;j_1,\ldots,j_s)}$ multifoka α. Tehát $\alpha^{(i)} = 1$ ha i az $i_1, \ldots, i_s, j_1, \ldots, j_s$ indexek egyike, és $\alpha^{(i)} = 0$ különben.

Csak azt kell belátnunk, hogy $B^{(i_1,\ldots,i_s;j_1,\ldots,j_s)}$ nem fejezhető ki alacsonyabb fokú Q-szorzatok és B-k kéttényezős szorzatainak összegeként. Vegyük észre, hogy egy ilyen kéttényezős szorzat mindig egy multihomogén polinom, mely csak úgy lehet α multifokú, ha két olyan (alacsonyabb multifokú) B-t szorzunk össze, melyek mindegyikének csupa különböző indexe van, és a két indexhalmaz diszjunkt egyesítése $\{i_1, \ldots, i_s, j_1, \ldots, j_s\}$. Egy ilyen szorzat viszont mindig *két* α multifokú B összege. Ilyen szorzatok tetszőleges lineáris kombinációja tehát mindig olyan lineáris kombinációja az α multifokú B-knek, amelyben az együtthatók összege nulla. Mivel $B^{(i_1,\ldots,i_s;j_1,\ldots,j_s)}$ nem ilyen, készen vagyunk.

(ii) A feltétel úgy fogalmazható, hogy az $I = \{i_1, \ldots, i_s\}$, $J = \{j_1, \ldots, j_s\}$, $I' = \{i'_1, \ldots, i'_s\}$, $J' = \{j'_1, \ldots, j'_s\}$ multihalmazokra $I + J = I' + J'$. Ezért vannak olyan E, F, G, H multihalmazok, melyekkel $I = E+G$, $J = F+H$, $I' = E+H$ és $J' = F+G$. Ekkor $|E| = |F|$, $|G| = |H|$, és

$$B^{(E;F)}B^{(G;H)} = B^{(E+G;F+H)} + B^{(E+H;F+G)} = B^{(I;J)} + B^{(I';J')}.$$

(iii) A már igazolt (ii) állítás miatt feltehetjük, hogy $i_1 = j_1$. Ekkor viszont

$$B^{(i_1,\ldots,i_s;j_1,\ldots,j_s)} = Q^{(i_1)}B^{(i_2,\ldots,i_s;j_2,\ldots,j_s)}.$$

□

Az állításból egyszerűen adódik a

2.3.2. Tétel. *(i) Az $R^{O(2)}_{2\times m}$ algebrát generálják a $Q^{(i)}$ és $B^{(i_1,\ldots,i_s;j_1,\ldots,j_s)}$ invariánsok, ahol $1 \le i \le m$, illetve $1 \le i_1 < \cdots < i_s < j_1 < \cdots < j_s \le m$.*

(ii) Az (i) alatti generátorrendszerből egyetlen elem sem hagyható el. Sőt, az $R^{O(2)}_{2\times m}$ algebra minden, multihomogén elemekből álló generátorrendszere tartalmazza a $Q^{(i)}$-k egy-egy nullától különböző skalárszorosát, továbbá tartalmaz egy α multifokú invariánst minden olyan $\alpha = \left(\alpha^{(1)}, \ldots, \alpha^{(m)}\right)$ 0-1-sorozat esetén, amelyben páros sok 1-es van.

Bizonyítás. (i) Elég belátni, hogy minden Q-kból álló szorzat és minden B kifejezhető a tételben szereplő generátorok polinomjaként. A Q-szorzatokra ez nyilvánvaló, a B-kre pedig 2.3.1(iii) és (ii) következménye.

(ii) A $Q^{(i)}$-nél kisebb vagy vele egyenlő multifokú multihomogén invariánsok csak $Q^{(i)}$ skalárszorosai. Ebből következik a $Q^{(i)}$-re vonatkozó állítás. A 0-1 sorozatokra vonatkozó állítás 2.3.1(i) következménye. □

2.4. A háromdimenziós eset

Ebben az alfejezetben feltesszük, hogy a k 2 karakterisztikájú test tökéletes. Azonosítsuk a k^3 háromdimenziós teret a nulla nyomú 2×2-es mátrixok $\mathfrak{sl}(2)$ terével. A $v = (x, y, z)^T$ vektornak a

$$V = \begin{pmatrix} z & x \\ y & z \end{pmatrix}$$

mátrix feleljen meg. Ekkor $q(v) = xy + z^2 = \det V$. Ebből világos, hogy tetszőleges $T \in SL(2)$ mellett

$$\mathrm{Ad}\, T : \mathfrak{sl}(2) \to \mathfrak{sl}(2), \qquad V \mapsto TVT^{-1}$$

egy ortogonális transzformáció.

2.4.1. Állítás. *Az $\mathfrak{sl}(2)$ háromdimenziós tér minden ortogonális transzformációja* Ad T *alakú, alkalmas $T \in SL(2)$-vel.*

Bizonyítás. Elegendő az $\mathfrak{sl}(2)/\ker\beta$ faktortéren való hatást vizsgálni. Legyen $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, ekkor

$$(\mathrm{Ad}\, T)\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}\begin{pmatrix} d & b \\ c & a \end{pmatrix} = \begin{pmatrix} * & a^2x + b^2y \\ c^2x + d^2y & * \end{pmatrix}.$$

Tehát az Ad T által az $\mathfrak{sl}(2)/\ker\beta$ faktortéren indukált transzformáció mátrixa a kanonikus bázisban $\begin{pmatrix} a^2 & b^2 \\ c^2 & d^2 \end{pmatrix}$, így az 1.2.4 állítás miatt elég belátni, hogy ez tetszőleges szimplektikus mátrix lehet. A k test tökéletessége alapján nyilvánvaló, hogy tetszőleges unimoduláris mátrix előáll ilyen alakban. $\square$

2.4.2. Következmény. *Legyen $i_1, \ldots, i_s \in \{1, \ldots, m\}$. A*

$$Tr^{(i_1,\ldots,i_s)} \stackrel{\text{def}}{=} \mathrm{Tr}\left(V^{(i_1)} \cdots V^{(i_s)}\right)$$

polinom $O(3)$-invariáns: $Tr^{(i_1,\ldots,i_s)} \in R_{3\times m}^{O(3)}$.

2.4.3. Állítás. (Domokos M., szóbeli közlés.) *Ha s páros, és az i_1, … , i_s indexek különbözőek, akkor $Tr^{(i_1,\ldots,i_s)}$ nem áll elő alacsonyabb fokú $O(3)$-invariáns polinomok polinomjaként.*

Bizonyítás. Legyen $s = 2\sigma$. Feltehetjük, hogy $i_1 = 1$, … , $i_{2\sigma} = 2\sigma$.

Ha egy $O(3)$-invariáns polinomban a $z^{(i)}$ változók helyett nullát írunk, akkor egy – az eredetinél nem magasabb fokú – $O(2)$-invariáns polinomot kapunk, hiszen az A 2×2-es ortogonális mátrixszal együtt az $A \oplus 1$ blokkdiagonális mátrix is ortogonális. Ezért elég belátni, hogy a

$$Tr^{(1,\ldots,2\sigma)}\,|_{z=0} = \mathrm{Tr}\left(\begin{pmatrix} 0 & x^{(1)} \\ y^{(1)} & 0 \end{pmatrix}\begin{pmatrix} 0 & x^{(2)} \\ y^{(2)} & 0 \end{pmatrix}\cdots\begin{pmatrix} 0 & x^{(2\sigma-1)} \\ y^{(2\sigma-1)} & 0 \end{pmatrix}\begin{pmatrix} 0 & x^{(2\sigma)} \\ y^{(2\sigma)} & 0 \end{pmatrix}\right) =$$
$$= \mathrm{Tr}\left(\begin{pmatrix} x^{(1)}y^{(2)} & \\ & y^{(1)}x^{(2)} \end{pmatrix}\cdots\begin{pmatrix} x^{(2\sigma-1)}y^{(2\sigma)} & \\ & y^{(2\sigma-1)}x^{(2\sigma)} \end{pmatrix}\right) = B^{(1,3,\ldots,2\sigma-1;2,4,\ldots,2\sigma)}$$

polinom nem áll elő 2σ-nál alacsonyabb fokú $O(2)$-invariáns polinomok polinomjaként. Ezt 2.3.1(i)-ből tudjuk. $\square$

2.4.4. Következmény. *Az $R_{3\times m}^{O(3)}$ algebra minden, multihomogén elemekből álló generátorrendszere tartalmazza a $Q^{(i)}$-k egy-egy nullától különböző skalárszorosát, továbbá tartalmaz egy α multifokú invariánst minden olyan $\alpha = \left(\alpha^{(1)}, \ldots, \alpha^{(m)}\right)$ 0-1-sorozat esetén, amelyben páros sok 1-es van.*

Bizonyítás. A Q-kra vonatkozó állítás ugyanúgy nyilvánvaló, mint a kétdimenziós esetben. A másik állítás a fentiből azonnal adódik. $\square$

2.5. A négydimenziós eset

Azonosítsuk a k^4 négydimenziós teret a 2×2-es mátrixok $\mathfrak{gl}(2)$ terével úgy, hogy a $v = (x_1, x_2, y_1, y_2)^T$ vektornak a

$$V = \begin{pmatrix} x_1 & x_2 \\ y_2 & y_1 \end{pmatrix}$$

mátrix feleljen meg. Ekkor $q(v) = x_1 y_1 + x_2 y_2 = \det V$. Ebből világos, hogy tetszőleges $S, T \in SL(2)$ mellett

$$\mathfrak{gl}(2) \to \mathfrak{gl}(2), \qquad V \mapsto SVT^{-1}$$

egy ortogonális transzformáció. Így adódik egy $\varphi : SL(2) \times SL(2) \to O(4)$ csoporthomomorfizmus. Ez injektív, mert ha $S, T \in SL(2)$ és $SVT^{-1} = V$ minden $V \in \mathfrak{gl}(2)$-re, akkor $S = T$ unimoduláris skalármátrix, és az egységmátrix az egyetlen ilyen. Az $\operatorname{im} \varphi$ kép éppen $SO(4)$ (lásd [9], 12.21 feladat. Az algebrailag zárt esetben a hivatkozás helyett úgy is érvelhetünk, hogy az $\operatorname{im} \varphi$ kép hatdimenziós irreducibilis részcsoportja $O(4)$-nek, ezért csak $SO(4)$ lehet). Az $SO(4)$ csoportnak ezt az interpretációját felhasználva mutatott rá Domokos Mátyás, S. G. Kuzmin és A. N. Zubkov a megjelenés alatt álló [2] cikkben arra, hogy az $R_{4\times m}^{SO(4)}$ invariánsalgebra a 2 karakterisztikájú esetben teljesen más szerkezetű, mint bármely más karakterisztika esetén, amennyiben nem generálható $(m-1)$-nél alacsonyabb fokú elemekkel. Azóta Domokos Mátyás – továbbra is a fenti interpretációból kiindulva – a következő egyszerűbb bizonyítást találta ugyanerre.

