Eötvös Loránd Tudományegyetem
Természettudományi Kar
Matematikai Intézet

Tükrözéscsoportok invariánselmélete

Frenkel Péter
Adjunktus

Koltai László András
Matematikus BSc

Budapest, 2019

Köszönetnyilvánítás

Először is, ezúton szeretném megköszönni a témavezetőmnek, Frenkel Péternek, a rengeteg segítséget és támogatást amit már az első félévtől kezdve nyújtott nekem, hogy mindig bizalommal fordulhattam hozzá amikor elbizonytalanodtam, a témafelvetést, a sok konzultációt, illetve, hogy átvészelte a helyesírásomat.

Szeretnék még köszönötet mondani Hoksza Zsoltnak, Némethi Andrásnak és Szűcs Andrásnak, akiknek hála számos érdekes témát ismerhettem meg és tömérdek örömet leltem a matematikában.

Végül szeretném megköszönni a családomnak és barátaimnak, hogy végig mellettem álltak, támogattak, és akik nélkül nem jutottam volna idáig.

Bevezetés

A szakdolgozat célja két tételnek a belátása, az egyik a Chevalley-Shephard-Todd, ami a tükrözéscsoportokat karakterizálja az invariánsgyűrűjükkel, a másik az úgynevezett Poincaré-polinom szorzatra bontása, ami egy tükrözéscsoport növekedését csípi nyakon a csoport invariánsgyűrűjével. Ennek a két tételnek belátásával szeretnénk kis ízelítőt adni az invariánselmélet szépségéből.

A dolgozat tartalma [1] James E. Humphreys - Reflection Groups and Coxeter Groups könyvet követi, kivétel a második fejezet eleje, ahol az [5] és [6] jegyzeteket használtam fel, illetve kivétel még a koinvariánsok modulusa alfejezet amihez [2] és [3] könyveket használtam fel, a dolgozatban még ötletet nyertem [4] cikkből.

A dolgozat két nagy fejezetből áll. Az első fejezetben véges tükrözéscsoportokkal fogunk foglalkozni, ebben bevezetjük a gyökrendszer fogalmát, aminek a segítségével a tükrözéscsoportoknak egy nagyon egyszerű prezentációját adjuk meg. Ezután megnézzük a tükrözcsoportok néhány speciális részcsoportját, majd részletesebben megvizsgáljuk a tükrözéscsoportok fundamentális tartományát, ezeknek kapcsolatát.

A második fejezet elején általánosan véges csoportok invariánsgyűrűjével foglalkozunk, bevezetünk egy átlagoló úgynevezett Reynolds-operátort, aminek a segítségével belátjuk, hogy véges csoport invariánsgyűrűje végesen generált, majd utána az első fejezet tételeit felhasználva belátjuk az előbb említett két főtételt.

Tartalomjegyzék

1. Véges tükrözéscsoportok

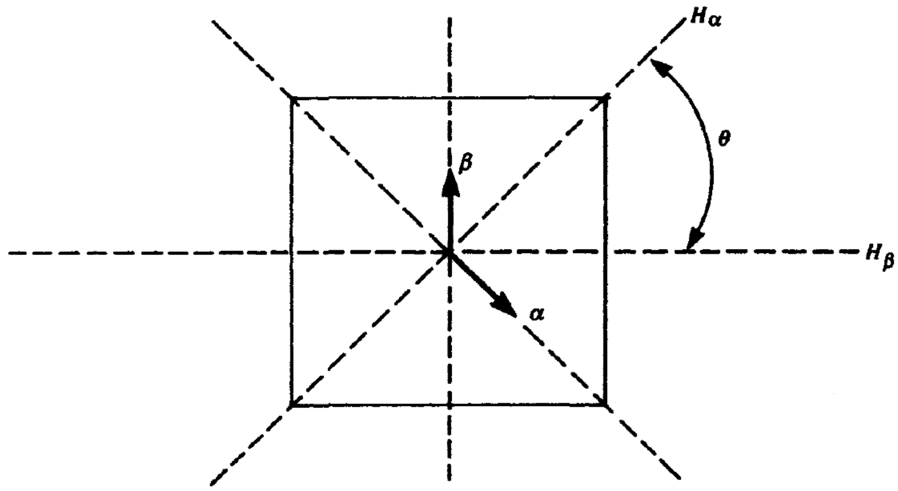
1.1. Tükrözések és gyökrendszerek

Legyen V egy véges dimenziós valós vektortér ellátva egy $(\cdot\,,\cdot)$ pozitív definit szimmetrikus bilineáris formával. Ekkor tükrözés alatt egy olyan s lineáris leképezést értünk, mely egy $\alpha \in V$ vektort elküld a $-\alpha$ vektorba, és közben pontonként fixen hagyja az α-ra merőleges H_α hipersíkot. Jelöljük s_α-val azt a tükrözést, ami az α vektort $-\alpha$ vektorba képzi, és jegyezzük meg, hogy $s_\alpha = s_{c\alpha}$ minden $0 \neq c \in \mathbb{R}$ számra. Egy egyszerű formula az s_α tükrözésre a következő:

$$s_\alpha \lambda = \lambda - 2\frac{(\lambda, \alpha)}{(\alpha, \alpha)}\alpha.$$

Könnyen belátható, hogy ez tényleg jó. Mostantól csak olyan véges csoportokkal fogunk foglalkozni, melyeket ilyen valós tükrözések generálnak. Ezeket nevezzük véges tükrözéscsoportoknak. Néhány példa véges tükrözéscsoportra:

($\mathbf{I}_2(m)$, $m \geq 3$) Legyen V az euklideszi sík, és legyen $\mathcal{D}_m$ a $2m$ rendű diédercsoport, mely azon ortogonális transzformációkból áll, amelyek egy szabályos, m csúcsú, origó középpontú sokszöget önmagába visznek. A $\mathcal{D}_m$ diédercsoport m darab forgatást és m darab tükrözést tartalmaz. Vegyük észre, hogy a forgatások egy 2 indexű részcsoportot alkotnak, amit egy $2\pi/m$ szögű forgatás generál.



1. ábra. m=4 eset

A $\mathcal{D}_m$ csoportot valójában tükrözések generálják, mivel egy $2\pi/m$ szögű forgatás elérhető kettő olyan tükrözés szorzataként, melyeknek a tengelye π/m szöget zár be.

($\mathbf{A}_{n-1}$, $n \geq 2$) Vegyük az $\mathcal{S}_n$ szimmetrikus csoportot. Az $\mathcal{S}_n$ csoportra gondolhatunk úgy is, mint $O(n, \mathbb{R})$ részcsoportja a következő módon: egy permutáció hasson úgy az $\mathbb{R}^n$ vektortéren, hogy permutálja az $e_1, \ldots, e_n$ standard bázisvektorokat. Vegyük észre, hogy egy (ij) transzpozíció tükrözésként hat, mely elküldi az $e_i - e_j$ vektort $-(e_i - e_j)$ vektorba, miközben az ortogonális kiegészítőjét pontonként fixálja. Mivel az $\mathcal{S}_n$ csoportot generálják a transzpozíciók, ezért ez a hatás tényleg egy tükrözéscsoportot ad.

Az imént definiált hatás az $e_1 + \cdots + e_n$ által kifeszített egyenest pontonként fixálja, mig annak ortogonális kiegészítőjét, azt a hipersíkot, melyben minden vektor koordinátáinak összege 0, stabilan hagyja. Tehát $\mathcal{S}_n$ egy $n-1$ dimenziós euklideszi téren is tükrözéscsoportként hat, ahol már egyedül az origó fixpont. Emiatt szerepel $n-1$ az alsó indexben.

($\mathbf{B}_n$, $n \geq 2$) Ismét legyen $V = \mathbb{R}^n$, és $\mathcal{S}_n$ hasson rajta úgy, mint előbb. Egyéb tükrözéseket is definálhatunk úgy, hogy az e_i vektort elküldjük a $-e_i$ vektorba, mig az összes többi e_j báziselemet fixen hagyjuk. Ezek az előjelváltások egy 2^n rendű csoportot generálnak, mely izomorf a $(\mathbb{Z}/2\mathbb{Z})^n$ csoporttal. Az előjelváltások által generált csoport és $\mathcal{S}_n$ csak az identitásban metszik egymást, továbbá egy előjel csere egy transzpozícióval konjugálva ismét előjel cserét ad, tehát $\mathcal{S}_n$ normalizálja az előjelváltásokat. Azt kaptuk tehát, hogy $\mathcal{S}_n$ és az előjelváltások által generált csoport szemidirekt szorzata egy új, $2^n \cdot n!$ rendű tükrözéscsoportot ad. Könnyen ellenőrízhető, hogy az egyetlen fixpont az origó.

($\mathbf{D}_n$, $n \geq 4$) Egy újabb tükrözéscsoportot kapunk az $\mathbb{R}^n$ vektortéren, ha B_n egy 2 indexű részcsoportját vesszük a következőképp: hasson az $\mathcal{S}_n$ csoport úgy mint eddig. Ekkor $\mathcal{S}_n$ nyilván normalizálja azt a csoportot, ami azokat a transzformációkat tartalmazza, amik páros sok e_i előjelét változtatják meg. Könnyen látható, hogy ezt a csoportot generálják azok a tükrözések, amik az $e_i + e_j$ vektort a $-(e_i + e_j)$ vektorba képzik, ahol $i \neq j$. Tehát a szemidirekt szorzatuk ismét egy tükrözéscsoportot ad, melynek $2^{n-1}n!$ a rendje.

Mostantól W egy véges tükrözéscsoportot jelöl, ami egy V euklideszi téren hat. Ahhoz, hogy jobban megértsük W belső struktúráját, előbb vizsgáljuk meg, hogy W hogyan is hat a V téren. Minden s_α tükrözés a W csoportban meghatároz egy H_α tükröző hipersíkot, és egy arra merőleges $L_\alpha = \mathbb{R}\alpha$ egyenest. A következő állítás azt mutatja, hogy W az így nyert egyeneseket permutálja.

1.1. Állítás. *Ha $t \in O(V)$ és $\alpha \in V$ egy nem nulla vektor, akkor $ts_\alpha t^{-1} = s_{t\alpha}$. Speciálisan ha $w \in W$, akkor $s_{w\alpha} \in W$ pontosan akkor, ha $s_\alpha \in W$.*

Bizonyítás. Az nyilvánvaló, hogy a $ts_\alpha t^{-1}$ leképezés a $t\alpha$ vektort a negatívjába küldi, tehát csak azt kell megmutatni, hogy a $H_{t\alpha}$ hipersíkot pontonként fixálja. Vegyük észre, hogy $\lambda \in H_\alpha$ pontosan akkor, ha $t\lambda \in H_{t\alpha}$ mivel $(\lambda.\alpha) = (t\lambda, t\alpha)$, tehát $(ts_\alpha t^{-1})(t\lambda) = ts_\alpha(\lambda) = t\lambda$. □

Tehát W permutálja az $s_\alpha \in W$ tükrözésekhez tartozó L_α egyeneseket, a következő módon: $w(L_\alpha) = L_{w\alpha}$. A W csoport csak az L_α egyenest határozza meg, az α vektort nem, azonban ha minden ilyen egyenesből kiválasztjuk az egység hosszú vektorpárokat, akkor az így kapott vektorok halmaza stabil lesz W hatása alatt. Valójában nekünk most nem is fontos, hogy azonos hosszúságú legyen minden vektor, csak az fontos, hogy stabil legyen W hatása alatt. Például a $\mathcal{D}_4$ diédercsoport stabilan hagyja a következő nyolc vektort:

$$\pm(1,0),\ \pm(1,1),\ \pm(0,1),\ \pm(-1,1).$$

1.2. Definíció. Legyen Φ nem nulla vektorok véges halmaza. A Φ halmazt gyökrendszernek nevezzük, ha teljesül rá a következő 2 feltétel:
($R1$) $\Phi \cap \mathbb{R}\alpha = \{\alpha, -\alpha\}$ minden $\alpha \in \Phi$ esetén
($R2$) $s_\alpha \Phi = \Phi$ minden $\alpha \in \Phi$ esetén

Legyen W az a csoport, amit az s_α ($\alpha \in \Phi$) elemek generálnak, ekkor a W csoportot a Φ gyökrendszerhez asszociált tükrözéscsoportnak nevezzük. A korábbi okoskodás szerint, minden tükrözéscsoport megkapható ilyen módon. Megfordítva, minden W tükrözéscsoport, ami egy Φ gyökrendszerből jön véges. Valóban, minden s_α ($\alpha \in \Phi$), tehát W minden eleme pontonként fixálja a Φ elemei által generált altér ortogonális kiegészítőjét, szóval egyedül az identitás tudja teljesen fixálni Φ minden elemét. Ez azt jelenti, hogy a természetes homomorfizmus a W csoportból a $\mathrm{Sym}(\Phi)$ csoportba injektív, tehát W véges.

1.2. Pozitív és egyszerű rendszer

Fixáljunk a V euklideszi térben egy Φ gyökrendszert, és legyen W a hozzá asszociált tükrözéscsoport. Bár a W csoportot teljesen meghatározza Φ, azért van egy komoly probléma a gyökrendszerekkel, mégpedig az, hogy Φ lehet egy hatalmas halmaz $\dim(V)$-hez képest. Például ha $W = \mathcal{D}_n$, akkor ugyanannyi gyök kell, mint ahány eleme van W csoportnak, közben $\dim(V) = 2$.

Ezt orvosolva, keresünk a Φ gyökrendszerben egy lineárisan független részhalmazt, egy "egyszerű rendszert", amiből valahogy visszakaphatjuk Φ-t. Kicsit pontosabban, azt akarjuk, hogy minden gyök előálljon "egyszerű" gyökök $\mathbb{R}$-lineáris kombinációjaként úgy, hogy minden együttható azonos előjelű legyen. Ilyen módon egy egyszerű rendszer particionálja a Φ halmazt 'pozitív' és 'negatív' gyökökre úgy, hogy minden $\{\alpha, -\alpha\}$ párból pontosan egy lesz pozitív. Ilyen felbontást könnyen kaphatunk, ha bevezetünk egy rendezést a V vektortéren. A V vektortér rendezése alatt egy tranzitív relációt értünk, amit $<$-vel jelölünk, és eleget tesz a következő feltételeknek:

(1) Legyen $\lambda, \mu \in V$, ekkor $\lambda < \mu,\ \lambda = \mu,\ \lambda > \mu$ közül pontosan egy teljesül.

(2) Legyen $\lambda, \mu, \nu \in V$, ekkor ha $\nu < \mu,$ akkor $\lambda + \nu < \lambda + \mu$.

(3) Ha $\nu < \mu,$ és $0 \neq c \in \mathbb{R},$ akkor $c\nu < c\mu$ ha $c > 0,$ és $c\nu > c\mu$ ha $c < 0$.

Ha van egy ilyen rendezésünk, akkor egy $\lambda \in V$ elemet pozitívnak nevezünk, ha $\lambda > 0$. Pozitív elemek összege pozitív, illetve egy pozitív elem pozitív skalárral szorozva pozitív. Most, hogy tudjuk mi a rendezés, adjunk is meg egyet a V vektortéren. Ehhez válasszunk egy tetszőleges $\lambda_1, \ldots, \lambda_n$ rendezett bázist, és a hozzá tartozó lexikografikus rendezést, azaz $\sum_{i=1}^{n} a_i\lambda_i < \sum_{j=1}^{n} b_j\lambda_j$ pontosan akkor ha $a_k < b_k$ az első olyan k indexre, ahol $a_k \neq b_k$.

Visszatérve a Φ gyökrendszerhez, egy $\Pi \subset \Phi$ részhalmazt pozitív rendszernek nevezünk, ha az összes pozitív gyököt tartalmazza V valamilyen rendezésére nézve (negatív gyököt nem tartalmazhat). Az világos, hogy létezik pozitív rendszer, sőt, mivel a gyökök $\{\alpha, -\alpha\}$ párban jönnek, ezért Φ a diszjunkt uniója a Π és a $-\Pi$ halmaznak. Ha Π rögzítve van, akkor $\alpha \in \Pi$ helyett néha azt írjuk, hogy $\alpha > 0$.

Egy $\Delta \subset \Phi$ részhalmazt egyszerűnek nevezünk, ha Δ a Φ által kifeszített altér bázisát adja, továbbá minden $\alpha \in \Phi$ előáll Δ elemeinek azonos előjelű $\mathbb{R}$-lineáris kombinációjaként. A Δ egyszerű rendszer elemeit egyszerű gyököknek hívjuk. Az már egyáltalán nem evidens, hogy létezik egyszerű rendszer.

1.3. Tétel. (a) *Ha Δ egy egyszerű rendszer a Φ gyökrendszerben, akkor egyértelműen létezik egy Π pozitív rendszer, ami tartalmazza a Δ rendszert.*
(b) *Minden Π pozitív rendszer Φ-ben tartalmaz egy egyértelmű Δ egyszerű rendszert, speciálisan létezik egyszerű rendszer.*

Bizonyítás. (a) Tegyük fel, hogy Δ benne van egy Π pozitív rendszerben, akkor minden gyök, ami nem negatív lineáris kombinációja Δ elemeinek szintén Π-ben van (a negatívjaik nem lehetnek benne). Tehát Π rendszert egyértelműen meghatározzák az ilyen gyökök. Ahhoz, hogy lássuk, hogy ilyen rendszer tényleg létezik terjesszük ki a Δ halmazt a V vektortér egy rendezett bázisává, és vegyük az ehhez tartozó lexikografikus rendezést. Legyen Π a Φ gyökrendszer pozitív elemeinek halmaza erre a rendezésre nézve, ekkor nyilván $\Delta \subset \Pi$.

(b) Egy pillanatra tegyük fel, hogy már van egy Π pozitív rendszerünk ami tartalmaz egy Δ egyszerű rendszert. A Δ rendszert úgy karakterizálhatjuk, mint azon $\alpha \in \Pi$ gyökök halmaza, melyek nem fejezhetőek ki kettő vagy több pozitív gyök szigorúan pozitív együtthatójú lineáris kombinációjaként. Tehát Δ egyértelműen meg van határozva Π által.

Már csak az a kérdés, hogy hogy találunk Δ egyszerű rendszert ha már megvan Π. Ehhez válasszuk a lehető legkisebb Δ részhalmazát Π-nek, ami még eleget tesz annak, hogy Π minden eleme előáll Δ elemeinek pozitív lineáris kombinációjaként. Ilyen halmaz létezik, például Π ilyen. Nekünk már csak azt kell belátnunk, hogy Δ elemei lineárisan függetlenek. A függetlenség a következő geometriai feltétel következménye lesz, amint mindjárt be is látunk.

$$(\alpha, \beta) \leq 0 \text{ minden } \alpha \neq \beta \in \Delta \text{ párra.} \tag{1.1}$$

Ha feltesszük, hogy az 1.1. egyenlet igaz, akkor nézzük meg, hogy mi lenne ha Δ nem lenne linárisan független, azaz $\sum_{\alpha \in \Delta} a_\alpha \alpha = 0$, ahol nem minden $a_\alpha = 0$. Hozzuk az egyenletet a következő alakra: $\sum b_\beta \beta = \sum c_\gamma \gamma$, ahol szummákat Δ két diszjunkt részhalmazán vesszük, és minden együttható szigorúan pozitív. Jelölje az összeget σ. Mivel σ pozitív elemek összege, ezért $\sigma > 0$, viszont az 1.1 miatt a következőt kapjuk:

$$0 \leq (\sigma, \sigma) = \left(\sum b_\beta \beta, \sum c_\gamma \gamma \right) \leq 0.$$

Tehát $\sigma = 0$, ami ellentmondás, tehát Δ lineárisan független.

Már csak azt kell belátni, hogy az 1.1. egyenltőtlenség tényleg igaz. Tegyük fel, hogy valamilyen $\alpha \neq \beta \in \Delta$ párra nem teljesül. A tükrözés formulája szerint akkor $s_\alpha \beta = \beta - c\alpha$, ahol $c = 2(\beta, \alpha)/(\alpha, \alpha) > 0$. Mivel $s_\alpha \beta \in \Phi$, ezért vagy ő vagy a negatívja benne van a Π pozitív rendszerben. Tegyük fel, hogy $s_\alpha \beta \in \Pi$, ekkor $s_\alpha \beta = \sum c_\gamma \gamma$, ahol $\gamma \in \Delta$ és $c_\gamma \geq 0$. Ha $c_\beta < 1$, akkor azt kapjuk, hogy $s_\alpha \beta = \beta - c\alpha = c_\beta \beta + \sum_{\gamma \neq \beta} c_\gamma \gamma$, vagyis $(1 - c_\beta)\beta$ előáll $\Delta \backslash \{\beta\}$ elemeinek pozitív együtthatós lineáris kombinációjaként, tehát β elhagyható, ami ellentmond Δ minimalitásának. Ha $c_\beta \geq 1$, akkor viszont azt kapjuk, hogy $0 = (c_\beta - 1)\beta + c\alpha + \sum_{\gamma \neq \beta} c_\gamma \gamma$, na de Δ elemeinek egy nem negatív együtthatós lineáris kombinációja, ahol legalább egy együttható szigorúan pozitív, nem lehet 0 a rendezés definíciója szerint. Tehát $s_\alpha \beta$ nem lehet pozitív. Hasonló érveléssel belátható, hogy $s_\alpha \beta$ negatív sem lehet, ami ellentmondás, tehát igaz az 1.1. egyenlőtlenség. $\square$

Mivel a Π pozitív rendszer egyértelműen meghatározza a benne lévő Δ egyszerű rendszert, ezért azt kaptuk, hogy az előző bizonyításban szereplő 1.1. egyenlőtlenség valójában minden egyszerű rendszerre fennál, tehát fennáll a következő állítás.

