Transzformációcsoportok jegyzetvázlat

Készítette: Nagy Gábor adjunktus

2001. február

Bevezető

Már az általános iskola óta ismeretes, hogy derékszögű koordinárendszer bevezetésével a euklideszi sík és a háromdimenziós tér pontjait illetve különböző geometriai objektumait valós számpárokkal és számhármasokkal történő számolással is le tudjuk írni. Ezen objektumok egy részének esetében a valós számtestnek csak a testaxiómákban megadott tulajdonságait használtuk ki. Például egy egyenes pontjai egy adott lineáris összefüggésnek eleget tevő számpárok halmazának felel meg; egy lineáris egyenlet felírásakor pedig csak azt használtuk ki, hogy $\mathbb{R}$-ben van egy jól definiált összeadás- és szorzásművelet. Ez azonban nem a valós számok sajátossága, hanem ami minden testben definíció szerint teljesül.

Ezzel szemben például a konvexitás fogalmának leírásakor azt is kihasználjuk, hogy $\mathbb{R}$-en értelmezve van egy „$\leq$" rendezési reláció, ami teljes rendezés és jól illeszkedik $\mathbb{R}$ testműveleteihez (pl. az összeadás monoton). Mint ismeretes, a komplex számok testén nincs ilyen rendezési reláció.

A továbbiakban olyan geometriai objektumokat fogunk vizsgálni, melyek a négy alapművelet segítségével már koordinátázhatóak. Algebrából ismeretes, hogy az összeadás és a szorzás segítségével előállítható függvények pontosan a polinomfüggvények. Általánosan tehát azt mondhatjuk, hogy a vizsgált objektum mindig egy polinomfüggvény által meghatározott struktúra. A geometriában ez a tulajdonságot gyakran az *„algebrai"* jelzővel jellemzik, ebben az értelemben beszélhetünk algebrai halmazokról, algebrai görbékről, algebrai csoportokról, stb.

A továbbiakban *transzformációcsoport* alatt mi mindig egy olyan csoportot értünk, melynek elemei egy geometriai-algebrai struktúra automorfizmusai. Munkánk során a csoportelemeket többnyire mátrixok írják le, melyek elemi egy rögzített testből valók. Ebből látható, hogy az téma megértéséhez számos csoportelméleti, lineáris algebrai és testelméleti ismeretre van szükségünk, ezeket az előadás elején nagy vonalakban áttekintjük.

Ezt követően elsőként a legegyszerűbb geometriai struktúra, az *egyenes*, majd az affin és a projektív tér transzformációit vizsgáljuk, majd a vizsgálatokat kiterjesztjük a másodfokú egyenletekkel megadható halmazokra (kúpszeletek és hiperboloidok) is. Ezek során a matematikában alapvető fontosságú csoportokkal ismerkedünk meg közelebbről, az ezek-

re vonatkozó eredményeket geometriailag szemléletessé téve fogjuk meggondolni. (Jóllehet a különbségtétel a geometriai és a lineáris algebrai módszerek között nem mindig könnyű, sőt megítélésünk szerint a legtöbb esetben a különbségtételnek nincs is értelme.)

Ez a jegyzetvázlat a JATE matematika tanárszak *Transzformációcsoportok* című blokktárgyához íródott. A szerző minden hibával és pontatlansággal kapcsolatos megjegyzést szívesen fogad a `nagyg@math.u-szeged.hu` e-mail címre.

Az előadáshoz sajnos jelenleg nincs magyar nyelvű szakirodalom. Idegen nyelveken az alábbi műveket javasoljuk.

Artin: Geometric Algebra

D. Taylor: The Geometry of Classical Groups

Huppert: Endliche Gruppen I.

Tartalomjegyzék

1. fejezet

Csoportelméleti alapfogalmak

1.1. Csoportok

Az algebrából jól ismert csoportfogalomnak számos különböző definíciója ismeretes. Ezek ekvivalenciáját nem különösebben nehéz meggondolni. Mi az alábbi definíciót adjuk meg.

1.1. Definíció. *Legyen adott a G halmaz a rajta értelmezett „$\cdot$" szorzásművelettel. A $(G, \cdot)$ pár* csoportot *alkot, ha az alábbi axiómák teljesülnek.*

(G1) *(Asszociativitás.) Minden $x, y, z \in G$ elem esetén $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ teljesül.*

(G2) *(Egységelem.) Létezik egy egyértelműen meghatározott $e \in G$ elem, amelyre $x \cdot e = e \cdot x = x$ teljesül minden $x \in G$ esetén.*

(G3) *(Inverz.) Minden $x \in G$ elemhez létezik egy egyértelműen meghatározott $x^{-1} \in G$ elem, amelyre teljesül $x \cdot x^{-1} = x^{-1} \cdot x = e$.*

A (G2) axióma miatt minden G csoportnak van legalább egy eleme. Egy $(G, \cdot)$ csoportot *kommutatívnak* vagy *Abel-félének* nevezünk, ha az asszociativitás mellett a kommutativitás is teljesül, azaz $xy = yx$ minden $x, y \in G$ esetén.

1.1. példa. A $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ vagy $\mathbb{C}$ számhalmazok bármelyike csoportot alkot az összeadásra mint műveletre nézve.

1.2. példa. A $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ és $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ halmazok csoportot alkotnak a szokásos szorzásművelettel.

1.3. példa. A vektorterek csoportot alkotnak az összeadással.

Az eddigi példák mind Abel-féle csoportot határoznak meg.

1.4. példa. A nem nulla determinánsú $n \times n$-es mátrixok csoportot alkotnak a közönséges mátrixszorzás műveletével.

1.5. példa. Az itt szereplő két példa jóval általánosabb, és a későbbiekben használt csoportok igen széles körét felöleli. Tetszőleges X halmaz esetén

definiálhatjuk az X-en értelmezett bijektív leképezések halmazát:

$$S(X) = \{\alpha : X \to X \text{ bijektív leképezés}\}.$$

Ha X-en egy adott Σ struktúra is értelmezve van, akkor legyen

$$S(X, \Sigma) = \{\alpha : X \to X \text{ bijektív leképezés, amely megőrzi a } \Sigma \text{ struktúrát}\}.$$

A Σ lehet pl. egy geometriai alakzat, egy távolságfüggvény, egy rendezési reláció, stb. Ezekben az esetekben beszélünk a szimmetriák, az izometriák, monoton leképezések, stb. csoportjáról. A szorzásművelet mindkét esetben a leképezések egymás utáni elvégzése: $f, g : X \to X$ esetén

$$f \circ g : X \to X, \qquad (f \circ g)(x) = f(g(x)).$$

Ez a művelet mindig asszociatív, hiszen

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x)))$$

és

$$((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))),$$

azaz $f \circ (g \circ h) = (f \circ g) \circ h$. A művelet egységeleme nyilván az

$$\mathrm{id} : X \to X, \qquad \mathrm{id}(x) = x$$

identikus leképezés. Az f leképezés inverzének létezése pedig egyenértékű f bijektivitásával, hiszen ekkor minden $y \in X$ elemre pontosan egy olyan $x \in X$ elem létezik, amelyre $y = f(x)$ teljesül. Ezt az elemet $x = f^{-1}(y)$ módon jelölve az $f^{-1} : X \to X$ bijektív leképezés az f kétoldali inverze: $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}$.

Azt is könnyen meg lehet gondolni, hogy a leképezések $S(X, \Sigma)$ halmaza is csoport, hiszen ha f, g megőrzi a Σ struktúrát, akkor ezek szorzata és inverzei is megőrzik azt.

Az alábbi példa ez utóbbi megfontolást próbálja szemléltetni, a későbbiekben gyakran fogjuk őt hasonló célokra felhasználni.

1.6. példa. Legyen $X = \mathbb{T}$ egy tetszőleges test, G pedig az

$$G = \{f : \mathbb{T} \to \mathbb{T} : f(x) = ax + b,\ a \in \mathbb{T}^*, b \in \mathbb{T}\}$$

elsőfokú polinommal megadható transzformációk halmaza. Könnyen leellenőrizhető, hogy az ilyen transzformációk bijektívek. Teljesül továbbá $f(x) = ax + b$ és $g(x) = cx + d$ esetén

$$(f \circ g)(x) = ac\,x + ad + b, \quad \text{és} \quad f^{-1}(x) = a^{-1}x - a^{-1}b.$$

Ezek a transzformációk tehát csoportot alkotnak, ezt a csoportot *affin lineáris csoportnak* nevezzük és a továbbiakban AGL-el jelöljük.

Az is könnyen látható, hogy a három utolsó példánk általában nemkommutatív csoportot határoz meg.

A következőkben összegyűjtöttük a csoport fogalmához tartozó fontosabb alapfogalmakat és ezek főbb tulajdonságait. A továbbiakban $(G, \cdot)$ mindig egy csoportot jelöl.

1.2. Részcsoportok, mellékosztályok

A G halmaz egy H részhalmazát *részcsoportnak* nevezzük, ha H zárt a szorzásra ($H \cdot H \subseteq H$) és az inverz képzésre ($H^{-1} \subseteq H$). Ennek jele: $H \leq G$.

A $H \leq G$ részcsoport szerinti *jobb oldali mellékosztálynak* nevezem a G halmaz $Hx = \{hx | h \in H\}$ alakú részhalamzait. Hasonló módon definiálhatom a xH alakú *bal oldali mellékosztályokat*. A későbbiekben többnyire a jobb oldali mellékosztályokat fogjuk használni, ezek halmazát G/H jelöli. Triviális módon tudunk a H bal és jobb oldali mellékosztályai között egy bijekciót létesíteni, így tehát a H bal és jobb oldali mellékosztályainak a száma megegyezik. Ezt a számot a H *indexének* nevezzük és $|G : H|$-val jelüljük. Ha G véges, akkor $|G : H| = |G| : |H|$. Ebből rögtön következik *Lagrange tétele*, miszerint $H \leq G$ esetén a H részcsoport rendje osztja a G csoport rendjét. Minden G-nek van legalább két részcsoportja, ez $\{1\}$ illetve maga G, ezeket G *triviális* vagy *nem valódi* részcsoportjának nevezzük.

1.3. Normálosztók, homomorfizmusok

Egy $N \leq G$ részcsoportot *normálosztónak* nevezünk, ha a jobb és bal oldali mellékosztályai megegyeznek, azaz $xN = Nx$ teljesül minden $x \in G$ esetén. Ezt $N \triangleleft G$-vel jelöljük. Ebben (és csak ebben!) az esetben a G/N mellékosztályok maguk is csoportot alkotnak, amit a G csoport N szerint *faktorcsoportjának* nevezünk. A triviális részcsoportok nyilván egyben normálosztók is.

Legyenek adottak a G_1 és G_2 csoportok. A $\alpha : G_1 \to G_2$ leképezést *homomorfizmusnak* nevezzük, ha megtartja a szorzásműveletet, azaz $\alpha(x) \cdot \alpha(y) = \alpha(xy)$ minden $x, y \in G_1$ esetén. Könnyen belátható, hogy ekkor α az invertálást is megőrzi, valamint a G_1 csoport $\alpha(G_1)$ képe a G_2-nek egy részcsoportja. Ha α egyben egy bijektív leképezés is G_1 és G_2 között, akkor *izomorfizmusnak* nevezzük, a G_1 és G_2 csoportokat pedig *izomorfaknak*. Ha $G_1 = G_2 = G$, akkor α-t automorfizmusnak hívjuk. A G csoport automorfizmusainak halmaza egy $S(X, \Sigma)$-típusú csoport, ahol $X = G$, Σ pedig

a csoportstruktúra. Ezt a csoportot G automorfizmuscsoportjának nevezzük és $\mathrm{Aut}(G)$-vel jelöljük.

Egy $\alpha : G_1 \to G_2$ homomorfizmus *magjának* nevezzük és $\ker\alpha$-val jelöljük a G_1 azon x elemeinek a halmazát, amelyekre $\alpha(x) = 1$. (Itt az 1 értelemszerűen a G_2 csoport egységelemét jelöli.) Könnyen ellenőrizhető, hogy $\ker\alpha \triangleleft G$, a csoportok homomorfia-tételeiből pedig következik, hogy $G_1/\ker\alpha$ izomorf a $\alpha(G_1)$ képpel.

1.4. Konjugálás, a csoport centruma

Legyen c a G csoport egy rögzített eleme és definiáljuk a $\varphi_c : G \to G$ leképezést:

$$\varphi_c(x) = cxc^{-1}, \qquad x \in G.$$

Ezt a leképezést a c elemmel való *konjugálásnak* nevezzük. Könnyen leellenőrizhető, hogy φ_c bijektív, sőt megtartja a szorzást, azaz $\varphi_c \in \mathrm{Aut}(G)$. Ezen túl, $\varphi_c \circ \varphi_d = \varphi_{cd}$ teljesül minden $c, d \in G$ esetén, azaz a

$$\varphi : c \mapsto \varphi_c$$

leképezés egy $G \to \mathrm{Aut}(G)$ homomorfizmus. Ebből az is következik, hogy a φ_c alakú automorfizmusok $\mathrm{Aut}(G)$ egy részcsoportját alkotják. Ennél több is igaz, ezek egy normálosztót alkotnak. Vegyünk ugyanis egy tetszőleges $\alpha \in \mathrm{Aut}(G)$ automorfizmust, ekkor

$$(\alpha\varphi_c\alpha^{-1})(x) = \alpha(c\alpha^{-1}(x)c^{-1}) = \alpha(c)x\alpha(c^{-1}) = \varphi_{\alpha(c)}(x).$$

Azt kaptuk, hogy $\alpha\varphi_c\alpha^{-1} = \varphi_{\alpha(c)}$. A φ_c alakú automorfizmusokat a G csoport *belső automorfizmusainak* is nevezzük, és az általuk alkotott csoportot $\mathrm{InnAut}(G)$-vel jelöljük.

Érdemes megvizsgálnunk a $\varphi : G \to \mathrm{Aut}(G)$ homomorfizmus magját. Ezt azon $c \in G$ elemek alkotják, amelyekre $\varphi = \mathrm{id}$, azaz minden $x \in G$-re $x = cxc^{-1}$. Ez ekvivalens azzal, hogy $cx = xc$ ($\forall x \in G$), magyarán c a G összes elemével felcserélhető. Az ilyen elemek halmazát a G *centrumának* nevezzük, és $Z(G)$-vel jelöljük. A homomorfia-tételek szerint tehát

$$\mathrm{InnAut}(G) \cong G/Z(G).$$

Végül, a definíciók alapján kijelenthetjük, hogy egy $H \leq G$ részcsoport akkor és csak akkor normálosztó, ha H *invariáns* a belső automorfizmusokra nézva, azaz $\varphi_c(H) \subseteq H$ teljesül minden $c \in G$ elemre.

1.5. Kommutátorrészcsoport

A G csoport egy másik fontos normálosztója a G *kommutátorrészcsoportja*. Ennek a konstrukciója kissé bonyolultabb. Először minden $x, y \in G$ csoportelemre definiáljuk az

$$[x, y] = x^{-1}y^{-1}xy$$

kommutátor elemet. Természetesen, ha az x és y elemek felcserélhetőek, akkor $[x, y] = 1$, és fordítva. A G' kommutátorrészcsoport a kommutátor elemek által generált részcsoport, azaz azon legszűkebb részcsoport, amely tartalmazza az összes kommutátor elemet. A kommutátor elemekre nyílván teljesül $\varphi_c([x, y]) = [\varphi_c(x), \varphi_c(y)]$, $\forall x, y, c \in G$, tehát azt mondhatjuk, hogy a kommutátor elemek halmaza invariáns a konjugálásra nézve. Ekkor viszont az általuk generált G' részcsoport is invariáns, azaz G' normálosztó.

Tekintsük a G/G' faktorcsoportot. Nyilván minden $x, y \in G$-re

$$[xG', yG'] = [x, y]G'.$$

Viszont definíció szerint $[x, y] \in G'$, azaz $[x, y]G' = G'$. Eszerint $(xG')^{-1} \cdot (yG')^{-1} \cdot (xG') \cdot (yG') = G'$, amiből $(xG') \cdot (yG') = (yG') \cdot (xG')$ következik, azaz a G/G' faktorcsoport Abel-féle. Ennél még egy kicsit több is igaz: bármely $N \triangleleft G$ esetén a G/N faktorcsoport akkor és csak akkor lesz Abel-féle, ha $G' \leq N$. Ezt most nem bizonyítjuk, jóllehet a bizonyítása nem nehéz.

2. fejezet

A csoporthatás fogalma

2.1. Transzformációcsoportok

Az eddigiekben a csoport absztrakt definícióját adtuk meg. Most viszont a tárgyalandó csoportokhoz hozzárendelünk egy Ω alaphalmazt is, így a csoport elemei már nem csupán absztrakt relációknak eleget tevő szimbólumok, hanem egy konkrét halmaz önmagára vett bijektív leképezései.

A fejezet további részében $(G, \cdot)$ mindig egy csoportot fog jelölni, Ω pedig egy halmazt. A csoportelemeket $g, g_1, g_2, \ldots, h, h_1, h_2, \ldots$ kis latin betűk jelölik, a G egységelemét pedig 1. Ω-t alaphalmaznak vagy *ponthalmaznak*, az elemeit pedig pontoknak hívjuk, és kis görög betűkkel $\alpha, \beta, \ldots$ jelöljük.

2.1. Definíció. *Legyen Ω egy tetszőleges alaphalmaz. A $G \leq S(\Omega)$ alakú csoportokat* Ω-n ható transzformációcsoportoknak *nevezzük. Abban az esetben, ha Ω véges halmaz, akkor szokás* permutációcsoportokról *is beszélni.*

Transzformációcsoportok esetén a csoportművelet mindig a leképezések szorzata, az f, g transzformáció esetén ezt a szorzatot az $f \circ g$ jelölés helyett gyakran fogjuk csak fg-vel jelölni.

Rögzítsünk egy Ω-n ható G permutációcsoportot. Ekkor Ω-n értelmezni tudunk egy ekvivalenciarelációt, nevezetesen, $\alpha \sim \beta$ akkor és csak akkor, ha létezik $g \in G$ elem úgy, hogy $g(\alpha) = \beta$. Ez valóban ekvivalenciareláció, hiszen $\mathrm{id}(\alpha) = \alpha$ (reflexivitás), $g(\alpha) = \beta$ esetén $g^{-1}(\beta) = \alpha$ (szimmetria) és $g(\alpha) = \beta, h(\beta) = \gamma$ esetén pedig $(gh)(\alpha) = \beta$ (tranzitivitás) teljesül. Ehhez az ekvivalenciarelációhoz tartozik egy osztályozás, ennek az ekvivalenciaosztályait nevezzük G *pályáinak* Ω-n. Ily módon tehát az Ω halmaz felbomlik G-pályák diszjunkt uniójára.

2.1. példa. Legyen Ω az euklédeszi sík pontjainak halmaza, G pedig az origó körüli forgatások csoportja. Ekkor G minden pályája egy origó középpontú kör, G nem tranzitív.

2.2. A tranzitivitás fogalma

2.2. Definíció. *Legyen G egy Ω-n ható transzformációcsoport.*

(T1) *Azt mondjuk, hogy a G transzformációcsoport* tranzitívan *hat Ω-n, ha csak egyetlen pálya van, azaz, ha bármely $\alpha, \beta \in \Omega$ elempárhoz létezik $g \in G$, amelyre $g(\alpha) = \beta$.*

(T2) *Azt mondjuk, hogy a G transzformációcsoport* élesen *vagy* szigorúan tranzitívan *hat Ω-n, ha bármely $\alpha, \beta \in \Omega$ elempárhoz létezik egy egyértelműen meghatározott $g \in G$, amelyre $g(\alpha) = \beta$.*

(T3) *Azt mondjuk, hogy a G transzformációcsoport k-*szorosan tranzitívan *vagy röviden k-*tranzitívan *hat Ω-n, ha bármely két, különböző pontokból álló $(\alpha_1, \dots, \alpha_k)$, $(\beta_1, \dots, \beta_k) \in \Omega^k$ pont-k-as párhoz*[1] *létezik $g \in G$, amelyre $g(\alpha_1) = \beta_1, \dots, g(\alpha_k) = \beta_k$.*

(T4) *Azt mondjuk, hogy a G transzformációcsoport* élesen *k-*tranzitívan *hat Ω-n, ha a különböző pontokból álló $(\alpha_1, \dots, \alpha_k)$, $(\beta_1, \dots, \beta_k) \in \Omega^k$ pont-k-as párhoz létezik egy egyértelműen meghatározott $g \in G$ transzformáció, amelyre $g(\alpha_1) = \beta_1, \dots, g(\alpha_k) = \beta_k$.*

Egy további fontos fogalom a transzformációcsoportok elméletében a *stabilizátor részcsoport*: Tetszőleges $\alpha \in \Omega$ esetén G_α jelöli azon G-beli g elemek halmazát, amelyek fixen hagyják az α pontot,

$$G_\alpha = \{g \in G; g(\alpha) = \alpha\}.$$

Nyilván $G_\alpha \leq G$ részcsoport. Az alábbi tétel megmutatja, hogy hogyan tudjuk leírni a G k-tranzitivitását a stabilizátorok segítségével.
2.2. példa. Az AGL affin lineáris csoportban a $0 \in \mathbb{T}$ elem stabilizátora az

$$AGL_0 = \{f : \mathbb{T} \to \mathbb{T} : f(x) = ax,\ a \in \mathbb{T}^*\}$$

leképezések csoportja. Gondoljuk meg, hogy AGL_0 izomorf a test $\mathbb{T}^*$ multiplikatív csoportjával.

2.3. Tétel. *Legyen G egy Ω-n ható transzformációcsoport.*

(i) *Minden $g \in G$ és $\alpha \in \Omega$ elemre teljesül $g\, G_\alpha\, g^{-1} = G_{g(\alpha)}$.*

(ii) *Ha G tranzitívan hat Ω-n, akkor a különböző pontokhoz tartozó stabilizátorok egymás konjugáltjai.*

(iii) *G akkor és csak akkor hat szigorúan tranzitívan Ω-n, ha tranzitívan hat, és valamely (s így bármely) α pont esetén $G_\alpha = \{\mathrm{id}\}$.*

[1] Ezt úgy kell érteni, hogy $i \neq j$ esetén $\alpha_i \neq \alpha_j$ és $\beta_i \neq \beta_j$. Ezzel szemben $\alpha_i = \beta_j$ megengedett.

(iv) *G akkor és csak akkor hat (élesen) k-tranzitívan Ω-n, ha tranzitívan hat és valamely (s így bármely) α pontra G_α (élesen) $(k-1)$-tranzitívan hat az $\Omega \setminus \{\alpha\}$ halmazon.*

Bizonyítás. Rögzítsük az $\alpha \in \Omega$ és $g \in G$ elemeket és legyen $\beta = g(\alpha)$. Ha $h \in G_\alpha$, akkor

$$(ghg^{-1})(g(\alpha)) = (gh)(\alpha) = g(\alpha),$$

azaz $\varphi_g(h) \in G_{g(\alpha)}$ és $\varphi_g(G_\alpha) \subseteq G_{g(\alpha)}$. Ugyanezt alkalmazva a $g' = g^{-1}$ és $\alpha' = g(\alpha)$ elemekre kapjuk, hogy $\varphi_{g^{-1}}(G_{g(\alpha)}) \subseteq G_\alpha$, ami $\varphi_{g^{-1}} = \varphi_g^{-1}$ miatt azt jelenti, hogy $\varphi_g(G_\alpha) = G_{g(\alpha)}$. Ez pontosan (i), és (ii) is közvetlenül adódik.

Ha G szigorúan tranzitívan hat, akkor az α-t önmagára képező elem is egyértelműen meg van határozva, úgyhogy ez csak az identitás lehet. Fordítva, tegyük fel, hogy G tranzitívan, de nem élesen tranzitívan hat. Ekkor van olyan $\beta, \gamma \in \Omega$, hogy léteznek különböző $g_1, g_2 \in G$ elemek, amelyre $g_1(\beta) = g_2(\beta) = \gamma$. Legyen $h = g_1^{-1}g_2$, ekkor $h \neq \mathrm{id}$ és $h(\beta) = \beta$, azaz $G_\beta \neq \{\mathrm{id}\}$. De a tranzitivitás miatt minden strabilizátor részcsoport G_α konjugált G_β-hoz, így $G_\alpha \neq \{\mathrm{id}\}$ adja (iii)-t.