Ha $i_1, \ldots, i_s; j_1, \ldots, j_s \in \{1 \ldots m\}$, akkor a

$$\det \begin{pmatrix} V^{(i_1)} & V^{(j_1)} & & & & \\ & V^{(i_2)} & V^{(j_2)} & & & \\ & & \ddots & \ddots & & \\ & & & V^{(i_{s-1})} & V^{(j_{s-1})} \\ V^{(j_s)} & & & & V^{(i_s)} \end{pmatrix}$$

polinom $SO(4)$-invariáns. Legyenek az $i_1, \ldots, i_s; j_1 \ldots, j_s$ indexek mind különbözőek. A fenti polinom $2s$-lineáris komponense is invariáns, jelölje azt $F^{(i_1,\ldots,i_s;j_1\ldots,j_s)} \in R_{4\times m}^{SO(4)}$.

2.5.1. Állítás. *Ha az $i_1, \ldots, i_s; j_1, \ldots, j_s \in \{1, \ldots, m\}$ indexek mind különbözőek, akkor $F^{(i_1,\ldots,i_s;j_1,\ldots,j_s)}$ nem áll elő alacsonyabb fokú $SO(4)$-invariáns polinomok polinomjaként.*

Bizonyítás. Ha egy $SO(4)$-invariáns polinomban az összes $x_2^{(i)}$ és $y_2^{(i)}$ változó helyett nullát írunk, akkor egy – az eredetinél nem magasabb fokú – $O(2)$-invariáns polinomot kapunk, hiszen az A 2×2-es ortogonális mátrixszal együtt az $A \oplus I$ és $A \oplus J$ blokkdiagonális mátrixok is ortogonálisak, és egyikük speciális (J-vel itt a $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ mátrixot jelöljük). Ezért elég belátni, hogy az

$$F^{(i_1,\ldots,i_s;j_1,\ldots,j_s)} |_{x_2=y_2=0}$$

polinom nem áll elő $2s$-nél alacsonyabb fokú $O(2)$-invariáns polinomok polinomjaként. De ez a

$$\det\begin{pmatrix}
x^{(i_1)} & 0 & x^{(j_1)} & 0 & & & & & & & & \\
0 & y^{(i_1)} & 0 & y^{(j_1)} & & & & & & & & \\
& & x^{(i_2)} & 0 & x^{(j_2)} & 0 & & & & & & \\
& & 0 & y^{(i_2)} & 0 & y^{(j_2)} & & & & & & \\
& & & & \ddots & & \ddots & & & & & \\
& & & & & & & & x^{(i_{s-1})} & 0 & x^{(j_{s-1})} & 0 \\
& & & & & & & & 0 & y^{(i_{s-1})} & 0 & y^{(j_{s-1})} \\
x^{(j_s)} & 0 & & & & & & & & & x^{(i_s)} & 0 \\
0 & y^{(j_s)} & & & & & & & & & 0 & y^{(i_s)}
\end{pmatrix}$$

determináns $2s$-lineáris komponense, ami pedig éppen a $B^{(i_1,\dots,i_s;j_1,\dots,j_s)}$ polinom. Így az állítás 2.3.1(i)-ből következik. □

2.5.2. Következmény. *Az $R^{SO(4)}_{4\times m}$ algebra minden, multihomogén elemekből álló generátorrendszere tartalmazza a $Q^{(i)}$-k egy-egy nullától különböző skalárszorosát, továbbá tartalmaz egy α multifokú invariánst minden olyan $\alpha = \left(\alpha^{(1)}, \dots, \alpha^{(m)}\right)$ 0-1-sorozat esetén, amelyben páros sok 1-es van.*

Bizonyítás. A Q-kra vonatkozó állítás ugyanúgy nyilvánvaló, mint a két- és háromdimenziós esetben. A másik állítás a fentiből azonnal adódik. □

2.6. A páros dimenziós eset

Ebben az alfejezetben megmutatjuk, hogy az $R^{O(2\nu)}_{2\nu\times m}$ algebrát nem generálják a $Q^{(i)}$ és $B^{(ij)}$ invariánsok, ha m elég nagy. Ezt $\nu = 1$ esetén már tudjuk.

Egy a $v^{(1)}, \dots, v^{(m)}$ 2ν-dimenziós vektoroktól multilineárisan függő monomot nevezzünk $\begin{pmatrix}\sigma_1 & \cdots & \sigma_\nu \\ \tau_1 & \cdots & \tau_\nu\end{pmatrix}$ típusúnak, ha tényezői között x_1-ből σ_1 darab, y_1-ből τ_1 darab, ..., x_ν-ből σ_ν darab, y_ν-ből τ_ν darab van. Ekkor tehát

$$m = \sigma_1 + \tau_1 + \cdots + \sigma_\nu + \tau_\nu.$$

2.6.1. Lemma. *Jelölje p azon monomok összegét, melyek a $v^{(1)}, \dots, v^{(6)}$ kétdimenziós vektoroktól szextilineárisan függenek, és típusuk $\begin{pmatrix}3\\3\end{pmatrix}$. Ekkor p unimoduláris invariáns: $p \in R^{SL(2)}_{2\times 6}$.*

Bizonyítás. A

$$\begin{pmatrix}c & \\ & 1/c\end{pmatrix} \qquad (c \in k^*)$$

transzformációkkal szembeni invariancia nyilvánvaló: p minden tagja invariáns. Elegendő az

$$A_c = \begin{pmatrix} 1 & c \\ & 1 \end{pmatrix} \qquad \text{és} \qquad A_c^T = \begin{pmatrix} 1 & \\ c & 1 \end{pmatrix} \qquad\qquad (c \in k)$$

transzformációkkal szembeni invarianciát igazolni. Sőt, szimmetria-okok miatt elég csak A_c-vel foglalkozni. A

$$p_c\left(v^{(1)}, \dots, v^{(6)}\right) = p\left(A_c v^{(1)}, \dots, A_c v^{(6)}\right)$$

transzformált polinomban csak olyan szextilineáris monomok szerepelnek, amelyeknek $\begin{pmatrix} \sigma \\ \tau \end{pmatrix}$ típusára (ahol persze $\sigma + \tau = 6$) fennáll a $\sigma \leq 3 \leq \tau$ egyenlőtlenség. Egy ilyen monom együtthatója $c^{\tau-3}\binom{\tau}{3}$. Ez csak akkor nem nulla, ha $\tau = 3$; és akkor 1. Ezért $p_c = p$. $\square$

Legyen $m \geq 2(3\nu - 1)$, és jelölje $f \in R_{2\nu \times 2(3\nu-1)} \leq R_{2\nu \times m}$ azon monomok összegét, melyek multilineárisan függenek az első $2(3\nu - 1)$ vektorváltozótól (a többitől nem függenek), továbbá típusuk két sora megegyezik, és soronként egy kettes és $(\nu - 1)$ hármas van benne.

2.6.2. Állítás. *Az f polinom ortogonális invariáns: $f \in R^{O(2\nu)}_{2\nu \times 2(3\nu-1)} \leq R^{O(2\nu)}_{2\nu \times m}$.*

Bizonyítás. Feltehetjük, hogy k algebrailag zárt, hiszen bővebb test felett több ortogonális transzformáció van. Elég belátni, hogy f invariáns az $O(2\nu)$ csoportnak az 1.3.9 következményben megadott generátoraira nézve.

Az $x_1 \leftrightarrow y_1$ tükrözés esetében ez nyilvánvaló, mert tetszőleges típust kijelölve, f olyan típusú tagjai egymás közt permutálódnak (persze másodrendű permutáció keletkezik).

Nézzük ezután az $\hat{A}$ transzformációkat. Persze elég A-t a $GL(\nu)$ csoport egy generátorrendszerén végigfuttatni.

Az

$$\hat{A}_{i,c} : x_i \mapsto c x_i, \quad y_i \mapsto c^{-1} y_i \qquad (i \in \{1, \dots, m\};\ c \in k^*)$$

transzformációkra nézve is nyilvánvaló az invariancia: f minden tagja invariáns.

Ezután már – szimmetria-okok miatt – elegendő az

$$\hat{A}_c : x_1 \mapsto x_1 + c x_2, \quad y_2 \mapsto c y_1 + y_2 \qquad (c \in k)$$

egyparaméteres részcsoportra vonatkozó invarianciát igazolni. Ehhez írjuk f-et $f = g + h$ alakba, ahol g az f azon tagjainak összege, amelyek típusának első két oszlopában csupa hármas van, h pedig a többi tag összege.

A fenti lemma alapján belátjuk, hogy g invariáns $\hat{A}_c$-vel szemben, sőt külön-külön az $x_1 \mapsto x_1 + c x_2$ és $y_2 \mapsto c y_1 + y_2$ transzformációkkal szemben is. Ezt – szimmetria-okok miatt – elég az $x_1 \mapsto x_1 + c x_2$ transzformációkra bizonyítani. Ehhez csoportosítsuk g tagjait aszerint, hogy melyik hat vektorváltozónak szerepel tényezőként az x_1 vagy x_2 koordinátája, és a többi vektorváltozónak melyik koordinátája szerepel. Az egy csoportba kerülő $\binom{6}{3}$ darab tag összege a fenti lemma szerint invariáns a szóban forgó transzformációkra.

Már csak azt kell bizonyítanunk, hogy h is invariáns $\hat{A}_c$-vel szemben. Ehhez csoportosítsuk h tagjait aszerint, hogy melyik tíz vektorváltozónak szerepel tényezőként az x_1, x_2,

y_1 vagy y_2 koordinátája, és a többi vektorváltozónak melyik koordinátája szerepel. Azt állítjuk, hogy az egy csoportba kerülő $2\binom{10}{5}\binom{5}{2}^2$ darab tag összege invariáns $\hat{A}_c$-vel szemben. Más szóval, azon monomok összege, melyek a $v^{(1)}, \ldots, v^{(10)}$ négydimenziós vektoroktól decilineárisan függenek, és típusuk $\begin{pmatrix} 2 & 3 \\ 2 & 3 \end{pmatrix}$ vagy $\begin{pmatrix} 3 & 2 \\ 3 & 2 \end{pmatrix}$, invariáns $\hat{A}_c$-vel szemben. Jelölje ezt az összeget r. Az

$$r_c\left(v^{(1)}, \ldots, v^{(10)}\right) = r\left(\hat{A}_c v^{(1)}, \ldots, \hat{A}_c v^{(10)}\right)$$

transzformált polinomban csak olyan decilineáris monomok szerepelhetnek, amelyeknek $\begin{pmatrix} \sigma_1 & \sigma_2 \\ \tau_1 & \tau_2 \end{pmatrix}$ típusára $\sigma_1 + \sigma_2 = \tau_1 + \tau_2 = 5$ teljesül. Egy ilyen monom együtthatója

$$c^{\sigma_2 - 3 + \tau_1 - 2}\binom{\sigma_2}{3}\binom{\tau_1}{2} + c^{\tau_1 - 3 + \sigma_2 - 2}\binom{\tau_1}{3}\binom{\sigma_2}{2} = c^{\sigma_2 + \tau_1 - 5}\left(\binom{\sigma_2}{3}\binom{\tau_1}{2} + \binom{\tau_1}{3}\binom{\sigma_2}{2}\right).$$

Ez csak akkor nem nulla, ha $\{\tau_1, \sigma_2\} = \{2, 3\}$; és akkor 1. Ezért $r_c = r$. □

2.6.3. Állítás. *Az f $O(2\nu)$-invariáns polinom nem fejezhető ki a $Q^{(i)}$ és $B^{(ij)}$ polinomok polinomjaként.*

Bizonyítás. Mivel f multilineáris, ezért csak úgy lehetne a Q-k és B-k polinomja, ha a B-k polinomja volna. Ezzel szemben megmutatjuk, hogy f nem szimplektikus invariáns: $f \notin R_{2\nu \times m}^{Sp(2\nu)}$.