1.4. Állítás. *Ha Δ egy egyszerű rendszer a Φ gyökrendszerben, akkor $(\alpha, \beta) < 0$ minden $\alpha \neq \beta \in \Delta$ párra.* $\square$

Az imént megmutattuk, hogy a pozitív és az egyszerű rendszerek egyértelműen meghatározzák egymást, viszont még mindig fennáll az a kellemetlen lehetőség, hogy két különböző egyszerű rendszer geometriailag teljesen különböző, ezért vizsgáljuk meg alaposabban a kapcsolatot két rendszer között.

A definícióból egyértelműen következik, hogy ha Δ egyszerű rendszer Π pozitív rendszerrel és $w \in W$, akkor $w\Delta$ szintén egyszerű rendszer $w\Pi$ pozitív rendszerrel. Ahhoz, hogy jobban megértsük az átjárást Π és $w\Pi$ között, először nézzünk meg egy speciális esetet, ahol $w = s_\alpha$, $\alpha \in \Delta$ egyszerű gyök. A következő állítás szerint ekkor Π és $s_\alpha\Pi$ pontosan egy gyökben tér el.

1.5. Állítás. *Legyen Δ egyszerű rendszer a Π pozitív rendszerben. Ha $\alpha \in \Delta$, akkor $s_\alpha(\Pi\backslash\{\alpha\}) = \Pi\backslash\{\alpha\}$.*

Bizonyítás. Legyen $\alpha \neq \beta \in \Pi$, ekkor $\beta = \sum_{\gamma\in\Delta} c_\gamma\gamma$, ahol $c_\gamma \geq 0$. Mivel az α gyök többszörösei a Φ gyökrendszerben $\pm\alpha$, ezért létezik egy $\gamma \neq \alpha$, amire $c_\gamma > 0$. Most alkalmazzuk mindkét oldalra az s_α leképezést: $s_\alpha\beta = \beta - c\alpha = \sum_{\gamma\in\Delta} c_\gamma\gamma - c\alpha$. Azt kaptuk, hogy $s_\alpha\beta$ egyszerű gyökök egy olyan lineáris kombinációja, amiben γ együtthatója változatlan. Mivel $s_\alpha\beta \in \Phi$, azaz $s_\alpha\beta$ továbbra is gyök, ezért minden együtthatónak azonos előjelűnek kell lennie, tehát $\beta \in \Pi$. Az $s_\alpha\beta$ gyök nem lehet α, mivel ha az lenne akkor azt kapnánk, hogy: $\beta = s_\alpha s_\alpha\beta = -\alpha$, ami ellentmondás, hiszen $-\alpha$ nem lehet a Π pozitív rendszerben. Tehát s_α a $\Pi\backslash\{\alpha\}$ egy önmagáró menő bijekciója. □

1.6. Tétel. *Bármely két pozitív rendszer a Φ gyökrendszerben ekvivalens egymással W alatt.*

Bizonyítás. Legyen Π és Π' két pozitív rendszer. Az $r = \mathrm{Card}(\Pi \cap -\Pi')$ szerint indukciózunk. Ha $r = 0$, akkor $\Pi = \Pi'$ és kész is vagyunk. Ha $r > 0$, akkor a $\Delta \subset \Pi$ egyszerű rendszer nem lehet teljesen a Π' pozitív rendszerben. Legyen $\alpha \in \Delta \cap -\Pi'$. Az előző állítás szerint $\mathrm{Card}(s_\alpha\Pi \cap -\Pi') = r - 1$. Az indukciós feltevés szerint ekkor létezik egy $w \in W$, hogy $w(s_\alpha\Pi) = \Pi'$. □

Most rögzítsünk egy Δ egyszerű rendszert a Φ gyökrendszerben. Az előző tétel szerint nem igazán számít, hogy melyik konkrét egyszerű rendszert választjuk. A következő célunk az, hogy belássuk, hogy a W csoportot generálják az egyszerű tükrözések, azaz az s_α, $\alpha \in \Delta$ alakú tükrözések. Először is, definiáljuk egy $\beta \in \Phi$ gyök magasságát. Írjuk fel a β gyököt az egyszerű gyökök lineáris kombinációjaként: $\beta = \sum_{\gamma\in\Delta} c_\gamma\gamma$, és legyen $\mathrm{ht}(\beta) = \sum c_\gamma$ a β gyök magassága a Δ egyszerű rendszerre nézve. Egyből adódik, hogy $\mathrm{ht}(\beta) = 1$ pontosan akkor, ha $\beta \in \Delta$.

1.7. Tétel. *Rögzített Δ egyszerű rendszer mellett, W csoportot generálják az s_α, $\alpha \in \Delta$ alakú tükrözések.*

Bizonyítás. Jelölje W' azt a csoportot, amit generálnak az s_α, $\alpha \in \Delta$ alakú tükrözések. Pár apró lépésben belátjuk, hogy $W = W'$.

(1) Ha $\beta \in \Pi$, akkor vizsgáljuk a $W'\beta \cap \Pi$ halmazt. Ez a halmaz nem üres, mivel β benne van, szóval választhatunk belőle egy minimális magasságú γ elemet. Azt állítjuk, hogy $\gamma \in \Delta$. Írjuk fel a γ gyököt egyszerű gyökök összegeként: $\gamma = \sum_{\alpha\in\Delta} c_\alpha\alpha$,

és vegyük észre, hogy $(\alpha, \alpha) = \sum c_\alpha(\gamma, \alpha)$, ami miatt $(\gamma, \alpha) > 0$ valamilyen α egyszerű gyökre. Ha $\gamma = \alpha$, akkor kész vagyunk, különben vizsgáljuk az $s_\alpha\gamma$ gyököt, ami az 1.5. állítás szerint pozitív. Mivel $s_\alpha\gamma$ gyököt úgy kapjuk, hogy levonjuk belőle α egy pozitív többszörösét, ezért $\mathrm{ht}(s_\alpha\gamma) < \mathrm{ht}(\gamma)$, és kész is az vagyunk, mivel $s_\alpha\gamma \in W'\beta \cap \Pi$, ami ellentmond γ választásának.

(2) Következő lépésként azt látjuk be, hogy $W'\Delta = \Phi$. Az imént épp azt mutattuk meg, hogy egy tetszőleges $\beta \in \Pi$ pozitív gyök W'-orbitja belemetsz a Δ egyszerű rendszerbe, tehát $\Pi \subset W'\Delta$. Másrészt, ha β negatív, akkor $-\beta \in \Pi$ pozitív gyök ekvivalens valami $\alpha \in \Delta$ gyökkel, azaz létezik egy $w' \in W'$ elem, amire $-\beta = w'\alpha$. Ha $-\beta = w'\alpha$ akkor $\beta = (w's_\alpha)\alpha$, ahol $w's_\alpha \in W'$, tehát $-\Pi \subset W'\Delta$.

(3) Végül vegyünk egy tetszőleges s_β generátorát a W tükrözéscsoportnak. Az előző lépés szerint $\beta = w'\alpha$, valamilyen $w \in W'$, és $\alpha \in \Delta$ elemekre. Akkor az 1.1. állítás szerint $s_\beta = ws_\alpha w^{-1} \in W'$, ami miatt $W' = W$. □

Az előző bizonyítás (1)-es részének triviális következménye a következő kis állítás, ami azt állítja, hogy tetszőleges $\beta \in \Phi$ gyök orbitja belemetsz egy előre rögzített Δ egyszerű rendszerbe.

1.8. Állítás. *Rögzítsük a Δ egyszerű rendszert, ekkor tetszőleges $\beta \in \Phi$ gyökhöz létezik egy $w \in W$ elem, melyre $w\beta \in \Delta$.* □

Most hogy láttuk, hogy a W csoportot egészen kevés tükrözéssel is tudjuk generálni, nekiállhatunk megkonstruálni W egy hatékony prezentációját, felhasználva az imént kapott generátorokat és a hozzájuk tartozó relációkat. Néhány reláció az s_α, $\alpha \in \Delta$ elemek között egyből adódik, ezek a következők:

$$(s_\alpha s_\beta)^{m(\alpha,\beta)} = 1,$$

ahol $m(\alpha, \beta)$ az $s_\alpha s_\beta$ szorzat rendje a W csoportban. A következő fejezetekben azt akarjuk belátni, hogy ezek a triviális relációk már elegek is lesznek nekünk, de ehhez előbb szükségünk lesz egy speciális függvényre.

1.3. Hosszfüggvény

Ahhoz, hogy megkaphassuk a kívánt prezentációját a W csoportnak, először alaposan szemügyre kell venni, hogy miképp is írható fel egy tetszőleges $w \in W$ elem egyszerű tükrözések szorzataként, mondjuk $w = s_1 \dots s_r$ alakban, ahol $s_i = s_{\alpha_i}$ valamilyen $\alpha_i \in \Delta$ egyszerű gyökre. Legyen egy $w \in W$ hossza $\ell(w)$ (egy rögzített Δ egyszerű rendszerre nézve) a minimuma azon r-eknek, amire létezik r tényezős, egyszerű tükrözésekből álló kifejezése a w elemnek. Egy minimális hosszú kifejezését a w elemnek hívjunk redukáltnak, és konvenció szerint legyen $\ell(1) = 0$.

Egyből adódik, hogy $\ell(w) = 1$ pontosan akkor, ha $w = s_\alpha$, ahol $\alpha \in \Delta$. Az is egyből látszik, hogy $\ell(w) = \ell(w^{-1})$, hiszen $w^{-1} = s_r \dots s_1$ miatt $\ell(w^{-1}) \leq \ell(w)$, és hasonlóan kapjuk a másik egyenlőtlenséget. A másik könnyen látható tulajdonsága a hosszfüggvénynek abból jön, hogy minden tükrözésnek -1 a determinánsa, és emiatt:

$$det(w) = (-1)^{\ell(w)}.$$

Sőt, ha w felírható r darab (egyszerű) tükrözés szorzataként, akkor r paritása megegyezik $\ell(w)$ paritásával. Ebből egyből következik, hogy $\ell(ww')$ paritása megegyezik $\ell(w)+\ell(w')$ paritásával, speciálisan, ha $\ell(w) = r$ és $\alpha \in \Delta$, akkor $\ell(s_\alpha w)$ vagy $r-1$ vagy $r+1$.

Következőnek azt szeretnénk belátni, hogy $\ell(w)$ geometriailag úgy jellemezhető, mint azon pozitív gyökök száma, amiket w negatív gyökbe képez. Vegyük észre, hogy ha $w = s_\alpha$ egyszerű tükrözés, akkor pont az 1.5. állítást kapjuk vissza. Ahhoz, hogy ezt a jellemzését az ℓ hosszfüggvénynek igazolhassuk, előbb kicsit alapozzunk.

Rögzítsünk egy Δ egyszerű rendszert a hozzá tartozó Π pozitív rendszerrel együtt. Legyen $n(w) = \mathrm{Card}(\Pi \cap w^{-1}(-\Pi))$. Vegyük észre, hogy $n(w) = n(w^{-1})$, mivel: $\Pi \cap w^{-1}(-\Pi) = w^{-1}(w\Pi \cap -\Pi) = -w^{-1}(\Pi \cap w(-\Pi))$, aminek ugyanakkora a számossága, mint a $\Pi \cap w(-\Pi)$ halmaznak.

1.9. Lemma. *Legyen $\alpha \in \Delta$, $w \in W$. Ekkor fennállnak a következők:*

(*a*) *Ha $w\alpha > 0$, akkor $n(ws_\alpha) = n(w) + 1$;*

(*b*) *Ha $w\alpha < 0$, akkor $n(ws_\alpha) = n(w) - 1$;*

(*c*) *Ha $w^{-1}\alpha > 0$, akkor $n(s_\alpha w) = n(w) + 1$;*

(*d*) *Ha $w^{-1}\alpha < 0$, akkor $n(s_\alpha w) = n(w) - 1$.*

Bizonyítás. Legyen $\Pi(w) = \Pi \cap w^{-1}(-\Pi)$, így $n(w) = \mathrm{Card}\,\Pi(w)$. Ha $w\alpha > 0$, akkor $\Pi(ws_\alpha)$ megegyezik $s_\alpha\Pi(w)$ és $\{\alpha\}$ diszjunkt uniójával, hála az 1.5. állításnak. Ha $w\alpha < 0$, akkor hasonlóan az 1.5. állításból következik, hogy $s_\alpha\Pi(ws_\alpha) = \Pi(w)\backslash\{\alpha\}$, mivel most $\alpha \in \Pi(w)$. Így megvan az (a), és (b). Ahhoz, hogy megkapjuk (c)-t és (d)-t, w helyett írjunk w^{-1}-et, és használjuk azt, hogy $n(w^{-1}s_\alpha) = n(s_\alpha w)$. □

1.10. Következmény. *Ha $w \in W$, akkor $n(w) \leq \ell(w)$.*

Bizonyítás. Tegyük fel, hogy $\ell(w) = r$, tehát $w = s_1 \dots s_r$, ahol mindegyik s_i egyszerű tükrözés. Ekkor ahogy r lépésben építjük fel a w elemet, úgy az n függvény értéke minden lépésben legfeljebb eggyel nőhet. □

A következő központi eredmény megmutatja, hogy egyszerű tükrözések szorzatát hogy lehet rövidíteni, ha még nem a lehető legrövidebb.

1.11. Tétel. *Rögzítsünk egy Δ egyszerű rendszert. Legyen $w = s_1 \dots s_r$ egy tetszőleges megadása a w elemnek egyszerű tükrözések szorzataként ($s_i = s_{\alpha_i}$, és az ismétlés megengedett). Tegyük fel, hogy $n(w) < r$. Akkor léteznek olyan $1 \leq i < j \leq r$ indexek, melyekre teljesülnek a következők:*

(a) $\alpha_i = (s_{i+1} \dots s_{j-1})\alpha_j$;

(b) $s_{i+1}s_{i+2} \dots s_j = s_i s_{i+1} \dots s_{j-1}$;

(c) $w = s_1 \dots \widehat{s_i} \dots \widehat{s_j} \dots s_r$, *ahol a kalap a kihagyást jelöli.*

Bizonyítás. (a) Mivel $n(w) < r$, ezért az előző lemma (a) részének iterálása azt mutatja, hogy létezik egy $j \leq r$ index, amire $(s_1 \dots s_{j-1})\alpha_j < 0$. Mivel $\alpha_j > 0$, ezért léteznie kell egy $i < j$ indexnek, amire $s_i(s_{i+1} \dots s_{j-1})\alpha_j < 0$, amíg az $(s_{i+1} \dots s_{j-1})\alpha_j > 0$. Abban az esetben, ha $i = j - 1$, az $s_{i+1} \dots s_{j-1}$ szorzatot identitásnak értelmezzük. Most emlékezzünk vissza az 1.5. állításra, ami szerint az s_i tükrözés egyedül az α_i gyököt képzi negatívba, tehát $(s_{i+1} \dots s_{j-1})\alpha_j = \alpha_i$.

(b) Legyen $\alpha = \alpha_j$, $w' = s_{i+1} \dots s_{j-1}$, így $w'\alpha = \alpha_i$ hála az (a) résznek. Az 1.1. állítás szerint $w's_\alpha w'^{-1} = s_{w'\alpha} = s_{\alpha_i}$, ami azt jelenti hogy:

$$(s_{i+1} \dots s_{j-1})s_j(s_{j-1} \dots s_{i+1}) = s_i$$

Ha most mindkét oldalt megszorozzuk jobb oldalról az $s_{i+1} \dots s_{j-1}$ szorzattal, akkor pontosan kívánt egyenletet kapjuk.

(c) Ez csak a (b) részben lévő egyenlet egy átírása. Szorozzuk be a (b) részbeli egyenletet jobbról az s_j egyszerű tükrözéssel, hogy megkapjuk a következő egyenletet:

$$s_{i+1} \dots s_{j-1} = s_i \dots s_j.$$

Ha az imént kapott egyenletet visszaírjuk az eredetibe, akkor megkapjuk a (c) részbeli egyenletet. □

1.12. Következmény. *Ha $w \in W$, akkor $n(w) = \ell(w)$.*

Bizonyítás. A 1.9. lemma következménye miatt $n(w) \leq \ell(w)$. Tegyük fel, hogy $n(w) < \ell(w) = r$, és legyen $w = s_1 \dots s_r$ a w elem egy redukált kifejezése. Az előző tétel (c) része szerint az w elemet felírhatom $r - 2$ egyszerű tükrözés szorzataként, ami ellentmond annak, hogy $\ell(w) = r$. □

Miután sikerült azonosítanunk az ℓ és n függvényt, az 1.9. lemmát átfogalmazhatjuk úgy, hogy $\ell(ws_\alpha) = \ell(w) + 1$ ha $w\alpha > 0$, illetve $\ell(ws_\alpha) = \ell(w) - 1$ ha $w\alpha < 0$. Az előző tétel (c) részét is újraértelmezhetjük a következő módon: ha adott egy $w = s_1 \dots s_r$ nem redukált kifejezés, akkor léteznek olyan $1 \leq i < j \leq r$ indexek, melyre $w = s_1 \dots \widehat{s_i} \dots \widehat{s_j} \dots s_r$. Ezt később törlési feltételnek fogjuk hívni. A törlési feltétel szerint akárhogy kapjuk a w elemet egyszerű tükrözések szorzataként, a megfelelő párok kidobálásával mindig eljutunk a w elem egy redukált kifejezéséig.

Ahhoz, hogy jobban értsük mit is mond a következmény, hasznos lehet megnézni, hogy egy adott w elem esetén hogy lehet felsorolni $\Pi(w)$ elemeit. Mivel $\mathrm{Card}\,\Pi(w) = n(w) = \ell(w)$, ezért a megoldás biztosan összefügg valahogy $w = s_1 \dots s_r$ ($s_i = s_{\alpha_i}$) redukált kifejezésével. Valóban, ha adva van w egy redukált kifejezése, akkor a vegyük a következő r gyököt:

$$\beta_i := s_r s_{r-1} \dots s_{i+1}(\alpha_i), \text{ és } \beta_r := \alpha_r.$$

Azt állítjuk, hogy $\Pi(w) = \{\beta_1, \dots, \beta_r\}$, ahol minden β_i különböző. Ahhoz, hogy ezt lássuk, legyen $\beta \in \Pi(w)$. Mivel $\beta > 0$, de $w\beta < 0$, ezért létezik olyan $i \leq r$ index, amire $s_{i+1} \dots s_r(\beta) > 0$, de $s_i \dots s_r(\beta) < 0$; abban az esetben, ha $i = r$, értelmezzük az $s_{i+1} \dots s_r$ szorzatot identitásnak. Tehát a β pozitív gyököt s_i negatívba képzi, és ekkor az 1.5. állítás szerint $s_{i+1} \dots s_r(\beta) = \alpha_i$, ami átrendezve azt adja, hogy $\beta = \beta_i$. Tehát $\Pi(w) \subseteq \{\beta_1 \dots \beta_r\}$, viszont $\mathrm{Card}\,\Pi(w) = r$, és így valójában $\Pi(w)$ megegyezik a $\{\beta_1 \dots \beta_r\}$ halmazzal, speciálisan minden β_i különböző.

Az 1.7. tétel szerint W tranzitívan permutálja a pozitív rendszereket, a 1.12. következmény pedig egyből maga után vonja a következő tételt, ami azt mutatja, hogy a W csoport hatása reguláris a pozitív rendszereken.

1.13. Tétel. *Legyen Δ egyszerű rendszer, és Π a hozzátartozó pozitív rendszer. Legyen $w \in W$, ekkor a következő állítások ekvivalensek:*

(*a*) $w\Pi = \Pi$;

(*b*) $w\Delta = w\Delta$;

(*c*) $n(w) = 0$;

(*d*) $\ell(w) = 0$;

(*e*) $w = 1$. □

A regularitásnak van egy érdekes következménye, amit megéri alaposabban megvizsgálni. A definíciók egy egyszerű következménye, hogy $-\Pi$ pozitív rendszer pontosan akkor, ha Π az. Az előző lemma szerint létezik egyértelműen egy $w_\circ \in W$ elem, ami a Π rendszert a $-\Pi$ rendszerbe képzi. Ráadásul $\ell(w_\circ) = n(w_\circ) = \mathrm{Card}(\Pi)$ a lehető legnagyobb, és nincs mégegy elem a W csoportban ami ilyen hosszú, speciálisan $w_\circ^{-1} = w_\circ$. Ennek van egy érdekes következménye. Legyen adva $w = s_1 \dots s_r$ redukált kifejezés, ekkor elkezdhetjük a w elemet jobbról szorozgatni egyszerű tükrözésekkel úgy, hogy mindig nőjön eggyel a hossza egészen addig amíg ez nem válik lehetlenné és megkapjuk a $w_\circ$ elemet. Tehát $w_\circ = ww'$, ahol $\ell(w_\circ) = \ell(w) + \ell(w')$ valamilyen $w' \in W$ elemre. Ezt átfogalmazva a következőt kaptuk:

$$\ell(w_\circ w) = \ell(w_\circ) - \ell(w), \text{ minden } w \in W \text{ elemre.}$$

1.4. Generátorok és relációk

Most már készen állunk ahhoz, hogy ellenőrízzük a W csoport korábban említett prezentációját. Emlékeztetőül $m(\alpha, \beta)$ az $s_\alpha s_\beta$ elem rendje a W csoportban.