Tegyük fel, hogy G k-tranzitív, és válasszunk két, különböző pontokból álló $(\alpha_1, \ldots, \alpha_{k-1}), (\beta_1, \ldots, \beta_{k-1})$ pont $(k-1)$-est $\Omega \setminus \{\alpha\}$-ból. Ezt kiegészíthetjük két, különböző pontokból álló $(\alpha_1, \ldots, \alpha_{k-1}, \alpha), (\beta_1, \ldots, \beta_{k-1}, \alpha)$ pont k-assá. A k-tranzitivitás miatt létezik $g \in G$, amire

$$g(\alpha_1) = \beta_1, \ldots, g(\alpha_{k-1}) = \beta_{k-1} \text{ és } g(\alpha) = \alpha,$$

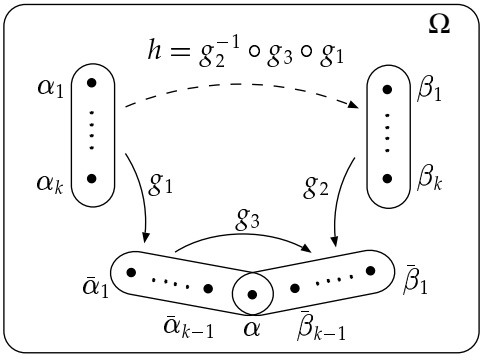
azaz $g \in G_\alpha$ és G_α k-tranzitív $\Omega \setminus \{\alpha\}$-n.

Fordítva, tegyük fel, hogy G tranzitív és G_α $(k-1)$-tranzitív valamely rögzített $\alpha \in \Omega$-ra. Rögzítsünk két megfelelő $(\alpha_1, \ldots, \alpha_k), (\beta_1, \ldots, \beta_k)$ pont k-ast. A tranzitivitás miatt létezik $g_1, g_2 \in G$ úgy, hogy $g_1(\alpha_k) = g_2(\beta_k) = \alpha$. Legyenek $\bar{\alpha}_i = g_1(\alpha_i)$ és $\bar{\beta}_i = g_2(\beta_i)$, $i = 1, \ldots, k-1$. Ekkor G_α $(k-1)$-tranzitivitása miatt pedig léteznie kell egy $g_3 \in G_\alpha$ elemnek, amire $g_3(\bar{\alpha}_i) = \bar{\beta}_i$, $i = 1, \ldots, k-1$. Legyen $h = g_2^{-1}g_3g_1$. Könnyen leellenőrizhető, hogy $h(\alpha_i) = \beta_i$ teljesül minden $i = 1, \ldots, k$ esetén, amivel (iii)-t is beláttuk (ld. a 2.1 ábrát).

Végül az élesen k-tranzitív eset megkapható, ha az utóbbi gondolatmenetet kibővítem az (iii) pont bizonyításának gondolatmenetével. □

2.3. példa. Legyen n egy természetes szám és X az $\{1, 2, \ldots, n\}$ halmaz. Ekkor az $S(X)$ csoport jelölésére az S_n jelet használjuk, és a csoportot az n-edfokú szimmetrikus csoportnak nevezzük. Könnyen meggondolható, hogy S_n n-szeresen tranzitívan hat $\{1, 2, \ldots, n\}$-en.

2.4. példa. Legyen Ω az euklédeszi sík pontjainak halmaza, G pedig a párhuzamos eltolások csoportja. Ekkor G szigorúan tranzitívan hat Ω-n.



2.1. ábra. A k-tranzitivitás és $(k-1)$-tranzitivitás kapcsolata.

2.5. példa. Az 1.6 példában szereplő AGL affin lineáris csoport egy élesen 2-tranzitív transzformációcsoport at $\Omega = \mathbb{T}$ halmazon. Valóban, ha rögzítünk $(x_1, x_2), (y_1, y_2) \in \mathbb{T}^2$ számpárokat úgy, hogy $x_1 \neq x_2$, $y_1 \neq y_2$, akkor az

$$ax_1 + b = y_1, \qquad ax_2 + b = y_2$$

egyenletrendszer egyértelműen megoldható:

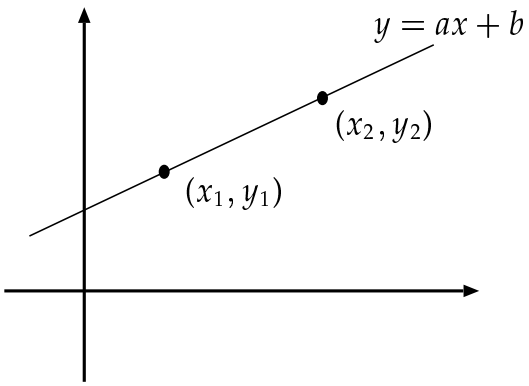
$$a = \frac{y_1 - y_2}{x_1 - x_2}, \qquad b = \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}.$$

Látható, hogy az $x_1 \neq x_2$, $y_1 \neq y_2$ feltételek teljesen ki is vannak használva, hiszen különben vagy nem lenne a meghatározva, vagy pedig $a = 0$ lenne, ami nem határoz meg AGL-beli transzformációt.

Az egyértelmű megoldhatóság természetesen szorosan összefügg azzal a jól ismert geometriai ténnyel, hogy az affin síkon két pontot pontosan egy egyenessel lehet összekötni. (2.2 ábra.) Geometriailag is nyilvánvaló, hogy az $x_1 \neq x_2$, $y_1 \neq y_2$ feltételek szükségesek, hiszen függőleges vagy vízszintes egyenesek nem határoznak meg megfelelő a értéket.

2.3. Csoporthatás

A következő definíció kis mértékben általánosítja a transzformációcsoport fogalmát.



2.2. ábra. Az AGL csoport 2-tranzitivitása

2.4. Definíció. *Legyen G egy csoport, Ω pedig egy tetszőleges halmaz. Egy $f : G \times \Omega \to \Omega$ leképezést* csoporthatásnak *nevezzük, ha teljesülnek az alábbiak.*

(H1) $f(1, \alpha) = \alpha$, *minden* $\alpha \in \Omega$ *esetén.*

(H2) $f(gh, \alpha) = f(g, f(h, \alpha))$, *minden* $\alpha \in \Omega$ *és* $g, h \in G$ *esetén.*

Ha a szóbanforgó f hatás a szövegkörnyezetből egyértelműen meghatározott, akkor az $f(g, \alpha) = g.\alpha$ jelölést alkalmazzunk. Ebben az esetben a két definiáló tulajdonság egyszerűen $1.\alpha = \alpha$ és $g.(h.\alpha) = (gh).\alpha$ alakban írható.

Nyilván minden Ω-n ható transzformációcsoport egyben csoporthatás is Ω-n a $g.\alpha = g(\alpha)$ értelemben. Valójában a csoporthatás csak annyival általánosabb, hogy megengedjuk, hogy $1 \neq h \in G$ elem *triviálisan hasson* Ω-n, azaz $h.\alpha = \alpha$ álljék fent minden $\alpha \in \Omega$ pontra. Ha minden G-beli elem triviálisan hat, akkor azt mondjuk, hogy a csoporthatás triviális.

2.6. példa. Minden G csoport szigorúan tranzitívan hat saját magán, ha a hatást a jobbról szorzással definiáljuk: $g, \alpha \in G$ esetén legyen $g.\alpha = g\alpha$.

2.7. példa. Minden G csoport hat saját magán a konjugálással, azaz ha a csoporthatást (mint már korábban) $h.g = \varphi_h(g) = hgh^{-1}$ definiálja. Ekkor a $Z(G)$ centrum elemei mind triviálisan hatnak G-n. Ha G Abel-csoport, akkor maga a csoporthatás is triviális.

2.8. példa. Legyen G egy tetszőleges csoport, $H \leq G$ pedig egy részcsoport. Definiáljuk G hatását a H bal oldali mellékosztályain a jobbról szorzással, azaz $g.(aH) = gaH$. Ez nyiván csoporthatás, továbbá ha H normá-

losztó és $h \in H$, akkor $haH = a \cdot hH = aH$, azaz a H-beli elemek triviálisan hatnak.

Világos, hogy a tranzitivitás különböző formáinak definíciói mind értelmesek általános csoporthatás esetén is, továbbá a 2.3 tétel is változtatás nélkül kiterjeszthető. A fentiek közül a 2.8 példa tranzitív, de $H \neq \{1\}$ esetén nem élesen tranzitív; $H = \{1\}$ estén pedig a 2.6 példával ekvivalens. A 2.7 példabeli hatás biztos, hogy nem tranzitív, mert az egységelemet minden G-beli elem fixen hagyja.

A következő tétel azt mondja ki, hogy az utolsó példa lényegében az általános esetet írja le tranzitív csoporthatás esetén.

2.5. Tétel. *Legyen G egy Ω-n tranzitívan ható csoport, és rögzítsünk egy $\alpha \in \Omega$ elemet. Ekkor G „ugyanúgy" hat Ω-n mint a G/G_α mellékosztályok halmazán. Azaz, létezik egy $s : \Omega \to G/G_\alpha$ bijektív megfeleltetés úgy, hogy minden $g \in G$ esetén $s(g.\alpha) = g.s(\alpha)$.*

Megjegyzés. Ha a G csoport hat az Ω_1 és az Ω_2 halmazokon, és létezik egy $s : \Omega_1 \to \Omega_2$ bijekció a fenti tulajdonsággal, akkor a két hatást *G-ekvivalensnek* mondjuk.

Bizonyítás. Minden $\beta \in \Omega$ esetén értelmezzük az

$$X_\beta = \{g \in G; g.\alpha = \beta\}$$

halmazt. Megmutatjuk, hogy valamely $h \in X_\beta$ esetén $X_\beta = hG_\alpha$, azaz X_β a G_α egy bal oldali mellékosztálya. Legyen ugyanis $h \in X_\beta$ és $g \in G_\alpha$ tetszőleges elemek, ekkor definíció szerint $(hg).\alpha = \beta$, azaz $hg \in X_\beta$. Fordítva, ha $g \in X_\beta$, akkor $(h^{-1}g).\alpha = \alpha$, azaz $h^{-1}g \in G_\alpha$ és $g \in G_\alpha h$. Ezzel a $X_\beta \subseteq G_\alpha h$ és $X_\beta \supseteq G_\alpha h$ tartalmazásokat egyaránt beláttuk, tehát $X_\beta = G_\alpha h$ teljesül.

Definiáljuk az $s : \Omega \to G/G_\alpha$, $\beta \mapsto X_\beta$ leképezést. A fentiek szerint ez értelmes, G tranzitivitása miatt szürjektív, X_β definíciója miatt pedig injektív. Az X_β halmazok definíciójából pedig adódik a

$$g.s(\beta) = gX_\beta = X_{g.\beta} = s(g.\beta)$$

összefüggés, ami bizonyítja a G-ekvivalenciát. □

3. fejezet

Testek

A bevezetőben említettek szerint a későbbiekben különböző testek által koordinátázott geometriák algebrai struktúráit és azok transzformációcsoportjait fogjuk vizsgálni. Ebben a fejezetben az ehhez szükséges testelméleti ismereteket gyűjtöttük össze. A csoportokhoz hasonlóan itt sem törekedtünk az elmélet részletes kifejtésére, hanem arra, hogy az anyagot már most a későbbi geometriai alkalmazások fényében tárgyaljuk.

3.1. Testekről általában

3.1. Definíció. *Legyen adott a T alaphalmaz a rajta értelmezett „$+$" összeadás- és „$\cdot$" szorzásművelettel. A $(T, +, \cdot)$ hármas* test, *ha az alábbi axiómák teljesülnek.*

(F1) $(T, +)$ *Abel-csoport, az additív egységelem jele a 0.*

(F2) $(T^*, \cdot)$ *Abel-csoport, ahol $T^* = T \setminus \{0\}$. A multiplikatív egységelem jele az 1.*

(F3) *(Disztributivitás.) Az összeadás es a szorzás műveletét összekapcsolja az $x \cdot (y + z) = x \cdot y + x \cdot z$ azonosság.*

Megjegyzés. Amennyiben a fenti axiómák a szorzás kommutativitása kivételével teljesülnek, akkor *ferdetestről* beszélülnk. Természetesen, ebben az esetben mindkét oldali disztributivitás meg kell követelnünk, azaz (F3) mellett $(x + y) \cdot z = x \cdot z + y \cdot z$.

A legismertebb példák testekre a racionális számok $\mathbb{Q}$, a valós számok $\mathbb{R}$ és a komplex számok $\mathbb{C}$ testjei.

Az (F1) és (F2) axiómák miatt tudjuk, hogy egy testnek mindig van legalább két eleme, a 0 és az 1. Ebből a két elemből a négy alapművelet segítségével minden racionális szám előállítható. Ebből az következik, hogy $\mathbb{R}$-ben $\mathbb{Q}$ a legszűkebb test.

Ezzel szemben $\mathbb{Q}$ és $\mathbb{R}$ között sok test található. Tekintsük pl. a

$$\mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \mathbb{Q}\sqrt{2} = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$$

halmazt. Ez nyilván zárt az összeadásra, a kivonásra, és a szorzást is könnyű leellenőrizni. Az osztásra való zártságot egy, a későbbiekben is gyakran használt egyszerű trükkel mutatjuk meg: az $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$ egyenlőségből következik

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}].$$

3.2. A komplex számok teste

A komplex számok testét a a valós testből az előzőhöz hasonló konstrukcióval nyerhetjük. Legyen ugyanis i egy szimbólum, amelyről csak azt tesszük fel, hogy $i^2 = -1$ (azaz gyöke az $X^2 + 1 = 0$ polinomnak), és hogy a vele való szorzás- és összeadásműveletben felcserélhető $\mathbb{R}$ minden elemével. Ekkor $\mathbb{C}$ definíciója

$$\mathbb{C} = \mathbb{R}[i] = \mathbb{R} + \mathbb{R}i = \{a + bi | a, b \in \mathbb{R}\}.$$

A testaxiómák mind könnyen leellenőrizhetők, ebben az esetben is egyedül az osztásnak szentelünk nagyobb figyelemet. Ehhez a jól ismert komplex konjugált és komplex norma fogalmát kell bevezetnünk:

$$\text{Az } z = a + bi \in \mathbb{C} \text{ esetén } \overline{z} = a - bi \text{ és } |z|^2 = z\overline{z} = a^2 + b^2 \in \mathbb{R}_0^+.$$

Eszerint a $z = a + bi$ komplex szám inverze

$$z^{-1} = \frac{\overline{z}}{|z|^2} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i \in \mathbb{C}.$$

Könnyű számolással meggondolható, hogy a komplex konjugálás testautomorfizmus, azaz

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2} \text{ és } \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}.$$

Ebből adódik, hogy a norma multiplikatív, vagyis $|z_1 z_2| = |z_1||z_2|$.

Világos, hogy $\mathbb{C}$ felfogható egy $\mathbb{R}$ feletti vektortérként, hiszen $\mathbb{C}$ elemeit össze tudom adni és a valós számokkal való szorzás is természetes módon adott. Az is nyilvánvaló, hogy $\dim \mathbb{C} = 2$. Így tehát definiálni tudunk egy kölcsönösen egyértelmű megfeleltetést $\mathbb{C}$ és $\mathbb{R}^2$ között:

$$z = a + bi \in \mathbb{C} \longleftrightarrow \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{R}^2.$$

Ha $z' = a' + b'i \in \mathbb{C}$, akkor zz'-nek a

$$\begin{pmatrix} aa' - b'b \\ ab' + a'b \end{pmatrix}$$

vektor felel meg.

Rögzítsünk most egy $z \in \mathbb{C}$ tetszőleges komplex számot és értelmezzük az

$$L_z : \mathbb{C} \to \mathbb{C}, \quad L_z(x) = zx$$

leképezést. L_z nyilván az $\mathbb{R}$ feletti vektortér egy lineáris leképezése:

$$\begin{array}{ll} L_z(x_1 + x_2) = L_z(x_1) + L_z(x_1) & \forall x_1, x_2 \in \mathbb{C} \text{ (disztibutivitás)}, \\ L_z(xt) = L_z(x)t & \forall x \in \mathbb{C}, t \in \mathbb{R}. \end{array}$$

Ily módon tehát egy $z \mapsto L_z$ leképezést definiáltunk $\mathbb{C}$-ből a kétdimenziós valós vektortér lineáris leképezéseinek gyűrűjébe.[1] Könnyen belátható, hogy ez a megfeleltetés megtartja a két alapműveletet, azaz

$$L_{z_1} + L_{z_2} = L_{z_1+z_2} \text{ és } L_{z_1} L_{z_2} = L_{z_1 z_2}$$

teljesül. Rögzítsünk most egy $z = u + vi$ komplex számot és tekintsük egy tetszőleges $z = a + bi \in \mathbb{C}$ elemet. Ekkor

$$L_z(x) = zx \longleftrightarrow \begin{pmatrix} ua - vb \\ va + ub \end{pmatrix} = \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix}.$$

Azaz, ha L_z-t mint a kétdimenziós valós vektortér lineáris transzformációját tekintem, az a $\begin{pmatrix} u & -v \\ v & u \end{pmatrix}$ mátrixalakban írható fel. Ezután már gyorsan be tudjuk látni az alábbi állítást.

3.2. Állítás. *A 2×2 valós mátrixok*

$$\left\{ \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \middle| \, u, v \in \mathbb{R} \right\}$$

halmaza egy, a komplex számtesthez izomorf testet alkot. Az izomorfiát a $z = u + vi \leftrightarrow \begin{pmatrix} u & -v \\ v & u \end{pmatrix}$ megfeleltetés definiálja, a komplex konjugálás művelete a mátrixtranszponálásnak, a komplex normanégyzet pedig a determinánsképzésnek felel meg.

[1] Egy V vektortér önmagára vett lineáris leképezései *gyűrűt* alkotnak a leképezések $(\alpha \circ \beta)(x) = \alpha(\beta(x))$ szorzatával és a pontonkénti $(\alpha + \beta)(x) = \alpha(x) + \beta(x)$ összeadással mint műveletekkel.

Bizonyítás. Az állítás minden pontja leellenőrizhető közvetlen számítással, ezek közül more csak a szorzásra vonatkozót részletezzük. Legyen $z = u + vi$, $z' = u' + v'i$, ekkor

$$\begin{aligned} zz' &= uu' - vv' + (uv' + vu')i \\ &\leftrightarrow \begin{pmatrix} u & -v \\ v & u \end{pmatrix} \begin{pmatrix} u' & -v' \\ v' & u' \end{pmatrix} = \begin{pmatrix} uu' - vv' & -uv' - vu' \\ uv' + vu' & uu' - vv' \end{pmatrix}. \end{aligned}$$ □

3.3. Véges testek

Ebben a fejezetben olyan testekről lesz szó, amelyeknek a tartóhalmaz véges. Azonban nem áll szándékunkban az idekapcsolódó algebrai elmélet részletes kifejtése, ezt a legtöbb algebrai bevezető tankönyben megtalalálhatja az olvasó (pl. Fuchs: Algebra). Ehelyett megpróbálunk egy szemléletes képet adni ezekről a testekről, a konstrukciójukról és a legfontosabb alaptulajdonságaikról.

Mint már említettük, a testaxiómákból következően minden testnek van legalább két eleme, a 0 és az 1. Az alapműveletek kis változtatásával olyan műveletekhez jutunk, amelyekkel ez a kételemű $\{0, 1\}$ halmaz ki fogja elégíteni az összes testaxiómat. Definiáljuk tehát az alapműveleteinket az alábbi táblázatok szerint.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

(3.1)

A műveletek egyszerűsége miatt gyorsan leellenőrizhető, hogy itt valóban testről van szo. Vegyük észre, hogy az $1 + 1$ kivételével az összes művelet eredményét a testaxiómák egyértelműen meghatározzák. Ezt a példát általánosítjuk a következő állításban.

3.3. Állítás. *Tetszőleges p prímszám esetén az $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ halmaz az*

$$x \oplus y = x + y \pmod{p} \qquad \text{és} \qquad x \odot y = x \cdot y \pmod{p}$$

műveletekkel mint összeadással és szorzással egy p-rendű testet alkot.

Bizonyítás. Mivel az $\mathbb{F}_p$ elemei egyértelműen meghatározottak modulo p, az új műveletek is jól definiáltak. Az (F1) és (F3) szintén öröklődik az eredeti összeadástól és szorzástól. A szorzás invertáhatóságához azt kell meggondolni, hogy bármely $x \in \mathbb{F}_p$ esetén az $y \mapsto x \odot y$ leképezés bijektív (tehát invertálható). Véges halmazról lévén szó, elegndő belátni, hogy injektív. Ha viszont nem lenne az, akkor $x \odot y_1 = x \odot y_2$, azaz $x \odot y_3 = 0$ állna fenn, ahol $y_3 = y_1 \ominus y_2 \neq 0$. Ebből az következik, hogy x vagy y_3 osztható p-vel, de $x \in \mathbb{F}_p^*$ és $y_3 \in \mathbb{F}_p$ miatt ez csak $y_3 = 0$ esetén lehetséges, ez pedig ellentmondás. Tehát $(\mathbb{F}_p^*, \odot)$ csoport, $(\mathbb{F}_p, \oplus, \odot)$ pedig test. □

A továbbiakban már a $\oplus$, $\odot$ jelek helyett is közönséges $+$ és $\cdot$ jeleket fogjuk használni.

A valós testeknél említettük, hogy az $\mathbb{R}$ legszűkebb részteste a $\mathbb{Q}$, mert annak minden eleme kifejezhető a 0 és az 1-el, a négy alapműveletet használva. Ilyen módon a $\mathbb{Q}$ egyértelműen meghatározott.[2]Nos, az előbbi példában szereplő $\mathbb{F}_p$ esetén is igaz, hogy minden eleme előáll a 0 és az 1 segítségével, sőt itt elegendő csak az összeadást használni. Az összeadásnál valójában csak a $p = 0$ szabályt kell bevezetnünk, ez már garantálja is az $\mathbb{F}_p$ egyértelműségét. Pontosabban

$$\underbrace{1 + \ldots + 1}_{p\text{-szer}} = 0. \tag{3.2}$$

Ehhez kapcsolódik a következő definíció.

3.4. Definíció. *Egy tetszőleges* $(T, +, \cdot)$ *test* karakterisztikájának *nevezzük azt a legkisebb* $p = \mathrm{char}(T)$ *pozitív egész számot, melyre* (3.2) *teljesül. Amennyiben ilyen pozitív szám nem létezik, akkor a karakterisztika definíció szerint* $\mathrm{char}(T) = 0$.

Megjegyzés. Világos, hogy $\mathrm{char}\,\mathbb{Q} = \mathrm{char}\,\mathbb{R} = \mathrm{char}\,\mathbb{C} = 0$ és $\mathrm{char}\,\mathbb{F}_p = p$. A testek nullaosztómentességének segítségével azt is könnyen meggondolhatjuk, hogy egy test karakterisztikája vagy 0 vagy pedig $p > 0$ prímszám. Mindezen túl a definíciót megelőző meggondolásból következik az alábbi állítás.

3.5. Állítás. *Ha a* T *test karakterisztikája 0, akkor a* T *által tartalmazott legszűkebb résztest izomorf* $\mathbb{Q}$*-val. Ha* $\mathrm{char}(T) = p > 0$*, akkor* p *prím és* T *legszűkebb részteste izomorf* $\mathbb{F}_p$*-vel. A* T *által tartalmazott legszűkebb résztestet a* T *prímtestének nevezzük.*

Világos, hogy a disztributivitás miatt (3.2) ekvivalens az

$$\underbrace{x + \ldots + x}_{p\text{-szer}} = 0$$

állítással minden $x \in T$ esetén.