Tekintsük a

$$T : x_1 \mapsto x_1 + y_1$$

szimplektikus transzformációt. Írjuk f-et $f = \tilde{g} + \tilde{h}$ alakba, ahol $\tilde{g}$ az f azon tagjainak összege, amelyekben három-három x_1 és y_1 szerepel tényezőként, $\tilde{h}$ pedig azoké, amelyekben kettő-kettő. A 2.6.1 állítás miatt $\tilde{g}$ invariáns T-vel szemben. Megmutatjuk viszont, hogy $\tilde{h}$ nem invariáns. Ehhez elég belátni, hogy a $v^{(1)}, \ldots, v^{(4)}$ kétdimenziós vektoroktól kvadrilineárisan függő, $\begin{pmatrix} 2 \\ 2 \end{pmatrix}$ típusú monomok összege nem invariáns. Ez világos: a T-vel transzformált polinomban az $x^{(1)}y^{(2)}y^{(3)}y^{(4)}$ monom $1 + 1 + 1 = 1$ együtthatóval szerepel. □

3. Algebro-geometriai megközelítés

Ebben a fejezetben mindig feltesszük, hogy a k alaptest algebrailag zárt; ezt nem fogjuk külön hangsúlyozni.

3.1. A nullkúp

Ebben az alfejezetben feltesszük, hogy k 2 karakterisztikájú.

3.1.1. Definíció. *Legyen* $S \leq k\left[v^{(1)}, \dots, v^{(m)}\right]$ *egy tetszőleges (egységelemes) részalgebra. A*

$$\left\{\left(v^{(1)}, \dots, v^{(m)}\right) \in k^{n \times m} : f\left(v^{(1)}, \dots, v^{(m)}\right) = f(0, \dots, 0) \text{ minden } f \in S \text{ esetén}\right\}$$

halmaz az S *algebrához tartozó nullkúp.*

A nullkúp definíciójában szereplő f polinomot természetesen elegendő az S algebra egy generátorrendszerén végigfuttatni. Célunk annak bizonyítása, hogy az $S = R_{n\times m}^{O(n)}$ algebrához tartozó nullkúpot már a $Q^{(i)}$ és $B^{(ij)}$ polinomok definiálják (noha, mint láttuk, az algebrát nem generálják). Ezek mind eltűnnek a $(0 \dots, 0)$ vektor-m-esen. Egy tetszőleges vektor-m-esen akkor és csak akkor tűnnek mind el, ha a vektor-m-es által kifeszített altér totálisan szinguláris (azaz q azonosan eltűnik rajta). Ezért először a totálisan szinguláris altereket vizsgáljuk.

3.1.2. Állítás. *Legyen* q *tetszőleges kvadratikus alak egy vektortéren. Legyen* β *a* q *polarizáltja. Ha* $\beta \equiv 0$*, de* $q \not\equiv 0$*, akkor azok a vektorok, amelyeken* q *eltűnik, egy 1 kodimenziós alteret alkotnak. Ha viszont* $\beta \not\equiv 0$*, akkor kifeszítik a teret.*

Bizonyítás. Ha $\beta \equiv 0$, de $q \not\equiv 0$, akkor az 1.1.4 állítás által biztosított koordinátarendszerben $q = z_1^2$ lesz, tehát $\{q = 0\} = \{z_1 = 0\}$.

Ha $\beta \not\equiv 0$, akkor q azonosan eltűnik a 1.1.4 állítás által biztosított koordinátarendszer bármelyik tengelyére megszorítva – kivéve esetleg a z_1-tengelyt. Ezenkívül nyilván van olyan nullhelye is q-nak, amelynek z_1 koordinátája 1. Ebből az állítás következik. □

A következő állítás már a standard ortogonális geometriára vonatkozik.

Egy alteret totálisan izotropnak nevezünk, ha β azonosan eltűnik rajta. Persze minden totálisan szinguláris altér egyben totálisan izotrop is.

3.1.3. Állítás. *Legyen* $n = 2\nu$ *vagy* $n = 2\nu + 1$*. Legyen* $W \leq k^n$ *egy maximális totálisan szinguláris altér. Ekkor* $\dim W = \nu$*, és*

$$k^n = W \oplus W_1 \oplus \ker \beta$$

írható egy szintén totálisan szinguláris W_1 *altérrel.*

Bizonyítás. Ha $n = 2\nu$, akkor β nem-elfajuló, ezért

$$\dim W + \dim W^{\perp} = 2\nu.$$

Ha $n = 2\nu + 1$, akkor $\dim \ker \beta = 1$, ezért

$$\dim W + \dim W^{\perp} = 2\nu + 1 \text{ vagy } 2\nu + 2.$$

Ezt az alábbiakban többször kihasználjuk.

Mivel W totálisan szinguláris, ezért totálisan izotrop, tehát $W \leq W^{\perp}$, így persze $W \oplus \ker \beta \leq W^{\perp}$. Belátjuk, hogy egyenlőség áll fenn. Tegyük fel indirekt módon, hogy $W \oplus \ker \beta < W^{\perp}$. Ekkor $\dim W \leq \dim W^{\perp} - 2$. A fenti 3.1.2 állítás következtében létezik $v \in W^{\perp} \backslash W$ szinguláris vektor. A $W \oplus kv$ altér totálisan szinguláris, ellentmondásban W maximalitásával. Ezzel beláttuk, hogy $W \oplus \ker \beta = W^{\perp}$, ahonnan $\dim W = \nu$.

A $W \oplus \ker \beta$ alteret csak 0-ban metsző totálisan szinguláris alterek közül legyen W_1 egy maximális. Ha léteznék $v \in W_1^{\perp} \backslash (W \oplus W_1 \oplus \ker \beta)$ szinguláris vektor, akkor a $W_1 \oplus kv$ totálisan szinguláris altér is csak 0-ban metszené a $W \oplus \ker \beta$ alteret, ellentmondásban W_1 maximalitásával. Ezért $W \oplus W_1 \oplus \ker \beta$ tartalmazza $W_1^{\perp}$ minden szinguláris vektorát. A 3.1.2 állítás következtében

$$\dim \left((W \oplus W_1 \oplus \ker \beta) \cap W_1^{\perp} \right) \geq \dim W_1^{\perp} - 1.$$

A bal oldalon szereplő altér éppen

$$\Big((W \oplus W_1)^{\perp} \oplus W_1 \Big)^{\perp},$$

ezért

$$\dim \Big((W \oplus W_1)^{\perp} \oplus W_1 \Big) \leq \dim W_1 + \dim \ker \beta + 1,$$

ahonnan

$$\dim (W \oplus W_1)^{\perp} \leq \dim \ker \beta + 1$$

és így $\dim W_1 \geq \nu - 1$. Egyenlőség esetén a 3.1.2 állítás szerint $W_1^{\perp}$ totálisan izotrop volna, de akkor

$$W_1^{\perp} \leq W_1^{\perp\perp} = W_1 \oplus \ker \beta$$

ellentmondáshoz vezetne. Tehát $\dim W_1 = \nu$, és W_1 direkt kiegészítője a $W \oplus \ker \beta$ altérnek. $\square$

3.1.4. Következmény. *Az $R_{n \times m}^{O(n)}$ invariánsalgebrához tartozó nullkúp megegyezik a $Q^{(i)}$ és $B^{(ij)}$ polinomok közös nullhelyeinek halmazával.*

Bizonyítás. Legyenek $v^{(1)}, \ldots, v^{(m)}$ olyan vektorok, amelyek kielégítik a $Q^{(i)} = 0$ és $B^{(ij)} = 0$ egyenleteket, tehát totálisan szinguláris alteret feszítenek ki. Legyen W egy őket tartalmazó maximális totálisan szinguláris altér. Legyen W_1 a fenti állítás által biztosított altér. Tetszőleges $t \in k^*$ esetén jelölje $A_t \in O(n)$ azt az ortogonális transzformációt, amely a W-beli vektorokat t-vel szorozza, a W_1-belieket t-vel osztja, a $\ker \beta$ altéren pedig identikus. Tetszőleges $f \in R_{n \times m}^{O(n)}$ polinom invariáns A_t-vel szemben is, ezért

$$f \left(tv^{(1)}, \ldots, tv^{(m)} \right) = f \left(v^{(1)}, \ldots, v^{(m)} \right).$$

Mivel ez tetszőleges $t \neq 0$ skalárra teljesül, és f egy polinom, ezért $t = 0$-ra is teljesül. Mivel $f \in R^{O(n)}_{n\times m}$ tetszőleges volt, ez azt jelenti, hogy a $\left(v^{(1)}, \dots, v^{(m)}\right)$ vektor-m-es benne van a nullkúpban. $\square$

A 3.1.4 következményből már pusztán általános elvek alapján levezethető, hogy $R^{O(n)}$ végesen generált mint az

$$A = k\left[Q^{(i)}, B^{(ij)} : 1 \leq i < j \leq m\right]$$

részalgebra feletti modulus. (A 2.6 alfejezetben azt bizonyítottuk, hogy ha n páros és m elég nagy, akkor $A \neq R^{O(n)}$. Páratlan n-re és $m \geq n$-re ez nyilvánvaló, mert $D^{(1\cdots n)} \in R^{O(n)} \setminus A$.)

Vázoljuk a bizonyítást. Nem nehéz belátni, hogy az $O(n)$ algebrai csoport reduktív, vagyis a radikálja (legnagyobb összefüggő feloldható normálosztója) egy tórusz. Ebből Nagata tétele (az [5]-beli 3.4 tétel) szerint következik, hogy az $R^{O(n)}$ algebra végesen generált.