1.14. Tétel. *Rögzítsünk egy Δ egyszerű rendszert a Φ gyökrendszerben. Ekkor a W csoportnak egy prezentációját adja az $S = \{s_\alpha \mid \alpha \in \Delta\}$ halmaz mint generátorrendszer a következő relációkkal:*

$$(s_\alpha s_\beta)^{m(\alpha,\beta)} = 1,\ \ \alpha, \beta \in \Delta.$$

Bizonyítás. Azt szeretnénk belátni, hogy ha a W csoportban fennáll valamilyen reláció, akkor az az előbb megadottak következménye. Pontosabban azt kell megmutatni, hogy minden

$$s_1 \dots s_r = 1,\ \text{ahol } s_i = s_{\alpha_i},\ \ \alpha_i \in \Delta \tag{1.2}$$

reláció kifejezhető a már megadott relációkkal. Vegyük észre, hogy r csakis páros lehet, mivel $\det(s_i) = (-1)$. Ha $r = 2$, akkor azt az egyenletet kapjuk, hogy $s_1 s_2 = 1$, amiből azt kapjuk, hogy $s_1 = s_2^{-1} = s_2$, mivel fennál az a reláció, hogy $s_2^2 = 1$. Az $r = 2q$ szerinti indukcióval haladunk tovább, ahol $q > 1$. Az $s_i^2 = 1$ relációt rendszeresen alkalmazzuk amikor újra akarunk írni egy egyenletet. Így például az 1.2. egyenlet a következő alakra hozható:

$$s_{i+1} \dots s_r s_1 \dots s_i = 1. \tag{1.3}$$

Ha most adva van az $r = 2q$ hosszú reláció, akkor rendezzük át úgy, hogy az első $q + 1$ elemet a bal oldalon hagyjuk, és a maradékot átvisszük jobb oldalra, azaz vizsgáljuk a következő egyenletet:

$$s_1 \dots s_{q+1} = s_r \dots s_{q+2}.$$

Mivel a jobb oldal legföljebb $q-1$ hosszú lehet, ezért a bal oldal nem lehet redukált kifejezés, tehát 1.11. tétel szerint léteznek olyan $1 \leq i < j \leq q + 1$ indexek, melyre

$$s_{i+1} \dots s_j = s_i \dots s_{j-1}. \tag{1.4}$$

Ha most rendezzük az egyenletet, akkor a következő relációt kapjuk:

$$s_i \dots s_{j-1} s_j \dots s_{i+1} = 1. \tag{1.5}$$

Ha az 1.5. egyenlet r-nél kevesebb tükrözést tartalmaz, akkor az indukciós feltevés szerint ezt a relációt levezethetjük a már meglévő relációkból. Így az egy megengedett lépés, hogy az 1.2. egyenletben az $s_{i+1} \dots s_j$ szorzatot kicseréljük az $s_i \dots s_{j-1}$

szorzattal, és a következő alakra hozzuk:

$$s_1 \dots s_i(s_i \dots s_{j-1})s_{j+1} \dots s_r = s_1 \dots \widehat{s_i} \dots \widehat{s_j} \dots s_r = 1.$$

Ismét az indukciós feltevés szerint ez a már meglévő relációkból levezethető, tehát az 1.2. egyenlet is levezethető a már meglévőkből. Az egyedüli probléma akkor van, ha az 1.5. egyenlet továbbra is r tükrözést tartalmaz. Ez csak akkor ferdulhat elő, ha $i = 1, j = q + 1$, és akkor az 1.4. egyenlet a következő:

$$s_2 \dots s_{q+1} = s_1 \dots s_q. \tag{1.6}$$

Ezt a zsákutcát megpróbálhatjuk úgy elkerülni, hogy az eredeti relációnkat más alakra hozzuk, mondjuk a következőre:

$$s_2 \dots s_r s_1 = 1$$

Így, ha megismételjük az előző lépéseket kész leszünk kivéve egy esetben, ha azt kapjuk, hogy:

$$s_3 \dots s_{q+2} = s_2 \dots s_{q+1} \tag{1.7}$$

Ha most az 1.6. és az 1.7. is fennáll, akkor egy másik stratégia kell. Ha be tudnánk látni, hogy az 1.7. egyenlet szintén a korábbi relációkból levezethető, akkor azt be tudnánk írni az eredeti relációba, és ugyanúgy kész lennénk mint először. Írjuk át újra az 1.7. egyenletet, hogy a következőt kapjuk:

$$s_3(s_2 s_3 \dots s_{q+1})s_{q+2} s_{q+1} \dots s_4 = 1$$

A bal oldal most megint r darab tükrözést tartalmaz, tehát újra próbálkozhatunk az eredeti érvelésünkkel. Ez az érvelés helyes lesz, kivéve egy esetet, ha azt kapjuk, hogy:

$$s_2 \dots s_{q+1} = s_3 s_2 s_3 \dots s_q. \tag{1.8}$$

Viszont ha az 1.8. és az 1.6. egyszerre teljesül, akkor azt kapjuk, hogy $s_1 = s_3$. Hasonlóan, ha ciklikusan permutálnánk az elemeket, akkor az eredeti érvelésünkkel kész lehetnénk, kivéve ha $s_2 = s_4$. Ha ezt lépésről lépésre folytatnánk, akkor vagy valamikor kész lennénk az eredeti érvelésünkkel, vagy abba az esetbe ütköznénk, hogy $s_1 = s_3 = \dots = s_{r-1}$ és $s_2 = s_4 = \dots = s_r$. Na de ha ezt visszahelyettesítjük az 1.2. eredeti relációnkba, akkor a következőt kapjuk:

$$s_\alpha s_\beta s_\alpha s_\beta \dots s_\alpha s_\beta = 1,$$

ami triviális következménye az $(s_\alpha s_\beta)^{m(\alpha,\beta)} = 1$ relációnak. □

1.5. Parabolikus részcsoport

Ebben a fejezetben W részcsoportjait szeretnénk jobban megérteni, azon belül is speciális típusú részcsoportokat, olyanokat, amiket néhány egyszerű tükrözés generál. Ehhez vezessünk be néhány új jelölést. Rögzített Δ egyszerű rendszer mellett legyen $S = \{s_\alpha \mid \alpha \in \Delta\}$ az egyszerű tükrözések halmaza. Tetszőleges $I \subseteq S$ halmaz esetén legyen W_I a W csoportnak az a részcsoportja, amit az $s_\alpha \in I$ elemek generálnak, és legyen $\Delta_I = \{\alpha \in \Delta \mid s_\alpha \in I\}$. Ekkor $W_\emptyset = \{1\}$ és $W_S = W$. Ha kicserélnénk a Δ egyszerű rendszert a $w\Delta$ egyszerű rendszerre, akkor W_I helyett a hozzá konjugált wW_Iw^{-1} részcsoportot kapnánk. Az így nyert részcsoportot parabolikus részcsoportnak nevezzük. Az ilyen részcsoportok rendszeresen felbukkannak tükrözéscsoportok további tanulmányozása, illetve alkalmazása közben, részben azért mert megkönnyítik az induktív érveléseket.

1.15. Állítás. *Rögzítsünk egy Δ egyszerű rendszert, és a hozzá tartozó egyszerű tükrözések halmazát jelölje S. Legyen $I \subseteq S$, és legyen $\Phi_I = \Phi \cap V_I$, ahol V_I a Δ_I rendszer által kifeszített altér.*

(a) Φ_I gyökrendszer a V (illetve V_I) vektortérben, Δ_I egyszerű rendszerrel, és hozzátartozó W_I tükrözéscsoporttal.

(b) Legyen ℓ_I a W_I tükrözéscsoport hosszfüggvénye a Δ_I egyszerű rendszerre nézve. Ekkor $\ell_I = \ell|_{W_I}$.

(c) Legyen $W^I = \{w \in W \mid \ell(ws) > \ell(w)$ minden $s \in I$ tükrözésre$\}$. Ha adva van egy tetszőleges $w \in W$ elem, akkor létezik pontosan egy $u \in W^I$ és $v \in W_I$, melyekre $w = uv$. Továbbá $\ell(w) = \ell(u) + \ell(v)$, és u az egyértelmű legkisebb hosszúságú elem a wW_I mellékosztályban.

Bizonyítás. (a) Az triviális, hogy W_I stabilizálja a V_I alteret, és az is világos, hogy Φ_I eleget tesz az (R1) és (R2) feltételeknek. Az is látszik, hogy Δ_I egyszerű rendszer a Φ_I gyökrendszerben, és W_I a megfelelő tükrözés csoport.

(b) Mint azt korábban láttuk $\ell(w)$ megegyezik azon pozitív gyökök számával, amiket w negatívba képez, ez igaz az ℓ_I hosszfüggvényre is, ahol azt, hogy "pozitív" a Δ_I egyszerű rendszerre nézve értjük. Könnyen látható, hogy ekkor a pozitív gyökök pontosan azok, akik a $\Phi^+ \cap \Phi_I$ metszetben vannak. Legyen $\alpha \in \Phi^+ \setminus \Phi_I$ pozitív gyök. Az, hogy α pozitív, de nincs benne a Φ_i halmazban azt jelenti, hogy α tartalmaz egy $\gamma \notin \Delta_I$ egyszerű gyököt, tehát minden $\beta \in \Delta_I$ egyszerű gyökre, $s_\beta\alpha$ továbbra is pozitív együtthatóval tartalmazza a γ gyököt. Ebből következik, hogy $s_\beta\alpha > 0$, amiből pedig következik, hogy minden $w \in W_I$ elemre $w\alpha > 0$. Tehát azok a gyökök a Φ^+ rendszerben, akiket w negatívba képez, pontosan azok a gyökök akik a Φ_I^+ rendszerben vannak, és w negatívba képez, emiatt $\ell(w) = \ell_I(w)$.

(c) Legyen $w \in W$, és válasszunk egy minimális hosszúságú $u \in wW_I$ reprezentánst, ekkor $w = uv$, ahol $v \in W_I$. Mivel minden $s \in I$ tükrözésre $us \in wW_I$, ezért $u \in W^I$. Legyen $u = s_1 \dots s_q$ és $v = s'_1 \dots s'_r$ az u és v elemeknek egy-egy redukált kifejezése. Mivel $w = uv$, ezért $\ell(w) \leq \ell(u) + \ell(v)$. Ha ez szigorú egyenlőtlenség lenne, akkor a törlési feltétel szerint elhagyhatunk két tényezőt az uv szorzatból anélkül, hogy változtatnánk a w elemen. Ha egy s_i tagot hagynánk el, akkor kapnánk egy az u elemnél rövidebb wW_I mellékosztálybeli reprezentánst, ami ellentmond az u elem választásának. Tehát akkor két tényezőt is elhagyhatok az $s'_1 \dots s'_r$ kifejezésből anélkül, hogy a v elem változna, ami annak mond ellent, hogy $s'_1 \dots s'_r$ redukált kifejezés, következésképpen $\ell(w) = \ell(u) + \ell(v)$.

Vegyük észre, hogy az egyetlen fontos tulajdonsága a w elemnek az, hogy benne van a wW_I mellékosztályban, valójában most azt láttuk be, hogy a wW_I mellékosztály összes eleme felírható uv alakban úgy, hogy $\ell(uv) = \ell(u) + \ell(v)$. Speciálisan u az egyértelmű minimális hosszuságú mellékosztály reprezentáns.

Tegyük fel, hogy van egy másik $u' \in W^I$ és $v' \in W_I$, amire $u'v' = w$. Mivel $v' \in W_I$, ezért $u' \in wW_I$, így az előző észrevétel szerint $u' = uv$, ahol $\ell(v) = r > 0$. Legyen $v = s_1 \dots s_r$ redukált kifejezés, és vegyük észre, hogy így $\ell(u's_r) < \ell(u')$, ami ellentmond annak, hogy $u' \in W^I$. $\square$

Az állítás (c) részének van egy szép alkalmazása a W csoport S generátorhalmazhoz viszonyított növekedésének tanulmányozására. Ezt a növekedést a következő sorozat méri:

$$a_n = \mathrm{Card}\{w \in W \mid \ell(w) = n\}$$

Ezt a sorozatot kézenfekvő úgy nézni, mint egy polinom együtthatói, azaz:

$$W(t) = \sum_{n \geq 0} a_n t^n = \sum_{w \in W} t^{\ell(w)}.$$

A $W(t)$ polinomot a W csoport Poincaré-polinomjának nevezzük. Kicsit általánosabban egy tetszőleges $X \subseteq W$ halmazra definiálhatjuk a következő polinomot:

$$X(t) := \sum_{w \in X} t^{\ell(w)}.$$

Vegyük észre, hogy ha $I \subseteq S$, akkor $W_I(t)$ egybeesik a W_I csoport Poincaré-polinomjával, mivel $\ell|_{W_I} = \ell_I$. A rövidség kedvéért legyen $(-1)^I = (-1)^{|I|}$. Emlékezzünk vissza, hogy a W csoportnak létezik egy egyértelmű $w_\circ$ maximális $|\Pi| = N$ hosszúságú eleme.

1.16. Állítás.
$$\sum_{I\subseteq S}(-1)^I\frac{W(t)}{W_I(t)}=\sum_{I\subseteq S}(-1)^I W^I(t)=t^N$$

Bizonyítás. Az első egyenlőség abból következik, hogy $W(t)=W_I(t)W^I(t)$, ami az előző állítás (c) részének azonnali következménye. Kicsit részletesebben:

$$W_I(t)W^I(t)=\sum_{w\in W_I,w'\in W^I} t^{\ell(w)+\ell(w')},$$

viszont az előző állítás (c) része szerint $\ell(w)+\ell(w')=\ell(ww')$, és minden $v\in W$ előáll egyértelműen ww' alakban, tehát $W_I(t)W^I(t)=W(t)$.

Most jöhet a második egyenlőség, ehhez pedig nézzük meg, hogy egy rögzített $w\in W$ pontosan miben is járul hozzá a második szummához. Ehhez definiáljuk a $K=\{s\in S\mid \ell(ws)>\ell(w)\}$ halmazt. Ekkor $w\in W^I$ pontosan akkor, ha $I\subseteq K$. Így azt kaptuk, hogy a második szummában $t^{\ell(w)}$ együtthatója megegyezik a $\sum_{I\subseteq K}(-1)^I$ összeggel. Ha K nem az üres halmaz, akkor ez a szumma 0 lesz, és $K=\emptyset$ pontosan akkor, ha $w=w_\circ$, és ezzel kész is vagyunk. □

1.6. Fundamentális tartomány

Fixáljunk egy Π pozitív rendszert, ami tartalmazza a Δ egyszerű rendszert. Minden H_α hipersíkhoz tartozik két féltér A_α, és A'_α, ahol

$$A_\alpha=\{\lambda\in V\,|\,(\lambda,\alpha)>0\,\},$$

és $A'_\alpha=-A_\alpha$. Legyen $C=\cap_{\alpha\in\Delta}A_\alpha$. Mivel C konvex nyílt halmazok véges metszete, ezért C maga is konvex nyílt halmaz, sőt C triviálisan egy kúp. Legyen $D=\overline{C}$ a C halmaz lezártja, azaz a $H_\alpha\cup A_\alpha$ zárt féltereknek metszete. Tehát

$$D=\big\{\lambda\in V\,|\,(\lambda,\alpha)\geq 0,\ \forall\,\alpha\in\Delta\,\big\}.$$

Nyilván D egy zárt konvex kúp. Azt szeretnénk megmutatni, hogy D a W hatásának fundamentális tartománya, azaz minden $\lambda\in V$ ekvivalens pontosan egy D halmazbeli elemmel.

1.17. Lemma. *Minden $\lambda\in V$ ekvivalens egy olyan $\mu\in D$ elemmel, hogy $\mu-\lambda$ nemnegatív lineáris kombinációja Δ elemeinek.*

Bizonyítás. Vezessünk be a V vektortéren egy parciális rendezést: $\lambda\leq\mu$ pontosan akkor, ha $\mu-\lambda$ nemnegatív lineáris kombinációja Δ elemeinek. Könnyen ellenőrizhető, hogy ez tényleg egy parciális rendezés. Tekintsük azon $\mu\in V$ elemeket, melyek ekvivalensek a λ elemmel W alatt, és amikre fennáll, hogy $\lambda\leq\mu$. Jelölje az imént definiált halmazt O_λ. Nyilván O_λ nem üres, mivel λ benne van, és így kiválaszthatunk belőle egy μ maximális elemet. Legyen $\alpha \in \Delta$, nyilván $s_\alpha \mu$ továbbra is ekvivalens a λ elemmel. Most gyorsan idézzük fel, hogy hogy is kapjuk meg az $s_\alpha \mu$ elemet: $s_\alpha \mu = \mu - 2\big((\mu, \alpha)/(\alpha, \alpha)\big)\alpha$. Mivel μ maximális eleme az O_λ halmaznak, ezért $(\mu, \alpha) \geq 0$. Tehát azt kaptuk, hogy tetszőleges $\alpha \in \Delta$ választásra, $(\mu, \alpha) \geq 0$, ami pontosan azt jelenti, hogy $\mu \in D$. $\square$

Tehát megkaptuk, hogy minden $\lambda \in V$ ekvivalens egy D halmazbeli elemmel. Ahhoz, hogy lássuk, hogy legföljebb egy ilyen elem van a D halmazban, elég lenne megmutatni, hogy D két különböző eleme nem lehet ekvivalens W alatt. A következő tételben ennél többet is belátunk, amihez nem árt bevezetni egy új fogalmat. Legyen $U \subseteq V$, ekkor U izotrópia-részcsoportja alatt azt a $W' \leq W$ részcsoportot értjük, mely az U halmazt pontonként fixáló elemekből áll.

1.18. Tétel. *Rögzítsük a $\Delta \subset \Pi$ rendszereket mint korábban.*

(a) Ha $w\lambda = \mu$, és $\lambda, \mu \in D$, akkor $\lambda = \mu$, és w olyan egyszerű tükrözések szorzata, melyek fixálják a λ elemet. Speciálisan, ha $\lambda \in C$, akkor λ izotrópia-részcsoportja triviális.

(b) D fundamentális tartománya a W csoport hatásának.

(c) Ha $\lambda \in V$, akkor λ izotrópia-részcsoportját a benne lévő s_α $(\alpha \in \Phi)$ tükrözések generálják.

(d) Ha $U \subseteq V$ tetszőleges halmaz, akkor U izotrópia-részcsoportját azon tükrözések generálják, amiket tartalmaz.

Bizonyítás. (a) Haladjunk $\ell(w) = n(w)$ szerinti indukcióval. Ha $n(w) = 0$, akkor $w = 1$ és nincs mit bizonyítani. Ha $n(w) > 0$, akkor biztosan létezik egy olyan $\alpha \in \Delta$ egyszerű gyök, hogy $w\alpha < 0$ (különben $w\Delta$, és így $w\Pi$ csak pozitív gyökökből állna). Hála az 1.9. lemmának $n(ws_\alpha) = n(w) - 1$. Továbbá ha $\lambda, \mu \in D$, és $w\alpha < 0$, akkor azt kapjuk, hogy $0 \geq (\mu, w\alpha) = (w^{-1}\mu, \alpha) = (\lambda, \alpha) \geq 0$, azaz $(\lambda, \alpha) = 0$, és így $s_\alpha \lambda = \lambda$. Következésképp $ws_\alpha \lambda = \lambda$. Az indukciós feltevés szerint ekkor $\lambda = \mu$, és ws_α olyan egyszerű tükrözések szorzata, melyek λ-t fixálják, és így w is olyan tükrözések szorzata.

(b) Ez egyből következik az (a) részből és az előző lemmából.

(c) Legyen $\lambda \in V$, és használjuk az előző lemmát, hogy találjunk egy $w \in W$ elemet, melyre $w\lambda = \mu$, ahol $\mu \in D$. Ekkor az állításunk (a) része szerint a μ elem W' izotrópia-részcsoportját generálják azok az egyszerű tükrözések, melyek fixálják μ-t. Az világos, hogy $w^{-1}W'w$ a λ elem izotrópia-részcsoportja, és mivel $w^{-1}s_\alpha w = s_{w^{-1}\alpha}$, ezért azt kaptuk, hogy λ izotrópia-részcsoportját generálják azok az s_α $(\alpha \in \Phi)$ tükrözések, melyeket tartalmaz.