Nyilvánvaló továbbá, hogy minden $\mathbb{K}$ prímtestű T test felfogható, mint egy $\mathbb{K}$ feletti vektortér. Ha T véges, akkor a 3.5 állítás miatt $\mathbb{K} = \mathbb{F}_p$ és a T vektortér $\mathbb{F}_p$ feletti $n = \dim_{\mathbb{K}} T$ dimenzió is véges. Ekkor viszont létezik egy n elemű bázis, és $|T| = p^n$.

[2]Pontosabban azt szoktuk mondani, hogy *izomorfia erejéig* egyértelműen meghatározott. Ez lényegében azt jelenti, hogy a racionális számok teste, akármilyen szimbólumokkal jelöljük is a számokat, mindig csak a racionális számok teste lesz.

Ez fordítva is igaz: minden $q = p^n$ alakú számhoz létezik q elemű véges test. Az általános eset bizonyításával nem foglalkozunk. Ehelyett tetszőleges p prímszám esetére konstruálunk egy p^2 rendű testet. Az általános konstrukció is hasonlóan működik, de ahhoz mélyebb algebrai jellegű megfontolások szükségesek.

A következő tétel a véges testek számunkra legfontosabb két tulajdonságát mondja ki.

3.6. Tétel. *Legyen $q = p^n$, ahol p prím.*

(i) *Létezik egy izomorfia erejéig egyértelműen meghatározott $\mathbb{F}_q$ q-rendű test,* $\operatorname{char}\mathbb{F}_q = p$.

(ii) *Az $\mathbb{F}_q$ test $\mathbb{F}_q^*$ multiplikatív csoportja ciklikus.*

Bizonyítás. Lásd Fuchs László: Algebra, VI.9. fejezet. □

Rögzítsünk először egy p páratlan prímszámot. $\mathbb{F}_p$-ben $1 + 1 \neq 0$, így $1 \neq -1$, azaz az $x \mapsto x^2$ leképezés nem injektív. De $\mathbb{F}_p$ véges halmaz, ezért szürjektív sem lehet. Azaz, van olyan $\sigma \in \mathbb{F}_p$, amely nem négyzete egyetlen $\mathbb{F}_p$-beli elemnek sem, $\sqrt{\sigma} \notin \mathbb{F}_p$. A $\mathbb{Q}[\sqrt{2}]$ és $\mathbb{C}$ testekhez hasonlóan meg tudjuk konstruálni az

$$\mathbb{F}_p[\sqrt{\sigma}] = \{a + b\sqrt{\sigma} | a, b \in \mathbb{F}_p\}$$

testet, ahol az $x = a + b\sqrt{\sigma}$ elem konjugáltja $\overline{x} = a - b\sqrt{\sigma}$ és $x\overline{x} = a^2 - b^2\sigma \in \mathbb{F}_p$. $\mathbb{F}_p[\sqrt{\sigma}]$ zártsága a három alapműveletre nyilvánvaló, az osztás pedig a szokott módon adódik:

$$x^{-1} = \frac{a}{a^2 - b^2\sigma} - \frac{b}{a^2 - b^2\sigma}\sqrt{\sigma},$$

ahol szükségképpen $a^2 - b^2\sigma \neq 0$, mert különben $\sqrt{\sigma} = a/b \in \mathbb{F}_p$ teljesülne. Tehát $\mathbb{F}_{p^2} = \mathbb{F}_p[\sqrt{\sigma}]$ egy p^2 elemű test.

Ez a konstrukció nem működik $p = 2$ esetén, hisz itt a négyzetre emelés művelete bijektív. Ehelyett tekintsük az $f(X) = X^2 + X + 1$ polinomot. Ennek nincs gyöke $\mathbb{F}_2$-ben (csak a 0 és 1 értékeket kell behelyettesíteni), azaz $\mathbb{F}_2$ felett irreducibilis. Bővítsük ki $\mathbb{F}_2$-t egy τ elemmel, amiről feltételezzük, hogy gyöke $f(X)$-nek. Az $\mathbb{F}_4 = \mathbb{F}_2[\tau]$ test elemei ekkor $\{0, 1, \tau, \tau + 1\}$, a műveleteket pedig a $\tau^2 + \tau + 1 = 0$ összefüggés egyértelműen meghatározza:

$+$	0	1	τ	$\tau+1$
0	0	1	τ	$\tau+1$
1	1	0	$\tau+1$	τ
τ	τ	$\tau+1$	0	1
$\tau+1$	$\tau+1$	τ	1	0

$\cdot$	1	τ	$\tau+1$
1	1	τ	$\tau+1$
τ	τ	$\tau+1$	1
$\tau+1$	$\tau+1$	1	τ

A számítások leellenőrzését az olvasóra bízzuk.

3.4. A kvaterniók ferdeteste

Ebben a fejezetben megismerkedünk a kvateniókkal, amelyek egy ferdetestet alkotnak. A ferdetesteknek ezt a példányát a klasszikus példának lehet nevezni.

A mi felépítésünkben a kvaterniókat mint a komplex számok egy bővítését fogjuk definiálni. A konstrukció nagyban hasonlatos lesz a korábbi ($\mathbb{Q}[\sqrt{2}]$, $\mathbb{C} = \mathbb{R}[i]$, $\mathbb{F}_{p^2} = \mathbb{F}_p[\sqrt{\sigma}]$) kvadratikus testbővítési eljárásokhoz.[3]Persze itt nem lehetséges egyszerűen egy irreducibilis másodfokú polinom gyökét venni, hiszen a komplex számtest felett ilyenek nem léteznek.

Tekintsünk ezért egy $j \notin \mathbb{C}$ elemet, amelyre $j^2 = -1$. Ha a kvaterniók halmazát mint

$$\mathbb{H} = \mathbb{C}[j] = \{z_1 + jz_2 | z_1, z_2 \in \mathbb{C}\}$$

akarjuk definiálni, akkor persze nem engedhetjük meg, hogy j felcserélhető legyen a $\mathbb{C}$ elemeivel, hiszen ekkor $\mathbb{H}$ egy (kommutatív) test lenne, amiben az $X^2 + 1 = 0$ polinomnak nem lehet kettőnél több gyöke. Ehelyett az fogjuk megkövetelni, hogy

$$j\, z = \overline{z}\, j \tag{3.3}$$

teljesüljön minden $z \in \mathbb{C}$ elem esetén. Ezzel a feltételezéssel, a kétoldali disztributivitással és az összeadás kommutativitásával már egyértelmű módon definiálva van $\mathbb{H}$-n szorzásművelet:

$$\begin{aligned}(z_1 + jz_2)(w_1 + jw_2) &= z_1w_1 + jz_2w_1 + z_1jw_2 + jz_2jw_2 \\ &= z_1w_1 - \overline{z}_2\, w_2 + j(z_2w_1 + \overline{z}_1\, w_2).\end{aligned} \tag{3.4}$$

Szokás szerint az osztással van a legnagyobb probléma, és ennek megoldásához, mint mindig, a konjugálást hívjuk segítségül. Ebben az esetben sem feledkezhetünk meg azonban arról, hogy a szorzás nem kommutatív. Ezért a definiálandó konjugálás nem testautomorfizmus lesz, hanem *anti-automorfizmus*, azaz

$$\overline{x_1 + x_2} = \overline{x}_1 + \overline{x}_2 \text{ és } \overline{x_1x_2} = \overline{x}_2\, \overline{x}_1 \qquad \forall x_1, x_2 \in \mathbb{C}.$$

Ebből következik, hogy az $x = z_1 + jz_2$ elem konjugáltja $\overline{x} = \overline{z}_1 - jz_2$. Ekkor a norma:

$$|x|^2 = x\, \overline{x} = (z_1 + jz_2)(\overline{z}_1 - jz_2) = z_1\, \overline{z}_1 + z_2\, \overline{z}_2 = |z_1|^2 + |z_2|^2 \in \mathbb{R}.$$

[3]Egy testbővítést *kvadratikusnak* nevezünk, ha a bővítéshez használt elem egy irreducibilis másodfokú polinom gyöke.

Ha $z_1 = x_1 + x_2 i$ és $z_2 = x_3 + x_4 i$, $(x_1, x_2, x_3, x_4 \in \mathbb{R})$, akkor

$$x\,\overline{x} = x_1^2 + x_2^2 + x_3^2 + x_4^2 \in \mathbb{R},$$

valamint

$$x^{-1} = \overline{x}/|x|^2.$$

Megjegyezzük, hogy szokás a kvaterniókat $x = x_1 + x_2 i + x_3 j + x_4 k$ alakban is írni, ahol $x_1, x_2, x_3, x_4 \in \mathbb{R}$ és $k = ij$. Ebben a felépítésben az i, j, k elemek szerepe teljesen szimmetrikus, többek között mindháromra egyformán teljesül a $-1 = i^2 = j^2 = k^2$ egyenlőség. Ez azt mutatja, hogy a (kommutatív) testekkel ellentétben egy ferdetest feletti polinomnak lehet a fokszámánál több gyöke.

Végül, a komplex számokéhoz hasonló eljárással mátrixalakban írjuk fel a kvaterniókat. Az rögtön adódik, hogy $\mathbb{H}$ a $\mathbb{C}$ test feletti kétdimenziós vektortér. Ebben az esetben azonban vigyázni kell azzal, hogy $\mathbb{H}$-t jobb vagy bal oldali vektortérként értelmezzük. A további számolásokban mi *jobb oldali* vektortérként fogjuk $\mathbb{H}$-t tekinteni, és bázisnak az 1-et és j-t választjuk, vagyis a $\mathbb{C}^2$ és $\mathbb{H}$ közötti

$$\left(\ z_1, z_2\ \right) \longleftrightarrow z_1 + j z_2,$$

lineáris megfeleltetést fogjuk használni. Ily módon az $L_x : y \mapsto xy$, $x, y \in \mathbb{H}$ balról szorzás lineáris leképezés lesz[4], hiszen $x(y_1 + y_2) = xy_1 + xy_2$ és $x(yc) = (xy)c$. Ez az L_x leképezés az $x = z_1 + jz_2$ és $y = w_1 + jw_2$ elemek esetén (3.4) szerint

$$L_x : \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \mapsto \begin{pmatrix} z_1 w_1 - \overline{z}_2\, w_2 \\ z_2 w_1 + \overline{z}_1\, w_2 \end{pmatrix} = \begin{pmatrix} z_1 & -\overline{z}_2 \\ z_2 & \overline{z}_1 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \end{pmatrix}$$

mátrixalakban írható. Ezzel beláttuk a 3.2 állítás kvaterniókra vonatkozó analogonját:

3.7. Tétel. *A 2×2 komplex mátrixok*

$$\left\{ \left(\begin{array}{cc} z_1 & -\overline{z}_2 \\ z_2 & \overline{z}_1 \end{array} \right) \middle| \, z_1, z_2 \in \mathbb{C} \right\}$$

halmaza a kvaterniók $\mathbb{H} = \mathbb{C} + \mathbb{C}[j]$ ferdetestjével izomorf ferdetestet alkot. Az izomorfiát az $x = z_1 + jz_2 \leftrightarrow \begin{pmatrix} z_1 & -\overline{z}_2 \\ z_2 & \overline{z}_1 \end{pmatrix}$ megfeleltetés adja meg, a $\mathbb{H}$-beli konjugálás a komplex mátrixok Hermite-konjugálásának, a $\mathbb{H}$-beli normanégyzet pedig a determinánsképzésnek felel meg.

[4] A $\mathbb{H}$ elemeivel történő $R_x : y \mapsto yx$ jobbról szorzás *nem* lesz lineáris, mert $R_x(yc) = (yc)x \neq R_x(y)c = (yx)c$.

4. fejezet

Lineáris transzformációk csoportja

Ennek a fejezetnek az első részében felelevenítjük a lineáris terekre és a lineáris leképezésekre vonatkozó ismereteinket. Ez utóbbiak a legismertebbek az általunk tanulmányozott transzformációcsoportok körében. A fejezet második részében az affin tereket és ezek transzformációit vizsgáljuk. Itt többek között példát fogunk látni élesen 2-tranzitív transzformációcsoportokra is.

A fejezet során $\mathbb{T} = (\mathbb{T}, +, \cdot)$ egy tetszőleges testet fog jelölni. Röviden érinteni fogjuk azt az esetet is, ha $\mathbb{T}$ ferdetest (azaz a szorzásművelet nemkommutatív), de ezt mindig külön említeni fogjuk.

4.1. Lineáris transzformációk

A vektortér vagy más néven lineáris tér és néhány hozzátartozó jól ismert fogalom definíciója:

4.1. Definíció.

(V1) *Azt mondjuk, hogy V egy $\mathbb{T}$* test feletti vektortér, *ha a V halmazon értelmezve van az összeadás és a $\mathbb{T}$ elemeivel (skalárokkal) való (jobb oldalról történő) szorzás művelete úgy, hogy $(V, +)$ Abel-csoport és a skalárokkal való szorzás disztributív és átzárójelezhető, azaz teljesülnek az alábbi axiómák:*

$$\begin{array}{ll} (\boldsymbol{v} + \boldsymbol{w})x = \boldsymbol{v}x + \boldsymbol{w}x & \forall \boldsymbol{v}, w \in V, x \in \mathbb{T} \\ \boldsymbol{v}(x + y) = \boldsymbol{v}x + \boldsymbol{v}y & \forall \boldsymbol{v} \in V, x, y \in \mathbb{T} \\ (\boldsymbol{v}x)y = \boldsymbol{v}(xy) & \forall \boldsymbol{v} \in V, x, y \in \mathbb{T} \\ \boldsymbol{v}1 = \boldsymbol{v} & \forall \boldsymbol{v} \in V. \end{array}$$

(V2) *A $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k$ vektorok* lineárisan függetlenek *($\mathbb{T}$ felett), ha $\boldsymbol{v}_1 x_1 + \ldots + \boldsymbol{v}_k x_k = \boldsymbol{0}$ kiárólag az $x_1 = \ldots = x_k = 0$ esetben teljesül.*

(V3) *A $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ vektorok a V vektortér* bázisát *alkotják, ha lineárisan függetlenek, és minden $\boldsymbol{w} \in V$ vektor előáll a $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ elemek ($\mathbb{T}$ feletti) lineáris kombinációjaként.*

(V4) *A bázis mérete egyértelműen meghatározott V-ben, ezt a számot vagy számosságot a V ($\mathbb{T}$ feletti)* dimenziójának *nevezzük.*

(V5) *Legyenek V és V' rögzített $\mathbb{T}$ feletti vektorterek. Az $\alpha : V \to V'$ leképezést* lineáris leképezésnek *nevezzük, ha megtartja a vektortérstruktúrát, azaz*

$$\alpha(\boldsymbol{v}x + \boldsymbol{w}y) = \alpha(\boldsymbol{v})x + \alpha(\boldsymbol{w})y \qquad \forall \boldsymbol{v}, w \in V, x, y \in \mathbb{T}.$$

A definícióban szereplő állítások és a fogalmakhoz kapcsolódó legfontosabb tulajdonságok bizonyítására mi nem térünk ki, a javasolt irodalom Fried E: Lineáris algebra c. könyve.

A legtermészetesebb példa vektorterekre a $\mathbb{T}$ test elemeiből képzett szám-n-esek halmaza. Ezek egy $\mathbb{T}$ feletti n-dimenziós vektorteret alkotnak, erre a $\mathbb{T}^n$ jelölést használjuk. Közismert, hogy minden végesdimenziós $\mathbb{T}$ feletti vektortér izomorf a $\mathbb{T}^n$ vektortérrel. Ehhez az izomorfiához nincs másra szükségünk, mint **rögzíteni egy** $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ **bázist.** Ezután a bázis definíciója szerint minden $\boldsymbol{w} \in V$ felírható

$$\boldsymbol{w} = \boldsymbol{v}_1 x_1 + \ldots + \boldsymbol{v}_n x_n$$

alakban, s így értelmezhető a

$$\boldsymbol{w} \longleftrightarrow \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \tag{4.1}$$

megfeleletés. Hangsúlyozzuk, hogy a megfeleltetés csak a bázis kiválasztása után értelmes, arra jellemző, azaz egy másik bázis választása egy más megfeleltetést definiál.

Ugyanez mondható el a a lineáris leképezések és a mátrixok kapcsolatáról. Legyen ugyanis $\alpha : V \to W$ lineáris leképezés a két vektortér között és rögzítsük a $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ és $\{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_m\}$ bázisokat. Ekkor egy $\boldsymbol{u} = \boldsymbol{v}_1 x_1 + \ldots + \boldsymbol{v}_n x_n \in V$ vektor képe az

$$\boldsymbol{u}' = \alpha(\boldsymbol{u}) = \alpha(\boldsymbol{v}_1)x_1 + \ldots + \alpha(\boldsymbol{v}_n)x_n \in W \tag{4.2}$$

vektor. Az $\alpha(\boldsymbol{v}_i)$ vektorok kifejezhetők

$$\alpha(\boldsymbol{v}_i) = \boldsymbol{w}_1 a_{1i} + \ldots + \boldsymbol{w}_m a_{mi} \in W$$

alakban. Ezt beírva (4.2)-be kapjuk, hogy

$$\boldsymbol{u}' = \boldsymbol{w}_1 \cdot \sum a_{1i} x_i + \ldots + \boldsymbol{w}_m \cdot \sum a_{mi} x_i,$$

ahol a szummáció szabálya egyszerű: minden kétszer előforduló indexre összegzünk. Ezek szerint–ha mindkét térben választottunk bázis–az α leképezéshez hozzárendelhetjük a

$$\alpha \longleftrightarrow A = \begin{pmatrix} a_{11} & \cdots & a_{n1} \\ & \ddots & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \tag{4.3}$$

mátrixot. Vegyük észre, hogy ennek a mátrixnak annyi oszlopa van, amekkora a kiindulási V tér dimenziója, és annyi sora, amennyi W tér dimenziója. Továbbá, az i-dik oszlopban pontosan az i-dik V-beli báziselem képének a W-báziselemekkel való együtthatóit látjuk. A (4.1) megfeleltetést használva pedig a jól ismert

$$\alpha : \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \longmapsto \begin{pmatrix} a_{11} & \cdots & a_{n1} \\ & \ddots & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

alakot kapjuk, amit szokás szerint a jóval egyszerűbb $\boldsymbol{x}' = A\boldsymbol{x}$ alakban is írhatunk. A továbbiakban legfőképp a V vektortér önmagára való lineáris leképezéseit fogjuk vizsgálni.

4.2. Tétel. *Legyen α a V végesdimenziós vektortér önmagára vett lineáris leképezése. Ekkor az alábbi állítások egymással ekvivalensek.*

(i) *Az α leképezés invertálható, azaz bijektív.*

(ii) *Az α leképezés szürjektív.*

(iii) *Az α leképezés injektív.*

(iv) *Az α leképezéshez* (4.3) *szerint tartozó négyzetes mátrix determinánsa nem nulla.*

(v) *Az α leképezéshez* (4.3) *szerint tartozó négyzetes mátrix sorai lineárisan függetlenek, azaz bázist alkotnak.*

(vi) *Az α leképezéshez* (4.3) *szerint tartozó négyzetes mátrix oszlopai lineárisan függetlenek, azaz bázist alkotnak.*

Bizonyítás. Lásd Fried: Lineáris algebra... □

Tekintsük most át röviden, mi is történik a (4.1), (4.3)) megfeleltetésekkel, ha az eredeti $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ bázisról áttérek egy másik $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ bázisra. Rögzítsük a $\boldsymbol{w} = \boldsymbol{v}_1 x_1 + \cdots + \boldsymbol{v}_n x_n$ vektort tetszőlgesen. Az eredeti $\boldsymbol{v}_j$ vektorok mindegyike kifejezhető az új bázisban valami $\boldsymbol{v}_j = \sum \boldsymbol{u}_i s_{ij}$ alakban. Ekkor viszont $\boldsymbol{w}$ alakja az új bázisban

$$\begin{aligned} \boldsymbol{w} &= \boldsymbol{v}_1 x_1 + \cdots + \boldsymbol{v}_n x_n \\ &= \boldsymbol{u}_1 \cdot \sum s_{1j} x_j + \ldots + \boldsymbol{u}_n \cdot \sum s_{nj} x_j, \\ &= \boldsymbol{u}_1 y_1 + \ldots + \boldsymbol{u}_n y_n \end{aligned}$$

azaz $\boldsymbol{y} = S\boldsymbol{x}$, ahol az $S = (s_{ij})$ mátrixot a *bázisátmenet mátrixának* is hívjuk.

Legyen most $\alpha : V \to V$ lineáris leképezés. Az előbbi bekezdés jelöléseit használva a $\boldsymbol{w}$ vektornak az első illetve második koordinátarendszerben az $\boldsymbol{x}$ illetve $\boldsymbol{y}$ vektorok felelnek meg, köztük fennáll az $\boldsymbol{y} = S\boldsymbol{x}$ összefüggés. A $\boldsymbol{w}'$ képvektort is kifejezhetjük a két koordinátarendszerben az $\boldsymbol{x}'$ és $\boldsymbol{y}'$ koordinátákkal, ekkor (4.3) szerint $\boldsymbol{x}' = A\boldsymbol{x}$ és $\boldsymbol{y}' = B\boldsymbol{y}$. Ezekből következik, hogy

$$\boldsymbol{y}' = S\boldsymbol{x}' = SA\boldsymbol{x} = SAS^{-1}\boldsymbol{y},$$

vagyis adódik az ismert

$$B = SAS^{-1} \tag{4.4}$$

összefüggés.

Megjegyzés. Ez utóbbi egyenlőség a determinánsok szorzástételével azt is maga után vonja, hogy az α-hoz rendelt mátrix determinánsának értéke bázisváltáskor nem változik, azaz értelmes magának az α leképezésnek a determinánsáról beszélni.

4.2. Az általános lineáris csoport

A továbbiakban mindig kizárólag végesdimenziós vektorterekkel foglalkozunk.

4.3. Definíció. *A V vektortér önmagára vett invertálható lineáris leképezései által alkotta csoportot a V tér* általános lineáris csoportjának *nevezzük, és a $GL(V)$ rövidítéssel jelöljük.*

Ha $V = \mathbb{T}^n$ a $\mathbb{T}$ és rögzítjük a

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

természetes bázist, akkor a lineáris leképezések egyértelműen mátrixalakban írhatók. Ebben az esetben a $\mathbb{T}$ feletti *n*-dimenziós általános lineáris csoportról *beszélünk és a $GL(n, \mathbb{T})$ jelölést használjuk:*

$$GL(n, \mathbb{T}) = \{A \ n \times n\text{-es mátrix}\ , \det(A) \neq 0\}.$$

Ez utóbbinak részcsoportja (sőt normálosztója) az

$$SL(n, \mathbb{T}) = \{A \ n \times n\text{-es mátrix}\ , \det(A) = 1\}.$$

speciális lineáris csoport.[1]

[1] Az angol *general linear* és *special linear* szavak rövidítései.

Az előző fejezetben elmondottak szerint egy rögzített bázis esetén minden V vektortér izomorf valami $\mathbb{T}^n$ vektortérrel. Egy ilyen izomofizmus persze definiál egy izomorfizmust a téren ható csoportok közt is, ezért azt mondhatjuk, hogy bázisválasztás után a $GL(V)$ és a $GL(n,\mathbb{T})$ csoportok izomorfak. Ezt foglalja össze az alábbi diagramm.

$$\begin{array}{ccc} V & \xrightarrow{(4.1)} & \mathbb{T}^n \\ \text{def}\downarrow & & \downarrow\text{természetes módon} \\ GL(V) & \xrightarrow[(4.3)]{} & GL(n,\mathbb{T}) \end{array}$$

Az előző fejezet utolsó megjegyzése szerint $SL(V)$ definíciója is értelmes lenne, ennek ellenére ezt a jelölést nem használjuk.

A most definiált csoportok nyilván az 1.5. példában említett típusba tartoznak, s így hatnak a V vektortéren. A fejezet hátralévő részében ezt a hatást vizsgáljuk pontosabban. Először egy lemmát bizonyítunk.