Legyen $h \in R^{O(n)}$ tetszőleges homogén elem. A 3.1.4 következmény és a Hilbert-féle nullhelytétel szerint h egy hatványa benne van az A által R-ben generált ideálban. Az [5]-beli 3.4.2 lemma szerint ebből következik, hogy h egy (esetleg magasabb) hatványa benne van az A által $R^{O(n)}$-ben generált ideálban is (itt ismét fel kell használni $O(n)$ reduktivitását).

Ezt az $R^{O(n)}$ algebra egy homogén elemekből álló véges generátorrendszerének minden h elemére alkalmazva az adódik, hogy $R^{O(n)}$ minden elég magas (mondjuk legalább d-ed)fokú homogén eleme benne van az A által $R^{O(n)}$-ben generált ideálban. Így $R^{O(n)}$-et, mint A-modulust, generálják a d-nél alacsonyabb fokú elemei. Ezek véges dimenziós vektorteret alkotnak, tehát közülük véges sok is elég.

David Hilbert ennek a gondolatmenetnek az eredeti, komplex test feletti változata kapcsán vezette be a nullkúp fogalmát és bizonyította be a nullhelytételt.

3.2. Általános segédtételek

A harmadik fejezet hátralévő részének fő célja az ortogonális csoporttal szemben invariáns racionális kifejezések testének leírása, de a 3.3 alfejezetben kitérőt teszünk és kevés számú vektorváltozó esetén leírjuk az invariáns polinomok algebráját. A jelen alfejezetben az ezekhez szükséges algebro-geometriai segédtételeket bizonyítjuk. Lényegében Roe Goodman és Nolan R. Wallach [3] könyvének „A” függelékét fogjuk követni, de az ott csak a komplex test felett tárgyalt tételeket minden algebrailag zárt k alaptest esetére kiterjesztjük.

Az alább bizonyítandó 3.2.8 tétel (i) állításából azonnal következik az a jól ismert általános tény, hogy a nullkarakterisztikájú esetben a racionális invariánsok testét akkor és csak akkor generálja néhány megadott racionális invariáns, ha ezek szétválasztják a csoport általános helyzetű pályáit (lásd pl.: [6], 2.2.1 lemma). (Ez tetszőleges algebrai csoport tetszőleges racionális reprezentációjának invariánsaira érvényes. Esetünkben $O(n)$ definiáló reprezentációjának önmagával való m-szeres direkt összegéről van szó.) A prímkarakterisztikájú esetben szükség van egy szeparábilitási feltételre is (lásd a 3.2.8 tétel (ii) állítását és a tételt követő megjegyzést).

Két tisztán algebrai tétellel kezdjük, amelyek k-értékű algebra-homomorfizmusok (azaz k-lineáris multiplikatív funkcionálok, más néven karakterek) kiterjeszthetőségéről szólnak.

Algebrán kommutatív, egységelemes k-algebrát értünk (k tetszőleges algebrailag zárt test). Ha A egy algebra, akkor $\mathrm{Hom}(A,k)$ az $A \to k$ algebra-homomorfizmusok halmazát jelöli (az azonosan nulla funkcionált nem tekintjük algebra-homomorfizmusnak). Ezeket A karaktereinek is nevezzük. Jelöljük $\mathrm{Hom}(A,k)^a$-val a $0 \neq a \in A$ elemen el nem tűnő karakterek halmazát. Ha $g(X)$ egy tetszőleges A feletti polinom és $\phi \in \mathrm{Hom}(A,k)$, akkor jelölje $g^\phi(X)$ azt a k feletti polinomot, melyet $g(X)$-ből úgy kapunk, hogy minden együtthatójára alkalmazzuk a ϕ karaktert.

3.2.1. Tétel. *Legyen B nullosztómentes algebra. Legyen $A \leq B$ egy részalgebra, és tegyük fel, hogy B végesen generált mint A feletti algebra. Ekkor tetszőleges $0 \neq b \in B$-hez van $0 \neq a \in A$ úgy, hogy minden $\phi \in \mathrm{Hom}(A,k)^a$ karakter kiterjed $\psi \in \mathrm{Hom}(B,k)^b$ karakterré. Ha B minden eleme egész A felett, és $b = 1$, akkor $a = 1$ megfelelő.*

Bizonyítás. Legyen először $B = A[u]$ egy $u \in B$ elemmel. Legyen $0 \neq b = f(u) \in B$ tetszőleges, ahol $f(X) \in A[X]$ egy A feletti polinom.

Ha u transzcendens A felett, akkor egyelőre tetszőleges $\lambda \in k$ skalárt választva kiterjeszthetjük B-re a ϕ karaktert a

$$\psi(g(u)) = g^\phi(\lambda) \qquad (g \in A[X]) \tag{4}$$

formulával. Ekkor $\psi(b) = f^\phi(\lambda)$. Mivel $b \neq 0$, így $f(X) \neq 0$, és a-nak választhatjuk az $f(X)$ polinom bármelyik nullától különböző együtthatóját. Valóban, ha $\phi(a) \neq 0$, akkor $f^\phi(X) \neq 0$, tehát van olyan $\lambda \in k$, mely nem gyöke f^ϕ-nek, és az azzal definiált ψ kiterjesztésre $\psi(b) \neq 0$.

Ha viszont u algebrai A felett, akkor b is az. Legyen

$$s(X) = a_m X^m + \cdots + a_1 X + a_0 \qquad \text{illetve} \qquad q(X) = c_n X^n + \cdots + c_1 X + c_0$$

az u illetve b minimálpolinomja A felett, ahol $a_m \neq 0$. Megmutatjuk, hogy $a = a_m c_0$ megfelelő. (Jegyezzük meg, hogy ha u egész A felett és $b = 1$, akkor $a_m = c_0 = 1$ választható, s e választással $a = 1$ lesz.)

Legyen $g(X) \in A[X]$ tetszőleges. Maradékos osztással kaphatunk egy $d \geq 0$ egészt és A feletti $h(X)$, $r(X)$ polinomokat úgy, hogy $\mathrm{gr}\, r(X) < m$ és

$$a_m^d g(X) = s(X)h(X) + r(X).$$

Ha $g(X)$ olyan, hogy $g(u) = 0$, akkor $r(X) = 0$, hiszen $r(u) = 0$ és $\mathrm{gr}\, r(X) < m$. Ezért ekkor $a_m^d g(X)$ osztható $s(X)$-szel $A[X]$-ben.

Legyen $\phi \in \mathrm{Hom}(A,k)^a$ és legyen λ az $s^\phi(X)$ polinom egy gyöke. Ha $g(u) = 0$, akkor

$$\phi(a_m)^d g^\phi(\lambda) = \phi\left(a_m^d g(\lambda)\right) = 0,$$

de $\phi(a_m) = \phi(a)/\phi(c_0) \neq 0$, ezért $g^\phi(\lambda) = 0$. Ez lehetővé teszi, hogy a $\psi \in \mathrm{Hom}(B,k)$ kiterjesztést a (4) formulával definiáljuk. Erre a kiterjesztésre

$$0 = \psi(0) = \psi(q(b)) = q^\phi(\psi(b)),$$

viszont 0 nem gyöke $q^\phi(X)$-nek, mivel $\phi(c_0) \neq 0$. Így $\psi(b) \neq 0$. Ezzel a $B = A[u]$ esetben beláttuk a tételt.

Tegyük fel, hogy a tétel igaz minden olyan esetben, amikor B generálható $(n-1)$ elemmel A felett, és tekintsük a $B = A[b_1, \ldots, b_n]$ esetet. Legyen $0 \neq b \in B$ adott. Legyen $\tilde{A} = A[b_1, \ldots, b_{n-1}]$ és $u = b_n$. Ekkor $B = \tilde{A}[u]$. A fentiek szerint van $0 \neq \tilde{a} \in \tilde{A}$ úgy, hogy minden $\tilde{\phi} \in \mathrm{Hom}(\tilde{A}, k)^{\tilde{a}}$ karakter kiterjed $\psi \in \mathrm{Hom}(B, k)^b$ karakterré. Az indukciós feltevést B és b helyett $\tilde{A}$-ra és $\tilde{a}$-ra alkalmazva azt kapjuk, hogy van $0 \neq a \in A$ úgy, hogy minden $\phi \in \mathrm{Hom}(A, k)^a$ karakter kiterjed $\tilde{\phi} \in \mathrm{Hom}(\tilde{A}, k)^{\tilde{a}}$ karakterré. Ez az a elem megfelelő lesz. □

3.2.2. Következmény. *Legyen B végesen generált nullosztómentes algebra. Ekkor tetszőleges $0 \neq b \in B$-hez van $\psi \in \mathrm{Hom}(B, k)$ úgy, hogy $\psi(b) \neq 0$.*

Bizonyítás. Alkalmazzuk a fenti tételt az $A = k, \quad \phi(\lambda) = \lambda \quad (\lambda \in k)$ szereposztással. □

3.2.3. Tétel. *Legyen B végesen generált nullosztómentes algebra, és legyen $A \leq B$ egy végesen generált részalgebra. Tegyük fel, hogy van $0 \neq b \in B$ úgy, hogy A-nak minden karaktere legfeljebb egyféleképpen terjed ki $\mathrm{Hom}(B, k)^b$-beli karakterré. Ekkor B minden eleme tisztán inszeparábilis A felett. (Azaz, B minden eleme tisztán inszeparábilis A hányadosteste felett, B hányadostestében.) Másként fogalmazva:*

(i) Ha $\mathrm{char}\, k = 0$, akkor B minden eleme benne van A hányadostestében.

(ii) Ha $\mathrm{char}\, k = p \neq 0$, akkor B minden elemének egy p-hatványadik hatványa benne van A hányadostestében.

Bizonyítás. Az előző tételhez hasonlóan, most is elég a $B = A[u]$ esettel foglalkozni (abból már indukcióval adódik a tétel). Legyen $b = f(u)$, ahol $f(X) = a_n X^n + \cdots + a_0$ egy A feletti polinom, mely persze nem azonosan nulla.

Először belátjuk, hogy u algebrai A felett. Tegyük fel indirekt módon, hogy u transzcendens. Legyen a az $f(X)$ egyik nullától különböző együtthatója, és legyen $\phi \in \mathrm{Hom}(A, k)^a$ tetszőleges. A (4) formula a ϕ karakternek egy $\mathrm{Hom}(B, k)^b$-beli ψ kiterjesztését definiálja minden olyan $\lambda \in k$ esetén, amely nem gyöke f^{ϕ}-nek. Ez pedig ellentmond az egyértelműségnek, hiszen $\psi(u) = \lambda$ folytán különböző λ skalárok különböző ψ kiterjesztéseket adnak. Így u valóban algebrai.