(d) Az a W' részcsoport, mely az U halmaz által feszített alteret fixálja (vagy annak egy $\lambda_1, \ldots, \lambda_t$ bázisát), nyilván ugyanaz, mint az a részcsoport, ami U-t fixálja. Tehát W' csak a λ_i izotrópia-részcsoportjainak metszete. Haladjunk t szerinti indukcióval. Ha $t = 1$, akkor azt az állításunk (c) része már elintézte. Legyen $t > 1$. Azt már tudjuk, hogy a λ_1 elem W'' izotrópia-részcsoportját azon s_α tükrözések generálják, melyeket W'' tartalmaz. Mivel $W'' \leq W$ tükrözéscsoport, ezért létezik egy $\Phi'' \subset \Phi$ gyökrendszer, amit stabilizál. Most vegye át a W csoport szerepét W''. Az indukciós feltevésünk szerint a $\{\lambda_2, \ldots, \lambda_t\}$ halmaz elemeit fixáló részcsoportot generálják azon s_α ($\alpha \in \Phi''$) tükrözések, melyeket tartalmaz. Na de ez a részcsoport pontosan W'. $\square$

Ebben a fejezetben minden Δ egyszerű rendszerhez hozzárendeltünk egy $C \subset V$ konvex nyílt kúpot, aminek minden pontja triviális izotrópia-részcsoporttal rendelkezik. Az így nyert nyílt kúpokat kamráknak nevezzük. Nyilvánvaló, hogy ha kicseréljük a Δ egyszerű rendszert $w\Delta$-ra, akkor csak ki kell cserélni a C kamrát a wC kamrára. Tehát a W csoport egyszeresen tranzitív hatását az egyszerű rendszereken, át tudtuk alakítani egy egyszeresen tranzitív hatássá a kamrákon. A kamrákat topologikusan úgy karakterizálhatjuk, mint $V \setminus \bigcup_\alpha H_\alpha$ összefüggő komponensei. Ha adva van egy Δ rendszerhez tartozó C kamra, akkor C falai definíció szerint a H_α ($\alpha \in \Delta$) hipersíkok. Minden falnak van egy "pozitív", és egy "negatív" oldala (C a pozitív oldalán van). A Δ gyökrendszert ekkor úgy karakterizálhatjuk, mint azok a gyökök, amik merőlegesek a C kamra egyik falára, és pozitívan irányítottak. Utolsó megjegyzésként vegyük észre, hogy tetszőleges kamra tetszőleges 2 falának egymással bezárt szöge π/k alakú, ahol $k \geq 2$.

Az előző tétel (d) részét felhasználva tisztább képet kaphatunk az $I \subseteq S$, W_I alakú parabolikus részcsoportok rendszeréről.

1.19. Állítás. *Rögzítsünk egy Δ egyszerű rendszert, és legyen S az egyszerű tükrözések halmaza. Az $I \mapsto W_I$ hozzárendeles egy hálóizomorfizmust ad S részhalmazai és a W_I ($I \subseteq S$) alakú parabolikus részcsoportok között.*

Bizonyítás. Az világos, hogy a $W_{I \cup J}$ részcsoportot generálja W_I és W_J ($I, J \subseteq S$). Azt állítjuk, hogy $W_I \cap W_J = W_{I \cap J}$ is fennáll, amiből már következik, hogy az $I \mapsto W_I$ egy-egy hozzárendelés, és háló izomorfizmus. A két tartalmazás közül az, hogy $W_{I \cap J} \subseteq W_I \cap W_J$ nyilvánvaló. Nézzük most a V_I, és V_J altereket. A definíciókból egyből adódik, hogy $V_I \cap V_J = V_{I \cap J}$. Most emlékezzünk vissza arra a lineáris algebrai tényre, hogy ha $A, B \subseteq V$, akkor $(A \cap B)^\perp = A^\perp + B^\perp$, ebből a következőt kapjuk:

$$V_I^\perp + V_J^\perp = (V_I \cap V_J)^\perp = V_{I \cap J}^\perp.$$

Most tegyük fel, hogy $w \in W_I \cap W_J$, ekkor w fixál minden vektort a $V_I^{\perp} + V_J^{\perp} = V_{I\cap J}^{\perp}$ altérben. Ekkor az 1.18. tétel (d) része szerint w olyan s_α tükrözések szorzata, melyek pontonként fixálják a $V_{I\cap J}^{\perp}$ alteret. Ez azt jelenti, hogy α merőleges erre a $V_{I\cap J}^{\perp}$ altérre, tehát $\alpha \in \Phi \cap V_{I\cap J} = \Phi_{I\cap J}$. Ebből következik, hogy $w \in W_{I\cap J}$, tehát $W_I \cap W_J \subseteq W_{I\cap J}$. $\square$

A 1.18. tételnek még egy hasznos következménye van, ami egy lehetséges furcsaságot segít tisztázni. Emlékezzünk vissza, hogy a W csoportot végig úgy tanulmányoztuk, hogy választottunk és rögzítettünk egy Φ gyökrendszert, és azt mondtuk, hogy W az a csoport, amit az s_α $(\alpha \in \Phi)$ tükrözések generálnak. A lehetséges furcsaság az, hogy a W csoportban vannak még egyéb tükrözések, amik nem s_α $(\alpha \in \Phi)$ alakúak, ami azért tényleg furcsa lenne. Szerencsére ilyen nem történhet, de azért ezt bizonyítsuk be.

1.20. Állítás. *A W csoportban minden tükrözés előáll s_α alakban, ahol $\alpha \in \Phi$.*

Bizonyítás. Legyen $s \in W$ egy tükrözés, és legyen H az s tükröző hipersikja. Az s tükrözés pontonként fixálja a H hipersíkot, tehát s benne van H izotrópia-részcsoportjában, ami ezáltal nem egy triviális részcsoport. Hála az 1.18. tétel (d) részének H izotrópia-részcsoportját generálja néhány s_α $(\alpha \in \Phi)$ tükrözés, viszont s_α nem tudja pontonként fixálni a H hipersíkot, kivéve akkor, ha $H = H_\alpha$ és $s = s_\alpha$. $\square$

1.7. A Coxeter-komplexus

Ebben a fejezetben a D fundamentális tartománynak adjuk meg egy részletesebb leírását parabolikus részcsoportok segítségével. Mint korábban rögzítsünk egy Δ egyszerű rendszert, és legyen S az egyszerű tükrözések halmaza. Kényelmi okokból feltesszük, hogy Δ kifeszíti V-t. Minden $I \subseteq S$ halmazra definiáljuk a következőt:

$$C_I = \{\, \lambda \in D \,|\, (\lambda, \alpha) = 0 \text{ minden } \alpha \in \Delta_I,\ (\lambda, \alpha) > 0 \text{ minden } \alpha \in \Delta \backslash \Delta_I \,\}$$

Tehát C_I néhány H_α hipersík és A_α nyílt féltér metszete. Az világos, hogy a C_I halmazok particionálják a D kúpot, továbbá azt is tudjuk, hogy a C_I halmaz által feszített altérnek $n - |I|$ a dimenziója, ahol $n = \dim(V)$.

Legyen $\mathcal{C}$ a wC_I $(w \in W,\ I \subseteq S)$ halmazoknak a rendszere. Ismét hála az 1.18. tételnek, a V vektorteret particionálja $\mathcal{C}$. Kissé pontosabban, ha I rögzített, akkor wC_I és $w'C_I$ diszjunkt, kivéve ha w, és w' W_I-nek ugyanabba a bal oldali mellékosztályába tartozik, mert akkor a két halmaz megegyezik. Ha két különböző $I, J \subseteq S$ halmazt rögzítünk, akkor wC_I, és $w'C_J$ mindig diszjunkt halmaz lesz. A $\mathcal{C}$ halmazrendszert a W csoport Coxeter-komplexusának nevezzük. Minden wC_I alakú halmazt I típusú lapnak nevezünk.

1.21. Állítás. *Minden $I \subseteq S$ részhalmazra a $C_I \in \mathcal{C}$ lapnak az izotrópia-csoportja pontosan W_I. Tehát a W csoport parabolikus részcsoportjai pontosan a $\mathcal{C}$ halmazrendszer elemeinek izotrópia-csoportjai.*

Bizonyítás. A C_I halmaz definíciójából látszik, hogy W_I minden eleme pontonként fixálja. Most tegyük fel, hogy $w \in W$ olyan, melyre fennáll, hogy $wC_I = C_I$. Ekkor az 1.18. tételnek (a) részéből következik, hogy w pontonként fixálja a C_I lapot.

Használjuk az 1.15. állítás (c) részét, hogy megkapjuk a $w = uv$ felírását w-nek, ahol $v \in W_I$, és $u \in W^I$, azaz minden s_α ($\alpha \in \Delta_I$) tükrözésre: $\ell(us_\alpha) > \ell(u)$. Az 1.9. lemma (a) része szerint ez pontosan azt jelenti, hogy $u\Delta_I \subseteq \Phi^+$. Tegyök fel, hogy u nem az identitás, akkor létezik egy $\alpha \in \Delta$ egyszerű gyök, amire $u\alpha < 0$, és az előző észrevétel miatt $\alpha \notin \Delta_I$. Válasszunk egy tetszőleges $\lambda \in C_I$ elemet, ekkor $w\lambda = u\lambda = \lambda$. Mivel $\alpha \notin \Delta_I$, ezért definíció szerint $(\lambda, \alpha) > 0$. Másrészt viszont $u\alpha < 0$ miatt azt kapjuk, hogy $(\lambda, \alpha) = (u\lambda, u\alpha) = (\lambda, u\alpha) \leq 0$, ami ellentmondás, tehát $u = 1$.

$\square$

Következő lépésként megadunk egy alternáló összeg formulát $\det(w)$ kiszámolására, amit úgy csinálunk, hogy minden dimenzióra megszámoljuk, hogy w hány elemet fixál a $\mathcal{C}$ komplexusban. Ennek a megadására előbb szükségünk lesz egy általánosabb kombinatorikus formulára.

Legyen $H_1, \ldots, H_r$ hipersíkok egy tetszőleges családja az n dimenziós V euklideszi térben, és csináljunk egy $\mathcal{K}$ komplexust belőlük, úgy ahogy a Coxeter-komplexust csináltuk. Minden $H = H^0$ hipersík meghatároz egy pozitív H^+, és egy negatív H^- félteret. Ekkor a $\mathcal{K}$ komplexusnak egy tetszőleges eleme előáll a következő alakban:

$$K = \bigcap H_i^{\epsilon_i}, \text{ ahol } \epsilon_i \in \{0, +, -\}.$$

Az üres metszetet nem vesszük be a $\mathcal{K}$ komplexusba. A K elem dimenziója $\dim(K) = i$, ha K egy i dimenziós alteret feszít ki. Vegyük észre hogy az az L altér amit kifeszít, azt úgy kapjuk, hogy összemetsszük a H_i^0 hipersíkokat amik előfordulnak K definíciójában. Tehát azt kaptuk, hogy K egy nyílt halmaz az L altérben, amit úgy kapunk, hogy az L alteret elmetsszük nyílt félterekkel.

1.22. Lemma. *Legyen n_i a $\mathcal{K}$ komplexusbeli i dimenziós elemek száma. Ekkor $\sum_i (-1)^i n_i = (-1)^n$.*

Bizonyítás. Indukciót alkalmazunk a $\mathcal{K}$ komplexust definiáló hipersíkok r számára. Az $r = 1$ eset, triviális. Most vizsgáljuk meg azt, hogy ha már megvan $H_1, \ldots, H_r$, akkor egy új H hipersík bevétele milyen hatással bír. Új elemeket csak úgy kaphatunk, ha H nem triviálisan metsz bele egy K elembe. Legyen L a K elem által feszített lineáris altér. Ha $x \in K \cap H$, akkor létezik az x elemnek egy olyan U nyilt környezete az L altérben, ami még a K elemben is benne van. Mivel a $H \cap L$ metszet egy-kodimenziós az L altérben, ezért világos, hogy U belemetsz a H^+ és H^- félterekbe. Tehát ilyenkor egy K elemet lecserélünk két $H^+ \cap K$, $H^- \cap K$ i dimenziós elemre, és egy $H^0 \cap K$ $i-1$ dimenziós elemre. Ez azt jelenti, hogy n_i és n_{i-1} pontosan eggyel nő, ami az összeg formulát nem változtatja meg. □

Rögzítsünk egy Δ egyszerű rendszert, és legyen S az egyszerű tükrözések halmaza. Vegyünk egy $I \subseteq S$ halmazt, és nézzük a vC_I lapokat; ezek bijekcióban állnak a vW_I balaloldi mellékosztályokkal. Minden $w \in W$ elemre legyen $f_I(w)$ azon I típusú lapok száma, melyeket w fixál (tehát pontonként fixál). Ez ugyanaz, mint azon vW_I mellékosztályok száma, melyeket stabilizál a w elemmel való balról szorzás. Mint múltkor, most is $(-1)^{|I|}$ helyett azt írjuk, hogy $(-1)^I$.

1.23. Állítás.

$$\sum_{I \subseteq S} (-1)^I f_I(w) = det(w)$$

Bizonyítás. Rögzítsünk egy $w \in W$ elemet, és legyen V' az az altér, amit w pontonként fixál (tehát az 1 sajátértékhez tartozó sajátaltér). Ekkor egy $\mathcal{C}$ komplexusbeli lap pontosan akkor marad fixen, ha a V' altérben van. Legyen $\mathcal{K}$ az a komplexus, amit úgy kaptunk, hogy $\mathcal{C}$ elemeit elmetsszük a V' altérrel. Ekkor az n_i darab i dimenziós lap a $\mathcal{C}$ komplexusban, ami V' altérben is benne van, az pontosan a $\mathcal{K}$ komplexus i dimenziós elemeinek száma, tehát alkalmazható rá az előző lemma:

$$\sum_i (-1)^i n_i = (-1)^c, \text{ ahol } c = \dim(V').$$

Ha most $n = \dim(V)$, és $\dim(C_I) = n - |I|$, akkor a következőt kapjuk:

$$n_i = \sum_{|I|=n-i} f_I(w).$$

Ha most ezeket összerakjuk, akkor a következőt kapjuk:

$$(-1)^n \Big(\sum_{I \subseteq S} (-1)^I f_I(w) \Big) = (-1)^c.$$

Most azt vegyük észre, hogy w egy ortogonális transzformáció, tehát a potenciális sajátértékei nem más mint 1 (c multiplicitással), b pár egység hosszú komplex konjugált szám, és -1 ($n - c - 2b$ multiplicitással). Tehát azt kaptuk, hogy $\det(w) = (-1)^{n-c-2b} = (-1)^{n-c}$, amiből már következik az állítás. □

2. Tükrözéscsoportok invariánselmélete

2.1. Véges generáltság

Mielőtt a tükrözéscsoportokkal foglalkoznánk, vizsgáljuk meg, hogy mit is mondhatunk $GL(V)$ egy tetszőleges véges részcsoportjának invariánsairól, ahol V véges dimenziós vektortér a K nulla karakterisztikájú test felett. Legyen $S = S(V^*)$ szimmetrikus algebra, ahol V^* a V vektortér duálisa. Ha rögzítünk egy bázist V-ben, akkor S azonosítható a $K[x_1, ..., x_n]$ gyűrűvel, ahol x_i az i-edik koordinátafüggvény.

Ha a G csoportnak adott egy bal oldali hatása a V vektortéren, akkor G kontragrediens hatása indukál egy bal oldali hatást az S szimmetrikus algebrán a következő módon:

$$(g \cdot f)(v) = f(g^{-1} \cdot v), \text{ ahol } g \in G,\ f \in S(V^*), \text{ és } v \in V.$$

Könnyen ellenőrizhető, hogy tetszőleges $g \in G$, $f, h \in S(V^*)$ elemekre teljesül, hogy $g(fh) = (gf)(gh)$, illetve $g(f+h) = gf+gh$. Mivel minden $g \in G$ szorzattartó, ezért szintén könnyen ellenőrizhető, hogy G hatása őrzi $S(V^*)$ "fokszám" szerinti gradálását.

Azt mondjuk, hogy egy $f \in S$ polinom G-invariáns, ha minden $g \in G$ esetén $gf = f$. Vegyük észre, hogy invariáns elemek összege és szorzata szintén invariáns, mivel minden $g \in G$ szorzat- és összegtartó. Ez azt jelenti, hogy a G-invariáns elemek részalgebrát alkotnak az S gyűrűben. Jelölje a G-invariánsok algebráját $R = S^G$. Könnyen belátható, hogy egy $f \in S$ polinom pontosan akkor invariáns, ha a homogén komponensei azok.

Tanulságos lehet megnézni G csoportnak az S hányadostestén indukált hatását. Jelöljük S hányadostestét L-lel, ami azonosítható a $K(x_1, ..., x_n)$ testtel, mely K egy tisztán transzcendens bővítése n transzcendenciafokkal, és $G \leq \mathrm{Aut}(L)$. Testelméleti tanulmányainkból tudjuk, hogy ekkor L véges Galois-bővítése az L^G testnek (G fixteste) G Galois-csoporttal. Ebből következik, hogy az L^G testnek is n a transzcendenciafoka K felett.

2.1. Állítás. *Legyen L az S hányadosteste, és $R = S^G$, ekkor R hányadosteste megegyezik L^G-vel. Speciálisan R-nek is $n = dim(V)$ a transzcendenciafoka.*

Bizonyítás. Az, hogy R hányadosteste része L^G-nek, triviális. A másik irányhoz tegyük fel hogy, $p/q \in L^G$ ahol $p, q \in S$. Bővítsük a törtet $\prod_{\substack{g\in G\\ g\neq 1}} g \cdot p$ -vel, azaz

$$p/q = \frac{p \cdot \prod_{g\in G,\ g\neq 1} gp}{q \cdot \prod_{g\in G,\ g\neq 1} gp} = \frac{\prod_{g\in G} gp}{q \cdot \prod_{g\in G,\ g\neq 1} gp}$$

Az új számláló G-invariáns, hiszen ha beszorzom egy $g \in G$ elemmel, akkor csak permutálom a szorzat elemeit, és mivel $p/q \in L^G$, ezért a nevezőnek is invariánsnak kell lennie, azaz L^G része az R hányadostestének. $\square$

2.2. Állítás. *Ha $G < GL(V)$ véges csoport, akkor az S gyűrű egész R felett.*

Bizonyítás. Azt kell belátnunk, hogy minden $f \in S$ polinomhoz van egy 1 főegyütthatójú $R[t]$ gyűrűbeli polinom, aminek gyöke az f polinom, és ez teljesül is, mert vegyük a következő $h_f(t)$ polinomot:

$$h_f(t) = \prod_{g \in G} (t - gf)$$

Ekkor a $h_f(t)$ polinom eltűnik az f elemen ($g = id_S$), 1 a főegyütthatója, és minden más együtthatója a gf elemek elemi szimmetrikus polinomja, tehát R-beliek. $\square$

Miután most láttuk, hogy R nem túl kicsi, most azt is megmutatjuk, hogy nem is túl nagy, azaz, hogy R végesen generált K-algebra. A terv az, hogy követjük Hilbert módszerét, és kihasználjuk, hogy egy test fölötti véges sok változós polinomgyűrű Noether-gyűrű.

Hilbert bázistételéből adódik, hogy Noether-gyűrűben tetszőleges ideál tetszőleges generátorhalmazából kiválaszthatunk egy véges generátorhalmazt. Az ötlet az, hogy vizsgáljuk az I Hilbert-ideált, melyet azon R-beli elemek generálnak, melyek konstans tagja nulla, azaz $I = SR^+$, ahol $R^+ = \{f \in R \mid f(0) = 0\}$. Válasszunk az I ideálhoz véges sok homogén generátort az R^+ gyűrűből. Megmutatjuk, hogy bármely így kapott halmaz, az 1-gyel együtt, generálja R-t, mint K-algebrát.

Ahhoz, hogy ezt belássuk, még szükségünk lesz egy operátorra, mely S minden elemét levetíti R-re.

2.3. Definíció. Legyen $f \in S$, ekkor $f^\# = \frac{1}{|G|} \sum_{g \in G} g \cdot f$.

Ezt az operátort Reynolds-operátornak nevezzük. Vegyük észre, hogy itt kihasználjuk, hogy $|G|$ nem osztható char$K$-val, másszóval $|G|$ a K testnek egy invertálható eleme. Ez az apróság valójában annyira fontos, hogy több olyan tétel, amit most belátunk, nem marad igaz, ha G rendje nem invertálható.

Világos, hogy ez az átlagoló operátor, mely egy f polinomhoz az $f^\#$ polinomot rendeli, egy $S \to R$ K-lineáris leképezés, mely megtartja a fokot, és R minden elemét fixálja.

2.4. *Megjegyzés.* Vegyük észre, hogy $p \in S,\ q \in R$ esetén $(pq)^\# = p^\# q$, hiszen

$$(pq)^\# = \frac{1}{|G|} \sum g(pq) = \frac{1}{|G|} \sum (gp)(gq) = \frac{1}{|G|} \sum (gp) \cdot q = p^\# q.$$

2.5. Tétel. *A fenti jelölésekkel élve, ha $f_1, f_2, \ldots, f_r$ homogén elemei R^+-nak, és generálják az $I = SR^+$ Hilbert-ideált, akkor az $1, f_1, f_2, \ldots, f_r$ generálja R-t mint K-algebrát.*

Bizonyítás. Meg kell mutatnunk, hogy minden $f \in R$ előáll, mint $f_1, f_2, \ldots, f_r$ polinomja (K-együtthatós). Feltehető, hogy f homogén, hiszen ha van egy $g \in R$, akkor elég belátni, hogy g minden homogén tagja előáll a megfelelő alakban.

Haladjunk f foka szerinti indukcióval. Ha $\deg f = 0$ akkor $f \in R$. Ha $\deg f > 0$, akkor $f \in I$, tehát f felírható a következő alakban:

$$f = s_1 f_1 + s_2 f_2 + \cdots + s_r f_r.$$

Mivel minden f_i homogén, és f homogén, ezért feltehető, hogy az s_i poinomok is azok, és így $\deg s_i = \deg f - \deg f_i$, tehát s_i foka szigorúan kisebb, mint f foka. Használjuk a $\#$ Reynolds-operátort.

$$f^\# = f = \sum_{i=1}^{r} (s_i f_i)^\# = \sum_{i=1}^{r} s_i^\# f_i.$$

Most minden $s_i^\#$ homogén eleme R-nek, és $\deg s_i < \deg f$. Az indukciós feltevés szerint minden s_i előáll az f_i polinomok polinomjaként, tehát f is előáll az f_i polinomok polinomjaként. □

Az előző számolás azt mutatja, hogy minden $G < GL(V)$ véges csoportra G invariánsgyűrűje végesen generált, viszont semmit sem tudtunk meg arról, hogy hány elemű lehet egy minimális generátorhalmaz, vagy hogy egy minimális generátorhalmazban legföljebb mekkora fokú elemek szerepelhetnek. A következő tétel éppen az utóbbira ad nekünk egy becslést, de először is definiáljuk egy V vektortér, és G csoport Noether-számát.