4.4. Lemma. *Legyen Ω_k a V vektortér lineárisan független rendezett vektor k-asainak a halmaza, ahol $k \leq n$. Ekkor $GL(V)$ tranzitívan hat Ω_k-n. Ha $k = n$, akkor a hatás élesen tranzitív.*

Bizonyítás. Legyen $k \leq n$ rögzített. Először meggondoljuk, hogy minden $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k) \in \Omega_k$ független vektor k-as kiegészíthető bázissá. Ha $k = n$, akkor ezen nincs mit belátni. Ha $k < n$, akkor elegendő belátni, hogy kiegészíthető egy vektor $(k+1)$-essé. Ez viszont nyilvánvaló, mert ha $k < n$, akkor $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k)$ nem bázis, tehát létezik olyan $\boldsymbol{v}'$ vektor, mely nem áll elő a $\boldsymbol{v}_i$-k lineáris kombinációjaként, s így $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k, \boldsymbol{v}') \in \Omega_{k+1}$.

Legyenek most $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k), (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k) \in \Omega_k$ tetszőleges elemek. Bővítsük ki mindkettőt

$$\mathcal{B} = (\boldsymbol{v}_1, \ldots, \boldsymbol{v}_k, \boldsymbol{v}_{k+1}, \ldots, \boldsymbol{v}_n), \quad \mathcal{C} = (\boldsymbol{u}_1, \ldots, \boldsymbol{u}_k, \boldsymbol{u}_{k+1}, \ldots, \boldsymbol{u}_n)$$

bázissá és definiáljuk az

$$\alpha : V \to V, \qquad \boldsymbol{v}_1 x_1 + \ldots + \boldsymbol{v}_n x_n \longmapsto \boldsymbol{u}_1 x_1 + \ldots + \boldsymbol{u}_n x_n \tag{4.5}$$

leképezést. Ez nyilván lineáris, invertálható és $\boldsymbol{v}_i \mapsto \boldsymbol{u}_i$, azaz $\mathcal{B} \mapsto \mathcal{C}$ teljesül. Továbbá, ez az egyetlen lineáris leképezés a $\mathcal{B} \mapsto \mathcal{C}$ tulajdonsággal. Ezzel $GL(n,\mathbb{T})$ tranzitivitását Ω_k-n és szigorú tranzitivitását Ω_n-en beláttuk. □

Vegyük észre, hogy a (4.5) szerint definiált leképezés mátrixa megegyezik a $\mathcal{C}$ bázisról $\mathcal{B}$ bázisra való átmenet mátrixával. Valóban, mindkét esetben a mátrix oszlopvektorai a $\mathcal{B}$ bázis elemeinek $\mathcal{C}$ bázisban való kifejezésének együtthatói. Ennek belátását az olvasóra bízzuk.

Legyen most $k < n$ és tekintsük az $(\boldsymbol{v}_1, \dots, \boldsymbol{v}_k), (\boldsymbol{u}_1, \dots, \boldsymbol{u}_k) \in \Omega_k$ tetszőleges elemeket. Bővítsük ki őket a $\mathcal{B} = (\boldsymbol{v}_1, \dots, \boldsymbol{v}_n)$, $\mathcal{C}_d = (\boldsymbol{u}_1, \dots, \boldsymbol{u}_n d)$ bázissá, ahol $d \in \mathbb{T}^*$ tetszőleges elem. Legyen α_d a $\mathcal{B} \mapsto \mathcal{C}_d$ által definiált leképezés. Az előbb elmondottak szerint az α_d leképezés A_d mátrixa megegyezik a fent definiált α leképezés A mátrixával, kivéve, hogy az A_d utolsó oszlopa d-szerese az A utolsó oszlopának. Emiatt $\det(A_d) = \det(A)d$. Mivel $\det(A) \neq 0$, a $d = 1/\det(A)$ választással elérjük, hogy $\det(A_d) = 1$ teljesüljön. Ekkor $A_d \in SL(n, \mathbb{T})$ és $A_d \boldsymbol{v}_i = \boldsymbol{u}_i$ $(i = 1, \dots, k)$. Ezzel beláttuk az következő lemmát.

4.5. Lemma. *Ha $V = \mathbb{T}^n$ és $k < n$, akkor $SL(n, \mathbb{T})$ tranzitívan hat Ω_k-n.*

A két lemma egyszerű geometriai következményei az alábbiak.

4.6. Következmény. *A $GL(n, \mathbb{T})$ és $SL(n, \mathbb{T})$ csoportok tranzitívan hatnak az origótól különböző pontok halmazán.*

4.7. Következmény. *A $GL(n, \mathbb{T})$ és $SL(n, \mathbb{T})$ csoportok $n \geq 2$ esetén kétszeresen tranzitívan hatnak az origóra illeszkedő egyenesek halmazán.*

4.3. A lineáris csoport centruma és kommutátora

Ezen alfejezet során $\mathbb{T}$ egy rögzített testet, V egy $\mathbb{T}$ feletti n-dimenziós vektorteret ($n \geq 2$), $G = GL(V)$ pedig a megfelelő általános lineáris csoportot fogja jelölni. Rögzítsünk egy $\alpha \in Z(G)$ elemet. Tegyük fel, hogy egy adott bázis esetén α mátrixa A. Ekkor $\alpha \in Z(GL(V))$ ekvivalens azzal, hogy $SAS^{-1} = A$ minden $S \in GL(n, \mathbb{T})$ mátrix esetén, ami a bázisváltoztatás (4.4) összefüggése miatt pontosan azt jelenti, hogy V bármilyen bázisa esetén α mátrixalakja A.

Tekintsünk most egy tetszőleges $\boldsymbol{w} \in V$ elemet. Megmutatjuk, hogy valamilyen $a \in \mathbb{T}^*$ esetén $\alpha(\boldsymbol{w}) = \boldsymbol{w}a$ teljesül. Ellenkező esetben ugyanis $\boldsymbol{w}$ és $\alpha(\boldsymbol{w})$ lineárisan függetlenek lennének, és minden $t \in \mathbb{T}$ elemhez létezne a $B_t = \{\boldsymbol{v}_1 = \boldsymbol{w}, \boldsymbol{v}_2 = \boldsymbol{w}t + \alpha(\boldsymbol{w}), \dots, \boldsymbol{v}_n\}$ bázis, amelyben $\alpha(\boldsymbol{v}_1) = \boldsymbol{v}_1 \cdot (-t) + \boldsymbol{v}_2$ és az α mátrixalakjának első oszlopa

$$\begin{pmatrix} -t \\ 1 \\ \vdots \\ 0 \end{pmatrix},$$

ami ellentmond A bázisvásztástól való függetlenségének.

Azt is könnyen meggondolhatjuk, hogy az $\alpha(\boldsymbol{w}) = \boldsymbol{w}a$ egyenlőségben szereplő a nem függ a $\boldsymbol{w}$ választásától. Vegyünk ugyanis egy másik $\boldsymbol{w}' \in V$ elemet. Ha $\boldsymbol{w}' = \boldsymbol{w}d$, akkor

$$\alpha(\boldsymbol{w}') = \alpha(\boldsymbol{w})d = \boldsymbol{w}ad = \boldsymbol{w}da = \boldsymbol{w}'a.$$

Ha pedig $\boldsymbol{w}$ és $\boldsymbol{w}'$ lineárisan függetlenek, akkor $\alpha(\boldsymbol{w}+\boldsymbol{w}') = \alpha(\boldsymbol{w}) + \alpha(\boldsymbol{w}')$ miatt

$$(\boldsymbol{w}+w')\cdot a'' = \boldsymbol{w}a'' + \boldsymbol{w}'a'' = \boldsymbol{w}a + \boldsymbol{w}'a'$$

áll fent. Ez viszont csak $a = a' = a''$ esetén teljesülhet. Azt kaptuk tehát, hogy minden $\alpha \in Z(GL(V))$ transzformáció

$$\alpha(\boldsymbol{w}) = \boldsymbol{w}a \qquad \forall \boldsymbol{w} \in V,$$

alakú, melynek mátrixa $A = Ia$, ahol I az $n \times n$-es egységmátrix. Könnyű meggondolni, hogy ez fordítva is igaz, vagyis minden $c \in \mathbb{T}^*$ elemre $Ic \in Z(GL(n,\mathbb{T}))$. Bebizonyítottuk tehát a következő tételt.

4.8. Tétel. *Az általános lineáris csoport centrumának elemei pontosan az origóból való $a \in \mathbb{T}^*$ elemmel történő nagyítások, azaz*

$$Z(GL(n,\mathbb{T})) = \{Ia | a \in \mathbb{T}^*\} \cong (\mathbb{T}^*, \cdot).$$

A kommutátorrészcsoport meghatározásához hosszadalmasabb meggondolásokra van szükségünk.

4.9. Definíció. *Legyen H a $V = V(n,\mathbb{T})$ vektortér egy hipersíkja. A $T(\neq I) \in GL(n,\mathbb{T})$ leképezést H-*hoz tartozó nyírásnak *nevezzük, ha*

$$T(\boldsymbol{v}) = \boldsymbol{v} \qquad \forall \boldsymbol{v} \in H$$

és

$$T(\boldsymbol{v}) - \boldsymbol{v} \in H \qquad \forall \boldsymbol{v} \in V$$

teljesül. A H hipersík és a V/H faktortér tehát pontonként fix.

4.10. Lemma. *Legyen T egy H hipersíkhoz tartozó nyírás és μ egy V-n értelmezett lineáris funkcionál, amelyre*

$$H = \{\boldsymbol{v} | \mu(\boldsymbol{v}) = 0\}$$

teljesül. Akkor létezik egy $\mathbf{0} \neq \boldsymbol{a} \in H$ (azaz $\mu(\boldsymbol{a}) = 0$) vektor úgy, hogy

$$T(\boldsymbol{v}) = \boldsymbol{v} - \mu(\boldsymbol{v})\boldsymbol{a} \tag{4.6}$$

áll fent minden $\boldsymbol{v} \in V$ esetén. Ebben az esetben a $T = T(\boldsymbol{a}, \mu)$ jelölést használjuk.

Fordítva, ha $\mu \neq 0$ egy V-n értelmezett funkcionál és $0 \neq \boldsymbol{a} \in V$ egy vektor, melyre teljesül $\mu(\boldsymbol{a}) = 0$, úgy a $T(\boldsymbol{v}) = \boldsymbol{v} - \mu(\boldsymbol{v})\boldsymbol{a}$ leképezés egy, a $H = \{\boldsymbol{v} | \boldsymbol{v} \in V, \mu(\boldsymbol{v}) = 0\}$ hipersíkhoz tartozó nyírás.

Bizonyítás. Tekintsük a lemma alapján adott $T \neq \mathrm{id}$ nyírást, H hipersíkot és μ mineáris funcionált. Egy tetszőleges $w \notin H$ vektorra a V tér minden eleme előáll $\boldsymbol{v} = \boldsymbol{h} + \boldsymbol{w}t$ ($t \in \mathbb{T}$) alakban, ráadásul $\boldsymbol{w}$ helyett egy alkalmas konstansszorosát választva elérhetjük, hogy $\mu(\boldsymbol{w}) = 1$ teljesüljön. Definiáljuk az $\boldsymbol{a} = \boldsymbol{w} - T(\boldsymbol{w})$ elemet, $T \neq \mathrm{id}$ miatt $\boldsymbol{0} \neq \boldsymbol{a} \in H$. Ekkor tetszőleges $\boldsymbol{h} \in H$ és $t \in \mathbb{T}$ elemek esetén a $\boldsymbol{v} = \boldsymbol{h} + \boldsymbol{w}t$ vektorra

$$\mu(\boldsymbol{v}) = \mu(\boldsymbol{h} + \boldsymbol{w}t) = \mu(\boldsymbol{h}) + \mu(\boldsymbol{w})t = t$$

és

$$T(\boldsymbol{v}) = T(\boldsymbol{h} + \boldsymbol{w}t) = \boldsymbol{h} + T(\boldsymbol{w})t = \boldsymbol{h} + (\boldsymbol{w} - \boldsymbol{a})t = \boldsymbol{v} - \boldsymbol{a}t = \boldsymbol{v} - \mu(\boldsymbol{v})\boldsymbol{a}$$

áll fenn. Ezzel beláttuk a lemma első állítását; a második állítás az első megfordítása és könnyen leellenőrizhető közvetlenül. □

A nyírásokra kapott alak segítségével az alábbi lemma egyeszerű utánaszámolással megkapható.

4.11. Lemma. *Legyenek $\boldsymbol{a}_1, \boldsymbol{a}_2$ és $\boldsymbol{a}$ a H hipersík nem-nulla vektorai, ahol*

$$H = \{\boldsymbol{v} | \mu(\boldsymbol{v}) = 0\}.$$

Ekkor igaz, hogy

$$T(\boldsymbol{a}_1, \mu)T(\boldsymbol{a}_2, \mu) = T(\boldsymbol{a}_1 + \boldsymbol{a}_2, \mu)$$

és

$$T(\boldsymbol{a}, \mu)T(-\boldsymbol{a}, \mu) = I.$$

Tehát egy rögzített H hipersíkhoz tartozó nyírások egy az identikus leképezéssel egy $\mathcal{T}(H)$-val jelölt Abel-csoportot alkotnak, amley a $(H, +)$ additív csoporttal izomorf. A

$$T(\boldsymbol{a}, \mu_1)T(\boldsymbol{a}, \mu_2) = T(\boldsymbol{a}, \mu_1 + \mu_2)$$

egyenlőség miatt

$$\mathcal{T}_{\boldsymbol{a}} = \{E, T(\boldsymbol{a}, \mu)|), 0 \neq \mu \text{ lineáris funkcionál, } \mu(\boldsymbol{a}) = 0\}$$

szintén a $GL(n, \mathbb{T})$ csoport egy Abel-féle részcsoportja.

4.12. Tétel. *Minden T nyírásra teljesül* $\det(T) = 1$, *azaz $T \in SL(n, \mathbb{T})$. A nyírások generálják az $SL(n, \mathbb{T})$ csoportot, azaz $SL(n, \mathbb{T})$ az általános lineáris csoport legszűkebb olyan részcsoportja, amely az összes nyírást tartalmazza.*

Bizonyítás. Legyen $T = T(\boldsymbol{a}, \mu)$ egy H hipersíkhoz tartozó nyírás. Válasszunk egy $\{\boldsymbol{a} = \boldsymbol{v}_1, \dots, \boldsymbol{v}_{n-1}\}$ bázist H-ban, ezt kiegészíthetjük a V tér egy $\{\boldsymbol{a} = \boldsymbol{v}_1, \dots, \boldsymbol{v}_n\}$ bázisává. Legyen $\boldsymbol{a} = \boldsymbol{v}_1 a_1 + \dots \boldsymbol{v}_{n-1} + \boldsymbol{v}_{n-1} a_{n-1}$. Definíció szerint $T(\boldsymbol{v}_i) = \boldsymbol{v}_i$ minden $i = 1, \dots, n-1$ esetén, és a 4.6 alak miatt

$$T(\boldsymbol{v}_n) = -\boldsymbol{v}_1 t + \boldsymbol{v}_n,$$

ahol $t = \mu(\boldsymbol{v}_n)$. Ebben a bázisban tehát a T mátrixalakja

$$\begin{pmatrix} 1 & \cdots & -t \\ & \ddots & \\ 0 & \cdots & 1 \end{pmatrix}.$$

Ebből rögtön adódik $\det(T) = 1$, azaz $T \in SL(n, \mathbb{T})$. Persze itt nem muszáj, hogy az első és az utolsó oszlop illetve sor kitünktetett helyzetben legyen, a báziselemek sorrendjének felcserélésével T mátrixalakja

$$B_{ij}(-t) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & \cdots & -t & & \\ & & & \ddots & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}$$

is lehet, ahol i és j a $-t$ elem pozíciói. Ismeretes, hogy a $B_{ij}(t)$ alakú mátrixszal történő jobbról szorzás a megszorzott mátrix i-dik oszlopának t-szeresét hozzáadja a j-dik oszlophoz; balról szorzás esetén a megszorzott mátrix j-dik sorának t-szeresét hozzáadja az i-dik sorhoz. Egy adott mátrixon ezeket az átalításokat elemi átalakításoknak nevezzük.

Legyen adott az $A \in GL(n, \mathbb{T})$ tetszőleges mátrix. Ismert, hogy a Gauss-elimináció segítségével bármely mátrix diagoális alakra hozható. Megmutatjuk, hogy $\det(A) = 1$ esetén a diagonális mátrix elemi átalakításokkal egységmátrixszá alakítható. Nyiván elegendő ezt 2×2-es mátrixra meggondolni, ez pedig az alábbi lépéssorból kïvetkezik:

$$\begin{aligned} \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} &\rightsquigarrow \begin{pmatrix} a & -a \\ 0 & c \end{pmatrix} \rightsquigarrow \begin{pmatrix} a & -a \\ c & 0 \end{pmatrix} \rightsquigarrow \begin{pmatrix} 0 & -a \\ c & 0 \end{pmatrix} \\ &\rightsquigarrow \begin{pmatrix} 0 & -a \\ c & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} ac & 0 \\ c & 1 \end{pmatrix} \rightsquigarrow \begin{pmatrix} ac & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Ez az jelenti, hogy $\det(A) = 1$ esetén léteznek (az adott koordinátarendszerben $B_{ij}(t)$ alakú) $T_1, \dots, T_k, \tilde{T}_1, \dots, \tilde{T}_\ell$ nyírások úgy, hogy

$$T_1 \cdots T_k A \tilde{T}_1 \cdots \tilde{T}_\ell = \mathrm{id},$$

azaz

$$A = T_k^{-1} \cdots T_1^{-1} \tilde{T}_\ell^{-1} \cdots \tilde{T}_1^{-1}.$$

Mivel nyírás inverze is nyírás, ezzel beláttuk, hogy A előáll nyírások szorzataként. □

4.13. Lemma. *Nyírás konjugáltja szintén nyírás, és minden nyírás konjugált egymáshoz a $GL(n,\mathbb{T})$ csoportban: bármely két T_1, T_2 nyírás esetén létezik $S \in GL(n,\mathbb{T})$ elem úgy, hogy $ST_1S^{-1} = T_2$ teljesül. Ha $n \geq 3$, akkor $S \in SL(n,\mathbb{T})$ elem is választható ezzel a tulajdonsággal. Az $SL(2,\mathbb{T})$ csoportban a $\mathcal{T}(H)$ részcsoportok konjugáltak.*

Bizonyítás. Rögzítsük a V tér egy olyan $\{\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n\}$ bázisát, amelyben a T_1 transzformáció mátrixa

$$A_1 = \begin{pmatrix} 1 & \cdots & 1 \\ & \ddots & \\ 0 & \cdots & 1 \end{pmatrix}$$

alakú. Legyen ebben a bázisban T_2 mátrixa A_2. Hasonlóan választhatunk V-ben egy olyan $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_n\}$ bázist, amelyben a T_2 nyírás B_2 mátrixa lesz a fenti alakú, azaz a (4.4) összefüggés szerint teljesül $A_1 = B_2 = SA_2S^{-1}$, ahol $S \in GL(n,\mathbb{T})$ a $\boldsymbol{v}_i \mapsto \boldsymbol{u}_i$ bázisátmenet mátrixa.

Legyen most $n \geq 3$. Ekkor a fentiek változatlanul érvényben maradnak, ha a második bázisban az $\boldsymbol{v}_2$ elem helyett a $\boldsymbol{v}_2' = \boldsymbol{v}_2 \cdot \det(S)^{-1}$ elemet tekintjük; ekkor a bázisátmenet S' mátrixa a második oszlopot kivéve megegyezik S-sel, az S' második oszlopában az S második oszlopának $\det(S)^{-1}$-szerese áll. Vagyis $\det(S') = 1$ és $S' \in SL(n,\mathbb{T})$.

Végül tegyük fel, hogy $n = 2$, és legyen H_1 és H_2 két hipersík (azaz két origóra illeszkedő egyenes). A 4.7 következmény szerint létezik $A \in SL(2,\mathbb{T})$ elem, amelyre $A(H_1) = H_2$. Legyen most $T \in \mathcal{T}(H_1)$, ennek az ATA^{-1} konjugáltja szintén nyírás, a hozzá tartozó hipersík pedig nem más, mint a fixpontjainak a halmaza. Mivel T fixpontjainak halmaza H_1, így ATA^{-1} fixponthalmaza $A(H_1) = H_2$, azaz $ATA^{-1} \in \mathcal{T}(H_2)$. Mivel a gondolatmenet megfordítható, azt kapjuk, hogy $\mathcal{T}(H_1)^A = \mathcal{T}(H_2)$. □

Ezen lemmák segítségével tudjuk belátni a következő fontos tételt.

4.14. Tétel. *Az $n \geq 3$ valamint az $n = 2$, $|\mathbb{T}| > 3$ esetben teljesül*

$$SL(n,\mathbb{T})' = GL(n,\mathbb{T})' = SL(n,\mathbb{T}).$$

Bizonyítás. Nyilván $SL(n,\mathbb{T})' \leq GL(n,\mathbb{T})'$. Tekintsük a $GL(n,\mathbb{T})'$ egy tetszőleges $[A,B]$ generátorelemét. Erre teljesül

$$\det([A,B]) = \det(A^{-1}B^{-1}AB) = \det(A)^{-1}\det(B)^{-1}\det(A)\det(B) = 1,$$

azaz $[A,B] \in SL(n,\mathbb{T})$, s így az általuk generált teljes csoportra $GL(n,\mathbb{T})' \leq SL(n,\mathbb{T})$. Eszerint csak az $SL(n,\mathbb{T}) \leq SL(n,\mathbb{T})'$ tartalmazást kell bizonyítani. Ehhez pedig a 4.12 tétel miatt elegendő megmutatni, hogy az összes nyírás benne van $SL(n,\mathbb{T})'$-ben.

Ismét az $n \geq 3$ esetet vizsgáljuk elsőként. Legyenek T és T' nyírások, a 4.13 lemma miatt létezik $A \in SL(n,\mathbb{T})$ elem, hogy $ATA^{-1} = T'$. Ekkor

$$T'SL(n,\mathbb{T})' = T\,[T,A^{-1}]\,SL(n,\mathbb{T})' = T\,SL(n,\mathbb{T})',$$

vagyis az összes nyírás az $SL(n,\mathbb{T})'$ azonos mellékosztályában van.

Legyen most $H = \{\boldsymbol{v} | \mu(\boldsymbol{v}) = 0\}$ egy V-beli hipersík. Mivel $\dim H = n-1 \geq 2$, H tartalmaz $\boldsymbol{a}_1, \boldsymbol{a}_2 \neq 0$ vektorokat úgy, hogy $\boldsymbol{a}_1 \neq -\boldsymbol{a}_2$. Ebben az esetben

$$T(\boldsymbol{a}_1,\mu)T(\boldsymbol{a}_2,\mu) = T(\boldsymbol{a}_1+\boldsymbol{a}_2,\mu),$$

s mivel az összes nyírás az $SL(n,\mathbb{T})$ ugyanabban a mellékosztályában helyezkedik el, következik, hogy

$$T(\boldsymbol{a}_1,\mu)^2\,SL(n,\mathbb{T})' = T(\boldsymbol{a}_1,\mu)\,SL(n,\mathbb{T})'.$$

Ebből pedig $T(\boldsymbol{a}_1,\mu) \in SL(n,\mathbb{T})'$ adódik, és így az összes nyírás $SL(n,\mathbb{T})$-ben van.