Azt kell belátnunk, hogy u tisztán inszeparábilis A felett. Jelölje $s(X)$ és $q(X)$ ugyanazt, mint az előző tétel bizonyításában, és legyen, mint ott, $a = a_m c_0$. Tegyük fel indirekt módon, hogy $s(X)$-nek van két különböző gyöke a felbontási testében. Legyen x és y két különböző gyök. Legyen $F = A[x, y]$. Legyen $\tilde{\phi} \in \mathrm{Hom}(F, k)^{a(x-y)}$ tetszőleges, és legyen $\phi \in \mathrm{Hom}(A, k)^a$ a $\tilde{\phi}$ karakter A-ra való megszorítása. Ekkor $\tilde{\phi}(x)$ és $\tilde{\phi}(y)$ két különböző gyöke $s^{\phi}(X)$-nek. Például,

$$s^{\phi}\left(\tilde{\phi}(x)\right) = \tilde{\phi}\left(s(x)\right) = 0.$$

Ha tehát a (4) formulában λ helyébe $\tilde{\phi}(x)$-et, illetve $\tilde{\phi}(y)$-t írunk, akkor két különböző $\psi \in \mathrm{Hom}(B, k)^b$ kiterjesztését kapjuk a ϕ karakternek, ami ellentmond a tétel feltételének. □

Rátérünk a fenti két tétel algebro-geometriai következményeire. A topológiai kifejezéseket, mint korábban, most is a Zariski-féle értelemben használjuk. Affin varietáson irreducibilis affin algebrai halmazt, kváziaffin varietáson pedig egy ilyenben nyílt halmazt értünk. Ha X egy tetszőleges affin algebrai halmaz, akkor jelölje A_X az X affin koordinátagyűrűjét. Ekkor A_X egy végesen generált algebra, mely pontosan akkor nullosztómentes, ha X irreducibilis. Az A_X koordinátagyűrű minden k-lineáris multiplikatív funkcionálja (azaz karaktere) realizálható mint az X halmaz egy pontjában való kiértékelés. (Ez az állítás a Hilbert-féle nullhelytétel ekvivalens alakjainak egyike.) Tehát a $\mathrm{Hom}(A_X, k)$ halmaz természetes módon azonosítható X-szel. Az azonosításnál a $\mathrm{Hom}(A_X, k)^a$ halmaznak az $X^a \stackrel{\text{def}}{=} \{x \in X : a(x) \neq 0\}$ nyílt halmaz felel meg (tetszőleges $0 \neq a \in A_X$ esetén) .

3.2.4. Definíció. *Legyenek X és Y affin algebrai halmazok. Az $f : X \dashrightarrow Y$ racionális leképezés domináns, ha az $f(X)$ kép sűrű Y-ban.*

3.2.5. Megjegyzés. *Ha $f : X \to Y$ reguláris, akkor f dominanciája ekvivalens az általa indukált $f^* : A_X \leftarrow A_Y$ algebra-homomorfizmus injektivitásával.*

3.2.6. Tétel. *Legyenek X és Y affin varietások és legyen $f : X \dashrightarrow Y$ domináns racionális leképezés. Legyen $\emptyset \neq M \subseteq X$ nyílt. Ekkor $f(M)$ tartalmazza Y-nak egy nem-üres nyílt részhalmazát.*

Bizonyítás. Legyen $0 \neq q \in A_X$ olyan reguláris függvény X-en, amellyel az f leképezés bármely koordinátafüggvényét megszorozva az egész X halmazon reguláris függvényt kapunk. Ekkor tehát f reguláris az X^q kváziaffin varietáson. Azonosítsuk X^q-t az

$$\tilde{X^q} = \{(x,t) \in X \times k : \ q(x)t = 1\}$$

affin varietással a természetes módon. Az $\tilde{f}(x,t) = f(x)$ formulával definiált $\tilde{f} : \tilde{X^q} \to Y$ leképezés reguláris. Ezért eleve feltehetjük, hogy f reguláris.

Legyen $B = A_X$ és $A = f^*A_Y$. Mivel X irreducibilis, ezért B nullosztómentes. Feltehető, hogy $M = X^b$ egy $0 \neq b \in B$ függvénnyel. Legyen $a \in A$ a 3.2.1 tétel által biztosított elem, és legyen $a = f^*(\bar{a})$, ahol $\bar{a} \in A_Y$. Belátjuk, hogy $f(X^b) \supseteq Y^{\bar{a}}$. Valóban, tetszőleges $y \in Y^{\bar{a}}$ pontnak olyan $\phi : A \to k$ karakter felel meg, amelyre $\phi(a) = \bar{a}(y) \neq 0$, azaz $\phi \in \mathrm{Hom}(A,k)^a$. Tehát – a választása folytán – ϕ kiterjeszthető $\psi \in \mathrm{Hom}(B,k)^b$ karakterré. De ψ szükségképpen egy $x \in X^b$ pontban való kiértékelés, és $g(f(x)) = g(y)$ minden $g \in A_Y$-ra, hiszen ψ kiterjesztése ϕ-nek. Ebből következik, hogy $f(x) = y$. □

3.2.7. Lemma. *Legyenek X és Y affin varietások, és legyen $F : X \to Y$ egy domináns reguláris leképezés. Tegyük fel, hogy F injektív az X varietás egy alkalmas nem-üres és nyílt U részhalmazára megszorítva.*

(i) Ha $\mathrm{char}\ k = 0$, akkor minden $X \dashrightarrow k$ racionális függvény racionális függvénye F-nek (ezen azt értjük, hogy $g \circ F$ alakú egy alkalmas $g : Y \dashrightarrow k$ racionális függvénnyel).

(ii) Ha $\mathrm{char}\ k = p$ prímszám, akkor minden $X \dashrightarrow k$ racionális függvény egy alkalmas p-hatványadik hatványa racionális függvénye F-nek.

Bizonyítás. Legyen $B = A_X$ az $X \to k$ reguláris függvények algebrája, $A = F^*A_Y$ pedig azon függvények alkotta részalgebra, amelyek F-nek reguláris függvényei. Feltehetjük, hogy $U = X^b$ egy $0 \neq b \in B$ függvénnyel. Ekkor A-nak minden ϕ karaktere legfeljebb egyféleképpen terjeszthető ki $\psi \in \mathrm{Hom}(B,k)^b$ karakterré. Valóban, ϕ realizálható egy

$y \in Y$ pontban való kiértékelésként, tetszőleges $\psi \in \mathrm{Hom}(B,k)^b$ kiterjesztés pedig egy olyan $x \in U$ pontban való kiértékelésként, amelyre $F(x) = y$. Ilyen tulajdonságú x pont pedig legfeljebb egyféleképpen választható.

A 3.2.3 tétel miatt B minden eleme tisztán inszeparábilis A felett. De minden $X \dashrightarrow k$ racionális függvény előáll két B-beli (azaz reguláris) függvény hányadosaként, amiből a tétel állítása következik. □

3.2.8. Tétel. *Legyenek M és N affin varietások, $f : M \to N$ reguláris leképezés és $h : M \dashrightarrow k$ egy racionális függvény. Tegyük fel, hogy van egy nem-üres, nyílt $U \subseteq M$ nyílt halmaz, amelyen h reguláris és csak f-től függ (ezen azt értjük, hogy ha $m', m'' \in U$ és $f(m') = f(m'')$, akkor $h(m') = h(m'')$).*

(i) Ha $\mathrm{char}\, k = 0$, akkor h racionális függvénye f-nek.

(ii) Ha $\mathrm{char}\, k = p \neq 0$, akkor h egy p-hatványadik hatványa racionális függvénye f-nek.

Bizonyítás. Jelölje Y az $f(M)$ kép lezárását, X pedig az $f \times h : M \dashrightarrow N \times k$ leképezés képének lezárását. Legyen $F : X \to Y$ az $N \times k \to N$ vetítés X-re való megszorítása. Ekkor F domináns, és injektív az $(f \times h)(U)$ halmazra megszorítva. A 3.2.6 tétel szerint pedig $(f \times h)(U)$ tartalmazza X-nek egy nem-üres nyílt részhalmazát. Ezért az F leképezés kielégíti a 3.2.7 lemma feltételeit. Alkalmazzuk a lemma állítását arra az $X \to k$ reguláris függvényre, amit úgy kapunk, hogy az $X \to N \times k$ beágyazást komponáljuk az $N \times k \to k$ vetítéssel. Pont a tétel állítását kapjuk. □

Az $f : k \to k$, $f(x) = x^p$ és $h : k \to k$, $h(x) = x$ példa mutatja, hogy a p karakterisztikájú esetben h nem feltétlenül racionális függvénye f-nek. Ha azonban f „maximális rangú", akkor mégis levonhatjuk ezt az erősebb következtetést. Az alábbiakban ezt bizonyítjuk a legegyszerűbb speciális esetben. Ehhez szükségünk lesz az alábbi egyszerű állításra.

3.2.9. Állítás. *Legyen X egy affin tér és $g : X \dashrightarrow k$ egy racionális függvény. Tegyük fel, hogy g minden parciális deriváltja azonosan nulla.*

(i) Ha $\mathrm{char}\, k = 0$, akkor g konstans.

(ii) Ha $\mathrm{char}\, k = p \neq 0$, akkor g egy racionális függvény p-edik hatványa.

Vegyük észre, hogy az állítás megfordítása mindkét esetben nyilvánvaló.

Bizonyítás. Legyen $g = r/q$, ahol r és q relatív prím polinomok. Jelöljük vesszővel bármelyik változó szerinti parciális deriválást; ekkor $qr' - q'r = 0$. Ezért q' osztható q-val, r' pedig r-rel, ahonnan $q' = r' = 0$. Azt kaptuk, hogy q és r minden parciális deriváltja is azonosan nulla. Tehát eleve feltehetjük, hogy g polinom, arra pedig az állítás nyilvánvaló. □

3.2.10. Következmény. *Legyenek M és N affin terek. Tegyük fel, hogy $f : M \to N$ és $h : M \dashrightarrow k$ olyanok, mint a 3.2.8 tételben. Tegyük fel, hogy f domináns, és van olyan $m \in M$ pont, ahol az f leképezés Jacobi-mátrixának rangja $\dim N$. Ekkor h racionális függvénye f-nek.*

Az f dominanciájára vonatkozó feltételt valójában el lehetne hagyni, mert következik a rangra vonatkozó feltételből.

Bizonyítás. Ha char $k = 0$, akkor a 3.2.8 tétel után már nincs mit bizonyítani. Legyen char $k = p$ prímszám. A 3.2.8 tétel miatt elég belátni, hogy ha h^p racionális függvénye f-nek, akkor h is az. Legyen tehát $h^p = g \circ f$, ahol $g : N \dashrightarrow k$ racionális. Azon M-beli pontok, ahol f Jacobi-mátrixának rangja $\dim N$, egy nem-üres és nyílt, következésképpen sűrű U halmazt alkotnak. Mivel f domináns, ezért az $f(U)$ kép is sűrű az N térben. Mivel a h^p függvény minden parciális deriváltja azonosan nulla, ezért a g függvény minden parciális deriváltja eltűnik az $f(U)$ halmaz minden pontjában, vagyis szintén azonosan nulla. A fenti 3.2.9 állítás szerint $\sqrt[p]{g}$ is racionális függvény. Így $h = \sqrt[p]{g} \circ f$ valóban racionális függvénye f-nek. $\square$

A következő egyszerű állítás független az előzőektől, bizonyításához csupán a Hilbert-féle nullhelytételt kell felhasználnunk.