2.6. Definíció. A V véges dimenziós vektortér Noether-száma a G csoport egy adott reprezentációjára nézve:

$$\beta(G, V) = \min \left\{ d \;\middle|\; R = S^G\text{-t mint gyűrűt generálja } \bigoplus_{i=0}^{d} S_i^G \right\}$$

2.7. Definíció. A G csoport Noether-száma:

$$\beta(G) = \sup \left\{ \beta(G, V) \;\middle|\; V \text{ véges dimenziós reprezentációja } G\text{-nek a } K \text{ test fölött} \right\}$$

2.8. *Megjegyzés.* Vegyük észre, hogy $\beta(G)$ függ attól, hogy milyen test fölött dolgozunk.

Emmy Noether 1915-ben belátta, hogy minden véges G csoportra $\mathbb{C}$ felett teljesül, hogy $\beta(G) \leq |G|$. Ha megvizsgáljuk a bizonyítását, akkor kiderül, hogy az igaz marad minden 0 karakterisztikájú test felett, továbbá minden $p > |G|$ karakterisztikájú test felett. Mi most egy gyengébb feltétel mellett látjuk ezt be. A következő tételt egymástól függetlenül bizonyította be P. Fleischmann és J. Fogarty 2000-ben. D. Benson később leegyszerűsítette Fogarty bizonyítását, azt tárgyaljuk.

2.9. Tétel. *Legyen V vektortér, és $G < GL(V)$, $|G| < \infty$. Ha $|G|$ invertálható a K testben, akkor $\beta(G, V) \leq |G|$.*

Bizonyítás. Legyen $m = |G|$, $[m] = \{1, 2, \dots, m\}$ és $S^+ = \{f \in S \mid f(0) = 0\}$. Először megmutatjuk, hogy $(S^+)^m$ benne van az $I = SR^+$ Hilbert-ideálban.

Ahhoz, hogy ezt lássuk, vegyünk tetszőleges $f_1, f_2, \dots, f_m \in S^+$ elemeket. Soroljuk fel G elemeit, azaz $G = \{g_1, g_2, \dots, g_m\}$, és tekintsük a következő szorzatot: $\prod_{i=1}^m (f_i - (gg_i)(f_i)) = 0$. Fejtsük ki a szorzatot, és summázzunk $g \in G$-re, ekkor a következőt kapjuk:

$$\sum_{A \subseteq [m]} (-1)^{m-|A|} h_A \prod_{i \in A} f_i = 0,$$

ahol $h_A = \sum_{g \in G} \prod_{i \in [m] \setminus A} g(g_i f_i) \in R^+$.

Az $A = [m]$-hez tartozó tag a summában pontosan $|G| f_1 f_2 \dots f_m$. Minden más A részhalmazhoz tartozik egy $h_A \in R^+$, azaz, ha rendezzük az egyenletet, azt kapjuk, hogy $f_1 f_2 \dots f_m \in I = SR^+$, tehát $(S^+)^m \subseteq I = SR^+$.

A Hilbert-bázistétel miatt létezik véges sok homogén invariáns, $h_1, \dots, h_r \in R^+$, melyek generálják az I ideált. Feltehető, hogy $h_1, h_2, \dots, h_r$ minimális generátorhalmaz (azaz ha egyet elhagyunk, már nem generálják I-t). Vegyük észre, hogy ha $\deg h_i > m$, akkor $h_i = \sum_{j=1}^n h_{ij} x_j$, ahol $h_{ij} \in S = K[x_1, \dots, x_n]$ homogén, és $\deg h_{ij} \geq m$, azaz $h_{ij} \in (S^+)^m \subseteq I$. Mivel $m \leq \deg h_{ij} < \deg h_i$, ezért h_{ij} benne van a $h_1, h_2, \dots, h_{i-1}, h_{i+1}, \dots, h_r$ által generált ideálban. Tehát ha $\deg h_i > m$, akkor h_i nem szükséges I generálásához. Tehát abból a feltevésből, hogy $h_1, h_2, \dots, h_r$ minimális generátorhalmaz, következik, hogy $\deg h_i \leq m$.

Ezzel kész is vagyunk, mivel azt már láttuk, hogy ha egy halmaz generálja az I ideált, akkor ugyanaz a halmaz és még az 1 generálja R-t mint K-algebrát. $\square$

Legyen most $K = \mathbb{C}$, és legyen μ egy n-edik primitív egységgyök, továbbá legyen $G = \mathbb{Z}_n$ n-edrendű ciklikus csoport, és legyen σ a $\mathbb{Z}_n$ csoport egy generátora. Ekkor $\sigma \mapsto \mu$ a $\mathbb{Z}_n$ csoport egy reprezentációja. Az, hogy egy $f \in \mathbb{C}[X]$ polinom invariáns, azt jelenti, hogy minden $i \in \{1, 2, \dots, n\}$ esetén $f(\mu^i \cdot x) = f(x)$, tehát $f(x) = g(x^n)$. Azaz $\mathbb{C}[X]^{\mathbb{Z}_n} \simeq \mathbb{C}[X^n]$, szóval erre a reprezentációra nézve $\beta(\mathbb{Z}_n, \mathbb{C}) = n$.

2.2. Molien-tétel

Invariánsok tanulmányozására úgy is gondolhatunk, mint bizonyos operátoroknak az 1 sajátértékhez tartozó sajátalterének vizsgálására. A következő lemma ad egy kényelmes és roppant elegáns módot arra, hogy tetszőleges $G < GL(V)$ véges csoportra kiszámoljuk a G-invariánsok terének dimenzióját.

2.10. Lemma. *Legyen V tetszőleges véges dimenziós vektortér a K nulla karakterisztikájú test felett, és legyen $G < GL(V)$ véges, illetve definiáljuk a következő a V vektortéren értelmezett operátort:*

$$z = \frac{1}{|G|} \sum_{g \in G} g. \tag{2.1}$$

Ekkor a V vektortérbeli fix vektorok terének dimenziója megegyezik a z operátornak a nyomával.

Bizonyítás. Minden $g \in G$ elemre teljesül, hogy $g \cdot z = z$, amiből következik, hogy $(\sum_{g \in G} g)z = |G|z$ ha leosztunk $|G|$-vel, akkor a számolás azt mutatja, hogy $z^2 = z$. Tehát z diagonalizálható, 0 és 1 sajátértékekkel, hiszen z minimálpolinomja osztja $x^2 - x$ polinomot. Legyen $V = V_0 \bigoplus V_1$ z sajátaltereire való felbontás. Az világos, hogy z nyoma megegyezik V_1 dimenziójával, már csak azt kéne látni, hogy V_1 megegyezik a fix vektortok alterével. Legyen $v \in V_1$ és $g \in G$ tetszőleges, ekkor:

$$gv = g(zv) = (gz)v = zv = v.$$

Tehát V_1 benne van a fix vektorok alterében, most vegyünk egy tetszőleges w fix vektort, ekkor:

$$zw = \left(\frac{1}{|G|} \sum_{g \in G} g \right) w = \frac{1}{|G|} \sum_{g \in G} gw = \frac{1}{|G|} \sum_{g \in G} w = \frac{1}{|G|} \cdot |G|w = w$$

Tehát a fix vektorok alterét tartalmazza V_1, tehát a két altér megegyezik és mi pont ezt akartuk belátni. □

2.11. Definíció. Tegyük fel, hogy adott a G csoportnak egy ρ reprezentációja, és legyen a_d a homogén d-edfokú invariánsok alterének dimenziója, ekkor a

$$\Phi(t) = \sum_{d=0}^{\infty} a_d t^d = \sum_{d=0}^{\infty} \dim{(R_d)} t^d$$

formális hatványsor a G csoport ρ reprezentációhoz tartozó Molien-sora.

A következő tételben feltesszük, hogy $K = \mathbb{C}$ vagy $\mathbb{R}$.

2.12. Tétel (Molien-tétel)**.** *Legyen G véges csoport és legyen V véges dimenziós K feletti vektortér, illetve legyen adva egy $\rho : G \to GL(V)$ reprezentáció. Ekkor*

$$\Phi(t) = \frac{1}{|G|}\sum_{g\in G}\frac{1}{det(I - t\rho(g))} \tag{2.2}$$

Bizonyítás. Legyen $\varphi : S \to R$ az a K-lineáris leképezés, mely egy $f \in S$ elemhez rendeli az $f^{\#}$ elemet. Ha f homogén d-edfokú, akkor $f^{\#}$ szintén homogén d-edfokú, ami azt jelenti, hogy φ indukál egy $\varphi|_{S_i} = \varphi_i : S_i \to R_i$ K-lineáris leképezést. Ekkor a 2.10. lemmát felhasználva azt kapjuk, hogy $\mathrm{Rank}(\varphi_i) = \mathrm{Tr}(\varphi_i) = a_i$. Ha ezt most beírjuk a 2.2. egyenletbe, akkor azt kapjuk, hogy

$$\Phi(t) = \sum_{i=0}^{\infty}\dim(R_i)t^i = \sum_{i=0}^{\infty}\mathrm{Tr}(\varphi_i)t^i = \frac{1}{|G|}\sum_{g\in G}\sum_{i=0}^{\infty}\mathrm{Tr}(\rho(g)|_{S_i})t^i =$$
$$\frac{1}{|G|}\sum_{g\in G}\left(\sum_{i=0}^{\infty}\mathrm{Tr}(\rho(g)|_{S_i})t^i\right).$$

Következő lépésként azt fogjuk belátni, hogy ha rögzítünk egy tetszőleges $g \in G$ elemet, akkor arra fennáll, hogy $\sum_{i=0}^{\infty}\mathrm{Tr}(\rho(g)|_{S_i})t^i = det(I - t\rho(g))^{-1}$. Ha $K = \mathbb{R}$ akkor terjesszük ki az alaptestet a $\mathbb{C}$ testre, hogy expliciten a sajátértékekkel és sajátvektorokkal dolgozhassunk. Mivel $\mathbb{C}$ algebrailag zárt, és minden g véges rendű, ezért g diagonalizálható. Legyen $x_1, \dots, x_n$ sajátvektorokból álló bázis az S_1 vektortérben és $\lambda_1, \dots, \lambda_n$ a hozzájuk tartozó sajátértékek. Az S_i vektortérben bázist fognak alkotni az $x_1, \dots, x_n$ változók i-edfokú monomjai. Vizsgáljuk meg egy konkrét $x_1^{\alpha_1}\dots x_n^{\alpha_n}$ monomra, hogy hat $\rho(g)|_{S_i}$:

$$\rho(g)(x_1^{\alpha_1}\dots x_n^{\alpha_n}) = \lambda_1^{\alpha_1}\dots\lambda_n^{\alpha_n}x_1^{\alpha_1}\dots x_n^{\alpha_n}.$$

Ez azt jelenti, hogy $\rho(g)|_{S_i}$ sajátértékei $\lambda_1^{\alpha_1}\dots\lambda_n^{\alpha_n}$, ahol $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ és $\sum\alpha_j = i$, ami azt jelenti, hogy

$$\mathrm{Tr}(\rho(g)|_{S_i}) = \sum_{\alpha_1+\dots+\alpha_n=i}\lambda_1^{\alpha_1}\dots\lambda_n^{\alpha_n}.$$

Ha most mindent összerakunk, akkor a következőt kapjuk:

$$\sum_{i=0}^{\infty}\mathrm{Tr}(\rho(g)|_{S_i})t^i = \prod_{j=1}^{n}\frac{1}{1 - t\lambda_j} = \frac{1}{det(I - t\rho(g))}.$$

Tehát $\Phi(t) = \dfrac{1}{|G|}\displaystyle\sum_{g\in G}\frac{1}{det(I - t\rho(g))}$. □

2.3. Chevalley-Shephard-Todd tétel

A következő néhány fejezetben a Chevalley-Shephard-Todd-tétellel fogunk foglalkozni, mely azt állítja, hogy egy csoportnak polinomgyűrű az invariánsgyűrűje akkor és csak akkor, ha a csoportot tükrözések generálják. Bár minket ez leginkább csak a valós számtest fölött érdekel, a tételek nagyrésze amiket belátunk kissé általánosabban is igaz a komplex számtest felett, komplex tükrözéscsoportokra is, mi most ezt tárgyaljuk, és ehhez először is be kell vezetnünk a tükrözéseknek egy megfelelő általánosítását.

2.13. Definíció. Legyen V véges dimenziós vektortér a K test felett. Egy $S : V \to V$ invertálható K-lineáris leképezést tükrözésnek nevezünk, ha véges a multiplikatív rendje, és $V^g = \{v \in V \mid S(v) = v\}$ egy-kodimenziós altér.

A definícióból egyből adódik, hogy egy S tükrözésnek az 1 $(n-1)$-szeres sajátértéke, és az n-edik sajátértéke egy egységgyök, ami nem lehet az 1. Ha az alaptest nulla karakterisztikájú, akkor egy tükrözés diagonalizálható (sőt, minden olyan esetben amikor az alaptest karakterisztikája és a leképezés rendje relatívprímek). Ha az alaptest $\mathbb{R}$, akkor minden tükrözés $\mathrm{diag}(1, 1, \ldots, 1, -1)$ alakra hozható, és ha a V vektortéren adott egy S-invariáns skaláris szorzás, akkor S egy szokásos tükrözés lesz.

Egy szó a tétel történetéről. Shephard és Todd 1954-ben adták ki a cikküket, melyben klasszifikálták a komplex tükrözéscsoportokat. Ebben a cikkben bebizonyítják az előző tételt, viszont az "akkor" irányt úgy tudták belátni, hogy fáradságosan egyesével leellenőrizték, hogy teljesül-e. 1955-ben Chevalley adott egy egységes bizonyítást az "akkor" irányra valós tükrözéscsoportokra, majd Serre észrevette, hogy a bizonyítás működik komplex tükrözéscsoportokra is.

2.14. Tétel (Chevalley-Shephard-Todd)**.** *Legyen $K = \mathbb{C}$ vagy $\mathbb{R}$, és legyen V egy K feletti n dimenziós vektortér. Ekkor ha adott egy $G < GL(V)$ véges csoport, akkor a következő három állítás ekvivalens:*
(a) A G csoportot tükrözések generálják
(b) Az R algebrát generálja n darab algebrailag független homogén invariáns.
(c) S szabad, végesen generált R-modulus

A tételt nem most egyben bizonyítjuk, hanem először belátjuk, hogy (a)-ból következik (b), azaz belátjuk a Chevalley-tételt, majd megnézzük ennek egy-két fontosabb következményét, ezután nem kevés előkészület után a Jacobi-kritérium című alfejezetben belátjuk, hogy (b)-ből következik (a), aztán a koinvariánsok algebrája című alfejezetben belátjuk azt is, hogy (a)-ból következik (c) illetve, hogy (c)-ből következik (b).

Mielőtt nekiesnénk a Chevalley-tételnek, még szükségünk lesz két lemmára, melyekre a későbbi bizonyításokban többször is hivatkozni fogunk.

2.15. Lemma (Oszthatósági lemma)**.** *Legyen K egy nulla karakterisztikájú test, legyen l egy homogén elsőfokú polinom, $x_1, x_2, \ldots, x_n$ változókkal, és tegyük fel, hogy az f polinom eltűnik l minden nullhelyén. Ekkor az l polinom osztja az f polinomot a $K[x_1, \ldots, x_n]$ gyűrűben, azaz létezik $q \in K[x_1, \ldots, x_n]$, hogy $f = l \cdot q$.*

Bizonyítás. Feltehető, hogy x_n szerepel l-ben nem nulla együtthatóval. Egy pillanatra gondoljunk f és l polinomra úgy, mint x_n polinomjai $K[x_1, \ldots, x_{n-1}]$ gyűrű felett. Osszuk el f polinomot l-el a szokásos egyváltozós osztó algoritmussal, hogy a következő egyenlőséget kapjuk:

$$f = l \cdot q + r,$$

ahol $q \in K[x_1, \ldots, x_n]$, és r-nek x_n-ben 0 a foka, vagyis $r \in K[x_1, \ldots, x_{n-1}]$. Ha $r \neq 0$, keressünk olyan $a_1, \ldots, a_{n-1} \in K$ elemeket melyre $r(a_1, \ldots, a_{n-1}) \neq 0$ (ilyen létezik, mert $|K| = \infty$). Ha ezeket behelyettesítjük l-be, akkor kapunk egy megoldható lineáris egyenletet, azaz létezik a_n melyre $l(a_1, \ldots, a_{n-1}, a_n) = 0$. Így találtunk egy $(a_1, \ldots, a_n) \in K^n$ elemet, melyre

$$f(a_1, \ldots, a_n) = \underbrace{l(a_1, \ldots, a_n)}_{=0} \cdot q(\underline{a}) + \underbrace{r(a_1, \ldots, a_{n-1})}_{\neq 0} \neq 0,$$

na de ha $l(\underline{a}) = 0$, akkor $f(\underline{a}) = 0$. □

2.16. Lemma (Kulcs-lemma)**.** *Legyen $K = \mathbb{C}$ vagy $\mathbb{R}$, legyen $f_1, \ldots, f_r \in R$, legyen J az $f_2, \ldots, f_r$ által generált R-beli ideál, továbbá tegyük fel hogy $f_1 \notin J$. Legyen $I = SR^+$ a szokásos Hilbert ideál. Tegyük fel, hogy $g_1, \ldots, g_r \in S$ homogén, melyre*

$$f_1 g_1 + \cdots + f_r g_r = 0. \tag{2.3}$$

Ekkor $g_1 \in I$.

Bizonyítás. Kezdésként vegyük észre, hogy f_1 nem lehet benne az $f_2, \ldots, f_r$ által generált S-beli ideálban, mert tegyük fel, hogy mégis, akkor

$$f_1 = f_2 h_2 + \cdots + f_r h_r, \quad h_i \in S.$$

Alkalmazzuk mindkét oldalra a Reynolds-operátort:

$$f_1^\# = f_1 = f_2 h_2^\# + \cdots + f_r h_r^\#, \quad h_i^\# \in R.$$

Ez pontosan azt jelenti, hogy $f_1 \in (f_2, \ldots, f_r)$, ami ellentmond az alapfeltevésünknek. Ahhoz, hogy belássuk, hogy $g_1 \in I$, indukciót fogunk alkalmazni g_1 fokára. Ha $g_1 \equiv c \neq 0$ konstans, akkor

$$f_1 = -\frac{h_2 f_2 + \cdots + h_r f_r}{c},$$

tehát f_1 benne van az $f_2, \ldots, f_r$ által generált S-beli ideálban, amiről az imént láttuk be, hogy nem lehet, tehát $g = 0 \in I$.

Tegyük fel, hogy $\deg g_1 > 0$. Vizsgáljunk meg egy tipikus $s \in W$ tükrözést, ahol H az s 1-hez tartozó sajátaltere, és legyen l az a lineáris polinom, melynek a H hipersík a nullhalmaza. Egyből adódik, hogy $s_\alpha g_i - g_i$ eltünik H hipersíkon, mivel s^{-1} pontonként fixálja H hipersíkot, és így használhatjuk a 2.15. oszthatósági lemmát, vagyis

$$sg_i - g_i = lh_i. \tag{2.4}$$

Mivel g_i és sg_i homogének azonos fokkal, ezért feltehető, hogy h_i is homogén, és $\deg h_i < \deg g_i$. Alkalmazzuk s tükrözést a 2.3 egyenletre:

$$0 = s(0) = s(f_1 g_1 + \cdots + f_r g_r) = f_1(sg_1) + \cdots + f_r(sg_r). \tag{2.5}$$

Ha kivonjuk egymásból a 2.3. és 2.5. egyenletet aztán behelyettesítjük a 2.4. egyenletbe, akkor azt kapjuk, hogy:

$$l(f_1 h_1 + \cdots + f_r h_r) = 0.$$

Mivel l nem konstans 0, ezért azt kaptuk, hogy $f_1 h_1 + \cdots + f_r h_r = 0$. Mivel $\deg h_i < \deg g_i$ speciálisan $\deg h_1 < \deg g_1$, ezért a h_1 polinomra alkalmazható az indukciós feltevésünk, tehát $h_1 \in I$. Ha ezt beírjuk a 2.4. egyenletbe, azt kapjuk, hogy $sg_1 - g_1 \in I$, más jelölésekkel $sg_1 \equiv g_1\ (I)$. Mivel W stabilizálja R^+ gyűrűt, ezért speciálisan stabilizálja I ideált is, így W természetesen hat S/I faktorgyűrűn. Az imént épp azt láttuk be, hogy tetszőleges s tükrözés triviálisan hat g_1 képén. Feltevésünk szerint W csoportot generálják a benne lévő tükrözések, így azt kapjuk, hogy tetszőleges $w \in W$ elemre

$$wg_1 \equiv g_1\ (I).$$

Tehát $g_1^{\#} \equiv g_1\ (I)$. Azt már tudjuk, hogy $g_1^{\#} \in R^+$ speciálisan $g_1^{\#} \in I$. Ha ezeket összerakjuk, akkor azt kapjuk, hogy $g_1 \equiv g_1^{\#} \equiv 0\ (I)$, ami pontosan azt jelenti, hogy $g_1 \in I$.