Az $n = 2$ esetben valamivel körültekintőbben kell eljárnunk. Legyen T a $H = \langle \boldsymbol{v}_1 \rangle$ hipersíkhoz (=egyeneshez) tartozó nyírás. Egy megfelelően választott $\boldsymbol{v}_1, \boldsymbol{v}_2$ bázis esetén

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Mivel $|\mathbb{T}| > 3$, létezik egy $d \in \mathbb{T} \setminus \{0,1,-1\}$ elem. Legyen

$$A = \begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \in SL(2,\mathbb{T}).$$

Ekkor

$$\begin{aligned}
[T,A] &= T^{-1}A^{-1}TA \\
&= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d & 0 \\ 0 & d^{-1} \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d^{-1} & 0 \\ 0 & d \end{pmatrix} \\
&= \begin{pmatrix} d & -d^{-1} \\ 0 & d^{-1} \end{pmatrix}\begin{pmatrix} d^{-1} & d \\ 0 & d \end{pmatrix} \\
&= \begin{pmatrix} 1 & d^2-1 \\ 0 & 1 \end{pmatrix},
\end{aligned}$$

ami egy T-től különböző nyírás $SL(n,\mathbb{T})'$-ben. Ekkor $SL(2,\mathbb{T})' \triangleleft GL(2,\mathbb{T})$ és a nyírások $GL(2,\mathbb{T})$-beli egymáshoz való konjugáltsága miatt az összes nyírás $SL(2,\mathbb{T})'$-ben van. □

Megjegyzés. Később majd látjuk, hogy az $SL(2,\mathbb{F}_2)$ és $SL(2,\mathbb{F}_3)$ csoportok esetén a tétel állítása nem igaz.

5. fejezet

Projektív lineáris csoportok

A 4. fejezetben már szerepeltek olyan lemmák, amelyek lineáris csoportoknak az origóra illeszkedő egyeneseken vett hatásával foglalkoznak. Az ilyen vizsgálatok természetes módon vezetnek lineáris csoportok *projektív téren* vett hatásának a vizsgálataihoz. Ezek a vizsgálatok a geometriában és a csoportelméletben központi jelentőségűek.

5.1. Projektív terek

5.1. Definíció. *Legyen $V = V(n+1, \mathbb{T})$ egy $\mathbb{T}$ feletti $n+1$-dimenziós vektortér, és jelölje V^* az origótól különböző vektorok halmazát. Vezessük be az alábbi ekvivalenciarelációt V^*-on:*

$$\boldsymbol{v} \sim \boldsymbol{w} \;\Leftrightarrow\; \boldsymbol{v} = \boldsymbol{w}c, c \in \mathbb{T}^*.$$

Ezen reláció ekvivalenciaosztályainak $V^*/\sim$ halmazát a $\mathbb{T}$ feletti n-dimenziós projektív térnek *nevezzük és $PG(n, \mathbb{T})$-vel jelöljük . Az ekvivalenciaosztályokat* projektív pontoknak, *a $k+1$-dimenziós lineáris altereket k-dimenziós* projektív altereknek *hívjuk.*

Szemléletesen tehát azt mondhatjuk, hogy a projektív tér pontjai az origóra illeszkedő egyenesek, a projektív egyenesek az origóra illeszkedő síkok, stb.

5.2. Állítás. *Legyen π_1, π_2 a $PG(n, \mathbb{T})$ tér d_1 illetve d_2 dimenziós projektív alterei. Ekkor $d_1 + d_2 \geq n$ esetén $\pi_1 \cap \pi_2 \neq \emptyset$.*

Bizonyítás. Tekintsük a projektív terünket meghatározó V vektorteret, és ennek azon U_1, U_2 altereit, amelyek π_1-t illetve π_2-t határozzák meg. Ekkor $\dim V = n+1$, $\dim U_1 = d_1 + 1$ és $\dim U_2 = d_2 + 1$; a $d_1 + d_2 \geq n$ összefüggés miatt pedig $\dim U_1 + \dim U_2 > \dim V$. Válasszunk bázisokat U_1-bek

és U_2-ben: $\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_{d_1}\}$ illetve $\{\boldsymbol{f}_1, \ldots, \boldsymbol{f}_{d_2}\}$. A V dimenziója miatt kell léteznie egy nem-triviális lineáris összefüggésnek a két bázis között:

$$a_1\boldsymbol{e}_1 + \ldots a_{d_1}\boldsymbol{e}_{d_1} + b_1\boldsymbol{f}_1 + \ldots + b_{d_2}\boldsymbol{f}_{d_2} = \boldsymbol{0},$$

vagy másképpen

$$\boldsymbol{v} = a_1\boldsymbol{e}_1 + \ldots a_{d_1}\boldsymbol{e}_{d_1} = -b_1\boldsymbol{f}_1 - \ldots - b_{d_2}\boldsymbol{f}_{d_2} \in U_1 \cap U_2.$$

A bázistulajdonság miatt $\boldsymbol{v} = \boldsymbol{0}$ esetén $a_1 = \ldots = b_1 = \ldots = 0$ állna fenn, ellentmondva a lineáris kombináció nem-trivialitásának. $U_1 \cap U_2$ tartalmaz tehát egy nem-nulla vektort, ami meghatározza a $\pi_1 \cap \pi_2$ projektív altár egy pontját. □

Megjegyzés. Az állításból következik például, hogy egy projektív térben egy egyenesnek és egy hipersíknak[1] mindig van közös pontja. Speciálisan, a projektív síkon két egyenesnek mindig van metszéspontja.

Legyen adott a $V = V(n+1, \mathbb{T})$ vektortér egy A lineáris leképezése. Mivel ez a leképezés megtartja az egydimenziós altereket, tekinthető a projektív tér egy transzformációjának is. Mivel pedig A a teljes altérstruktúrát megtartja, ezért a projektív tér altereit is megtartja. Ez úgy is kifejezhetjük, hogy A egy *projektív transzformációt* vagy *kollineációt indukál*.

Vizsgáljuk meg, hogy mi szükséges ahhoz, hogy két A és B lineáris transzformáció ugyanazt a kollineációt indukálja. Ez akkor és csak akkor következik be, ha $A^{-1}B$ minden projektív pontot önmagára képez, azaz minden vektorhoz a konstansszorosát rendeli. Az 1.4 alfejezet elején már alkalmazott trükk felhasználásával belátható, hogy a konstans szorzó nem függhet a vektortól, azaz $A^{-1}B = Ic$ alakú kell legyen.

Mivel az Ic alakú mátrixok csoportja fontos szerepet játszik a következőkben, bevezetjük a

$$Z_n = Z(GL(n, \mathbb{T})) = \{Ic; c \in \mathbb{T}^*\}$$

jelölést. A fentiekhez hasonlóan pedig az $(n+1) \times (n+1)$ mátrixok halmazán is értelmezzük az alábbi kongruenciarelációt:

$$A \approx B \;\Leftrightarrow\; A = Bc, c \in \mathbb{T}^*.$$

5.3. Definíció. *Legyen H a $GL(n+1, \mathbb{T})$ csoport egy részcsoportja. A H által indukált $P(H)$ projektív lineáris csoport definíció szerint a*

$$P(H) = H/Z_{n+1} = H/\approx$$

faktorcsoport. $P(H)$ természetes módon hat az n-dimenziós projektív téren.

[1] Az n dimenziós projektív tér $(n-1)$-dimenziós altereit nevezzük *hipersíkoknak.*

5.1. táblázat. A projektív mag mérete

$\mathbb{T}$	$\mathbb{R}$	$\mathbb{C}$	$\mathbb{F}_q$
$\lvert Z(GL(n+1,\mathbb{T}))\cap SL(n+1,\mathbb{T})\rvert$	$(2,n+1)$	$n+1$	$(q-1,n+1)$

Megjegyzés. A 4.8 tételből következik, hogy a fenti H csoport esetén a $\approx$ ekvivalencia osztályai pontosan $Z_n \cap H$ normálosztó mellékosztályai.

Speciálisan, definiáljuk a

$$PGL(n+1,\mathbb{T}) = P(GL(n+1,\mathbb{T})) = GL(n+1,\mathbb{T})/Z_{n+1}$$

projektív általános lineáris csoportot és a

$$PSL(n+1,\mathbb{T}) = P(SL(n+1,\mathbb{T})) = SL(n+1,\mathbb{T})/(Z_{n+1}\cap SL(n+1,\mathbb{T}))$$

projektív speciális lineáris csoportot.

Már láttuk korábban, hogy

$$Z_{n+1} = Z(GL(n+1,\mathbb{T})) \cong \mathbb{T}^*.$$

Most vizsgáljuk meg a $Z(GL(n+1,\mathbb{T}))\cap SL(n+1,\mathbb{T})$ csoportot. Ez

$$Z(GL(n+1,\mathbb{T}))\cap SL(n+1,\mathbb{T}) = \{Ic : \det(Ic) = c^{n+1} = 1\},$$

azaz izomorf a $\mathbb{T}$-beli $n+1$-dik egységgyökök csoportjával. Meghatározzuk ezt a csoportot a $\mathbb{T}$ néhány különböző változata esetén.

Ha $\mathbb{T} = \mathbb{R}$, akkor az $n+1$-dik egységgyökök $\{1\}$ vagy $\{1,-1\}$ attól függően, hogy $n+1$ páratlan vagy páros.

Ha $\mathbb{T} = \mathbb{C}$, akkor az $n+1$-dik egységgyökök $\{\epsilon^k : 0 \le k < n+1\}$, ahol ϵ egy primitív $n+1$-dik egységgyök.

Legyen végül $\mathbb{T} = \mathbb{F}_q$ véges test. Tudjuk, hogy a véges testek multiplikatív csoportja ciklikus (3.6 tétel). Létezik tehát egy $g \in \mathbb{F}_q^*$ elem úgy, hogy $\mathbb{F}_q^* = \{g, g^2, \dots, g^{q-1} = 1\}$. Az $x^{n+1} = 1$ polinom megoldása ezért a $g^{(n+1)k} = 1$ egyenlőség, azaz a $k(n+1) \equiv 0 \pmod{q-1}$ kongruencia k szerinti megoldásával ekvivalens. Ez utóbbiak viszont $i(q-1)/d$ alakúak, ahol $d = (q-1, n+1)$ és $0 \le i < d$. Az $(n+1)$-dik egységgyökök $\mathbb{F}_q$-ban tehát a

$$\{g^{\frac{i(q-1)}{d}} : 0 \le i < d\}$$

elemek. A szóbanforgó csoport méretét az 5.1 táblázatból olvashatjuk le.

5.4. Tétel. *Legyen $\mathbb{T} = \mathbb{F}_q$ véges test. Ekkor*

$$\begin{aligned}
|GL(n+1,q)| &= q^{\frac{n(n+1)}{2}} \prod_{i=1}^{n+1}(q^i-1),\\
|SL(n+1,q)| &= q^{\frac{n(n+1)}{2}} \prod_{i=2}^{n+1}(q^i-1),\\
|PGL(n+1,q)| &= q^{\frac{n(n+1)}{2}} \prod_{i=2}^{n+1}(q^i-1),\\
|PSL(n+1,q)| &= \frac{1}{(q-1,n+1)} q^{\frac{n(n+1)}{2}} \prod_{i=2}^{n+1}(q^i-1).
\end{aligned}$$

Bizonyítás. Vezessük be az $N = |GL(n+1,q)|$ jelölést. $|Z_{n+1}| = |GL(n,q) : SL(n,q)| = q-1$ egyenlőségek miatt a csoportok definícióiból következik, hogy $|SL(n+1,q)| = |PGL(n+1,q)| = N/(q+1)$ és $|PSL(n+1,q)| = |PGL(n+1,q)|/(q-1,n+1)$ (ld. az 5.1 táblázatot).

Most meghatározzuk N értékét. Ez nyilván megegyezik a $V(n+1,q)$ vektortér bázisainak a számával. Azt állítjuk, hogy a $V(n+1,q)$ bázisainak száma

$$N = (q^{n+1}-1)(q^{n+1}-q)\cdots(q^{n+1}-q^n).$$

Valóban, az első báziselem kiválasztáskor $q^{n+1}-1$ lehetőségünk van, hiszen az bármely origótól különböző elem lehet. A második báziselem kiválasztásakor az a megkötés, hogy az ne legyen az első skalárszorosa, így q eset záródik ki. Tegyük fel, hogy i báziselemet már kiválasztottunk. Az $i+1$-dik választásánál a kizárt esetek azok a vektorok, amelyek az első i elem lineáris kombinációjaként előállnak, az ilyen lineáris kombinációk száma pedig q^i, tehát a választási lehetőségek száma $q^{n+1}-q^i$. Tehát N valóban egyenlő a fent adott értékkel, ami pedig átalakítás után az állításban szereplő szám. □

5.2. A $PSL(n,\mathbb{T})$ csoport egyszerű

A csoportelmélet különösen fontos szerepet töltenek be az egyszerű csoportok, vagyis azok, amelyeknek nincs valódi normálosztójuk. A legkönnyebben megkonstruálható egyszerű csoport az A_n alternáló csoport, amely rögtön egyszerű csoportok egy végtelen osztályát jelenti. A fejezetünk hátralévő részében egyszerű csoportoknak egy másik nagyon fontos osztályát fogjuk megadni. Először egy lemmát bizonyítunk.

5.5. Lemma (Huppert). *Legyen G egy Ω-n 2-tranzitívan ható transzformációcsoport, és tegyük fel, hogy az alábbi két feltétel teljesül.*

(1) $G' = G$.

(2) *A* G_α $(\alpha \in \Omega)$ *részcsoport tartalmaz egy Abel-féle* K *normálosztót, amelyre*

$$\langle gKg^{-1} : g \in G \rangle = G.$$

Ekkor G *egyszerű csoport.*

Bizonyítás. Tegyük fel, hogy $N \neq \{1\}$ a G csoport egy normálosztója. Öt részállítás belátásával megmutatjuk, hogy $N = G$.
1. állítás. G_α maximális részcsoport G-ben.
Biz. Tegyük fel, hogy G_α nem maximális, azaz létezik egy $G_\alpha < H < G$ részcsoport, és rögzítsünk egy $h \in H \setminus G_\alpha$ és egy $g \in G \setminus H$ elemet. Ekkor $h(\alpha) = \beta \neq \alpha$ és $g(\alpha) = \gamma \neq \alpha$. A G 2-tanzitivitása miatt választhatunk egy $u \in G$ elemet, amelyre $u(\alpha) = \alpha$ és $u(\gamma) = \beta$. Vizsgáljuk meg a $v = h^{-1}ug \in G$ elemet.

$$v(\alpha) = h^{-1}(u(g(\alpha))) = h^{-1}(u(\gamma)) = h^{-1}(\beta) = \alpha,$$

azaz $v \in G_\alpha$. De ekkor $g = u^{-1}hv \in G_\alpha H G_\alpha \subseteq HHH = H$, ellentmondás.
2. állítás. $NG_\alpha = G$.
Biz. Nyilván $G_\alpha \leq NG_\alpha \leq G$, és az 1. állítás miatt valahol egyenlőségnek kell teljesülnie. De $G_\alpha = NG_\alpha$ csak úgy lenne lehetséges, ha $N \leq G_\alpha$ lenne. Ekkor viszont minden $g \in G$ esetén $N = gNg^{-1} \leq gG_\alpha g^{-1} = G_{\alpha^g}$ teljesülne (vö. 2.3 Tétel (ii) pont), azaz N minden eleme stabilizálná az összes $\beta = g(\alpha)$ elemet. Ez G tranzitivitása miatt azt jelenti, hogy N minden eleme stabilizálja Ω minden elemét, s mivel G transzformációcsoport, ez csak úgy lehetséges, ha $N = \{1\}$, ellentmondás. Tehát az $NG_\alpha = G$ oldalon kell az egyenlőségnek teljesülnie.
3. állítás. $NK \lhd G$.
Biz. $G = NG_\alpha$ miatt elegendő belátni, hogy $nNKn^{-1} = NK$ és $gNKg^{-1} = NK$ minden $n \in N$ és minden $g \in G_\alpha$ elem esetén, az utóbbi pedig a $K \lhd G_\alpha$ alapján nyilvánvaló. Az előbbi pedig következik a

$$n(Nk)n^{-1} \leq NkNk^{-1}k \leq Nk$$

egyenlőségből következik, amely minden $k \in K$ esetén fennáll.
4. állítás. $NK = G$.
Biz.

$$G = \langle gKg^{-1} : g \in G \rangle \leq \langle (NK)^g : g \in G \rangle = NK.$$

5. állítás. $N = G$.
Biz. Az izomorfiatételek szerint a NK/N és $K/(N \cap K)$ faktorcsoportok izomorfak és K Abel-féle, azaz NK/N is Abel-féle, s így N tartalmazza a G' kommutátor részcsoportot (vö. 1.5). Ez viszont azt jelenti, hogy $N \geq (NK)' = G' = G \geq N$, s így az $N = G$ egyenlőségnek teljesülnie kell. □

5.6. Tétel. *A $PSL(n,\mathbb{T})$ csoport egyszerű, kivéve az $n=2$, $\mathbb{T}=\mathbb{F}_2$ és az $n=2$, $\mathbb{T}=\mathbb{F}_3$ eseteket.*

Bizonyítás. (Iwasava.) Legyen $G=PSL(n,\mathbb{T})$, Ω az $n-1$-dimenziós projektív tér ponthalmaza, és tegyük fel, hogy $n=2$ esetén $\mathbb{T}\neq\mathbb{F}_2$ és $\mathbb{T}\neq\mathbb{F}_3$. A 4.7 következmény szerint G 2-tranzitívan hat Ω-n. A 4.14 tétel szerint az $n=2$, $\mathbb{T}=\mathbb{F}_2$ vagy $\mathbb{T}=\mathbb{F}_3$ eseteket kivéve $SL(n,\mathbb{T})'=SL(n,\mathbb{T})$, amiből könnyű számolással adódik, hogy $PSL(n,\mathbb{T})'=PSL(n,\mathbb{T})$.

A Huppert-lemma alkalmazásához tehát már csak egy megfelelő K részcsoportot kell találni. Legyen $\boldsymbol{a}$ egy tetszőleges, origótól különböző n-dimenziós vektor, és jelölje P az $\boldsymbol{a}$ ekvivalenciaosztálya által meghatározott projektív pontot. Tekintsük a

$$\mathcal{T}_{\boldsymbol{a}}=\{T(\boldsymbol{a},\mu):\mu \text{ lineáris funkcionál, } \mu(\boldsymbol{a})=0\} \tag{5.1}$$

csoportot, ez a 4.11 lemma szerint Abel-csoport. Legyen $K=P(\mathcal{T}_{\boldsymbol{a}})$ a $\mathcal{T}_{\boldsymbol{a}}$ által indukált projektív transzformációcsoport, nyilván $K\leq G_P$. Legyen $A\in G_P$, ekkor A felírható egy $n\times n$ mátrix segítségével, és $A(P)=P$ miatt $A\boldsymbol{a}=\boldsymbol{a}c$ kell fennálljék. Tudjuk, hogy $A\mathcal{T}_{\boldsymbol{a}}A^{-1}$ elemei szintén nyírások, és a $T=T(\boldsymbol{a},\mu)\in\mathcal{T}_{\boldsymbol{a}}$ elemre az

$$(ATA^{-1})(\boldsymbol{v})=\boldsymbol{v}-\mu(A^{-1}\boldsymbol{v})\,A\boldsymbol{a}=\boldsymbol{v}-c\mu(A^{-1}\boldsymbol{v})\,\boldsymbol{a}$$

összefüggésből adódik, hogy az ATA^{-1} konjugált szintén $T(\boldsymbol{a},\mu')$ alakú, azaz $A\mathcal{T}_{\boldsymbol{a}}A^{-1}=\mathcal{T}_{\boldsymbol{a}}$ és $K\lhd G_P$.

Le kell még ellenőrizni, hogy

$$G=\langle gKg^{-1}:g\in G\rangle,$$

amihez elegendő belátni, hogy

$$SL(n,\mathbb{T})=\langle A\mathcal{T}_{\boldsymbol{a}}A^{-1}:A\in SL(n,\mathbb{T})\rangle.$$

Az (5.1) formula szerint azonban teljesül $B\mathcal{T}_{\boldsymbol{a}}B^{-1}=\mathcal{T}_{B\boldsymbol{a}}$ és minden T nyírás benne van egy $\mathcal{T}_{B\boldsymbol{a}}$ csoportban valamilyen $B\in SL(n+1,\mathbb{T})$ elem esetén, azaz az utolsó egyenlőség jobb oldala az összes nyírást tartalmazza. Mivel pedig a nyírások generálják $SL(n,\mathbb{T})$, így $SL(n+1,\mathbb{T})$-t generálják a $\mathcal{T}_{\boldsymbol{a}}$ csoport konjugáltjai, és $PSL(n+1,\mathbb{T})$-t generálják a $P(\mathcal{T}_{\boldsymbol{a}})$ csoport konjugáltjai. Ekkor pedig a Huppert-lemmából következik, hogy $G=PSL(n+1,\mathbb{T})$ egyszerű. □

Megjegyzés. A $PSL(2,\mathbb{T})$ csoport a 4.7 következmény szerint 2-tranzitívan hat az egydimenziós projektív téren, azaz a projektív egyenesen. A projektív egyenes csak a végtelen távoli pontban különbözik az affin egyenestől, vagyis a pontjai megfeleltethetők a $\mathbb{T}\cup\{\infty\}$ halmaznak. Ezek szerint $PSL(2,\mathbb{F}_2)$ illetve $PSL(2,\mathbb{F}_3)$ 2-tranzitívan hat egy 3 illetve 4 pontból álló

halmazon, vagyis S_3 illetve S_4 részcsoportjainak tekinthetők. A 5.4 tétel szerint $|PSL(2,\mathbb{F}_2)| = 6$ és $|PSL(2,\mathbb{F}_3)| = 12$, ebből pedig következik, hogy $PSL(2,\mathbb{F}_2) \cong S_3$ és $PSL(2,\mathbb{F}_3) \cong A_4$. Ezek a csoportok viszont *feloldhatóak*, s így a kommutatátor részcsoport szigorúan kisebb magánál a csoportnál.

Ebből az is adódik, hogy a $PSL(2,\mathbb{F}_2)$ és $PSL(2,\mathbb{F}_3)$ csoportokra sem a 4.14 sem pedig az 5.6 tétel állítása nem teljesül.

5.3. A törtlineáris leképezések csoportja

Az előző alfejezetben szereplő csoportok közül most behatóbban megvizsgáljuk a $PGL(2,\mathbb{T})$ csoportot. Ez, mint a fentiekből is kiderül, az 1-dimenziós projektív téren azaz a $\mathbb{P}_1$ projektív egyenesen hat. Ennek az egyenesnek a pontjait homogén számpárok segítségével írhatjuk le, a homogenitást a $(x : y)$ jelöléssel fogjuk kihangsúlyozni. Ez persze az $y = 0$ esetben is értelmes, hiszen itt nem osztásról van szó, hanem annak a ténynek a kiemeléséről, hogy az $(x_1 : y_1)$, $(x_2 : y_2)$ pontpárok akkor és csak akkor írják le ugyanazt a pontot, ha $x_1y_2 = x_2y_1$.

A $PGL(2,\mathbb{T})$ csoport elemeit mátrixokkal írjuk le, az $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (mátrix által előállított) csoportelem hatása

$$(x : y) \mapsto (ax + by : cx + dy), \tag{5.2}$$

ami nyilván az

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$$

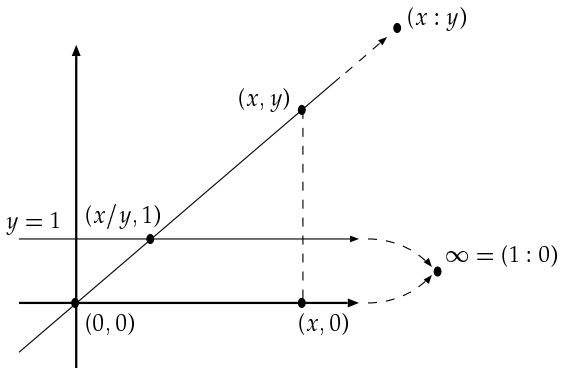
mátrixszorzásból adódik.

A projektív egyenes előállítására létezik egy másik, talán szemléletesebb mód is, hiszen az nem más, mint egy közönséges affin egyenes kibővítése egy végtelen távoli ponttal. Az affin egyenest, mint számegyenest tekintve így azt kapjuk, hogy $\mathbb{P}_1 = \mathbb{T} \cup \{\infty\}$.

Ezt a megközelítést könnyen összhangba hozhatjuk a korábbiakkal. Tekintsük ugyanis az xy-síkban az $e : y = 1$ affin egyenest. Egyrészt minden $A = (x : y)$ homogén számpár meghatároz egy g_A egyenest oly módon, hogy az origót összekötjük az (x, y) ponttal, és fordítva. Az is világos, hogy a szóbanforgó origóra illeszkedő egyenes akkor és csak akkor párhuzamos az x-tengellyel, ha $y = 0$.