3.2.11. Állítás. *Legyen M egy affin algebrai halmaz, N pedig egy affin tér. Legyen $f : M \to N$ egy szürjektív reguláris leképezés, $g : N \dashrightarrow k$ pedig egy racionális függvény. Ha $g \circ f$ reguláris, akkor g is az.*

Valójában nincs szükség arra, hogy N affin tér legyen; elég, ha normális varietás (azaz koordinátagyűrűje integrálisan zárt). A szürjektivitás is gyengíthető: elég volna feltenni, hogy a kimaradó halmaz lezárásának kodimenziója (a normális képvarietásban) legalább 2.

Bizonyítás. Legyen $g = r/q$, ahol $r, q \in A_N$ relatív prím polinomok. Mivel $g \circ f$ reguláris, ezért $r \circ f$ osztható $q \circ f$-fel az A_M algebrában. Ezért ahol $q \circ f$ eltűnik, ott $r \circ f$ is. Mivel f szürjektív, az adódik, hogy ahol q eltűnik, ott r is. A Hilbert-féle nullhelytétel szerint r egy hatványa osztható q-val. Mivel $(q, r) = 1$, ezért q egység. $\square$

3.3. A kevés vektor esete

Ebben az alfejezetben mindig feltesszük, hogy a k algebrailag zárt test 2 karakterisztikájú. Célunk annak bizonyítása, hogy ha $n = 2\nu$ vagy $n = 2\nu + 1$, és $m \leq 2\nu$, akkor az $R_{n\times m}^{O(n)}$ invariánsalgebrát generálják a $Q^{(i)}$ és $B^{(ij)}$ másodfokú invariánsok.

3.3.1. Állítás. *Legyen $W \leq k^n$ egy m dimenziós altér, amelyen q nem-elfajuló, és amelyre $W \cap \ker \beta = 0$. (Páros n esetén az utóbbi feltétel felesleges, hiszen $\ker \beta = 0$. Páros m esetén is felesleges, hiszen ekkor $q\mid_W$-vel együtt $\beta\mid_W$ sem elfajuló.) Válasszunk olyan $\left(e^{(1)}, \ldots, e^{(m)}\right)$ bázist W-ben, amelyhez tartozó koordinátarendszerben $q\mid_W$ az 1.1.4 állítás szerinti kanonikus alakú. Ekkor ez a bázis kiegészíthető k^n egy olyan $\left(e^{(1)}, \ldots\ldots, e^{(n)}\right)$ bázisává, amelyhez tartozó koordinátarendszerben a következők teljesülnek:*

(i) Ha m páros, akkor q kanonikus alakú.

(ii) Ha m páratlan, akkor q a kanonikus alakú kvadratikus alakból az m-edik koordináta négyzetének hozzáadásával kapható.

Bizonyítás. (i) Mivel $\beta\,|_W$ nem elfajuló, ezért $k^n = W \oplus W^\perp$. Legyen $\left(e^{(m+1)}, \dots, e^{(n)}\right)$ olyan bázis $W^\perp$-ben, amelyhez tartozó koordinátarendszerben $q\,|_{W^\perp}$ kanonikus alakú.

(ii) Mivel $W \cap \ker\beta = 0$, és $e^{(m)}$ lineárisan független az $e^{(1)}, \dots, e^{(m-1)}$ vektoroktól, ezért van olyan $e^{(m+1)} \in \left\langle e^{(1)}, \dots, e^{(m-1)}\right\rangle^\perp$ vektor, amelyre $\beta\left(e^{(m)}, e^{(m+1)}\right) = 1$. Az $e^{(m+1)}$ vektor úgy is megválasztható, hogy $q\left(e^{(m+1)}\right) = 0$ legyen (az eredeti választásunkhoz $e^{(m)}$ alkalmas skalárszorosát hozzáadva). Legyen $\tilde{W} = W \oplus k e^{(m+1)}$.

Mivel $\beta\,|_{\tilde{W}}$ nem elfajuló, ezért $k^n = \tilde{W} \oplus \tilde{W}^\perp$. Legyen $\left(e^{(m+2)}, \dots, e^{(n)}\right)$ olyan bázis $\tilde{W}^\perp$-ben, amelyhez tartozó koordinátarendszerben $q\,|_{\tilde{W}^\perp}$ kanonikus alakú. □

Ebből azonnal következik Witt egy nevezetes tételének ([9], 7.4 tétel) alábbi speciális esete:

3.3.2. Állítás. *Legyenek $W', W'' \leq k^n$ olyan alterek, mint a fenti állításban szereplő W. Legyen $A : W' \to W''$ izometrikus (azaz q-t megtartó) izomorfizmus. Ekkor A kiterjeszthető $\tilde{A} \in O(n)$ ortogonális transzformációvá.*

3.3.3. Következmény. *Legyen $n = 2\nu$ vagy $n = 2\nu + 1$, és legyen $m \leq 2\nu$. Ekkor létezik egy $U \subset k^{n\times m}$ nem-üres nyílt halmaz a következő tulajdonsággal: ha $\left(v^{(1)'}, \dots, v^{(m)'}\right) \in U$ és $\left(v^{(1)''}, \dots, v^{(m)''}\right) \in U$ olyanok, hogy $Q^{(i)'} = Q^{(i)''}$ minden i-re és $B^{(ij)'} = B^{(ij)''}$ minden (i,j) párra, akkor van olyan $A \in O(n)$ ortogonális transzformáció, amellyel $Av^{(i)'} = v^{(i)''}$ minden i-re.*

Bizonyítás. Legyen U az olyan vektor-m-esek halmaza, amelyeknek a $k^n/\ker\beta$ faktortérben adódó képe független vektor-m-es, és amelyek által kifeszített m-dimenziós altéren q nem-elfajuló. Az 1.4.1 állítás segítségével könnyen látható, hogy U nyílt. Bármely U-beli vektor-m-es által kifeszített W altérre $W \cap \ker\beta = 0$. Ha $\left(v^{(1)'}, \dots, v^{(m)'}\right) \in U$ és $\left(v^{(1)''}, \dots, v^{(m)''}\right) \in U$ olyanok, hogy $Q^{(i)'} = Q^{(i)''}$ minden i-re és $B^{(ij)'} = B^{(ij)''}$ minden (i,j) párra, akkor az

$$Av^{(i)'} = v^{(i)''} \qquad (i = 1, \dots, m)$$

által definiált, a kifeszített alterek közötti izometrikus izomorfizmus kiterjeszthető ortogonális transzformációvá. □

3.3.4. Megjegyzés. *A fenti 3.3.3 következmény valójában tetszőleges m esetén is igaz.*

Bizonyítás. Legyen $m \geq n$. Legyen U azon vektor-m-esek halmaza, amelyek első n vektora bázist alkot a k^n térben. Ha két ilyen vektor-m-es kielégíti a 3.3.3 következményben kirótt feltételeket, akkor az a lineáris transzformáció, amely a $v^{(1)'}, \dots, v^{(n)'}$ bázist a $v^{(1)''}, \dots, v^{(n)''}$ bázisba viszi, nyilvánvalóan ortogonális, és megfelelő lesz. □

3.3.5. Állítás. *Legyen m teszőleges pozitív egész, és $\left(\beta^{(ij)}\right)$ teszőleges olyan $m \times m$-es mátrix, melynek rangja $r \leq 2\nu$. Ekkor léteznek $u^{(1)}, \dots, u^{(m)} \in k^{2\nu}$ vektorok úgy, hogy*

$$\beta\left(u^{(i)}, u^{(j)}\right) = \beta^{(ij)} \qquad (i,j = 1, \dots, m).$$

Bizonyítás. Jól ismert, hogy $\left(\beta^{(ij)}\right)$ kogrediens a $J \oplus 0 = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \oplus 0$ mátrixszal, ahol J mérete $r \times r$ (tehát r mindig páros). Ezért elegendő az utóbbi mátrix esetére bizonyítani az állítást, arra pedig triviális. □

3.3.6. Állítás. *Legyen $m \leq n$. Legyen $\left(\beta^{(ij)}\right)$ teszőleges $m \times m$-es alternáló mátrix, és legyenek $q^{(1)}, \ldots, q^{(m)} \in k$ tetszőlegesek. Ekkor léteznek $v^{(1)}, \ldots, v^{(m)} \in k^n$ vektorok úgy, hogy*

$$\beta\left(u^{(i)}, u^{(j)}\right) = \beta^{(ij)} \qquad (i, j = 1, \ldots, m)$$

és

$$q\left(v^{(i)}\right) = q^{(i)} \qquad (i = 1, \ldots, m).$$

Bizonyítás. Legyen, mint mindig, $\nu = [n/2]$. Válasszuk meg az $u^{(1)}, \ldots, u^{(m)} \in k^{2\nu}$ vektorokat az előző állítás szerint.

Legyen először $n = 2\nu + 1$. Mivel a $\ker \beta$ egydimenziós altér nem szinguláris, ezért a q kvadratikus alak minden $\ker \beta$ szerinti mellékosztályon minden értéket felvesz. Van tehát olyan $v^{(i)} \in k^{2\nu+1}$, mely a $k^{2\nu+1} \to k^{2\nu+1}/\ker \beta = k^{2\nu}$ természetes leképezésnél $u^{(i)}$-be megy át, és amelyre $q\left(v^{(i)}\right) = q^{(i)}$. Az így kapott $v^{(1)}, \ldots, v^{(m)}$ vektorok megfelelőek.

Legyen ezután $n = 2\nu$. Tekintsük először azt az esetet, amikor az $u^{(1)}, \ldots, u^{(m)}$ vektorok bázist alkotnak k^n-ben (ekkor persze $m = n$). Definiáljuk a q^* kvadratikus alakot a

$$q^*\left(\sum_{i=1}^{m} \lambda_i u^{(i)}\right) = \sum_{i=1}^{m} \lambda_i^2 q^{(i)} + \sum_{1 \leq i < j \leq m} \lambda_i \lambda_j \beta^{(ij)}$$

formulával. Legyen β^* a q^* polarizáltja. Mivel

$$\beta^*\left(u^{(i)}, u^{(j)}\right) = q^*\left(u^{(i)} + u^{(j)}\right) - q\left(u^{(i)}\right) - q\left(u^{(j)}\right) = \beta^{(ij)} = \beta\left(u^{(i)}, u^{(j)}\right),$$

ezért $\beta^* \equiv \beta$. Emiatt q^* sem elfajuló. Az 1.1.4 állítás miatt van olyan $A : k^n \to k^n$ lineáris izomorfizmus, amellyel $q(Au) = q^*(u)$ minden $u \in k^n$-re. Ekkor persze

$$\beta\left(Au', Au''\right) = \beta^*\left(u', u''\right) = \beta\left(u', u''\right)$$

minden $u', u'' \in k^n$-re (azaz $A \in Sp(n)$). Legyen $v^{(i)} = Au^{(i)}$ $(i = 1, \ldots, m)$. Ekkor

$$\beta\left(v^{(i)}, v^{(j)}\right) = \beta\left(u^{(i)}, u^{(j)}\right) = \beta^{(ij)}$$

és

$$q\left(v^{(i)}\right) = q^*\left(u^{(i)}\right) = q^{(i)},$$

tehát $v^{(1)}, \ldots, v^{(m)}$ megfelelő.