$\square$

2.4. Chevalley-tétel

Chavalley tételének bizonyításánál fontos lesz parciális deriváltakkal foglalkoznunk. Amíg az alaptest $\mathbb{R}$, addig a parciális deriválás összes tulajdonságaira hivatkozhatunk, egyébiránt ezeket a tulajdonságokat n változós polinomok fölött, tisztán algebrailag is definiálhatnánk, mely minden test fölött működne. Mindenesetre szükségünk lesz egy jól ismert formulára.

2.17. Állítás (Euler-formula)**.** *Legyen K egy tetszőleges test, ekkor tetszőleges $f \in K[x_1, \dots, x_n]$ homogén polinomra teljesül, hogy:*

$$\sum_{i=1}^{n} x_i \cdot \frac{\partial f}{\partial x_i} = \deg f \cdot f.$$

□

2.18. Tétel (Chevalley-tétel)**.** *Legyen $K = \mathbb{C}$ vagy $\mathbb{R}$, legyen R a $K[x_1, \dots, x_n]$ gyűrűnek W-invariáns részalgebrája, ahol a W egy véges tükrözéscsoport. Ekkor az R gyűrűt, mint K-algebrát generálja n darab homogén algebrailag független, pozitív fokú homogén polinom, az 1-gyel együtt.*

Bizonyítás. Mint korábban, most is vizsgáljuk az I Hilbert-ideált, melyet a pozitív fokú homogén invariáns polinomok generálnak. Hilbert bázistétele miatt az I ideálhoz választható egy minimális generátorhalmaz: $f_1, \dots, f_r$, melyek homogén pozitív fokúak. A fő célunk az, hogy megmutassuk $f_1, \dots, f_r$ algebrai függetlenségét. Miután ez megvan, akkor 2.5. tétel miatt tudjuk, hogy $f_1, \dots, f_r$ az 1-gyel együtt generálja az R gyűrűt mint K-algebrát, és 2.1. állítás miatt azt is tudjuk, hogy $r = \dim(V)$.

Az algebrai függetlenség belátása kissé trükkös lesz. Először is tegyük fel, hogy $f_1, \dots, f_r$ algebrailag összefügg, tehát létezik egy $h(y_1, \dots, y_r) \in K[y_1, \dots, y_r]$ polinom, melyre:

$$h(f_1, \dots, f_r) = 0. \tag{2.6}$$

Ahhoz, hogy a fokokat nyomon tudjuk követni, h-t kicsit átalakítjuk. Legyen $ay_1^{e_1} \dots y_r^{e_r}$ egy h-ban szereplő monom, továbbá ha $\deg f_i = d_i$, akkor $d = \sum_{i=1}^{r} d_i e_i$ az $af_1^{e_1} \dots f_r^{e_r}$ polinom foka az $x_1, \dots, x_n$ változókban. Válogassuk ki azokat a monomokat, melyek ugyanazt a d fokot adják, és legyen ez az új h polinomunk. Ez nyilván egy nem 0 polinom $y_1, \dots, y_n$ változókban, és erre is teljesül a 2.6 egyenlet. Adott a 2.6. egyenlet, deriváljuk le mindkét oldalt x_k szerint minden k-ra.

$$\sum_{i=1}^{r} h_i \frac{\partial f_i}{\partial x_k} = 0, \text{ ahol } h_i = \frac{\partial h}{\partial y_i}(f_1, \dots, f_r). \tag{2.7}$$

Vegyük észre, hogy h_i homogén elemei R gyűrűnek $d - d_i$ fokkal, továbbá $\frac{\partial f_i}{\partial x_k}$ homogén elemei S-nek. Szeretnénk a 2.16. kulcs-lemmát használni, de sajnos nem biztos, hogy h_i polinomok eleget tesznek a feltételnek. Ha kell számozzuk újra h_i polinomokat úgy, hogy $h_i, \ldots, h_m$ minimális generátor halmaza legyen az összes h_i által generált R-beli ideálnak (természetesen $1 \leq m \leq r$). Ha $i > m$ akkor legyen

$$h_i = \sum_{j=1}^{m} g_{ij} h_j,\ g_{ij} \in R. \tag{2.8}$$

Mint $x_1, \ldots, x_n$ polinomja h_i homogén $d - d_i$ fokú szóval, ha kidobjuk a redundáns tagokat akkor feltehető, hogy a g_{ij} polinomok homogén $d_j - d_i = \deg h_i - \deg h_j$ fokúak. Ha behelyettesítjük a 2.8. egyenletet a 2.7. egyenletbe, akkor fix k-ra azt kapjuk, hogy:

$$\sum_{i=1}^{m} h_i \left(\frac{\partial f_i}{\partial x_k} + \sum_{j=m+1}^{r} g_{ji} \frac{\partial f_j}{\partial x_k} \right) = 0. \tag{2.9}$$

A zárójelben lévő kifejezést nevezzük p_i-nek és vegyük észre, hogy p_i az $x_1, \ldots, x_n$ változókban homogén $d_i - 1$ fokú polinom. Most már alkalmazható a 2.16. lemma, és levonhatjuk azt a következtetést, hogy $p_1 \in I$, és így azt kapjuk, hogy:

$$\frac{\partial f_1}{\partial x_k} + \sum_{j=m+1}^{r} g_{j1} \frac{\partial f_j}{\partial x_k} = \sum_{i=1}^{r} f_i q_i,\ q_i \in S. \tag{2.10}$$

Ez első ránézésre nem tűnik hasznosnak, de ha mindkét oldalt beszorozzuk x_k-val majd összegzünk k-ra, akkor használhatjuk a 2.17. Euler-formulát és a következőt kapjuk:

$$d_1 f_1 + \sum_{j=m+1}^{r} d_j g_{j1} f_j = \sum_{i=1}^{r} f_i r_i,\ \deg r_i > 0. \tag{2.11}$$

A bal oldalon minden elem homogén d_1 fokú, ami azt jelenti, hogy a jobb oldalon $f_1 r_1$ polinomnak ki kell esnie, és az összes többi olyan tagnak, melynek a foka különbözik d_1-től. Miután kidobtunk minden d_1 fokútól különböző polinomot, azt látjuk, hogy 2.11. egyenlet szerint f_1 polinom benne van az $f_2, \ldots, f_r$ által generált S-beli ideálban, ami ellentmond annak a feltevésünknek, hogy $f_1, \ldots, f_r$ minimális generátorhalmaz. □

Az előző tétellel meg is van a Chevalley-Shephard-Todd tétel "(a)-ból következik (b)" állítás. A megfordításhoz szükségünk lesz arra, hogy alaposabban megvizsgáljuk az alapinvariánsokat. A tömörség kedvéért az R gyűrűt generáló homogén algebrailag független (pozitív fokú) polinomok halmazát R egy alapinvaráns halmazának fogjuk mostantól nevezni.

2.5. A fokok egyértelműsége

Az emberben felmerülhet az a romantikus gondolat, hogy ha G tükrözéscsoport, akkor a hozzá tartozó $R = S^G$ invariánsgyűrű algebrailag független generátorai egyértelműek, azaz egyetlen alapinvariáns halmaz van. Ez sajnos nem igaz. Például, ha vesszük a kétváltozós szimmetrikus polinomokat, akkor az $x+y$, x^2+y^2 pontosan ugyanolyan jó algebrailag független generátorrendszernek, mint az $x+y$, xy elemi szimmetrikus polinomok. Szemet szúrhat viszont, hogy a két generátorhalmazban a polinomok fokai megegyeznek, és ez nem is véletlen. Ebben az alfejezetben végig feltesszük, hogy $K = \mathbb{C}$ vagy $\mathbb{R}$.

2.19. Állítás. *Tegyük fel, hogy $f_1, \dots, f_n$ és $g_1, \dots, g_n$ az R gyűrűnek két alapinvariáns halmaza. Ha $deg(f_i) = d_i$ és $deg(g_i) = e_i$, akkor megfelelő újraszámozás után $d_i = e_i$.*

Bizonyítás. Minden f_i felírható egyértelműen g_i-k polinomjaként, és fordítva, ami azt jelenti, hogy minden $(i.j)$ párra használhatjuk a láncszabályt hogy kiértékelhessük a $\frac{\partial f_i}{\partial f_j}$ parciális deriváltakat.

$$\frac{\partial f_i}{\partial f_j} = \sum_{k=1}^{n} \frac{\partial f_i}{\partial g_k} \frac{\partial g_k}{\partial f_j} = \delta_{ij},$$

azaz a $\left(\frac{\partial f_i}{\partial g_j}\right)$ és $\left(\frac{\partial g_i}{\partial f_j}\right)$ mátrixok egymás inverzei, tehát nem nulla a determinánsuk. Ha az első mátrix determinánsát kiírjuk, mint előjeles összeget, akkor azt kapjuk, hogy biztosan létezik egy π permutáció, melyre $\prod_{i=1}^{n} \frac{\partial f_i}{\partial g_{\pi(i)}} \neq 0$. A g_i polinomok megfelelő átszámozása után feltehető, hogy π az identikus permutáció. Azaz f_i mint $g_1, \dots, g_n$ polinomja biztosan tartalmazza a g_i polinomot. Miután kidobtuk a redundáns tagokat, feltehető, hogy minden $g_1^{k_1} \dots g_n^{k_n}$ monom, ami az f_i polinomban szerepel, eleget tesz annak, hogy $d_i = \sum_{j=1}^{n} e_j k_j$, tehát $e_i \leq d_i$; speciálisan az is igaz, hogy $\sum e_i \leq \sum d_i$. Csináljuk meg ugyanezt a másik mátrixszal, azzal megkapjuk a fordított egyenlőtlenségeket, végül azt kapjuk, hogy $e_i = d_i$. □

Ezeket a $d_1, \dots, d_n$ számokat a G tükrözéscsoport fokainak hívják. Az, hogy a fokok egyértelműek, nemsokára fontos lesz nekünk, amikor a Chevalley-tétel megfordítását szeretnénk bebizonyítani.

2.20. Állítás. *Mindkét oldalt a t hatványsorának tekintve a következőt kapjuk:*

$$\frac{1}{|G|} \sum_{g \in G} \frac{1}{det(I - tg)} = \prod_{i=1}^{n} \frac{1}{1 - t^{d_i}}. \tag{2.12}$$

Bizonyítás. A bal oldalon t^k együtthatója a Molien-tétel (2.12) szerint R_k dimenziója, viszont R_k dimenzióját másképp is megkaphatjuk. Ha $f_1, \dots, f_n$ egy alapinvariáns halmaz, d_i fokokkal, akkor a $f_1^{e_1} \dots f_n^{e_n}$, $\sum d_i e_i = k$ monomok bázist alkotnak R_k-ban. Az olyan $(e_1, \dots, e_n)$ szám-n-esek száma, melyekre $\sum d_i e_i = k$, éppen t^k együtthatója a következő hatványsorból:

$$(1 + t^{d_1} + t^{2d_1} + \dots)(1 + t^{d_2} + t^{2d_2} + \dots) \dots (1 + t^{d_n} + t^{2d_n} + \dots),$$

mely pontosan a jobb oldali szorzat. □

2.21. Tétel. *Legyenek $d_1, \dots, d_n$ a G tükrözéscsoport fokai, illetve legyen N a G-beli tükrözések száma, ekkor $d_1 d_2 \dots d_n = |G|$ és $d_1 + d_2 + \dots + d_n = N + n$.*

Bizonyítás. Először is vegyük észre, hogy G elemei közül egyedül az identitásra teljesül, hogy a karakterisztikus polinomjának n-szeres gyöke az 1, illetve, csak az identitásnak és az N darab tükrözésnek $(n-1)$-szeres gyöke az 1, tehát a $\det(I - tg)$ karakterisztikus polinom egyenlő az $(1-t)^n$ polinommal ha g az identitás, és egyenlő az $(1-t)^{n-1}(1-\alpha_g t)$ polinommal, ha g komplex tükrözés, minden egyéb $g \in G$ elemre g karakterisztikus polinomja nem osztható az $(1-t)^{n-1}$ polinommal, ezért ha a 2.12. egyenletet beszorzom az $(1 - t)^n$ polinommal a következőt kapom:

$$\prod_{i=1}^{n} \frac{1-t}{1-t^{d_i}} = \prod_{i=1}^{n} \frac{1}{1 + \dots + t^{d_i - 1}} = \frac{1}{|G|}\Big(1 + (1-t)\Big(\sum_{g \in H} \frac{1}{1-\alpha_g t}\Big) + (1-t)^2 G(t)\Big),$$

ahol H a G-ben lévő tükrözések halmaza, α_g a g tükrözésnek a sajátértéke, mely egy n-edik egységgyök valamilyen $n > 1$-re, és a $G(t)$ nevezőjét nem osztja az $(1 - t)$. Ezért ha most behelyettesítek t helyére 1-et, akkor azt kapom, hogy:

$$\prod_{i=1}^{n} \frac{1}{d_i} = \frac{1}{|G|}.$$

Tehát a fokok szorzata megegyezik a csoport rendjével. Most deriváljuk formálisan mindkét oldalt t szerint. Ekkor a bal oldal a következő lesz:

$$\left(\prod_{i=1}^{n} \frac{1}{1 + t + \dots + t^{d_i - 1}}\right)\left(\sum_{i=1}^{n} -\frac{1 + 2t + 3t^2 + \dots + (d_i - 1)t^{d_i - 2}}{1 + t + \dots + t^{d_i - 1}}\right).$$

Ha most t helyére 1-et írunk, akkor azt kapjuk, hogy a bal oldal megegyezik a $\frac{-1}{2|G|} \sum_{i=1}^{n} (d_i - 1)$ számmal. Most vizsgáljuk meg, hogy a jobb oldalból mi lett a deriválás után:

$$\frac{1}{|G|} \sum_{g \in H} -\frac{1-\alpha_g}{(1-\alpha_g t)^2} + H(t),$$

ahol $H(t)$ számlálója osztható $(1-t)$-vel, ezért, ha most t helyére 1-et írunk, azt kapjuk, hogy

$$\frac{1}{|G|}\sum_{g\in H} -\frac{1}{1-\alpha_g}.$$

Csoportosítsuk a tükrözéseket aszerint, hogy melyik L hipersíkot hagyják pontonként fixen. Rögzített L hipersíkra, az L hipersíkot fixáló tükrözések az identitással együtt, egy $P_L \in \mathbb{N}$ rendű ciklikus csoportot alkotnak, ahol $(P_L - 1)$ az L-t fixáló tükrözések száma a G csoportban. Ebből adódóan azt kaptuk, hogy minden fix hipersíkhoz tartozik egy külön szumma, ami a következő alakban írható:

$$-\left(\frac{1}{1-\Phi_L}+\frac{1}{1-\Phi_L^2}+\cdots+\frac{1}{1-\Phi_L^{P_L-1}}\right) = -\frac{1}{2}(P_L-1),$$

ahol $\Phi_L = exp(\frac{2\pi i}{P_L})$. Szummázunk L-re, hogy a következőt kapjuk:

$$-\frac{1}{2|G|}\sum_{i=1}^{n}(d_i-1) = \frac{1}{|G|}\sum_{L}\left(\sum_{i=1}^{P_L-1} -\frac{1}{1-\Phi_L^i}\right) = -\frac{1}{2|G|}N$$

Ha most mindkét oldalt felszorozzuk a $(-\frac{1}{2|G|})$ számmal, akkor azt kapjuk, hogy $\sum_{i=1}^{n}(d_i-1) = N$, tehát $\sum d_i = N+n$. □

2.6. Jacobi-kritérium

Van egy egyszerű kritérium az algebrai függetlenség ellenőrzésére tetszőleges nulla karakterisztikájú test felett n darab $f_1,\dots,f_n$ n változós polinom esetében. Ennek a tételnek a birtokában már elintézhetjük a Chevalley-tétel megfordítását.

Jelölje $J(f_1,\dots,f_n)$ annak a mátrixnak a determinánsát, melynek (i,j)-edik eleme $\frac{\partial f_i}{\partial x_j}$. Ezt a $J(f_1,\dots,f_n)$ polinomot Jacobi-determinánsnak nevezzük.

2.22. Tétel (Jacobi-kritérium). *Az $f_1,\dots,f_n \in K[x_1,\dots,x_n]$ polinomok akkor és csak akkor algebrailag függetlenek a (tetszőleges nulla karakterisztikájú) K test felett, ha $J(f_1,\dots,f_n)$ nem az azonosan nulla polinom.*

Bizonyítás. Tegyük fel, hogy $f_1,\dots,f_n$ algebrailag összefügg, tehát létezik $h(y_1,\dots,y_n)\neq 0$, melyre $h(f_1,\dots,f_n)\equiv 0$. Továbbá tegyük fel azt is, hogy h foka a lehető legkisebb. Deriváljuk mindkét oldalt x_j szerint:

$$\sum_{i=1}^{n}\frac{\partial h}{\partial y_i}(f_1,\dots,f_n)\frac{\partial f_i}{\partial x_j} = 0 \tag{2.13}$$

Ez az egyenlet minden j-re $(1\le j\le n)$ egy egyenletrendszert ad $K(x_1,\dots,x_n)$ felett, ahol az együtthatómátrix (i,j)-edik eleme $\frac{\partial f_i}{\partial x_j}$, és a "változók" $\frac{\partial h}{\partial y_i}(f_1,\dots,f_n)$. Mivel

h nem konstans, ezért nem fog minden $\frac{\partial h}{\partial y_i}$ eltűnni, és mivel minden parciális deriváltnak kisebb a foka h polinomnál, ezért $\frac{\partial h}{\partial y_i}(f_1, \ldots, f_n)$ polinomok nem az azonosan nulla polinomok. Ez azt jelenti, hogy $K(x_1, \ldots, x_n)$ test felett van egy nem triviális megoldása az $n \times n$-es homogén egyenletrendszernek, tehát $J(f_1, \ldots, f_n) = 0$.

A fordított irány kevésbé egyenes. Mivel $K(x_1, \ldots, x_n)$ transzcendencia foka K felett n, ezért minden i-re $x_i, f_1, \ldots, f_n$ algebrailag összefügg. Legyen $h_i(y_0, y_1, \ldots, y_n)$ a lehető legkisebb fokú pozitív fokú, melyre

$$h_i(x_i, f_1, \ldots, f_n) \equiv 0 \tag{2.14}$$

Deriváljuk 2.14. egyenletet x_k szerint. Ekkor a következőt kapjuk:

$$\sum_{i=1}^{n} \frac{\partial h_i}{\partial y_j}(x_i, f_1, \ldots, f_n)\frac{\partial f_j}{\partial x_k} + \frac{\partial h_i}{\partial y_0}(x_i, f_1, \ldots, f_n)\delta_{ik} = 0 \tag{2.15}$$

Mivel $f_1, \ldots, f_n$ algebrailag függetlenek, ezért minden i-re h_i polinomnak y_0 változóban pozitív a foka. Mivel $\frac{\partial h_i}{\partial y_0}$ foka kisebb mint h_i polinomé, ezért $\frac{\partial h_i}{\partial y_0}$ az $(x_i, f_1, \ldots, f_n)$ helyen nem 0 (nem az azonosan 0 polinom). Az 2.15. egyenlet minden ilyen tagját vigyük át a jobb oldalra, és írjük az egyenletrendszert mátrix formában, hogy a következőt kapjuk:

$$\frac{\partial h_i}{\partial y_j}\frac{\partial f_i}{\partial x_j} = -\delta_{ij}\frac{\partial h_i}{\partial x_j} \tag{2.16}$$

Itt a jobb oldal egy diagonális mátrix nem nulla elemekkel, tehát nem nulla a determinánsa, és így $J(f_1, \ldots, f_n)$ sem lehet 0. □

2.23. Következmény. *Tegyük fel, hogy $f_1, \ldots, f_n$ algebrailag független homogén polinomok, és $\deg(f_i) = d_i$, ekkor $J(f_1, \ldots, f_n)$ homogén $\sum(d_i - 1) = N$ fokú.*

Bizonyítás. Az előző tétel azt mutatja, hogy $J(f_1, \ldots, f_n) \neq 0$, és ha kifejtük a determinánst összeg alakban, akkor minden egyes tag

$$\frac{\partial f_1}{\partial x_{\pi(1)}} \cdot \ldots \cdot \frac{\partial f_n}{\partial x_{\pi(n)}}$$

alakú, valamely π permutációra. A szummában minden egyes (nem nulla) ilyen típusú szorzatra igaz, hogy a benne szereplő polinomok homogén $d_1 - 1, \ldots, d_n - 1$ fokúak, azaz a szorzatpolinom foka $\sum(d_i - 1) = N$. □

2.24. Tétel. *Legyen $K = \mathbb{C}$ vagy $\mathbb{R}$, és legyen V egy n dimenziós K feletti vektortér. Ha $G < GL(V)$ véges csoport, és az S^G gyűrűt generálja n darab algebrailag független homogén invariáns, akkor a G csoportot generálják azon tükrözések, melyeket G tartalmaz.*

Bizonyítás. Nézzük azt a $H \subseteq G$ részcsoportot, melyet a G-beli tükrözések generálnak, ekkor a 2.18. Chevalley-tétel szerint az S^H gyűrűt generálja n darab algebrailag független homogén invariáns: $f_1, \ldots, f_n$. Legyenek $g_1, \ldots, g_n$ az S^G gyűrű generátorai, illetve legyen $d_i = \deg(f_i)$ és $e_i = \deg(g_i)$. Mivel $H \subseteq G$, ezért $S^G \subseteq S^H$, ezért a g_i invariánsok felírhatók az f_i elemek polinomjaként. Miután a redundáns tagokat kidobtuk, feltehető, hogy minden g_i polinomban szereplő $f_1^{k_1} \ldots f_n^{k_n}$ monomra teljesül, hogy $\sum k_j d_j = e_i$. Szeretnénk valahogy összehasonlítani a d_i és e_i fokokat, ehhez deriváljuk a g_i polinomot az x_k változó szerint, és használjuk a láncszabályt, hogy megkapjuk a következőt:

$$\frac{\partial g_i}{\partial x_k} = \sum_{j=1}^{n} \frac{\partial g_i}{\partial f_j} \frac{\partial f_j}{\partial x_k}$$

Hála az előző tételnek, a $\det(\frac{\partial g_i}{\partial x_k})$ Jacobi-determináns nem nulla, szóval az a Jacobi-determináns sem nulla, mely a $\frac{\partial g_i}{\partial f_j}$ elemeket tartalmazza. Ez azt jelenti, hogy megfelelő átszámozás után, ha kifejtjük a determinánst, akkor azt kapjuk, hogy:

$$\frac{\partial g_1}{\partial f_1} \cdots \frac{\partial g_n}{\partial f_n} \neq 0$$

Amiből levonhatjuk azt a következtetést, hogy $d_i \leq e_i$ minden i-re. Viszont a 2.21. tétel alkalmazható H és G csoportra is, azaz $\sum(e_i - 1) = N = \sum(d_i - 1)$, tehát minden i-re $d_i = e_i$, de szintén a 2.21. tételből tudjuk, hogy $|G| = \prod e_i = \prod d_i = |H|$, tehát $H = G$. □

2.7. Koinvariánsok modulusa

Ebben a fejezetben befejezzük a Chevalley-Shephard-Todd-tétel bizonyítását. Először az (a)-ból (c) irányt látjuk be, majd utána a (c)-ből (b) irányt.