Ha nem ez a helyzet, azaz $y \neq 0$, akkor a g_A egyenesek kölcsönösen egyértelműen megfeleltethetők az $y = 1$ egyenes $(x/y, 1)$ pontjainak. Ha $y = 0$, akkor g_A párhuzamos e-vel, azaz g_A az e végtelen távoli pontját határozza meg. Leegyszerűsítve az mondhatjuk, hogy az

$$(x : y) \longleftrightarrow x/y$$



5.1. ábra. A projektív egyenes és $\mathbb{T} \cup \infty$ ekvivalenciája.

egy bijekció a homogén számpárok halmaza és a ∞ szimbólummal kibővített $\mathbb{T} \cup \{\infty\}$ számtest között. A $\mathbb{P}_1$ projektív egyenes utóbbi típusú előállításában az

$$\frac{ax+by}{cx+dy} = \frac{a\dfrac{x}{y}+b}{c\dfrac{x}{y}+d}$$

azonosság és az (5.2) definíció értelmében

$$z \mapsto \frac{az+b}{cz+d} \tag{5.3}$$

alakban írható. A $\mathbb{T} \cup \{\infty\}$ halmaz ilyen típusú leképezéseit *törtlineáris leképezéseknek* nevezzük.

5.7. Tétel. *A törtlineáris leképezések csoportot alkotnak, amely szigorúan 3-tranzitívan hat a $\mathbb{T} \cup \{\infty\}$ halmazon.*

Bizonyítás. A definícióból még az is adódik közvetlenül, hogy a törtlineáris leképezések G csoportja izomorf a $PGL(2, \mathbb{T})$ csoporttal. Rögzítsünk egy tetszőleges $z_0 \in \mathbb{T} \cup \{\infty\}$ elemet. Ha $z_0 = \infty$, akkor legyen $f(z) = \dfrac{1}{z}$, különben legyen $f(z) = z + z_0$. Ekkor f egy törtlineáris leképezés, melyre $f(0) = z_0$, tehát G tranzitív.

Tekintsük most a ∞ elem G_∞ stabilizátor részcsoportját, ezekre a leképezésekre teljesül $f(\infty) = a/c = \infty$, ami pontosan azt jelenti, hogy $a \neq 0$ és $c = 0$. Mivel $d = 0$ nem lehetséges, így f az $f(z) = az + b$ alakra hozható. A G_∞ csoport tehát nem más, mint az 1.6 példában leírt AGL affin lineáris csoport, ami élesen 2-tranzitív (ld. a 2.5 példát). A 2.3 tétel szerint viszont ez pontosan azt jelenti, hogy G élesen 3-tranzitív. □

Itt érdemes még egy pillanatig elidőzni a G_∞ 1-dimenziós affin lineáris csoportnál. Azt látjuk ugyanis, ha ebben a csoportban még a 0-t is stabilizáljuk, akkor az $f(z) = ax + b$ leképezésre $f(0) = b = 0$ adódik, vagyis $f(z) = az$, ahol $a \in \mathbb{T}^*$ és $G_{\infty,0} \cong \mathbb{T}^*$.

5.4. Projektív kúpszeletek

Az affin síkon a kúpszeletek pontosan a másodfokú, kétváltozós polinomok zéróhelyei:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0.$$

Ebből azonnal adódik, hogy a projektív síkon *kúpszeletnek* a *másodfokú, 3-változós, homogén* polinomok zéróhelyeit nevezzük. A továbbiakban feltételezzük, hogy a $\mathbb{T}$ test, amellyel a projektív síkunkat koordinátázzuk, nem 2 karakterisztikájú, $\mathrm{char}(\mathbb{T}) \neq 2$. Ebben az esetben a kúpszelet egyenlete felírható

$$a_{00}x_0^2 + 2a_{01}x_0x_1 + 2a_{02}x_0x_2 + a_{11}x_1^2 + 2a_{12}x_1x_2 + a_2x_2^2 = 0,$$

alakban, ami

$$\boldsymbol{x} = \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}, \qquad A = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix}$$

jelöléssel az egyszerű

$$\boldsymbol{x}^t A \boldsymbol{x} = 0$$

formában adható meg. A további meggondolásokhoz rögzítsünk most egy tetszőleges $\mathcal{K} : \boldsymbol{x}^t A \boldsymbol{x} = 0$ projektív kúpszeletet.

Ha adott egy e projektív egyenes két pontja, $P(\boldsymbol{x}), Q(\boldsymbol{y})$, akkor e minden pontja $R(\lambda\boldsymbol{x} + \mu\boldsymbol{y})$ alakban írható. Az e egyenes metszete a $\mathcal{K}$ kúpszelettel azon R pontokból áll, amelyekre teljesül

$$0 = (\lambda\boldsymbol{x}^t + \mu\boldsymbol{y}^t)A(\lambda\boldsymbol{x} + \mu\boldsymbol{y}) = \lambda^2(\boldsymbol{x}^t A\boldsymbol{x}) + 2\lambda\mu(\boldsymbol{x}^t A\boldsymbol{y}) + \mu^2(\boldsymbol{y}^t A\boldsymbol{y}). \quad (5.4)$$

Egy két ismeretlenes, homogén, másodfokú egyenlet megoldásai $(\lambda : \mu)$ alakúak, a megoldások száma pedig 0, 1 vagy 2 lehet, feltéve, hogy (5.4) nem azonosan nulla. Ha (5.4) azonosan nulla, akkor minden $(\lambda : \mu)$ megoldás. Ez azt jelenti, hogy e-nek vagy 0, 1, 2 közös pontja van $\mathcal{K}$-val, vagy $e \subseteq \mathcal{K}$ teljesül.

Nagyon fontos az az eset, amikor (5.4) azonosan nulla vagy pedig amegoldásainak száma 1. Ekkor $|e \cap \mathcal{K}| = 1$ vagy $e \subseteq \mathcal{K}$ áll fenn; azt mondjuk, hogy ekkor *e érinti $\mathcal{K}$-t.* Ez a tény nyilván ekvivalens az

$$(\boldsymbol{x}^t A \boldsymbol{y})^2 - (\boldsymbol{x}^t A \boldsymbol{x})(\boldsymbol{y}^t A \boldsymbol{y}) = 0 \tag{5.5}$$

egyenlőség teljesülésével.

Tételezzük most fel, hogy $P \in \mathcal{K}$, ekkor $\boldsymbol{x}^t A \boldsymbol{x} = 0$ és a PQ egyenes pontosan abban az esetben érinti a $\mathcal{K}$ kúpszeletet, ha fennáll $\boldsymbol{x}^t A \boldsymbol{y} = 0$. Ha $\det(A) \neq 0$ akkor $\boldsymbol{x}^t A \neq \boldsymbol{0}$ és $\boldsymbol{x}^t A \boldsymbol{y} = 0$ egy egyértelműen meghatározott, $P(\boldsymbol{x})$-re illeszkedő egyenes egyenlete; ezt az egyenest a kúpszelet *P-beli érintőjének* tekintjük.

Ha $\det(A) = 0$, akkor A sorai lineárisan függők, tehát létezik egy $\boldsymbol{x} \neq \boldsymbol{0}$ vektor, amelyre $\boldsymbol{x}^t A = \boldsymbol{0}$. Ekkor nyilván $\boldsymbol{x}^t A \boldsymbol{x} = 0$ teljesül, azaz az $\boldsymbol{x}$ vektor által meghatározott $P(\boldsymbol{x})$ pont illeszkedik $\mathcal{K}$-ra. Továbbá azt látjuk, hogy P olyan pontja $\mathcal{K}$-nak, amelyre illeszkedő összes egyenes érinti $\mathcal{K}$-t, hiszen minden $Q(\boldsymbol{y})$ esetén $\boldsymbol{x}^t A \boldsymbol{y} = 0$ teljesül és (5.5) fennáll. Megmutattuk tehát a következő állítást:

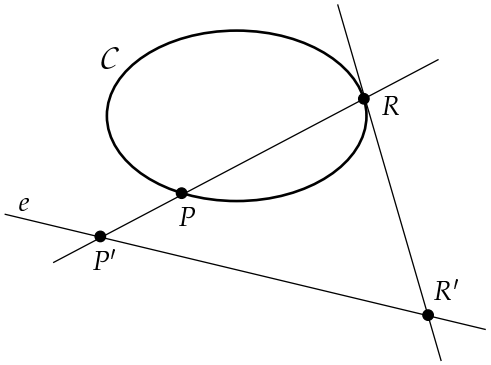
5.8. Állítás. *Legyen A egy 3×3-as, szimmetrikus mátrix egy $\neq 2$ karakterisztikájú test felett és tekintsük a $\mathcal{K} : \boldsymbol{x}^t A \boldsymbol{x} = 0$ kúpszeletet. Ha* $\det(A) \neq 0$, *akkor $\mathcal{K}$ minden pontjába egyértelműen húzható érintő. Ha* $\det(A) = 0$, *akkor $\mathcal{K}$-nak létezik legalább egy olyan pontja, amelyben az érintő nincs egyértelműen meghatározva.*

A kúpszelet azon pontját, amelyben nincs egyértelmű érintő, a kúpszelet *szinguláris pontjának* nevezzük, a szinguláris ponttal rendelkező kúpszeleteket pedig *elfajulónak* hívjuk.

Ezen fejezet hátralévő részében $\mathcal{K}$ mindig egy *nem-elfajuló projektív kúpszeletet* fog jelölni, és az egyszerűség kedvéért feltételezzük azt is, hogy $\mathcal{K}$-nak van legalább két $\mathbb{T}$ feletti pontja. Ekkor bármely egyenes 0, 1 vagy 2 pontban metszi $\mathcal{K}$-t.

Rögzítsük most a $\mathcal{K}$ egy tetszőleges Q pontját és legyen e egy projektív egyenes, amely nem illeszkedik Q-ra. Definiáljuk a $\mathcal{K} \to e$ leképezést az 5.2. ábrán látható módon: Ha $Q \neq P \in \mathcal{K}$, akkor $P' = e \cap PQ$, ha $P = Q$, akkor Q' az e és a $\mathcal{K}$ Q-beli érintőjének metszéspontja. Mivel a $\mathcal{K}$ P-beli éritőjét kivéve minden P-re illeszkedő egyenes pontosan egy további pontban metszi $\mathcal{K}$-t, ezért az imént definiált leképezés bijekció.

5.9. Állítás. *A nem-elfajuló $\mathcal{K}$ kúpszeletet a $P \in \mathcal{K}$ pontjából a P-re nem illeszkedő e egyenesre vett vetítés bijekció $\mathcal{K}$ és e ponthalmazai között.*



5.2. ábra. A projektív egyenes és kúpszelet ekvivalenciája

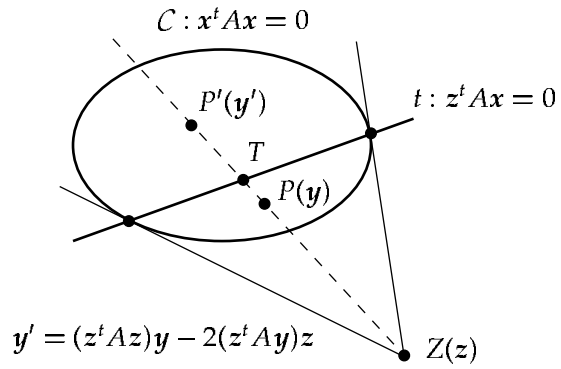
Ebben az alfejezetben két további fontos fogalmat említünk meg. Először is definiáljuk a $P(\boldsymbol{z})$ projektív pontnak a $\mathcal{K} : \boldsymbol{x}^t A\boldsymbol{x} = 0$ nem-elfajuló kúpszeletre vett *polárisát:* ez az $e : \boldsymbol{z}^t A\boldsymbol{x} = 0$ projektív egyenes. A fentiek szerint a $P \in \mathcal{K}$ esetben az e poláris a $\mathcal{K}$ P-beli érintője.

A másik tény annak megfontolása, hogy előfordulhat, hogy az $\boldsymbol{x}^t A\boldsymbol{x} = 0$ egyenletnek nincs nem-triviális megoldása $\mathbb{T}$ test felett. Például a $\mathbb{T} = \mathbb{R}$ esetben az $x_0^2 + x_1^2 + x_2^2 = 0$ egyenletnek csak a triviális $(0, 0, 0)$ megoldása létezik, az viszont nem határoz meg pontot a valós projektív síkon. Ennek ellenére a szóbanforgó egyenletről továbbra is mint kúpszelet egyenletéről fogunk beszélni, és a fentiek szerint az ilyen kúpszeletet nem-elfajulónak tekintjük. Ennek a meggondolásnak a pontos oka az, hogy áttérve a $\mathbb{T}$ test egy megfelelő bővítésére (a példánk esetében pl. a komplex számtestre) ez a probléma lényegében megoldódik, vagyis az ilyen kúpszeleteket úgy tekintjük, mint amelyeknek *csupa képzetes pontjuk van*.

5.5. A projektív kúpszelet automorfizmusai

Ebben az alfejezetben a projektív sík azon projektív lineáris transzformációit vizsgáljuk, amelyek invariánsan hagynak egy nem-elfajuló kúpszeletet.

5.10. Definíció. *Legyen $\mathcal{K}$ a $PG(2, \mathbb{T})$ projektív sík egy nem-elfajuló kúpszelete. Azt mondjuk, hogy az β projektív lineáris transzformáció a $\mathcal{K}$ egy* automorfiz-



5.3. ábra. Kúpszelet vetítése önmagára

musa, *ha* $\beta(\mathcal{K}) = \mathcal{K}$ *teljesül. A* $\mathcal{K}$ *automorfizmusainak halmazát* $PO(\mathcal{K})$*-val jelöljük.*

Elsőként megismerkedünk $\mathcal{K}$ egy speciális automorfizmusával. Tekintsük a $V = \mathbb{T}^3$ lineáris teret és annak egy tetszőleges z elemét, amelyre $z^t Az \neq 0$ teljesül. Definiáljuk az

$$S_z : \mathbb{T}^3 \to \mathbb{T}^3, \qquad y \mapsto (z^t Az)y - 2(z^t Ay)z$$

lineáris leképezést. Nyilván fennáll az $S_{\lambda z} = \lambda^2 S_z$ összefüggést.

Rögzítsük most a $PG(2, \mathbb{T})$ projektív sík egy tetszőleges $Z(z)$ pontját. A fentiek szerint az S_z által meghatározott projektív lineáris transzformáció független a Z pontot előállító z vektor megválasztásától; így joggal jelölhetjük az S_z által indukált projektív transzformációt σ_Z-vel. (Lásd az 5.3. ábrát.)

5.11. Lemma. *A* σ_Z *projektív transzformációra teljesül* $\sigma_Z \in PO(\mathcal{K})$, $\sigma_Z^2 = \mathrm{id}$, $\sigma_Z(Z) = Z$ *és* $\sigma_Z(P) = P$*, a* Z *pont* $\mathcal{K}$ *szerinti* t *polárisának minden* P *pontjára. Igaz továbbá, hogy a* Z *pontra illeszkedő összes egyenest* σ_Z *fixen hagyja.*

Bizonyítás. Tekintsük először a $\mathcal{K}$ egy $P(y)$ pontját, erre teljesül $y^t Ay = 0$. A P képe legyen $P'(y')$, ahol $y' = (z^t Az)y - 2(z^t Ay)z$. Ekkor

$$(y')^t Ay' = (z^t Az)^2(y^t Ay) - 4(z^t Az)(z^t Ay)^2 + 4(z^t Az)(z^t Ay)^2 = 0,$$

azaz $P' \in \mathcal{K}$, és így $\sigma_Z \in PO(\mathcal{K})$.

A $Z(\boldsymbol{z})$ pontra nyilván teljesül $\boldsymbol{z}' = -(\boldsymbol{z}^t A\boldsymbol{z})\boldsymbol{z}$, vagyis $\sigma_Z(Z) = Z$. Vegyünk most a t poláris egy tetszőleges $P(\boldsymbol{y})$ pontját. Ez kielégíti a $\boldsymbol{z}^t A\boldsymbol{y} = 0$ egyenletet, amiből adódik $\boldsymbol{y}' = (\boldsymbol{z}^t A\boldsymbol{z})y$, vagyis $P = P'$ minden $P \in t$ esetén.

Tekintsünk végül egy tetszőleges $P(\boldsymbol{y})$ pontot, és legyen $\sigma_Z(P) = P'(\boldsymbol{y}')$ és $\sigma_Z(P) = P''(\boldsymbol{y}'')$. Ekkor fennáll

$$\begin{aligned}
\boldsymbol{y}'' &= (\boldsymbol{z}^t A\boldsymbol{z})\boldsymbol{y}' - 2(\boldsymbol{z}^t A\boldsymbol{y}')\boldsymbol{z} \\
&= (\boldsymbol{z}^t A\boldsymbol{z})[(\boldsymbol{z}^t A\boldsymbol{z})\boldsymbol{y} - 2(\boldsymbol{z}^t A\boldsymbol{y})\boldsymbol{z}] - 2(\boldsymbol{z}^t A[(\boldsymbol{z}^t A\boldsymbol{z})\boldsymbol{y} - 2(\boldsymbol{z}^t A\boldsymbol{y})\boldsymbol{z}])\boldsymbol{z} \\
&= (\boldsymbol{z}^t A\boldsymbol{z})^2\boldsymbol{y} - 2(\boldsymbol{z}^t A\boldsymbol{z})(\boldsymbol{z}^t A\boldsymbol{y})\boldsymbol{z} - 2(\boldsymbol{z}^t A\boldsymbol{z})(\boldsymbol{z}^t A\boldsymbol{y})\boldsymbol{z} + 4(\boldsymbol{z}^t A\boldsymbol{z})(\boldsymbol{z}^t A\boldsymbol{y})\boldsymbol{z} \\
&= (\boldsymbol{z}^t A\boldsymbol{z})^2\boldsymbol{y},
\end{aligned}$$

amiből $P'' = P$ és $\sigma_Z^2 = \mathrm{id}$ adódik.

Végyül pedig, mivel a Z pontunk nem illeszkedik $\mathcal{K}$-ra, ezért $\boldsymbol{z}^t A\boldsymbol{z} \neq 0$, és így $Z \notin t$. Ez azt jelenti, hogy minden Z-re illeszkedő egyenes egy Z-től különböző pontban metszi t-t, azaz két fixponttal rendelkezik, vagyis maga is fix. □

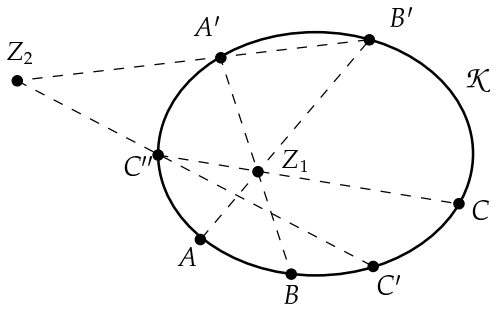
Az olyan transzformációkat, amelyek négyzete az identitás, *involúcióknak* nevezzük. Ha egy kollineáció egy egyenest pontonként fixen hagy, akkor az egyenest a kollineáció *tengelyének* hívjuk. Duálisan, azt mondjuk, hogy P egy kollineáció *centruma*, ha minden P-re illeszkedő egyenes fix. Ismeretes, hogy ha egy projektív kollinációnak van tengelye, akkor van centruma is, és fordítva (ld. Horvay-Reiman: Projektív geometria, IV.7.&). Az ilyen kollineációkat *centrális-axiális* kollineációknak nevezzük.

Az is világos, hogy egy identitástól különböző kollineációnak legfeljebb egy centruma lehet, hiszen különben minden pontra illeszkedne két fixegyenes, azaz minden pont fixpont lenne. Hasonlóan adódik, hogy legfeljebb egy tengely van. Ebből az is következik, hogy egy centrális-axiális kollineációnak nincs a centrumtól és a tengely pontjaitól különböző fixpontja, ez ugyanis ekkor egy második centrum lenne.

A fentiekből következik, hogy σ_Z valójában egy Z középpontú vetítésként hat $\mathcal{K}$-n, azaz felcseréli a $\mathcal{K}$ olyan P, P' pontpárjait, amelyekre teljesül $Z \in PP'$.

5.12. Tétel. *A $\mathcal{K}$ nem-elfajuló kúpszelet automorfizmusainak $PO(\mathcal{K})$ csoportja élesen 3-tranzitívan hat $\mathcal{K}$-n.*

Bizonyítás. Elsőként megmutatjuk, hogy $PO(\mathcal{K})$ 3-tranzitívan hat; rögzítsük ehhez a $\mathcal{K}$ különböző pontokból álló két ponthármasát, A, B, C-t és A', B', C'-t. Legyen Z_1 az AB' és $A'B$ egyenesek metszéspontja és legyen C'' a CZ_1 egyenes *második* metszéspontja $\mathcal{K}$-val. Ez utóbbit úgy kell érteni, hogy ha CZ_1 két különböző pontban metszi $\mathcal{K}$-t, akkor $C'' \neq C$, ha CZ_1 a



5.4. ábra. A vetítések szorzatai 3-tranzitívan hatnak.

$\mathcal{K}$ C-beli érintője, akkor $C'' = C$. Akkor sincs gond, hogy ha pl. $A = B'$, ekkor az AB' egyenes alatt a $\mathcal{K}$ A-beli érintőjét értjük.

Legyen továbbá Z_2 az $A'B'$ és $C'C''$ egyenesek metszéspontja. Az 5.4. ábráról könnyen leellenőrizhető, hogy a $\beta = \sigma_{Z_2} \circ \sigma_{Z_1} \in PO(\mathcal{K})$ projektív transzformációra teljesül $A \mapsto A'$, $B \mapsto B'$ és $C \mapsto C'$.

Az élességgel kapcsolatosan elegendő megvizsgálni $\mathcal{K}$ azon β automorfizmusait, amelyek három különböző pontot fixen hagynak. Jelöljük a három fixpontot A, B, C-vel, és legyen D az A és B-beli érintők metszéspontja. A két érintő nyilván fixegyenese β-nak, így D is fixpont. Könnyen leellenőrizhető, hogy az A, B, C és D fixpontok közül semelyik 3 nincs egy egyenesen, ekkor azonban a β projektív lineáris transzformáció csak az identitás lehet, amiből következik, hogy $PO(\mathcal{K})$ hatása élesen 3-tranzitív. □

Megjegyzés. Az 5.4 alfejezet végén láttuk, hogy vetítés segítségével egy nem-elfajuló kúpszelet azonosítható a projektív egyenessel. Megmutatható, hogy ezzel az azonosítással a $PO(\mathcal{K})$ csoport hatása $\mathcal{K}$-n megegyezik a $PGL(2, \mathbb{T})$ csoportnak a projektív egyenesen vett hatásával. Ez utóbbiról pedig az 5.3 alfejezetben láttottak alapján tudjuk, hogy megegyezik a törtlineáris leképezések csoportjának a $\mathbb{T} \cup \{\infty\}$ kibővített számtesten vett hatásával.

6. fejezet

Projektív kvadrikák

Ebben a fejezetben minden egy rögzített, $\mathbb{T}$ test feletti, n-dimenziós projektív térben fog lejátszódni, ahol $n \geq 2$; erre a projektív térre a $PG(n, \mathbb{T})$ jelölést fogjuk használni. Feltételezzük továbbá, hogy a térben rögzítettünk egy *homogén koordinátarendszert*, amelyben a pontokat vagy $n+1$ hosszúságú oszlopvektorokkal, vagy pedig $(x_0 : x_1 : \ldots : x_n)$ alakú sorvektorokkal adjuk meg.