Tekintsük végül azt az esetet, amikor $n = 2\nu$, de az $u^{(1)}, \ldots, u^{(m)}$ vektorok nem feszítik ki a k^n teret. Legyen $0 \neq u^{(0)} \in \left\langle u^{(1)}, \ldots, u^{(m)} \right\rangle^{\perp}$ egy rögzített vektor. Legyen $f : k^n \to k$ olyan lineáris funkcionál, amelyre $f\left(u^{(0)}\right) \neq 0$. Definiáljuk a q^* kvadratikus alakot a

$$q^* = q + \lambda f^2$$

formulával, ahol a $\lambda \in k$ paraméter értéke úgy választandó, hogy $q^*\left(u^{(0)}\right) \neq 0$ legyen. Mivel f^2 polarizáltja azonosan nulla, ezért q^* polarizáltja β. Ebből következik, hogy q^* nem-elfajuló. Tehát van olyan $A : k^n \to k^n$ lineáris izomorfizmus, amellyel $q(Au) = q^*(u)$ minden $u \in k^n$-re. Persze $A \in Sp(n)$. Az $Au^{(i)}$ vektorokra

$$\beta\left(Au^{(i)}, Au^{(j)}\right) = \beta\left(u^{(i)}, u^{(j)}\right) = \beta^{(ij)}.$$

Továbbá $Au^{(0)} \in \left\langle Au^{(1)}, \ldots, Au^{(m)}\right\rangle^{\perp}$ és $q\left(Au^{(0)}\right) \neq 0$. Az utóbbiból következik, hogy q minden $kAu^{(0)}$ szerinti mellékosztályon minden értéket felvesz. Tehát van olyan $v^{(i)} \in Au^{(i)} + kAu^{(0)}$ vektor, amelyre $q\left(v^{(i)}\right) = q^{(i)}$. Az így kapott $v^{(1)}$, ... , $v^{(m)}$ vektorok megfelelőek. □

3.3.7. Tétel. *Legyen $n = 2\nu$ vagy $n = 2\nu+1$, és legyen $m \leq 2\nu$. Ekkor az $R^{O(n)}_{n\times m}$ algebrát generálják a $Q^{(i)}$ és $B^{(ij)}$ invariánsok (ahol $1 \leq i \leq m$, illetve $1 \leq i < j \leq m$).*

Bizonyítás. Jelölje $f : k^{n\times m} \to k^{\binom{m+1}{2}}$ azt a reguláris leképezést, melynek koordinátafüggvényei a $Q^{(i)}$ és $B^{(ij)}$ polinomok. Legyen $h \in R^{O(n)}_{n\times m}$ tetszőleges. A 3.3.3 következmény szerint van egy nem-üres nyílt halmaz, amelyen h csak f-től függ.

Tekintsük azt a vektor-m-est (mint $k^{n\times m}$-beli pontot), amely a k^n tér standard bázisának első m vektorából áll. Megmutatjuk, hogy az f leképezés e pontban vett Jacobi-mátrixának rangja $\binom{m+1}{2}$. Ehhez feltehetjük, hogy $n = 2\nu$. Írjuk fel a parciális deriváltakat:

$$\frac{\partial Q^{(i)}}{\partial x_t^{(i)}} = y_t^{(i)}, \qquad \frac{\partial Q^{(i)}}{\partial y_t^{(i)}} = x_t^{(i)}, \tag{5}$$

a $Q^{(i)}$ polinom többi parciális deriváltja pedig nulla. Tehát a $Q^{(i)}$ parciális deriváltjaiból álló $2\nu \times m$-es mátrixot úgy kapjuk, hogy az i-edik oszlopba beírjuk az i-edik standard bázisvektort úgy, hogy az x_t és y_t koordinátát felcseréljük (egyszerre minden t-re). Továbbá,

$$\frac{\partial B^{(ij)}}{\partial x_t^{(i)}} = y_t^{(j)}, \qquad \frac{\partial B^{(ij)}}{\partial y_t^{(i)}} = x_t^{(j)}, \qquad \frac{\partial B^{(ij)}}{\partial x_t^{(j)}} = y_t^{(i)}, \qquad \frac{\partial B^{(ij)}}{\partial y_t^{(j)}} = x_t^{(i)}, \tag{6}$$

a $B^{(ij)}$ polinom többi parciális deriváltja pedig nulla. Tehát a $B^{(ij)}$ parciális deriváltjaiból álló $2\nu \times m$-es mátrixot úgy kapjuk, hogy az i-edik oszlopba beírjuk a j-edik, a j-edik oszlopba pedig az i-edik standard bázisvektort úgy, hogy az x_t és y_t koordinátát felcseréljük (egyszerre minden t-re).

Azt kell belátnunk, hogy a kapott $\binom{m+1}{2}$ darab 0-1-mátrix lineárisan független. Tekinthetjük helyettük azokat a mátrixokat, amelyeket a standard bázisvektorokból ugyanúgy kapunk, azzal a különbséggel, hogy az $x_t \leftrightarrow y_t$ cserét sehol sem végezzük el. E mátrixok $m\times m$ méretű bal felső sarkai az $m\times m$-es szimmetrikus mátrixok $\binom{m+1}{2}$ dimenziós terének standard bázisát alkotják. Ezzel az f leképezés rangjára vonatkozó állításunkat beláttuk.

A 3.2.10 következmény szerint h racionális függvénye f-nek. De h reguláris, és a 3.3.6 állítás szerint f szürjektív. A 3.2.11 állítás azt adja, hogy h reguláris függvénye f-nek. □

3.4. A racionális invariánsok teste

Ebben az alfejezetben is mindig feltesszük, hogy a k algebrailag zárt test 2 karakterisztikájú.

Mindenekelőtt a 3.3.3 következményt általánosítjuk.

3.4.1. Állítás. *(i) Legyen $n = 2\nu$ és legyen m tetszőleges. Ekkor létezik egy $U \subset k^{n\times m}$ nem-üres nyílt halmaz a következő tulajdonsággal: ha*

$$\left(v^{(1)'}, \ldots, v^{(m)'}\right) \in U \text{ és } \left(v^{(1)''}, \ldots, v^{(m)''}\right) \in U$$

olyanok, hogy

$$\begin{aligned} Q^{(i)'} &= Q^{(i)''} && (1 \le i \le 2\nu), \\ B^{(ij)'} &= B^{(ij)''} && (1 \le i < j \le m, \quad i \le 2\nu), \end{aligned}$$

akkor van olyan $A \in O(n)$ ortogonális transzformáció, amellyel $Av^{(i)'} = v^{(i)''}$ minden $1 \le i \le m$-re.

(ii) Legyen $n = 2\nu + 1$ és legyen m tetszőleges. Ekkor létezik egy $U \subset k^{n\times m}$ nem-üres nyílt halmaz a következő tulajdonsággal: ha

$$\left(v^{(1)'}, \ldots, v^{(m)'}\right) \in U \text{ és } \left(v^{(1)''}, \ldots, v^{(m)''}\right) \in U$$

olyanok, hogy

$$\begin{aligned} Q^{(i)'} &= Q^{(i)''} && (1 \le i \le 2\nu), \\ B^{(ij)'} &= B^{(ij)''} && (1 \le i < j \le m, \quad i \le 2\nu), \\ D^{(1,\cdots,2\nu,l)'} &= D^{(1,\cdots,2\nu,l)''} && (2\nu + 1 \le l \le m), \end{aligned}$$

akkor van olyan $A \in O(n)$ ortogonális transzformáció, amellyel $Av^{(i)'} = v^{(i)''}$ minden $1 \le i \le m$-re.

Bizonyítás. A 3.3.3 következmény miatt feltehetjük, hogy $m \ge 2\nu$. Legyen U azon vektor-m-esek halmaza, amelyek első 2ν vektorának természetes képe bázist alkot a $k^n/\ker\beta$ faktortérben. Egy ilyen vektor-m-es első 2ν vektora mindig olyan 2ν dimenziós W alteret feszít ki, amelyre $W \cap \ker\beta = 0$. Ha $\left(v^{(1)'}, \ldots, v^{(m)'}\right) \in U$ és $\left(v^{(1)''}, \ldots, v^{(m)''}\right) \in U$ teljesítik az állításban kirótt feltételeket, akkor a 3.3.2 állítás miatt van olyan $A \in O(n)$ ortogonális transzformáció, amelyre

$$Av^{(i)'} = v^{(i)''} \qquad (i = 1, \ldots, 2\nu).$$

Megmutatjuk, hogy ez megfelelő lesz.

(i) Mivel β nem-elfajuló és a $v^{(1)''}$, ..., $v^{(2\nu)''}$ vektorok bázist alkotnak a $k^{2\nu}$ térben, ezért elég belátni, hogy $1 \le j \le m$ és $1 \le i \le 2\nu$ esetén

$$\beta\left(v^{(i)''}, Av^{(j)'}\right) = \beta\left(v^{(i)''}, v^{(j)''}\right). \tag{7}$$

Ez világos, mert a bal oldal $\beta\left(Av^{(i)\prime}, Av^{(j)\prime}\right)$-vel, a jobb $\beta\left(v^{(i)\prime}, v^{(j)\prime}\right)$-vel egyenlő, ezek pedig egymással egyenlőek A ortogonális volta miatt.

(ii) A (7) egyenlőség most is ugyanúgy bizonyítható, mint az (i) esetben, de ezúttal csak annyit mutat, hogy $Av^{(j)\prime}$ csak a z koordinátájában különbözhetik $v^{(j)\prime\prime}$-től. A z koordináták egyenlőségének bizonyításához elég megmutatni, hogy

$$\det\left(v^{(1)\prime\prime}, \ldots, v^{(2\nu)\prime\prime}, Av^{(j)\prime}\right) = \det\left(v^{(1)\prime\prime}, \ldots, v^{(2\nu)\prime\prime}, v^{(j)\prime\prime}\right), \tag{8}$$

hiszen ha mindkét determinánst az utolsó oszlop szerint kifejtjük, akkor ugyanazokat a tagokat kapjuk, kivéve az utolsó vektor z-koordinátáját tartalmazó egy-egy tagot, ezekben pedig a két z-koordináta együtthatója ugyanaz a nullától különböző $2\nu \times 2\nu$ méretű aldetermináns.