2.25. Lemma. *Legyen a B egységelemes gyűrű része az A integritásitartománynak, és legyen $F = frac(B)$ illetve $E = frac(A)$. Tegyük fel, hogy E/F véges testbővítés. Ekkor ha A egy szabad B-modulus n ranggal, akkor $[E : F] = n$, sőt A bármely B-modulus-bázisa vektortér-bázis E-ben.*

Bizonyítás. Legyen $a_1, \ldots, a_n$ egy bázisa az A modulusnak. Legyen $p, q \in A$, $q \neq 0$. Azt szeretnénk belátni, hogy p/q előáll az $a_1, \ldots, a_n$ elemek F-lineáris kombinációjaként. Ehhez elég belátni, hogy $1/q$ előáll, mert tegyük fel, hogy $p = \sum_{i=1}^{n} f_i a_i$, és $1/q = \sum_{j=1}^{n} g_j a_j$, ahol $f_i, g_j \in F$, akkor:

$$p/q = \left(\sum_{i=1}^{n} f_i a_i\right) \left(\sum_{j=1}^{n} g_j a_j\right) = \sum_{i,j=1}^{n} f_i g_j \cdot a_i a_j,$$

ahol $f_i g_j \in F$ és minden $(i.j)$ párra $a_i a_j$ előáll $a_1, \dots a_n$ elemek B-lineáris kombinációjaként, tehát p/q előáll az a_i elemek F-lineáris kombinációjaként.

Most lássuk be, hogy $1/q$ előáll a kívánt alakban. Mivel A véges bővítése a B gyűrűnek, ezért minden $a \in A$ egész B felett. Tehát létezik egy $m_q(x) \in B[x]$ egy főegyütthatójú polinom, melyre $m_q(q) = 0$, azaz:

$$q^l + b_{l-1}q^{l-1} + \cdots + b_0 = 0.$$

Mivel A tartomány, ezért feltehető, hogy b_0 nem 0, mert ha 0 lenne, akkor csak kiemelném x-et az m_q polinomból, így ha rendezzük az egyenletet, a következőt kapjuk:

$$q(q^{l-1} + b_{l-1}q^{l-2} + \cdots + b_1) = -b_0.$$

Mivel $q^i \in A$ $(i = 1, \dots, l)$, ezért a zárójelben lévő kifejezés előáll az a_i elemek B-lineáris kombinációjaként, így ha még leosztunk a $(-b_0)q$ elemmel, akkor megkapjuk $1/q$ kívánt alakját.

A függetlenség triviális, mert ha kapnánk egy F-lineáris összefüggést E-ben, akkor a nevezőkkel felszorozva az A gyűrűben is kapnánk egy B-lineáris összefüggést, ami csakis a triviális lehet. $\square$

2.26. Tétel. *Legyen $K = \mathbb{C}$ vagy $\mathbb{R}$, és V egy K feletti vektortér. Ha a $G < GL(V)$ véges csoportot tükrözések generálják, akkor S szabad R-modulus $|G|$ ranggal.*

Bizonyítás. A bizonyítás alap ötlete az, hogy összeshasonlítjuk az S R-modulust az S/I vektortérrel, ahol az $I = SR^+$ ideál a szokásos Hilbert-ideál. Először is válasszunk olyan $g_\alpha \in S$ homogén polinomokat, melyeknek $\overline{g_\alpha} = g_\alpha + I$ mellékosztályai kifeszítik az S/I vektoretet. Azt állítjuk, hogy ekkor a g_α polinomok kifeszítik az S gyűrűt mint R-modulust. Nyilván az a T modulus amit generálnak fokszám szerint gradált, tehát elég d-re való indukcióval belátni, hogy $T_d = S_d$. Mivel $S_0 \cap I = 0$, ezért valamely g_α polinomnak 0 fokúnak kell lennie, tehát $T_0 = S_0$. Legyen $d > 0$, és vegyünk egy $f \in S_d$ polinomot. Az f polinomot felírhatjuk a következő alakban:

$$f = \sum_\alpha c_\alpha g_\alpha + \sum_\beta f_\beta h_\beta$$

ahol $c_\alpha \in K$, $h_\beta \in R^+$ homogén invariáns, és $f_\beta \in S$ szintén homogén, melynek szigorúan kisebb a foka $\deg f$-nél, tehát f_β polinomokra alkalmazhatjuk az indukciós feltevésünket, azaz $f_\beta \in T$, így megkaptuk az f polinomot a g_α polinomok R-lineáris kombinációjaként, tehát $f \in T$.

Most tegyük fel, hogy $g_1, \dots, g_m \in S$ homogén polinomok, melyeknek $\overline{g_i}$ mellékosztályai lineárisan függetlenek S/I vektortérben. Belátjuk m szerinti indukcióval, hogy ekkor ezek az elemek függetlenek az S-ben mint R-modulusuban is. Ha $m = 1$

akkor kész vagyunk. Most tegyük fel, hogy a g_i polinomoknak van egy R-lineáris kombinációja, ami a 0-t adja:

$$f_1 g_1 + \dots + f_m g_m = 0. \tag{2.17}$$

Feltehető, hogy mindegyik $f_i \in R$ homogén polinom. Mivel $g_1 \notin I$, ezért most alkalmazhatjuk a 2.16. kulcs-lemmát, és levonhatjuk azt a következtetést, hogy

$$f_1 = h_1 f_2 + \dots + h_m f_m,$$

ahol $h_i \in R$ homogén. Ezt helyettesítsük vissza a 2.17 egyenletbe, hogy a következőt kapjuk:

$$f_2(g_2 + h_2 g_1) + f_3(g_3 + h_3 g_1) + \dots + f_m(g_m + h_m g_1) = 0.$$

Vegyük észre, hogy minden $g_i + h_i g_1$ polinom homogén, és a mellékosztályaik továbbra is lineárisan függetlenek az S/I vektortérben, tehát alkalmazhatjuk az indukciós feltevésünket, ami szerint $f_2, \dots, f_m = 0$, és így $f_1 = 0$.

Összességében azt kaptuk, hogy ha veszünk egy bázist az S/I vektortérben, akkor az ad egy bázist az S R-modulusnak, tehát S szabad R-modulus. Az előző lemma szerint pedig S rangja megyezik $\mathrm{frac}(S)$ testnek a $\mathrm{frac}(R)$ test feletti dimenziójával, ami az első fejezet 2.1. állítása szerint éppen $|G|$. □

2.27. Lemma. *Legyen B egy K-algebra (K egy tetszőleges test) és A egy részalgebrája. Ha B végesen generált K-algebra, és egész A felett, akkor A végesen generált K felett.*

Bizonyítás. Mivel B végesen generált K-algebra, ezért $B = K[b_1, \dots, b_s]$. Mivel B egész A felett, ezért a b_i elemek eleget tesznek egy A együtthatós egyenletnek:

$$b_i^{n_i} + a_{i,1} b_i^{n_i - 1} + \dots + a_{i,n_i} = 0$$

Legyen $a_1, \dots, a_t \in A$ azon elemek halmaza, melyek előfordulnak együtthatóként, és legyen $A' = K[a_1, \dots, a_t]$. Az A' gyűrű Noether, hiszen $K[x_1, \dots, x_t]$ hányadosa, továbbá B egész A' felett, szóval B véges A'-modulus. Mivel A' Noether-gyűrű, és A részmudulusa a B A'-modulusnak, ezért A szintén végesen generált A'-modulus. Legyen $a_{t+1}, \dots, a_n \in A$ az A egy generátorhalmaza, ekkor $A = K[a_1, \dots, a_n]$. □

2.28. Lemma. *Legyen $A = \bigoplus_{d \geq 0} A_d$ egy gradált K-algebra (K egy tetszőleges test). Ha az $A^+ = \bigoplus_{d > 0} A_d$ homogén ideált véges sok elem generálja, akkor az A gyűrű végesen generált A_0-algebra.*

Bizonyítás. Először is vegyük észre, hogy a gradáltság definíciója garantálja, hogy A_0 egy gyűrű, tehát az állítás értelmes, ami kezdésnek egész jó. Tegyük fel, hogy az A^+ ideált az $a_0, \dots, a_s \in A^+$ homogén elemek generálják. Azt állítjuk, hogy ekkor $A = A_0[a_0, \dots, a_s]$. Az, hogy $A_0[a_0, \dots, a_s] \subseteq A$ triviális, a másik irányhoz d szerinti indukcióval azt látjuk be, hogy $A_d \subseteq A_0[a_0, \dots, a_s]$. Ha $d = 0$ akkor kész vagyunk. Tegyük fel, hogy $d > 0$, és $a \in A_d$, ekkor $a = b_1 a_1 + \dots + b_s a_s$, ahol $b_i \in A_{i_j}$, $i_j < d$, ezért b_i elemekre alkalmazhatjuk az indukciós feltevésünket, és így azt kapjuk, hogy minden i-re $b_i = \sum c_{j,i} a_i$, ha ezt visszaírjuk akkor azt látjuk, hogy $a \in A_0[a_0, \dots, a_s]$. □

A következő állításban V egy n dimenziós vektortér a K nulla karakterisztikájú test felett, és $S = S(V^*)$, ahogy eddig is, V duális terének szimmetrikus algebrája, ami azonosítható a $K[x_1, \dots, x_n]$ gyűrűvel.

2.29. Állítás. *Ha S egy véges rangú, szabad R-modulus homogén bázissal, valamilyen $R \subseteq S$ gradált részalgebrára, akkor R-et mint K-algebrát generálja n darab algebrailag független homogén elem.*

Bizonyítás. Mivel S véges R-modulus, ezért egész is R felett, tehát alkalmazható a 2.27. lemma, amiből azt kapjuk, hogy R Noether-gyűrű. Legyen $R^+ = \bigoplus_{d>0} R_d$ ideál az R gyűrűben. Mivel R Noether, és R^+ egy homogén ideál, ezért R^+ generálható véges sok homogén $f_1, \dots, f_m$ elemmel. A 2.28. lemma szerint ekkor R megegyezik a $K[f_0, \dots, f_m]$ gyűrűvel, tehát nekünk már "csak" az algebrai függetlenséggel kell foglalkoznunk.

Az algebrai függetlenség belátása kb ugyanúgy néz ki, mint a Chevalley-tételnél, azzal a különbséggel, hogy most nincs kulcs-lemmánk, de sebaj, másoljuk a korábbi bizonyítást amíg lehet, és amint elakadunk, elkezdhetünk gondolkodni. Először is azonosítsuk az S gyűrűt a $K[x_1, \dots, x_n]$ gyűrűvel, és tegyük fel, hogy $f_1, \dots, f_m$ algebrailag összefügg, tehát létezik egy $h \in K[y_1, \dots, y_m]$ polinom, melyre

$$h(f_1, \dots, f_m) = 0 \tag{2.18}$$

Tegyük fel, hogy h minimális fokú melyre teljesül, hogy eltünik az $(f_1, \dots, f_m)$ helyen. Legyen $\deg f_i = d_i$, és megint válogassuk ki azokat a h polinombeli monomokat, melyek az f_i polinomok behelyettesítése után az x_i változókban ugyanazt a d fokot adják. Ez a csonkított h továbbra is minimális fokú, és eltűnik az $(f_1, \dots, f_n)$ helyen. Megint mint múltkor, deriváljuk a 2.18. egyenletet, hogy a következőt kapjuk:

$$\sum_{i=1}^{m} h_i \frac{\partial f_i}{\partial x_l} = 0, \text{ ahol } h_i = \frac{\partial h}{\partial y_i}(f_1, \dots, f_m) \tag{2.19}$$

Mint múltkor, most is $h_i \in R$ homogén $d - d_i$ fokú polinom, továbbá nem mind nulla mivel h minimális fokú. Vegyük a $h_1, \dots, h_m$ polinomok által generált J ideált az

R gyűrűben. Megfelelő átszámozás után feltehető, hogy $h_1, \ldots, h_s$ minimális generátorhalmaza a J ideálnak. Mivel $h_1, \ldots, h_s$ generálja a J ideált, ezért minden i-re $(s+1 \leq i \leq m)$ létezik $g_{ij} \in R$, melyre:

$$h_i = \sum_{j=1}^{s} g_{ij} h_j \tag{2.20}$$

Ha ezt visszaírjuk a 2.19. egyenletbe, akkor a következőt kapjuk:

$$\sum_{i=1}^{s} h_i \left(\frac{\partial f_i}{\partial x_l} + \sum_{j=s+1}^{m} g_{ji} \frac{\partial f_j}{\partial x_l} \right) = 0 \tag{2.21}$$

Nevezzük el a zárójelben lévő kifejezést P_{il} -nek, és vegyük észre, hogy a $P_{il} \in R$ polinom homogén $(d_i - 1)$ fokú. A Chevalley-tételnél itt használtuk a kulcs-lemmát ahhoz, hogy belássuk, hogy P_{il} kifejezhető az f_i polinomokkal, és most is ezt szeretnénk belátni, pontosabban azt, hogy $P_{il} \in R^+$. Most nincs kulcs-lemmánk, viszont tudjuk, hogy $P_{il} \in S$, és az S gyűrűnek létezik R felett egy $e_\lambda \in S$, $\lambda \in \Lambda$ bázisa, ahol e_λ homogén, és Λ véges halmaz. Tehát P_{il} felírható e_λ polinomok R-beli együtthatós kombinációjaként:

$$P_{il} = \sum_{\lambda} P_{il\lambda} e_\lambda \tag{2.22}$$

Mivel e_λ homogén, ezért feltehető, hogy $P_{il\lambda} \in R$ szintén homogén. Most azt szeretnénk megkapni, hogy $P_{il\lambda} \in R^+$, ehhez írjuk vissza a 2.22. egyenletet a 2.21. egyenletbe, hogy a következőt kapjuk:

$$\sum_{i=1}^{s} h_i P_{il\lambda} = 0 \tag{2.23}$$

Mivel $h_1, \ldots, h_s$ minimális generátorrendszer, ezért ha egy $P_{il\lambda}$ polinom nem nulla, akkor biztosan pozitív fokú homogén, tehát $P_{il\lambda} \in R^+$. Mivel $P_{il\lambda} \in R^+$, ezért $P_{il} \in R^+$, tehát P_{il} megkapható az f_i polinomokkal:

$$P_{il} = \frac{\partial f_i}{\partial x_l} + \sum_{j=s+1}^{m} g_{ji} \frac{\partial f_j}{\partial x_l} = \sum_{h=1}^{m} u_{ilh} f_h \tag{2.24}$$

Mivel minden f_i homogén, ezért teljesül az Euler-formula, azaz:

$$d_i f_i = \sum_{l=1}^{n} x_l \frac{\partial f_i}{\partial x_l}$$

Rögzítsünk egy i-t ($1 \leq i \leq s$), majd szorozzuk be P_{il} polinomot x_l-el, és szummázunk l-re, hogy a következőt kapjuk:

$$d_i f_i + \sum_{j=s+1}^{m} d_j r_{ji} f_j = \sum_{h=1}^{m} \sum_{l=1}^{n} u_{ilh} x_l f_h \tag{2.25}$$

Ha vesszük a homogén d_i fokú tagokat, akkor azt kapjuk, hogy f_i S-lineáris kombinációja a többi f_j polinomnak ($j \neq i$). Mivel S szabad R felett, és $f_1, \ldots, f_m \in R$, ezért f_i polinomot megkaphatjuk az f_j polinomok R-lineáris kombinációjaként is, ami ellentmond annak, hogy $f_1, \ldots, f_m$ minimális generátorrendszer. □

Vegyük észre, hogy az előző állításnak speciális esete az, ami a Chevalley-Shephard-Todd-tételben szerepel, tehát ezzel tényleg beláttuk a három állítás ekvivalenciáját.

2.8. Példák

Mostantól visszatérünk a valós esethez, tehát az alaptest mindig $\mathbb{R}$, és valós tükrözéscsoportok invariánsgyűrűjével fogunk foglalkozni. Ebben a fejezetben megadjuk az $\mathbf{A}_n$, $\mathbf{B}_n$, $\mathbf{D}_n$ valós tükrözéscsoportoknak egy-egy alapinvariáns halmazát. Ezeknek a megadása a következő állításon múlik.

2.30. Állítás. *Legyen $g_1, \ldots, g_n$ homogén invariánsai a W tükrözéscsoportnak, és legyen $deg(g_i) = e_i$ minden i-re. Ekkor ha a $g_1, \ldots, g_n$ polinomok algebrailag függetlenek, és $\prod e_i = |W|$, akkor $g_1, \ldots, g_n$ egy alapinvariáns halmaza a W csoportnak.*

Bizonyítás. Először is feltehető, hogy $e_1 \leq e_2 \leq \cdots \leq e_n$. Legyen $f_1, \ldots, f_n$ egy alapinvariáns halmaz, $d_1 \leq d_2 \leq \cdots \leq d_n$ fokokkal. Mivel g_1 az f_i polinomok polinomja, ezért nyilvánvaló, hogy $e_1 \geq d_1$. Azt állítjuk, hogy ez az egyenlőtlenség fennáll minden i-re, különben tegyük fel, hogy k az első olyan index amire $e_k < d_k$. Ez azt jelenti, hogy $g_1, \ldots, g_k$ polinomok az $f_1, \ldots, f_{k-1}$ polinomok polinomjai. Viszont a $g_1, \ldots, g_k$ polinomok által generált racionális törtfüggvények teste k transzcendenciafokú az $\mathbb{R}$ test felett, és azt nem tartalmazhatja egy nála kisebb transzcendenciafokkal rendelkező test.

Hála a 2.21. tételnek, és a feltevésünknek $\prod d_i = |W| = \prod e_i$, ami miatt $e_i = d_i$ minden i-re. Így azt látjuk, hogy minden rögzített d-re a g_i polinomok által generált algebrában a homogén d fokú elemek dimenziója megegyezik az f_i polinomok által generált algebra homogén d fokú elemeinek dimenziójával. Következésképp a g_i polinomok alapinvariáns halmazt alkotnak. □

Ezzel az állítással a tarsolyunkban nekiállhatunk megadni az imént említett csoportok alapinvariánsait. Először nézzük a $W = \mathcal{S}_{n+1}$, $\mathbf{A}_n$ típusú csoportot. Mint azt írtuk, az $\mathcal{S}_{n+1}$ csoport úgy hat az $\mathbb{R}^{n+1}$ téren, hogy permutálja a koordinátákat. Ahelyett, hogy az elemi szimmetrikus polinomokat néznénk, vegyük inkább a következő polinomokat:

$$f_i = x_1^i + x_2^i + \cdots + x_{n+1}^i, \text{ ahol } 1 \leq i \leq n+1.$$

Ezen polinomok szorzatának a foka $(n+1)! = |W|$, tehát már csak az algebrai függetlenséget kell ellenőrizni, ehhez pedig használjuk a Jacobi-kritériumot.

Legyen $1 \leq i, j \leq (n+1)$, ekkor

$$\frac{\partial f_i}{\partial x_j} = i x_j^{i-1}.$$

Tehát azt kaptuk, hogy $J = J(f_1, \ldots, f_{n+1})$ nem más, mint $(n+1)! \cdot V$, ahol V a Vandermonde-determináns. Tehát $f_1, \ldots, f_{n+1}$ egy alapinvariáns halmaz.