A $PG(n, \mathbb{T})$ tér $n-1$-dimenziós projektív altereit *hipersíkoknak* nevezzük, egy hipersík mindig egy

$$u_0 x_0 + \ldots + u_n x_n = 0$$

alakú egyenlettel adható meg, ahol az $(u_0, \ldots, u_n)$ vektor nem nulla és egy konstans szorzó erejéig van meghatározva. Vegyük észre, hogy ez nem jelent mást, mint hogy a $PG(n, \mathbb{T})$ tér homogén koordinátázása automatikusan egy homogén koordinátázást biztosít a tér hipersíkjainak a számára.

6.1. A projektív leképezések alaptétele

Ha adott a $PG(n, \mathbb{T})$ tér $k \leq n$ pontja, akkor biztos létezik egy legfeljebb $k-1$-dimenziós projektív altér, amely ezeket tartalmazza. Tekintsük ugyanis a pontokat megadó $(x_0^{(1)} : \ldots : x_n^{(1)}), \ldots, (x_0^{(k)} : \ldots : x_n^{(k)})$ vektorokat, ezek az $n+1$-dimenziós $\mathbb{T}$-vektortérnek egy legfeljebb k-dimenziós lineáris alterért feszítik ki, ami definíció szerint $PG(n, \mathbb{T})$-nek egy legfeljebb $k-1$-dimenziós alterét határozza meg. A k pontot tartalmazó legszűkebb projektív alteret a *pontok által kifeszített projektív altérnek* nevezzük.

6.1. Definíció. *Azt mondjuk, hogy a $PG(n, \mathbb{T})$ tér pontjainak egy X halmaza általános helyzetű, ha minden $k \leq n+1$ esetén az X bármely k elemű részhalmaza a $PG(n, \mathbb{T})$ tér egy $k-1$-dimenziós alterét feszíti ki.*

Vezessük be az alábbi jelölést:

$$\begin{aligned} \boldsymbol{e}^{(0)} &= (1:0:\ldots:0),\\ \boldsymbol{e}^{(1)} &= (0:1:\ldots:0),\\ &\vdots\\ \boldsymbol{e}^{(n)} &= (0:0:\ldots:1),\\ \boldsymbol{e}^{(n+1)} &= (1:1:\ldots:1), \end{aligned}$$

és jelölje E_i az $\boldsymbol{e}^{(i)}$ vektor által megadott projektív pontot ($i = 0, \ldots, n+1$). ezeket a pontokat a *koordinátarendszer alappontjainak* is nevezzük. Nyilvánvaló, hogy akárhogy választunk ki $n+1$ pontot a fenti $n+2$-ből, a vektoraikból alkotott $(n+1) \times (n+1)$-es mátrix determinánsa nem nulla, azaz az általuk kifeszített lineáris altér dimenziója $n+1$. Ez pontosan azt jelenti, hogy a kiválasztott $n+1$ pont a teljes n-dimenziós projektív teret kifeszíti, vagyis az $n+2$ darab alappont általános helyzetű.

6.2. Lemma. *Legyen adott a $PG(n, \mathbb{T})$ tér tetszőleges $n+2$ általános helyzetű pontja: $P_0, \ldots, P_{n+1}$. Ekkor létezik egy egyértelműen meghatározott φ projektív lineáris transzformáció, amelyre $\varphi(E_i) = P_i$ teljesül minden $i = 0, 1, \ldots, n+1$ esetén.*

Bizonyítás. Jelöljük a P_i pontot megadó vektort $\boldsymbol{a}^{(i)} = (a_0^{(i)} : a_1^{(i)} : \ldots : a_n^{(i)})$-vel. Vezessük be a $\xi_0, \ldots, \xi_n$ ismeretleneket, és tekintsük az

$$A = \begin{pmatrix} a_0^{(0)} & \cdots & a_0^{(n)} \\ \vdots & & \\ a_n^{(0)} & \cdots & a_n^{(n)} \end{pmatrix}, \qquad M = \begin{pmatrix} \xi_0 a_0^{(0)} & \cdots & \xi_n a_0^{(n)} \\ \vdots & & \\ \xi_0 a_n^{(0)} & \cdots & \xi_n a_n^{(n)} \end{pmatrix}$$

$(n+1) \times (n+1)$ mátrixokat. A feltételek szerint a $P_0, \ldots, P_n$ pontok kifeszítik a teljes teret, azaz az A oszlopai lineárisan függetlenek, s így $\det(A) \neq 0$. Teljesül továbbá $\det(M) = \xi_0 \cdots \xi_n \det(A)$ és

$$M\boldsymbol{e}^{(i)} = \xi_i \boldsymbol{a}^{(i)} \qquad i = 0, 1, \ldots, n \tag{6.1}$$

$$M\boldsymbol{e}^{(n+1)} = \xi_0 \boldsymbol{a}^{(0)} + \ldots + \xi_n \boldsymbol{a}^{(n)}. \tag{6.2}$$

Vegyük észre, hogy a a (6.1) azonosságok egyértelműen meghatározzák az M mártix fenti alakját. Az A mátrix oszlopainak függetlenségéből adódik, hogy a $\xi_0, \ldots, \xi_n$ ismeretlenek értékét egy konstans c szorzó erejéig egyértelműen meg tudjuk úgy határozni, hogy $M\boldsymbol{e}^{(n+1)} = c\boldsymbol{a}^{(n+1)}$ teljesüljön.

Most megmutatjuk, hogy a $\xi_0, \ldots, \xi_n$ számok közül egyik sem lehet nulla. Példának okáért tegyük ugyanis fel, hogy $\xi_0 = 0$. Ekkor $\boldsymbol{a}^{(n+1)}$ kifejezhető lenne csupán az $\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(n)}$ vektorok lináris kombinációjaként, azaz az $n+1$ darab $\boldsymbol{a}^{(1)}, \ldots, \boldsymbol{a}^{(n+1)}$ vektor egy n-dimenziós lineáris teret feszítene ki. Ez egyenértékű lenne azzal, hogy a $P_1, \ldots, P_{n+1}$ pontok egy

$n-1$-dimenziós projektív alteret feszítenek ki, ami pedig ellentmondana a $P_0, \ldots, P_{n+1}$ ponthalmaz általános helyzetének.

Így viszont, hogy semelyik ξ_i nem nulla, az M mátrix determinánsa sem nulla, tehát meghatároz egy φ projektív lineáris transzformációt. A ξ_i értékek megválasztása és a (6.1), (6.2) egyenlőségek miatt $\varphi(E_i) = P_i$ teljesül minden $i = 0, \ldots, n+1$ esetén. Végül pedig a φ egyértelműsége adódik abból, hogy az M mátrix konstans szorzó erejéig egyértelműen meghatározott. □

A továbbiakban fontos szerepet fognak játszani a $\mathbb{T}$ alaptest *automorfizmusai*; a $\sigma \in \mathrm{Aut}(\mathbb{T})$ jelölés jelentése:

$$\sigma(x+y) = \sigma(x) + \sigma(x), \qquad \sigma(xy) = \sigma(x)\sigma(x) \qquad \forall x, y \in \mathbb{T}.$$

Az $\boldsymbol{x} = (x_0, \ldots, x_n)$ $\mathbb{T}$ feletti vektor esetén használni fogjuk a

$$\sigma(\boldsymbol{x}) = (\sigma(x_0), \ldots, \sigma(x_n))$$

jelölést.

6.3. Definíció. *A $\mathbb{T}$ test feletti $V = \mathbb{T}^n$ vektortér* szemilineáris leképezésének *nevezzük a*

$$V \to V, \qquad \boldsymbol{x} \mapsto M\sigma(\boldsymbol{x})$$

alakú leképezéseket, ahol M egy $n \times n$-es mátrix és $\sigma \in \mathrm{Aut}(\mathbb{T})$.

A $PG(n, \mathbb{T})$ projektív tér egy olyan transzformációját, amelyet a teret koordinátázó vektortér önmagára vett szemilineáris leképezése indukál, projektív szemilineáris leképezésnek *nevezzük.*

6.4. Lemma. *Egy szemilineáris leképezés akkor és csak akkor indukál egy projektív transzformációt, ha* $\det(M) \neq 0$. *Ebben az esetben az indukált projektív transzformáció illeszkedéstartó.*

Bizonyítás. Ha $\det(M) = 0$, akkor van olyan nullától különböző $\boldsymbol{x}$ vektor, melynek képe a nullvektor, s ekkor a leképezés nem értelmezett a projektív téren. Ha viszont $\det(M) \neq 0$, akkor a lineáris leképezés bijektív és ahhoz, hogy projektív leképezést indukáljon, meg kell mutatnunk, hogy minden origóra illeszkedő egyenes képe origóra illeszkedő egyenes. Mi ennél többet mutatunk meg, nevezetesen, hogy lineáris altér képe lineáris altér; ebből az indukált projektív leképezés illeszkedéstartása is következik.

Tekintsük tehát az $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_k$ vektorok által kifeszített

$$\{\lambda_1\boldsymbol{x}_1 + \ldots + \lambda_k\boldsymbol{x}_k : \lambda_1, \ldots, \lambda_k \in \mathbb{T}\}$$

lineáris alteret. Ennek képe

$$\{\sigma(\lambda_1)M\sigma(\boldsymbol{x}_1) + \ldots + \sigma(\lambda_k)M\sigma(\boldsymbol{x}_k) : \lambda_1, \ldots, \lambda_k \in \mathbb{T}\},$$

és mivel σ szürjektív, ez pontosan az $M\sigma(\boldsymbol{x}_1), \ldots, M\sigma(\boldsymbol{x}_k)$ vektorok által kifeszített lineáris altér. Tehát az indukált projektív leképezés értelmes és illeszkedéstartó. □

Az imént definiált fogalmak segítségével kimondhatjuk a projektív tér transzformációiról szóló egyik legfontosabb tételt.

6.5. Tétel (A projektív leképezések alaptétele). *A $PG(n, \mathbb{T})$ projektív tér illeszkedéstartó transzformációi pontosan a projektív szemilineáris leképezések.*

Bizonyítás. Legyen φ a $PG(n, \mathbb{T})$ projektív tér egy illeszkedéstartó transzformációja és jelölje $P_0, \ldots, P_{n+1}$ a megfelelő $E_0, \ldots, E_{n+1}$ alappontok φ melletti képét. A 6.2 lemma szerint ekkor létezik egy nem-elfajuló M mátrix, amely által meghatározott α_M projektív lineáris transzformációra teljesül

$$\alpha_M(E_i) = P_i = \varphi(E_i), \qquad i = 0, \ldots, n+1.$$

Vizsgáljuk most a $\beta = \alpha_M^{-1} \circ \varphi$ transzformációt; ez nyilván illeszkedéstartó, és

$$\beta(E_i) = E_i$$

fennáll minden $i = 0, \ldots, n+1$ esetén. Megmutatjuk, hogy β-t egy $\boldsymbol{x} \mapsto \sigma(\boldsymbol{x})$ leképezés indukálja, ahol $\sigma \in \mathrm{Aut}(\mathbb{T})$.

Definiáljuk az $(n+1)$-dimenziós vektortér alábbi részhalmazait:

$$A_k = \{(x_0, \ldots, x_{k-1}, 1, 0, \ldots, 0) : x_0, \ldots, x_{k-1} \in \mathbb{T}\}, \qquad k = 0, \ldots, n$$

és legyen

$$A = A_0 \cup \cdots \cup A_{n+1}.$$

Könnyen konstruálható egy kölcsönösen egyértelmű megfeleltetés A és a $PG(n, \mathbb{T})$ tér pontjhalmaza között: egy P pont homogén $\boldsymbol{x} = (x_0 : \ldots : x_n)$ koordinátázásban válasszuk a legnagyobb k indexű $x_k \neq 0$ koordinátát 1-nek, ekkor $\boldsymbol{x} \in A_k$. Eszerint a projektív tér β transzformációja megfelel az A halmaz egy önmagára vett $\boldsymbol{f}$ bijekciójának. A különböző koordinátákat tekintve az $\boldsymbol{f}$ leképezés

$$\boldsymbol{f}(\boldsymbol{x}) = (f_0(\boldsymbol{x}), \ldots, f_n(\boldsymbol{x})), \qquad (\boldsymbol{x} \in A)$$

alakban írható fel.

1. lépés: Azt állítjuk, hogy $i \neq j$ esetén az f_i függvény nem függ x_j-től. Az egyszerűség kedvéért a bizonyítást az $i = 1$, $j = 0$ esetre végezzük el, az általános eset bizonyítása is hasonlóan történik. Ha $(x_1, \dots, x_n) = 0$, akkor csak $x_0 = 1$ lehetséges, ekkor tehát $\beta(E_0) = E_0$ miatt mondhatjuk, hogy $f_2(x_0, 0, \dots, 0) = 0$ minden x_0 esetén. Tegyük fel, hogy $(x_1, \dots, x_n) \neq (0, \dots, 0)$ és mutassuk meg, hogy $f_1(x_0, x_1, \dots, x_n) = f_1(0, x_1, \dots, x_n)$ minden $\boldsymbol{x} = (x_0, \dots, x_n) \in A$ esetén.

Egyrészt az E_0, $P(\boldsymbol{x})$ és a $P_0(0, x_1, \dots, x_n)$ pontok egy egyenesre illeszkednek. Másrészt P_0 illeszkedik az $x_0 = 0$ hipersíkra, amelyet az $E_1, \dots, E_n$ pontok feszítenek ki, s így azt β fixen hagyja. Az E_0, P, P_0 kollineáris ponthármas β melletti képei is kollineárisak, ezeknek a képeknek a koordinátái $E_0(1, 0, \dots, 0)$, $P'(f_0(\boldsymbol{x}), f_1(\boldsymbol{x}), \dots, f_n(\boldsymbol{x}))$ és

$$P_0'(0, f_1(0, x_1, \dots, x_n), \dots, f_n(0, x_1, \dots, x_n)).$$

Az E_0P' egyenes metszete az $x_0 = 0$ hipersíkkal egyrészt P_0', másrészt pedig $(0, f_1(x_0, x_1, \dots, x_n), \dots, f_n(x_0, x_1, \dots, x_n))$ számolással, amiből a koordináták összehasonlása után $f_1(x_0, x_1, \dots, x_n) = f_1(0, x_1, \dots, x_n)$ adódik.
2. lépés: Azt állítjuk, hogy $f_i = f_j$. Ismét feltételezhetjük, hogy $i = 0, j = 1$ az általánosság megszorítása nélkül. Mivel az $E_2, \dots, E_{n+1}$ n darab általános helyzetű pont mindegyike kielégíti az $x_0 - x_1 = 0$ egyenlőséget, ezért ők pontosan az $x_0 - x_1 = 0$ hipersíkot feszítik ki. Ez az n pont mind a β fixpontja, így az $x_0 - x_1 = 0$ hipersík is fix. Tekintsük ennek a hipersíknak egy tetszőleges $P(x_0, x_0, x_2, \dots, x_n)$ pontját, az első lépésben látottak alapján ennek a képe $P'(f_0(x_0), f_1(x_0), f_2(x_2), \dots, f_n(x_n))$. Nyilván P' is illeszkedik az $x_0 - x_1 = 0$ hipersíkhoz, azaz $f_0(x_0) = f_1(x_0)$ teljesül.
3. lépés: Azt állítjuk, hogy $\boldsymbol{f}(\boldsymbol{x}) = \sigma(\boldsymbol{x})$, ahol $\sigma \in \mathrm{Aut}(\mathbb{T})$. Eddig láttuk, hogy

$$\boldsymbol{f}(x_0, \dots, x_n) = (f(x_0), \dots, f(x_n))$$

egy megfelelő $f : \mathbb{T} \to \mathbb{T}$ függvénnyel. Tudjuk továbbá, hogy $f(0) = 0$ és $f(1) = 1$.

Egyrészt az $(1 : 0 : 1 : 0 : \dots : 0)$, $(0 : 1 : 1 : 0 : \dots : 0)$, $E_3, \dots, E_n$ n darab általános helyzetű pontnégyes kifeszíti az $x_0 + x_1 - x_2 = 0$ hipersíkot. Másrészt $f(0) = 0$ és $f(1) = 1$ miatt ez csupa fixpont, tehát az $x_0 + x_1 - x_2 = 0$ hipersík is fix β mellett. Tekintsük ennek a hipersíknak egy $P(x_0 : x_1 : x_0 + x_1 : 0 : \dots : 0)$ pontját, ennek $P'(f(x_0) : f(x_1) : f(x_0 + x_1) : \dots : 0)$ képe ismét illeszkedik rá, tehát $f(x_0) + f(x_1) - f(x_0 + x_1) = 0$, azaz

$$f(x_0) + f(x_1) = f(x_0 + x_1)$$

teljesül minden $x_0, x_1 \in \mathbb{T}$ esetén.

Vegyük most a

$$P(a : b : 1 : 0 : \dots : 0)$$
$$Q(1 : c : 1 : 0 : \dots : 0)$$
$$E_2(0 : 0 : 1 : 0 : \dots : 0)$$

pontokat, illetve ezek képeit:

$$P'(f(a) : f(b) : 1 : 0 : \ldots : 0)$$
$$Q'(1 : f(c) : 1 : 0 : \ldots : 0)$$
$$E_2(0 : 0 : 1 : 0 : \ldots : 0).$$

Nyilván P, Q, E_2 akkor és csak akkor kollineáris, ha

$$\det \begin{pmatrix} a & b & 1 \\ 1 & c & 1 \\ 0 & 0 & 1 \end{pmatrix} = 0,$$

azaz ha $b = ac$. Továbbá a három pont akkor és csak akkor kollineáris, ha a képeik azok, azaz ha $f(b) = f(a)f(c)$. Tehát bármely $a, c \in \mathbb{T}$ esetén $b = ac$ választással $f(a)f(c) = f(b) = f(ac)$ adódik. Ezekből pedig következik, hogy $f = \sigma \in \mathrm{Aut}(\mathbb{T})$.

Ezzel tehát beláttuk, hogy a β illeszkedéstartó transzformációt egy σ testautomorfizmus indukálja. Mivel pedig definíció szerint

$$\varphi = \alpha_M \circ \beta,$$

így kapjuk, hogy φ-t az $\boldsymbol{x} \mapsto M\sigma(\boldsymbol{x})$ szemilineáris kollineáció indukálja. □

Ennek a pontnak a végén ejtünk még néhány szót az általunk ismert testek automorfizmusairól. A legkönnyebb azt meggondolni, hogy a racionális számok $\mathbb{Q}$ testének csak triviális (=identikus) automorfizmusa létezik. Minden racionális számot fel tudunk ugyanis írni az 1 és a négy alapművelet felhasználásával, és mivel az 1-et minden testautomorfizmus fixen hagyja, az alapműveleteket pedig megőrzi, így minden racionális szám fix marad.

A valós számok $\mathbb{R}$ testénél ugyanez a helyzet, ehhez azonban már valamivel hosszabb számolás szükséges.

6.6. Állítás. *A valós számok $\mathbb{R}$ testének az egyetlen automorfizmusa az identitás.*

Bizonyítás. Tekintsünk ugyanis egy $\sigma \in \mathrm{Aut}(\mathbb{R})$ testautomorfizmust, erre szükségszerűen teljesül $\sigma(0) = 0$ és $\sigma(1) = 1$. Ha n egy pozitív egész, akkor

$$\sigma(n) = \sigma(1 + \ldots + 1) = \sigma(1) + \ldots + \sigma(1) = n$$

teljesül. Ha $n < 0$ negatív egész, akkor

$$n^2 = \sigma(n^2) = \sigma(n)^2,$$

s így $\sigma(n) = \pm n$. Már tudjuk, hogy $\sigma(-n) = -n$, ezért a σ injektivitása miatt $\sigma(n) \neq -n$, vagyis $\sigma(n) = n$. Ha $r = n/m \in \mathbb{Q}$, ahol $n, m \in \mathbb{Z}$ egészek, akkor

$$n = \sigma(n) = \sigma(rm) = \sigma(r)\sigma(m) = \sigma(r)m,$$

amiből $\sigma(r) = n/m = r$ adódik.

Megmutatjuk most, hogy $x < y$ esetén $\sigma(x) < \sigma(y)$ teljesül minden $x, y \in \mathbb{R}$ valós szám esetén. Ekkor ugyanis létezik egy $a > 0$ valós szám, amelyre $y - x = a^2$ áll fenn, amiből azt kapjuk, hogy

$$\sigma(y) - \sigma(x) = \sigma(x - y) = \sigma(a^2) = \sigma(a)^2 > 0.$$

Tegyük végül fel, hogy létezik $x \in \mathbb{R}$ valós szám, amelyre $\sigma(x) \neq x$. Mivel $\sigma(x)$ is valós, így ekkor létezik egy $r \in \mathbb{Q}$ racionális szám, amely x és $\sigma(x)$ közé esik, ha például $x < \sigma(x)$, akkor $x < r < \sigma(x)$. σ monotonitása miatt viszont $x < r$-ből $\sigma(x) < \sigma(r) = r$ kellene következzen, tehát ellentmondáshoz jutottunk. Nyilván ugyanígy ellentmondást kapunk, ha $x > \sigma(x)$-et tételezzük fel. Vagyis egyetlen $x \in \mathbb{R}$ esetén sem állhat fent $x \neq \sigma(x)$, azaz $\sigma = \mathrm{id}$. □

Ebből és a 6.5 tételből azonnal adódik az alábbi következmény.

6.7. Következmény. *Egy valós test feletti projektív tér illeszkedéstartó leképezési pontosan a projektív lineáris leképezések.*

A komplex számok $\mathbb{C}$ testének egy igen fontos automorfizmusával, az $x \mapsto \bar{x}$ konjugálással már találkoztuk.

Vizsgáljuk meg végül azt az esetet, amikor $\mathbb{T} = \mathbb{F}_q$ véges test. Tudjuk, hogy ekkor a test rendje $q = p^e$ prímhatvány, ahol a p prím a test karakterisztikája. Megmutatjuk, hogy egy p karakterisztikájú testben az $\Phi : x \mapsto x^p$ hatványozás automorfizmus. Az ilyen testek $x \mapsto x^{p^k}$ alakú automorfizmusait *Frobenius-automorfizmusoknak* nevezzük.

Az nyilvánvaló, hogy $\Phi(xy) = \Phi(x)\Phi(y)$ teljesül, hiszen a szorzás kommutativitása miatt szorzat hatványa a hatványok szorzata. Vizsgáljuk meg most $\Phi(x + y)$-t a binomiális tétel segítségével:

$$(x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + \binom{p}{1}xy^{p-1} + y^p.$$

Ennek persze csak úgy van értelme, hogy a $\binom{p}{i}$ egész számot modulo p mint $\mathbb{T}$-beli elemet tekintem. Megmutatjuk azonban, hogy minden $0 < i < p$ esetén $\binom{p}{i} \equiv 0 \pmod{p}$, azaz a fenti egyenlőség megadja a keresett $(x + y)^p = x^p + y^p$ összefüggést. Valóban, a binomiális együttható definíciója szerint

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdots i},$$

azaz $0 < i < p$ esetén a számláló osztható p-vel, a nevező viszont nem. Ezzel beláttuk, hogy egy p karakterisztikájú testben a p-dik hatványra emelés csakugyan testhomomorfizmus. A leképezés bijektivitása véges test esetén következik az injektivitásából: $x^p = y^p$ esetben vagy $x = y = 0$, vagy egyik sem nulla, és ekkor $(xy^{-1})^p = 1$, azaz $(xy^{-1} - 1)^p = 0$ áll fenn, amiből $xy^{-1} = 1$ és $x = y$ következik.

6.2. Korrelációk, polaritások

Már említettük, hogy a $PG(n,\mathbb{T})$ projektív tér hipersíkjai $n+1$ hosszúságú homogén koordinátákkal adható meg: a $P(\boldsymbol{x})$ pont akkor és csak akkor illeszkedik az $\boldsymbol{u} = (u_0 : \ldots : u_n)$ koordinátákkal megadott $H(\boldsymbol{u})$ hipersíkra, ha

$$\boldsymbol{u}^t\boldsymbol{x} = u_0x_0 + \ldots + u_nx_n = 0$$

teljesül.

Jelöljük a továbbiakban $\mathcal{P}$-vel a $PG(n,\mathbb{T})$ tér ponthalmazát és $\mathcal{H}$-val a tér hipersíkjainak halmazát.