A (8) egyenlőség azzal ekvivalens, hogy

$$\det\left(Av^{(1)\prime}, \ldots, Av^{(2\nu)\prime}, Av^{(j)\prime}\right) = \det\left(v^{(1)\prime}, \ldots, v^{(2\nu)\prime}, v^{(j)\prime}\right),$$

ez pedig A ortogonális volta miatt fennáll. □

3.4.2. Tétel. *Legyen $m \geq 2\nu$. Ekkor a $K_{2\nu\times m}^{O(2\nu)}$ testet generálják az algebrailag független*

$$Q^{(i)} \qquad (1 \leq i \leq 2\nu)$$

és

$$B^{(ij)} \qquad (1 \leq i < j \leq m, \quad i \leq 2\nu)$$

invariánsok.

Bizonyítás. Jelölje

$$f : k^{2\nu\times m} \to k^{2\nu+\binom{m}{2}-\binom{m-2\nu}{2}} = k^{2\nu m-\binom{2\nu}{2}}$$

azt a reguláris leképezést, melynek koordinátafüggvényei a tételben szereplő invariáns polinomok. Ez domináns, mert ha koordinátafüggvényei számára olyan $q^{(i)}$ és $\beta^{(ij)}$ értékeket írunk elő, hogy a $\left(\beta^{(ij)}\right)_{i,j=1}^{2\nu}$ mátrix reguláris legyen, akkor a 3.3.6 állítás által biztosított $v^{(1)}, \ldots, v^{(2\nu)}$ vektorok bázist alkotnak a $k^{2\nu}$ térben, és ezért kiegészíthetők olyan vektor-m-essé, amelyen f koordinátafüggvényei az előírt értékeket veszik fel. Ezzel beláttuk, hogy a tételben felsorolt invariánsok algebrailag függetlenek.

Tekintsük azt a vektor-m-est (mint $k^{2\nu\times m}$-beli pontot), amely a $k^{2\nu}$ tér standard bázisának 2ν vektorából és $m-2\nu$ darab nullvektorból áll. Megmutatjuk, hogy az f leképezés e pontban vett Jacobi-mátrixának rangja $2\nu m - \binom{2\nu}{2}$.

A parciális deriváltakat megadó (5) és (6) formulák most is érvényesek; az ott nem szereplő parciális deriváltak most is azonosan nullák. Ha tehát $i \leq 2\nu$, akkor a $Q^{(i)}$ parciális deriváltjaiból álló $2\nu \times m$-es mátrixot úgy kapjuk, hogy az i-edik oszlopba beírjuk az i-edik standard bázisvektort úgy, hogy az x_t és y_t koordinátákat felcseréljük. Továbbá, ha $i < j$ és $i \leq 2\nu$, akkor a $B^{(ij)}$ parciális deriváltjaiból álló $2\nu \times m$-es mátrixot úgy kapjuk, hogy az i-edik oszlopba beírjuk a j-edik standard bázisvektort (illetve $j > 2\nu$ esetén a nullvektort), a j-edik oszlopba pedig az i-edik standard bázisvektort úgy, hogy az x_t és y_t koordinátákat felcseréljük.

Azt kell belátnunk, hogy ez a $2\nu m - \binom{2\nu}{2}$ darab 0-1-mátrix lineárisan független. Tekinthetjük helyettük azokat a mátrixokat, amelyeket a standard bázisvektorokból ugyanúgy kapunk, azzal a különbséggel, hogy az $x_t \leftrightarrow y_t$ cserét sehol sem végezzük el. E mátrixok a $2\nu \times m$-es „szimmetrikus" mátrixok $2\nu m - \binom{2\nu}{2}$ dimenziós terének standard bázisát alkotják (szimmetrián azt értjük, hogy ha két elem a bal felső sarokból induló „főátlóra" nézve szimmetrikusan helyezkedik el, akkor egyenlőek). Ezzel az f leképezés rangjára vonatkozó állításunkat beláttuk.

Legyen $h \in K_{2\nu\times m}^{O(2\nu)}$ tetszőleges. A 3.4.1 állítás szerint van egy nem-üres nyílt halmaz, amelyen h (reguláris és) csak f-től függ. A 3.2.10 következmény szerint h racionális függvénye f-nek. □

3.4.3. Megjegyzés. *Ha a tételben szereplő invariánsokhoz hozzáveszünk egy tetszőleges $K_{2\nu\times m}^{SO(2\nu)} \setminus K_{2\nu\times m}^{O(2\nu)}$-beli racionális kifejezést, akkor a $K_{2\nu\times m}^{SO(2\nu)}$ test egy generátorrendszerét kapjuk.*

Bizonyítás. Az előző tétel és a 2.1.5 megjegyzés azonnali következménye. □

3.4.4. Tétel. *Legyen $m \geq 2\nu$. Ekkor a $K_{(2\nu+1)\times m}^{O(2\nu+1)}$ testet generálják az algebrailag független*

$$Q^{(i)} \qquad (1 \leq i \leq 2\nu),$$

$$B^{(ij)} \qquad (1 \leq i < j \leq m, \quad i \leq 2\nu),$$

és

$$D^{(1,\dots,2\nu,l)} \qquad (2\nu + 1 \leq l \leq m)$$

invariánsok.

Bizonyítás. Jelölje

$$f : k^{(2\nu+1)\times m} \to k^{2\nu+\binom{m}{2}-\binom{m-2\nu}{2}+m-2\nu} = k^{2\nu m-\binom{2\nu}{2}+m-2\nu}$$

azt a reguláris leképezést, melynek koordinátafüggvényei a tételben szereplő invariáns polinomok. Ez domináns, mert ha koordinátafüggvényei számára olyan $q^{(i)}$, $\beta^{(ij)}$ és $d^{(1,\dots,2\nu,l)}$ értékeket írunk elő, hogy a $\left(\beta^{(ij)}\right)_{i,j=1}^{2\nu}$ mátrix reguláris legyen, akkor a 3.3.6 állítás által biztosított $v^{(1)}, \dots, v^{(2\nu)}$ vektorok bázist alkotnak a $k^{2\nu+1}/\ker\beta$ faktortérben, és ezért kiegészíthetők olyan vektor-m-essé, amelyen f koordinátafüggvényei az előírt értékeket veszik fel. Ezzel beláttuk, hogy a tételben felsorolt invariánsok algebrailag függetlenek.

Tekintsük azt a vektor-m-est (mint $k^{(2\nu+1)\times m}$-beli pontot), amely a $k^{2\nu+1}$ tér standard bázisának első 2ν vektorából és $m-2\nu$ darab nullvektorból áll. (A nullvektorok helyett tetszőleges $\ker\beta$-beli, azaz a z-tengely irányába mutató vektorokat vehetnénk.) Megmutatjuk, hogy az f leképezés e pontban vett Jacobi-mátrixának rangja $2\nu m - \binom{2\nu}{2} + m - 2\nu$.

A parciális deriváltakat megadó (5) és (6) formulák most is érvényesek; az ott nem szereplő parciális deriváltak most is azonosan nullák. Ha tehát $i \leq 2\nu$, akkor a $Q^{(i)}$ parciális deriváltjaiból álló $(2\nu+1) \times m$-es mátrixot úgy kapjuk, hogy az i-edik oszlopba beírjuk az i-edik standard bázisvektort úgy, hogy az x_t és y_t koordinátákat felcseréljük. Továbbá, ha $i < j$ és $i \leq 2\nu$, akkor a $B^{(ij)}$ parciális deriváltjaiból álló $(2\nu+1) \times m$-es mátrixot úgy kapjuk, hogy az i-edik oszlopba beírjuk a j-edik standard bázisvektort (illetve $j > 2\nu$ esetén a nullvektort), a j-edik oszlopba pedig az i-edik standard bázisvektort úgy, hogy az x_t és y_t koordinátákat felcseréljük. Tehát a $Q^{(i)}$-k és $B^{(ij)}$-k parciális deriváltjaiból álló mátrixok utolsó sorában csupa nulla van, de (mint az előző tétel bizonyításában láttuk) ez a $2\nu m - \binom{2\nu}{2}$ darab mátrix lineárisan független. Ezért elég belátni, hogy a $D^{(1,\ldots,2\nu,l)}$ polinomok parciális deriváltjaiból álló mátrixok utolsó sorai függetlenek. Ez nyilvánvaló: ha $2\nu + 1 \leq l, l' \leq m$, akkor

$$\frac{\partial D^{(1,\ldots,2\nu,l)}}{\partial z^{(l')}} = \delta^{(l)}_{(l')}.$$

Ezzel az f leképezés rangjára vonatkozó állításunkat beláttuk.

Legyen $h \in K^{O(2\nu+1)}_{(2\nu+1)\times m}$ tetszőleges. A 3.4.1 állítás szerint van egy nem-üres nyílt halmaz, amelyen h (reguláris és) csak f-től függ. A 3.2.10 következmény szerint h racionális függvénye f-nek. $\square$

Hivatkozások

[1] C. De Concini, C. Procesi: *A Characteristic Free Approach to Invariant Theory,* Advances in Mathematics **21** (1976), 330 – 354. oldal

[2] M. Domokos, S. G. Kuzmin, A. N. Zubkov: *Rings of matrix invariants in positive characteristic,* J. Pure Appl. Alg., közlésre elfogadva

[3] R. Goodman, N. R. Wallach: *Representations and Invariants of the Classical Groups,* Cambridge University Press, 1998

[4] J. Harris: *Algebraic Geometry – A First Course,* Graduate Texts in Mathematics, Springer-Verlag, 1992

[5] P. Newstead: *Introduction to moduli problems and orbit spaces,* Tata Inst. Lecture Notes, Springer-Verlag, 1978

[6] V. L. Popov, E. B. Vinberg: *Invariant Theory.* In: *Algebraic Geometry IV,* Encyclopedia of Mathematical Sciences **55**, Springer Verlag, 1994

[7] D. R. Richman: *The Fundamental Theorems of Vector Invariants,* Advances in Mathematics **73** (1989), 43 – 78. oldal

[8] E. Study: *Ueber die Invarianten der projectiven Gruppe einer quadratischen Mannigfaltigkeit von nichtverschwindender Discriminante,* Ber. Sächs. Akad. Wissensch. (1897), 443 – 461. oldal

[9] D. E. Taylor: *The Geometry of the Classical Groups,* Heldermann Verlag Berlin, 1992

[10] H. Weyl: *Randbemerkungen zu Hauptproblemen der Mathematik,* Math. Zeitschr. **20** (1924)

[11] H. Weyl: *The Classical Groups – Their Invariants and Representations,* Princeton University Press, 1946

Tartalomjegyzék