Ha a W csoport $\mathbf{B}_n$ típusú akkor nagyon hasonlóan érvelhetünk mint előbb. Most W úgy hat a változókon, hogy permutálja őket, vagy megváltoztatja az előjelüket, tehát az előzőkhoz hasonló polinomokkal próbálkozhatunk, csak egy kis modosítással el kell érni, hogy invariáns maradjon az előjelváltások alatt, amit a négyzetre emeléssel el is érhetünk, ennek okán nézzük a következő polinomokat:

$$f_i = x_1^{2i} + x_2^{2i} + \cdots + x_n^{2i}, \text{ ahol } 1 \leq i \leq n.$$

Most az f_i polinomok szorzatának a foka $2^n \cdot n! = |B_n|$, tehát ismét csak az algebrai függetlenség kell. Egyszerű számolásból látszik, hogy az így kapott jacobi-determináns $J(f_1, \ldots, f_n) = 2^n \cdot n! \cdot \prod_{1 \leq i < j \leq n} (x_j^2 - x_i^2)$, ami nem a konstans nulla.

Ha most a W csoport $\mathbf{D}_n$ típusú, akkor úgy hat az $x_1, \ldots, x_n$ változókon, hogy permutálja őket, vagy páros soknak megváltoztatja az előjelét. Mivel a hatás nagyon hasonlít az előzőhöz, ezért nem túl meglepő módon, az előző polinomok egy kis változtatásával megkaphatjuk ennek a csoportnak az alapinvariánsait, azaz nézzük a következő polinomokat:

$$f_i = \sum_{j=1}^{n} x_j^{2i}, \text{ ha } 1 \leq i \leq n-1, \text{ és } f_n = x_1 x_2 \ldots x_n.$$

Most a szorzatnak a foka $2^{n-1} \cdot n! = |W|$, tehát a rend rendben van. Az algebrai függetlenség szintén fennáll, mert kissé macerás számolás után kijön, hogy $J(f_1, \ldots, f_n) = 2^{n-1}(n-1)! \prod_{1 \leq i < j \leq n} (x_j^2 - x_i^2)$, ami nem a nulla polinom.

2.9. A Jacobi-determináns szorzatra bontása

Eddig a fejezetig leginkább csak az érdekelt minket a Jacobi-determinánsal kapcsolatban, hogy azonosan nulla-e vagy sem. Ebben a fejezetben megadjuk, hogy hogy lehet szorzatra bontani az $S(V^*)$ polinomgyűrűben, és hogy annak mi is a pontos szerepe. Ehhez nézzük az l_α ($\alpha \in \Phi$) polinomokat, ahol l_α egy olyan lineáris polinom, aminek a H_α, az α gyökre merőleges hipersík a nullhalmaza. Mivel ilyen l_α lineáris polinomból több is van, ezért válasszuk azt, amelyik egy λ vektorhoz hozzárendeli a (λ, α) számot. Gyors számolásból kijön, hogy tetszőleges α, β gyökökre fennáll, hogy $s_\beta \cdot l_\alpha = l_{s_\beta \alpha}$, és $l_{-\alpha} = -l_\alpha$.

Nevezzünk egy $f \in S$ polinomot alternálónak, ha tetszőleges $w \in W$ elemre fennáll, hogy $w \cdot f = \det(w)f$. Az alternáló polinomok egy A alteret alkotnak az S gyűrűben. Könnyen látszik, hogy egy $f \in S$ polinom pontosan akkor alternáló, ha a homogén komponensei azok, tehát az A altér előáll az $A_k = A \cap S_k$ homogén komponensei összegeként.

2.31. Állítás. *Rögzitsük a W csoportnak egy $f_1, \dots, f_n$ alapinvariáns halmazát, és legyen J a hozzájuk tartozó Jacobi-determináns. Minden $\alpha \in \Phi$ gyökre definiáljuk az l_α polinomot mint előbb. Ekkor fennállnak a következők:*

(a) $J = c\prod_{\alpha\in\Phi^+} l_\alpha$, ahol $c \neq 0$ valamilyen konstans, ami az f_i polinomok választásától függ.

(b) Egy $f \in S$ polinom pontosan akkor alternáló, ha előáll J és egy W-invariáns polinom szorzataként.

(c) Minden k-ra $dim(A_k) = dim(R_{k-N})$, ahol N a W csoportban lévő tükrözések száma.

Bizonyítás. (a) Legyen $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ a következő leképezés:

$$\varphi(a_1, \dots, a_n) = (f_1(a_1, \dots, a_n), \dots, f_n(a_1, \dots, a_n))$$

Tegyük fel, hogy $a = (a_1, \dots, a_n) \in H_\alpha$, valamilyen $\alpha \in \Phi$ gyökre. Ekkor a minden nyílt környezete tartalmaz két különböző b, c pontot, amire $s_\alpha b = c$. Na de ekkor minden i-re fennáll, hogy $f_i(c) = f_i(s_\alpha b) = (s_\alpha \cdot f)(b) = f_i(b)$, tehát $\varphi(c) = \varphi(b)$. Az inverzfüggvény-tétel szerint minden a pontra, ahol J nem tűnik el, φ az a valamilyen kis környezetét bijektív módon képzi le a $\varphi(a)$ valamilyen kis környézetére. Ebből levonhatjuk azt a következtetést, hogy J eltűnik minden H_α ($\alpha \in \Phi$) hipersíkon. Hála a 2.15. oszthatósági lemmának, azt kapjuk, hogy minden l_α osztja a J Jacobi-determinánst. Mivel minden l_α ($\alpha \in \Phi^+$) irreducibilis, és egymásnak nem számszorosai, ezért a szorzatuk is osztja a J polinomot. Viszont az l_α ($\alpha \in \Phi^+$) polinomok szorzatának a foka éppen N, ami megegyezik a J Jacobi-determináns fokával a 2.23. következmény szerint.

(b) Miután már megvan az (a), nyugodtan feltehetjük, hogy:

$$J = \prod_{\alpha \in \Phi^+} l_\alpha.$$

Azt kell belátnunk, hogy egy $f \in S$ polinom alternáló akkor és csak akkor, ha előáll J és egy W-invariáns polinom szorzataként. Először lássuk be, hogy a J Jacobi-determináns alternáló; ehhez alkalmazzuk azt az észrevételt, hogy $s_\beta \cdot l_\alpha = l_{s_\beta \alpha}$. Ha β egyszerű gyök, akkor s_β elküldi a β gyököt a negatívjába, mig a többi pozitív gyököt permutálja, tehát:

$$s_\beta \cdot \prod_{\alpha \in \Phi^+} l_\alpha = - \prod_{\alpha \in \Phi^+} l_\alpha.$$

Ha most ezt a számolást iteráljuk, akkor azt kapjuk, hogy $w \cdot J = \det(w)J$, ahogy akartuk. Az triviális, hogy egy W-invariáns polinom és J szorzata alternáló.

Most vegyünk egy tetszőleges $f \in S$ alternáló polinomot. Erre fennáll, hogy $s_\alpha \cdot f = -f$ tetszőleges s_α ($\alpha \in \Phi$) tükrözésre, tehát ha $a \in H_\alpha$, akkor a következőt kapjuk:

$$-f(a) = (s_\alpha \cdot f)(a) = f(s_\alpha a) = f(a),$$

ami miatt tudjuk, hogy $f(a) = 0$. Mivel az f polinom eltűnik az összes H_α hipersíkon, ezért az előző érveléshez hasonlóan azt kapjuk, hogy J osztja az f polinomot, tehát létezik valamilyen $g \in S$ polinom, amire fennáll, hogy $f = gJ$. Most ha egy tetszőleges $w \in W$ elemet alkalmazunk mindkét oldalra, akkor a következőt kapjuk:

$$\det(w)f = (w \cdot f) = (w \cdot g)(w \cdot J) = \det(w)(w \cdot g)J,$$

amiből levonhatjuk azt a következtetést, hogy $w \cdot g = g$. Tehát egy tetszőleges $f \in A$ polinom előáll J és egy W-invariáns szorzataként.

(c) Ez egyből következik a (b) részből, és abból hogy $\deg(J) = N$. □

2.10. A Poincaré-polinom szorzatra bontása

Mielőtt még nekiesnénk a Poincaré-polinomnak, szükségünk van egy új fogalom bevezetésére, és annak néhány alapvető tulajdonságára, szóval kezdjük is azzal. Legyen G egy véges csoport, ekkor egy $\chi : G \to \mathbb{C}$ leképezést osztályfüggvénynek nevezünk, ha χ konstans a G csoport konjugált osztályain. Rögzítsünk egy G csoportot, és annak egy H részcsoportját. Ekkor ha χ egy osztályfüggvény a G csoporton, akkor χ megszorítása a H részcsoportra egy χ_H osztályfüggvényt ad a H részcsoporton. Fordítva, ha adva van egy φ osztályfüggvény a H részcsoporton, akkor az indukál egy φ^G osztályfüggvényt a G csoporton a következő módon:

$$\varphi^G(g) = \frac{1}{|H|}\sum_{x\in G}\varphi(xgx^{-1}),$$

ahol az összegzés azokon az $x \in G$ elemeken fut, amelyekre $xgx^{-1} \in H$.

Abban a speciális esetben, amikor $\varphi = 1_H$, a H részcsoporton konstans 1 függvény, akkor az indukált osztályfüggvénynek van egy hasznos interpretációja: $1_H^G(g)$ értéke nem más, mint $1/|H|$ szorozva azon $x \in G$ elemek számával, amire $xgx^{-1} \in H$, vagy másképp $gx^{-1}H = x^{-1}H$. Tehát $1_H^G(g)$ azon különböző $x^{-1}H$ bal oldali mellékosztályok száma, amik fixen maradnak a g elemmel való balról szorzás alatt. Ha visszaemlékezünk arra, hogy hogy is nézett ki az 1.23. állítás, akkor észrevehetjük, hogy az f_I függvény nem más, mint az 1_{W_I} osztályfüggvény által indukált függvény. Erre a nyelvre átfordítva ujra fogalmazhatjuk az 1.23. állítást a következőképp:

$$\sum_{I\subseteq S}(-1)^I 1_{W_I}^W(w) = \det(w), \text{ minden } w \in W \text{ elemre.}$$

2.32. Lemma. *(a) Ha χ egy G csoporton értelmezett tetszőleges osztályfüggvény, akkor $\chi \cdot 1_H^G = (\chi_H)^G$.*

(b) Ha φ egy tetszőleges osztályfüggvény a H részcsoporton, akkor fennáll a következő:

$$\frac{1}{|G|}\sum_{g\in G}\varphi^G(g) = \frac{1}{|H|}\sum_{h\in H}\varphi(h).$$

Bizonyítás. (a) Nézzük a következő számolást:

$$\begin{aligned}(\chi_H)^G(g) =& \frac{1}{|H|}\sum \chi_H(xgx^{-1})\\ =& \frac{1}{|H|}\sum \chi(g)\\ =& \chi(g)\frac{1}{|H|}\sum 1\\ =& \chi(g)1_H^G(g).\end{aligned}$$

Minden egyes lépésben azon $x \in G$ elemekre szummázunk, amikre $xgx^{-1} \in H$. A második egyenlőségnél azt használjuk, hogy χ valójában az egész G csoporton értelmezett osztályfüggvény, az utolsó egyenlőségnél pedig csak az indukált leképezés definícióját alkalmaztuk az 1_H osztályfüggvényre.

(b) Először is nézzük meg, hogy mit is jelent a bal oldal:

$$\frac{1}{|G|}\sum_{g\in G}\varphi^G(g) = \frac{1}{|G|}\sum_{g\in G}\Big(\frac{1}{|H|}\sum_{\substack{x\in G\\ xgx^{-1}\in H}}\varphi(xgx^{-1})\Big) = \frac{1}{|G||H|}\sum_{\substack{(x,g)\in G\times G\\ xgx^{-1}\in H}}\varphi(xgx^{-1}).$$

Azt kaptuk tehát, hogy a bal oldalon egy összegzés megy a $G \times G$ olyan (x, g) elemein, amire $xgx^{-1} \in H$. Most rögzítsünk egy $(x, g) \in G \times G$ párt, és legyen $h = (xgx^{-1})$. Azt állítjuk, hogy $|G|$ darab különböző (y, f) pár van, amire $yfy^{-1} = h$. Először is legyen $A_h = \{(x, g) \in G \times G \,|\, xgx^{-1} = h\}$, ekkor ha $(x, g) \in A_h$, akkor tetszőleges $b \in G$ elemre fennáll, $(xb, b^{-1}gb) \in A_h$, mivel:

$$h = xgx^{-1} = x(bb^{-1})g(bb^{-1})x^{-1} = (xb)(b^{-1}gb)(xb)^{-1}.$$

Mivel $x = xb$ pontosan akkor, ha $b = 1$, ezért azt már látjuk is, hogy A_h legalább $|G|$ elemű. Most azt állítjuk, hogy ha van egy $(y, f) \in A_h$ pár, akkor az előáll $(xd, d^{-1}gd)$ alakban valamilyen $d \in G$ elemre. Valóban, mivel f és g is konjugált a h elemmel, ezért létezik egy $d' \in G$ elem, amire $f = d'gd'^{-1}$. Ez azt jelenti, hogy:

$$yfy^{-1} = y(d'gd'^{-1})y^{-1} = (yd')g(yd')^{-1} = xgx^{-1} = h$$

Ha most rendezzük kicsit a fenti egyenletet, akkor a következőt kapjuk:

$$(x^{-1}yd')g = g(x^{-1}yd')$$

Ez azt jelenti, hogy $x^{-1}yd'$ benne van a g elem $C(g)$ centralizátorában, vagyis létezik egy $c \in C(g)$, amire $y = xcd'^{-1}$. Legyen $d = cd'^{-1}$, mivel ekkor $y = xd$, és $d^{-1}gd = f$. Tehát $(y, f) = (xd, d^{-1}gd)$, ahogy állítottuk, és így minden $h \in G$ elemre fennáll, hogy $|A_h| = |G|$.

Most térjünk vissza az eredeti állításra, ami innentől kezdve csak egy egyszerű egyenlet rendezés:

$$\frac{1}{|G||H|} \sum_{\substack{(x,g)\in G\times G \\ xgx^{-1}\in H}} \varphi(xgx^{-1}) = \frac{1}{|G||H|} \sum_{h\in H} \Big(\sum_{\substack{(x,g)\in G\times G \\ xgx^{-1}=h}} \varphi(h) \Big) = \frac{1}{|G||H|} \sum_{h\in H} (|G|\varphi(h))$$
$$= \frac{1}{|H|} \sum_{h\in H} \varphi(h)$$

$\square$

Mostmár szép lassan rátérhetünk a fejezetünk főtételére, de előbb még felsoroljuk, hogy mik kellenek majd a belátásához:

(A) Az 1.16. állítás, ami szerint:

$$\sum_{I\subseteq S} (-1)^I \frac{W(t)}{W_I(t)} = t^N.$$

(B) A 1.23. állítás, ami kifejezi a $\det(w)$ számot, mint a különböző W_I parabolikus részcsoportokon értelmezett konstans 1 függvény által indukált osztályfüggvények alternáló összege.

(C) A 2.10. lemma, aminek a segítségével ki tudjuk számolni egy W csoporthatás fix alterének a dimenzióját, ami nem más, mint a következő operátor nyoma:

$$\frac{1}{|W|}\sum_{w\in W} w.$$

(D) A 2.20. következmény, aminek a bizonyításánál láttuk, hogy a

$$\prod \frac{1}{1-t^{d_i}}$$

szorzat hatványsor alakjában a t^k együtthatója nem más, mint homogén k fokú invariánsok R_k terének dimenziója.

(E) A 2.31. állítás (c) része, ami azt mondja, hogy a homogén k fokú alternáló polinomok A_k terének dimenziója megegyezik az R_{k-N} tér dimenziójával, ahol N a W csoportbeli tükrözések száma.

Ezek mellett még a következő lemmára lesz szükségünk.

2.33. Lemma. *Legyen R_I a W_I parabolikus részcsoport invariánsgyűrűje az S polinomgyűrűben, és legyen $(R_I)_k = R_I \cap S_k$. Ekkor*

$$\sum_{I\subseteq S} dim\big((R_I)_k\big) = dim(A_k).$$

Bizonyítás. Először is vegyük észre, hogy R_I előáll a homogén komponenseinek összegeként. Rögzítsünk egy k számot, és legyen $\chi(w) = \mathrm{Tr}_{S_k}(w)$, ez nyilvánvalóan egy osztályfüggvény a W csoporton. Jelölje χ_I a χ osztályfüggvény megszorítását a W_I részcsoportra. Ekkor az előző lemma (a) része szerint azt kapjuk, hogy:

$$(\chi_I)^W = \chi \cdot 1_{W_I}^W.$$

Most a (B) szerint a következőt kapjuk:

$$\sum_{I\subseteq S} (-1)^I (\chi_I)^W(w) = \det(w)\chi(w), \tag{2.26}$$

minden $w \in W$ elemre. Most átlagoljuk ki a bal oldalát a 2.26. egyenletnek W szerint, és alkalmazzuk a 2.32. lemma (b) részét:

$$\frac{1}{|W|}\sum_{I\subseteq S}(-1)^I \sum_{w\in W} (\chi_I)^W(w) = \sum_{I\subseteq S}(-1)^I \frac{1}{|W_I|}\sum_{z\in W_I} \chi_I(z),$$

ami a (C) állítás szerint ugyanaz, mint:

$$\sum_{I\subseteq S}(-1)^I \dim\big((R_I)_k\big).$$

Ha most a 2.26. egyenlet jobb oldalát átlagoljuk W szerint, akkor a következőt kapjuk:

$$\frac{1}{|W|}\sum_{w\in W}\det(w)\chi(w).$$

Ismét hála a (C) állításnak, a fenti szumma megadja a W-invariánsok terének dimenzióját az S_k lineáris altérben a következő hatás alatt: $w\mapsto \det(w)w$. Ennek az új hatásnak az invariánsai viszont pontosan az alternáló polinomok, tehát a 2.26. egyenlet jobb oldala nem mást mint $\dim(A_k)$, és mi pont ezt akartuk belátni. $\square$

2.34. Tétel. *Legyen W egy valós tükrözéscsoport, és legyen $W(t)$ a W csoport Poincaré-polinomja, illetve legyenek $d_1,\ldots,d_n$ a W csoport fokai. Ekkor*

$$W(t)=\prod_{i=1}^{n}\frac{t^{d_i}-1}{t-1}.$$

Bizonyítás. A bizonyítás ötlete az, hogy indukciót alkalmazunk a W csoport rendjére, kihasználva az (A) állítást. Ha $|W|=1$, akkor triviálisan teljesül az állítás, nem mellesleg hasonlóan triviális ha $|W|=2$. Tegyük fel, hogy $|W|>2$, és vezessük be a következő polinomokat:

$$Q(t)=\prod\frac{t^{d_i}-1}{t-1},$$

és hasonlóan definiáljuk a $Q_I(t)$ polinomot, csak ott a W_I fokai szerepelnek. Következő lépésként azt szeretnénk belátni, hogy egy (A) szerű tulajdonság fennáll ezekre az új polinomokra, azaz:

$$\sum_{I\subseteq S}(-1)^I\frac{Q(t)}{Q_I(t)}=t^N, \tag{2.27}$$

vagy egy ezzel ekvivalenset:

$$\sum_{I\subseteq S}\frac{1}{(1-t)^n Q_I(t)}=\frac{t^N}{(1-t)^n Q(t)}. \tag{2.28}$$

Most az a feladatunk, hogy összehasonlítsuk mindkét oldalon a t^k együtthatóját, miután mindkét oldalt felírtuk hatványsorként. A jobb oldal a következővel egyenlő:

$$t^N\prod\frac{1}{1-t^{d_i}}.$$

tehát a (D) állítás szerint t^k együtthatója $\dim(R_{k-N})$, ami megegyezik $\dim(A_k)$-val, az (E) állítás szerint.

Ahhoz, hogy a 2.27. egyenlet bal oldalát jobban értsük, nézzük W_I hatását a Δ_I által feszített altérben. Legyen ennek a hatásnak a fokai $e_1, \ldots, e_I$. Mivel W_I pontonként fixálja a Δ_I által feszített altér ortogonális kiegészítőjét, ezért W_I hatásnak a fokai az egész V téren $e_1, \ldots, e_I, 1, \ldots, 1$. Ebből a következőt kapjuk:

$$\frac{1}{(1-t)^n Q_I(t)} = \frac{1}{(1-t)^{n-|I|}} \prod_{i=1}^{|I|} \frac{1}{1-t^{e_i}}.$$

Tehát ha ezt kifejtjük hatványsorként, akkor azt kapjuk, hogy t^k együtthatója $\dim\big((R_I)_k\big)$. Az előző lemma szerint viszont $\sum_{I\subseteq S}(-1)^I \dim\big((R_I)_k\big) = \dim(A_k)$, tehát a 2.27. egyenlet két oldala megegyezik. Az indukciós feltevés szerint ekkor minden W_I valódi részcsoportra fennáll, hogy $W_I(t) = Q_I(t)$. Most már csak össze kell hasonlítani az (A)-t és a 2.27. egyenletet, és ezzel kész is vagyunk. $\square$

3. Hivatkozások

[1] Humphreys, J. E. *Reflection groups and Coxeter groups.* (Cambridge University Press, 1990).

[2] Howard, H. *Geometry of Coxeter groups.* (Pitman Pub., 1982).

[3] Springer, T. A. *Invariant Theory.* (Springer, 1977).

[4] Shephard, G. C. & Todd, J. A. *Finite Unitary Reflection Groups.* Canadian Journal of Mathematics 6, 274–304 (1954).

[5] Verma, J. K. *Rings of invariants of finite groups.* http://www.math.iitb.ac.in/~jkv/invar.pdf

[6] Wehlau, D. L. *The Noether number in invariant theory.* https://pdfs.semanticscholar.org/fbac/250d44d2fe6c2ae633b44c0237f3aa7dbb64.pdf