6.8. Definíció. *A $\rho : \mathcal{P} \cup \mathcal{H} \to \mathcal{P} \cup \mathcal{H}$ leképezés a $PG(n,\mathbb{T})$ projektív tér* korrelációja, *ha ρ pontot hipersíkra, hipersíkot pedig pontra képez úgy, hogy eközben az illeszkedést megtartja.*

Adott koordinátázás mellett a legegyszerűbben megadható korreláció az, amelyik a $P(\boldsymbol{z})$ pontot a $H(\boldsymbol{z}) : \boldsymbol{z}^t\boldsymbol{x} = 0$ hipersíkra, a $H(\boldsymbol{u}) : \boldsymbol{u}^t\boldsymbol{x} = 0$ hipersíkot pedig a $P(\boldsymbol{u})$ pontra képezi le. Az $\boldsymbol{u}^t\boldsymbol{x} = \boldsymbol{x}^t\boldsymbol{u}$ egyenlőségből azonnal adódik, hogy ez a leképezés megtartja a pontok és hipersíkok közötti illeszkedést.

A projektív kollineációk és a korrelációk közötti szoros kapcsolatot fejezi ki az alábbi tétel.

6.9. Tétel (Projektív korrelációk alaptétele). *A projektív tér minden korrelációja előáll*

$$P(\boldsymbol{z}) \mapsto H(A\sigma(\boldsymbol{z})) : \sigma(\boldsymbol{z})^t M^t\boldsymbol{x} = 0$$

alakban, ahol M egy $(n+1)\times(n+1)$-es $\mathbb{T}$ feletti nem-elfajuló mártix és $\sigma \in \operatorname{Aut}\mathbb{T}$.

Bizonyítás. Legyen ρ a $PG(n,\mathbb{T})$ projektív tér egy korrelációja, és jelöljük τ-val a fentebb leírt korrelációt: $P(\boldsymbol{z}) \mapsto H(\boldsymbol{z})$, $H(\boldsymbol{u}) \mapsto P(\boldsymbol{u})$. A $\tau \circ \sigma$ szorzat leképezés nyilván a projektív tér ponthalmazának egy önmagára vett illeszkedéstartó leképezését határozza meg, azaz a 6.5 tétel szerint

$$\tau \circ \sigma : P(\boldsymbol{z}) \mapsto P(M\sigma(\boldsymbol{z}))$$

alakba írható megfelelő M mártix és σ testautomorfizmussal. τ definíciója szerint, $\tau^2 = \mathrm{id}$ felhasználásával pontosan a

$$\rho : P(\boldsymbol{z}) \mapsto H(A\sigma(\boldsymbol{z})) : \sigma(\boldsymbol{z})^t M^t\boldsymbol{x} = 0$$

alakot kapjuk. □

A bizonyításban láttuk, hogy a fenti példánk korrelációra azzal a speciális tulajdonsággal is rendelkezik, hogy *involutív*, azaz a négyzete az identitás.

6.10. Definíció. *Azokat a korrelációkat, amelyeknek a négyzete az identitás a $\mathcal{P} \cup \mathcal{H}$ halmazon,* polaritásoknak *nevezzük.*

Tekintsük most azt a korrelációt, amelynek a $\mathcal{P}$-n megadott hatása $\boldsymbol{z} \mapsto \sigma(\boldsymbol{z})^t A\boldsymbol{x} = 0$. Azt állítjuk, hogy ekkor a hipersíkokon vett hatás szükségszerűen

$$\boldsymbol{H}(\boldsymbol{u}) : u^t\boldsymbol{x} = 0 \mapsto P(A^{-1}\sigma(\boldsymbol{u})).$$

Az illeszkedéstartásból következik, hogy egy korrelációt a ponthalmazon vett hatása egyértelműen meghatározza, így elegendő megmutatni, hogy a hipersíkokon fentebb megadott hatás illeszkdéstartó $\mathcal{P} \cup \mathcal{H} \to \mathcal{P} \cup \mathcal{H}$ leképezést határoz meg. Csakugyan, ekkor egy rögzített $H(\boldsymbol{u}) : \boldsymbol{u}^t\boldsymbol{x} = 0$ hipersík esetén a $P(\boldsymbol{z})$ pont $H'(A^t\sigma(\boldsymbol{z}))$ képe akkor és csak akkor illeszkedik a $H(\boldsymbol{u})$ hipersík $P'(A^{-1}\boldsymbol{u})$ képéhez, ha

$$0 = \sigma(\boldsymbol{z})^t A \cdot A^{-1}\sigma(\boldsymbol{u}) = \sigma(\boldsymbol{u}^t\boldsymbol{z})$$

fennáll, ami pedig ekvivalens azzal, hogy P illeszkedik H-hoz.

Vizsgáljuk most meg, hogy mit jelent az, hogy egy korreláció involutív. A korrelációk alaptétele szerint a $P(\boldsymbol{z})$ pont képe a $H(A^t\sigma(\boldsymbol{z})) : \sigma(\boldsymbol{z})^t A\boldsymbol{x} = 0$ hipersík, a fentiek szerint pedig ennek a képe a

$$P'(A^{-1}\sigma(A^t\sigma(\boldsymbol{z})))$$

pont. Tehát a korreláció akkor és csak akkor involutív, ha a

$$\boldsymbol{z} \mapsto A^{-1}\sigma(A^t)\sigma^2(\boldsymbol{z})$$

szemilineáris leképezés az identikus projektív leképezést határozza meg, azaz ha

$$A^{-1}\sigma(A^t)\sigma^2(\boldsymbol{z}) = \lambda\boldsymbol{z} \tag{6.3}$$

áll fenn valamely $\boldsymbol{z}$-től független $\lambda \in \mathbb{T}^*$ számmal. A $\boldsymbol{z} = \boldsymbol{e}^{(i)}$ $(i = 0, \ldots, n)$ behelyettesítésekből ekkor a (6.3) azonosságból

$$A^{-1}\sigma(A^t) = \lambda I \tag{6.4}$$

következik, ahol I a megfelelő méretű egységmártixot jelöli. Majd a (6.3) és a (6.4) egyenlőségekből

$$\sigma^2 = \mathrm{id} \tag{6.5}$$

adódik. A (6.4) és (6.5) kombinálásából kapjuk, hogy

$$A = \sigma^2(A) = \sigma(\lambda A^t) = \sigma(\lambda)\lambda A,$$

s így teljesül

$$\sigma(\lambda)\lambda = 1. \tag{6.6}$$

Most két esetet különböztetünk meg.
I. eset: $x + \sigma(\lambda)\sigma(x) = 0$ *teljesül minden* $x \in \mathbb{T}$ *esetén.* Ekkor $x = 1$ helyettesítéssel $\sigma(\lambda) = -1$, tehát $\lambda = -1$ adódik. Ebből a feltétel szerint $x - \sigma(x) = 0$ minden $x \in \mathbb{T}$ elemre, azaz $\sigma = \mathrm{id}$. Az A mártixra (6.4) szerint kapjuk, hogy $A^t = -A$. Ebben az esetben *nullpolaritásról* beszélünk.
II. eset: $x + \sigma(\lambda)\sigma(x) = y \neq 0$ *valamely rögzített* $x \in \mathbb{T}$ *esetén.* Ekkor (6.5) és (6.6) miatt

$$\sigma(y) = \sigma(x) + \lambda x = \lambda\sigma(\lambda)\sigma(x) + \lambda x = \lambda y,$$

azaz $\lambda = y^{-1}\sigma(y)$ áll fenn. A homogén koordinátázás miatt nem jelent megszorítást, ha az A mártixról áttérünk annak egy skalárszorosára: $A' = y^{-1}A$. A fentiek szerint ekkor

$$\sigma(A') = \sigma(y^{-1}A) = \sigma(y)^{-1}\sigma(A) = y^{-1}\lambda^{-1}\lambda A^t = (A')^t$$

és $\lambda' = 1$ teljesül. Ebben az esetben tehát a polaritás $\boldsymbol{z} \mapsto \sigma(\boldsymbol{z})^t A\boldsymbol{x} = 0$ alakban lesz felírható, ahol $\sigma^2 = \mathrm{id}$ és $\sigma(A) = A^t$. Abban az esetben, ha $\sigma = \mathrm{id}$, *szimmetrikus polaritásról*, ha pedig $\sigma \neq \mathrm{id}$, akkor *Hermite-féle polaritásról* beszélünk.

Bebizonyítottuk tehát a következő tételt.

6.11. Tétel. *Legyen* ρ *a* $PG(n,)$ *projektív tér egy polaritása. Ekkor*

$$\rho : P(\boldsymbol{z}) \mapsto \sigma(\boldsymbol{z})^t A\boldsymbol{x} = 0$$

és a ρ*, az* A *mártix és* σ *testautomorfizmus eleget tesz az alábbiak valamelyikének.*

- *(i)* ρ *szimmetrikus polaritás,* $\sigma = \mathrm{id}$ *és* $A^t = A$.
- *(ii)* ρ *nullpolaritás,* $\sigma = \mathrm{id}$ *és* $A^t = -A$.
- *(iii)* ρ *Hermite-féle polaritás,* $\sigma^2 = \mathrm{id}$ *és* $A^t = \sigma(A)$. □

6.3. Polaritások abszolút pontjai

6.12. Definíció. *Azt mondjuk, hogy a* P *pont a* ρ *projektív polaritás* abszolút pontja, *ha* P *illszekedik a* $\rho(P)$ *hipersíkra. Duálisan, a* H *hipersík a* ρ abszolút hipersíkja, *ha a* $\rho(H)$ *pont illeszkedik* H*-ra.*

A továbbiakban a célunk az lesz, hogy a koordináta rendszer megfelelő megválasztásával elérjük azt, hogy egy polaritás abszolút pontjainak halmát a lehető legegyszerűbben tudjuk koordinátákkal megadni.

Az egyszerűbb jelölés kedéért a σ testautomorfizmus helyett $\sigma(x) = \bar{x}$ írásmódot fogjuk alkamazni, σ involutivitása miatt nyilván $\bar{\bar{x}} = x$ minden $x \in \mathbb{T}$ esetén. Legyen továbbá

$$\mathbb{T}_0 = \{x \in \mathbb{T} : \bar{x} = x\}.$$

Ekkor $\mathbb{T}_0 = \mathbb{T}$, ha $x \mapsto \bar{x}$ az identitás, egyébként pedig $\mathbb{T}_0$ a $\mathbb{T}$ valódi részteste.

6.13. Lemma (Főtengelytranszformáció). *Legyen adott az*

$$\mathcal{F} = \{P(\boldsymbol{x}) : \sum_{i,j=0}^{n} a_{ij} x_i \bar{x}_j = 0\}$$

felület, ahol $\bar{a}_{ij} = a_{ji} \in \mathbb{T}$ minden $i, j = 0, \ldots, n$ esetén. Ekkor $\mathcal{F}$ egyenlete $\mathbb{T}$ feletti lináris transzformációval

$$c_0 x_0 \bar{x}_0 + \ldots + c_n x_n \bar{x}_n = 0, \qquad (c_i \in \mathbb{T}_0)$$

alakra hozható.

Bizonyítás. Egy adott test feletti lineáris transzformáció helyett mondhatunk olyan

$$\begin{aligned} x_0 &= u_{00} y_0 + \ldots + u_{0n} y_n \\ &\vdots \\ x_n &= u_{n0} y_0 + \ldots + u_{nn} y_n \end{aligned}$$

behelyettesítést, ahol az u_{ij} együtthatók az adott test elemei és a belőlük alkotott $U = (u_{ij})$ mátrix nem-elfajuló, $\det(U) \neq 0$. Nyilván ilyen behelyettesítések szorzata is ilyen, ezért a bizonyítást több behelyettesítés összefűzésével végezzük el.

Tekintsük most az

$$f(x_0, \ldots, x_n) = \sum_{i,j=0}^{n} a_{ij} x_i \bar{x}_j$$

függvényt. Ha minden a_{ij} együttható nulla, akkor egyáltalán nincs mit bizonyítanunk.

Ha valamely $i \in \{0, \ldots, n\}$ indexre $a_{ii} \neq 0$, akkor a változók felcserélésével elérhetjük, hogy $a_{00} \neq 0$ álljon fenn. Mivel a változók felcserélése lineáris behelyettesítás, ez egy lineáris transzformációnak felel meg.

Ha minden a_{ii} együttható nulla, akkor tekintsünk egy $a_{k\ell} \neq 0$ együtthatót és az

$$\begin{aligned} x_i &= y_i, && i \neq k \\ x_k &= y_k + y_\ell \end{aligned}$$

behelyettesítést. Ekkor

$$f(x_0, \ldots, x_n) = \tilde{f}(y_0, \ldots, y_n) = \sum_{i,j=0}^{n} b_{ij} y_i \bar{y}_j,$$

ahol a b_{ii} együtthatók közül csak $b_{kk} = 2a_{k\ell} \neq 0$. Ezzel visszavezettük a problémát az előző esetre.

Feltételezhetjük tehát, hogy $a_{00} \neq 0$. Alkalmazhatunk továbbá indukciót n-re; $n = 0$ esetén az állítás értelmes és igaz, jóllehet geometriai jelentése ekkor nincs. Tegyük tehát azt is fel, hogy $n-1$ változós függvényekre az állítás teljesül. Alkalmazván az

$$\begin{aligned} y_0 &= x_0 + a_{01}a_{00}^{-1}\, x_1 + \ldots + a_{0n}a_{00}^{-1}\, x_n \\ y_1 &= x_1 \\ &\vdots \\ y_n &= x_n \end{aligned}$$

behelyettesítést és $\bar{a}_{ij} = a_{ji}$ egyenlőségeket, azt kapjuk, hogy

$$\begin{aligned} f(x_0, \ldots, x_n) &= \textstyle\sum_{i,j=0}^{n} a_{ij} x_i \bar{x}_j \\ &= a_{00}x_0\bar{x}_0 + a_{01}(x_0\bar{x}_1 + \bar{x}_0 x_1) + \cdots + a_{0n}(x_0\bar{x}_n + \bar{x}_0 x_n) \\ &\qquad + f_1(x_1, \ldots, x_n) \\ &= a_{00}(x_0 + a_{01}a_{00}^{-1}\, x_1 + \ldots)(\bar{x}_0 + a_{10}a_{00}^{-1}\, \bar{x}_1 + \ldots) \\ &\qquad + f_2(x_1, \ldots, x_n) \\ &= a_{00}y_0\bar{y}_0 + f_2(y_1, \ldots, y_n). \end{aligned}$$

Mivel $a_{00} \in \mathbb{T}_0$, az indukciós lépés felhasználásával azonnal adódik, hogy egy alkalmas

$$\begin{aligned} y_0 &= z_0 \\ y_1 &= u_{11}z_1 + \ldots + u_{1n}z_n \\ &\vdots \\ y_n &= u_{n1}z_1 + \ldots + u_{nn}z_n \end{aligned}$$

behelyettesítés megadja a keresett

$$f(x_0, \ldots, x_n) = a_{00}y_0\bar{y}_0 + f_2(y_1, \ldots, y_n) = c_0z_0\bar{z}_0 + c_1z_1\bar{z}_1 + \ldots + c_nz_n\bar{z}_n$$

alakot. □

6.14. Definíció. *Az* $\mathcal{F} : \sum_{i,j=0}^{n} a_{ij} x_i \bar{x}_j = 0$ *felület* rangjának *nevezzük a 6.13 lemma szerinti* $c_0 x_0 \bar{x}_0 + \ldots + c_n x_n \bar{x}_n = 0$ *alakban szereplő nullától különböző* c_i *együtthatók számát. Az* $\mathcal{F}$ *felület* nem-elfajuló, *ha a rangja maximális, azaz* $n+1$.

Az külön megfontolás igényelne, hogy az $\mathcal{F}$ rangja geometriai fogalom, azaz előfordulhat-e, hogy különböző $\boldsymbol{x} = U\boldsymbol{y}$, $\boldsymbol{x} = U'\boldsymbol{y}'$ lineáris helyettesítésekkel kapott $c_0 y_0 \bar{y}_0 + \ldots + c_n y_n \bar{y}_n = 0$ és $c'_0 y'_0 \bar{y}'_0 + \ldots + c'_n y'_n \bar{y}'_n = 0$ alakokban különböző számú nullától különböző együttható található. Ezzel mi most nem foglalkozunk, csak a nem-elfajuló felületek esetét vizsgáljuk meg.

6.15. Állítás. *Az* $\mathcal{F} : \sum_{i,j=0}^{n} a_{ij} x_i \bar{x}_j = 0$ *felület akkor és csak akkor nem-elfajuló, ha* $\det(a_{ij})_{i,j=0}^{n} \neq 0$.

Bizonyítás. A felület megadására a szummás jelölés helyett használhatjuk az $\mathcal{F} : \bar{\boldsymbol{x}}^t A \boldsymbol{x} = 0$ alakot és legyen $\boldsymbol{x} = U\boldsymbol{y}$ az a lineáris transzformáció, amellyel $\mathcal{F}$ a $c_0 y_0 \bar{y}_0 + \ldots + c_n y_n \bar{y}_n = 0$ alakra hozható ($\bar{U} = U$). Ez azt jelenti, hogy $\bar{\boldsymbol{x}}^t A \boldsymbol{x} = \bar{\boldsymbol{y}}^t U^t A U \boldsymbol{y} = \bar{\boldsymbol{y}}^t C \boldsymbol{y}$, ahol $C = U^t A U$ diagonális mátrix. Ebben a megfogalmazásban már nyilvánvaló, hogy $\mathcal{F}$ akkor és csak akkor nem-elfajuló, ha $\det(C) = c_0 \cdots c_n \neq 0$, ami $\det(C) = \det(U)^2 \det(A)$ miatt ekvivalens azzal, hogy $\det(A) \neq 0$. □

Később látni fogjuk, hogy a nem-elfajuló felületek egy bizonyos részének a jellemzése tisztán geometriai eszközökkel is elvégezhető.

Az alábbi tételben összefoglaljuk az alfejezet abszolút ponthalmazokra vonatkozó eredményeit.

6.16. Tétel. *Legyen* $\rho : P(\boldsymbol{z})$ *a* $PG(n, \mathbb{T})$ *projektív tér egy polaritása, és jelöljük* $\mathcal{F}$*-el a* ρ *abszolút pontjainak a halmazát. Ekkor az alábbi esetek fordulhatnak elő.*

(i) Ha ρ *szimmetrikus polaritás, akkor* $\mathcal{F}$ *egy nem-elfajuló kvadratikus felület, amely megfelelő koordináta transzformációval*

$$a_0 x_0^2 + \ldots + a_n x_n^2 = 0$$

alakra hozható.

(ii) Ha ρ *nullpolaritás, akkor minden pont abszolút.*

(iii) Ha ρ *Hermite-féle polaritás, akkor a* $\mathcal{F}$ *egy nem-elfajuló Hermite-sokaság, amely megfelelő koordináta transzformációval*

$$a_0 x_0 \bar{x}_0 + \ldots + a_n x_n \bar{x}_n = 0$$

alakra hozható, ahol minden együtthatóra teljesül $\bar{a}_i = a_i$.

Bizonyítás. A 6.11 tétel szerint a ρ leképezést $P(\boldsymbol{z}) \mapsto H(A\bar{\boldsymbol{z}}) : \bar{\boldsymbol{z}}^t A\boldsymbol{x} = 0$ alakban adhatjuk meg, ahol a $x \mapsto \bar{x}$ a $\mathbb{T}$ alaptest egy involutív automorfizmusa és $\bar{A} = \pm A^t$ egy nem-elfajuló $(n+1) \times (n+1)$-es mátrix. Ebből adódik, hogy a $P(\boldsymbol{x})$ pont pontosan akkor lesz ρ abszolút pontja, ha kielégíti az

$$\bar{\boldsymbol{x}}^t A\boldsymbol{x} = \sum_{i,j=0}^{n} a_{ij} x_i \bar{x}_j = 0$$

egyenlőséget.

Ha ρ szimmetrikus vagy Hermite-féle polaritás, akkor a 6.13 lemma szerint főtengelytranszformációval $\mathcal{F}$ egyenlete $a_0 x_0 \bar{x}_0 + \ldots + a_n x_n \bar{x}_n = 0$ alakra hozható; ez bizonyítja (i)-t és (iii)-t.

Ha ρ nullpolaritás, akkor $x = \bar{x}$ minden $x \in \mathbb{T}$ esetén, az A mátrix pedig antiszimmetrikus: $A^t = -A$. Ekkor tetszőleges $\boldsymbol{x}$ vektorra teljesül

$$\boldsymbol{x}^t A\boldsymbol{x} = (\boldsymbol{x}^t A\boldsymbol{x})^t = \boldsymbol{x}^t A^t \boldsymbol{x} = -\boldsymbol{x}^t A\boldsymbol{x},$$

ami pedig csak $\boldsymbol{x}^t A\boldsymbol{x} = 0$ esetén lehetséges. Tehát ebben az esetben minden $P(\boldsymbol{x})$ pont abszolút, vagyis (ii) teljesül. □

A tételünkben szereplő normálalak meglétének geometriai jelentést is adhatunk.

6.17. Definíció. *Azt mondjuk, hogy a $P_0, \ldots, P_n$ pontok a $PG(n, \mathbb{T})$ tér* ortogonális helyzetű ponthalmazát *alkotják a ρ polaritásra nézve, ha teljesül*

$$P_i \in \rho(P_j) \qquad \Longleftrightarrow \qquad i \neq j, i, j = 0, \ldots, n.$$

Ortogonális helyzetű ponthalmazokról nyilván csak szimmetrikus és Hermite-féle polaritások esetén beszélhetünk.

6.18. Állítás. *Ha a ρ polaritás szimmetrikus vagy Hermite-féle, akkor létezik rá nézve ortogonális ponthalmaz.*

Bizonyítás. A koordinátarendszer megválasztásával (azaz projektív lineáris transzformációval, lásd a 6.13 lemmát) elérhetjük, hogy a ρ polaritás alakja $P(\boldsymbol{z}) \mapsto \bar{\boldsymbol{z}}^t C\boldsymbol{x} = 0$, ahol C nem-szinguláris diagonális mátrix. Ekkor az $E_0, \ldots, E_n$ alappontok egy ρ-ra nézve ortogonális pontrendszert alkotnak, hiszen

$$(\bar{\boldsymbol{e}}^{(i)})^t C\boldsymbol{e}^{(j)} = c_j (e^{(i)})^t \boldsymbol{e}^{(j)} = \begin{cases} 0 & \text{ha } i \neq j, \\ c_i & \text{ha } i = j. \end{cases}$$ □

Megjegyzés. Nem túl bonyolult az állítás bizonyítását kiegészíteni olyan módon, hogy a kitűnjön, hogy az valójában *ekvivalens* a 6.13 lemmával.

6.4. Kvadratikus felületek

6.19. Definíció. *A projektív tér*

$$Q = \{P(\boldsymbol{x}) : \boldsymbol{x}^t A\boldsymbol{x} = \sum_{i,j=0}^{n} a_{ij}x_i x_j = 0\}$$

alakú, azaz egy homogén, másodfokú polinommal megadható ponthalmazait projektív kvadratikus felületeknek *vagy röviden csak* kvadrikának *nevezzük.*

A definícióban ugyan nem szerepel az $A = (a_{ij})$ mátrix szimmetrikussága, azt azonban mindig feltételezhetjük, hiszen $x_i x_j = x_j x_i$ és a test karakterisztikája $\mathrm{char}(\mathbb{T}) \neq 2$. A továbbiakban mindig élni is fogunk az $A^t = A$ feltételezéssel, így könnyen adódik az alábbi állítás is.

6.20. Állítás. *Egy projektív Q kvadrika pontosan akkor áll elő szimmetrikus polaritás abszolút ponthalmazaként, ha nem-elfajuló.*

Bizonyítás. A 6.16 tétel (i) pontja szerint elegendő megmutatni, hogy minden nem-elfajuló kvadrikához tudunk szimmetrikus polaritást konstruálni. De ha Q nem-eljauló, akkor $\det(A) \neq 0$, és így a $P(\boldsymbol{z}) \mapsto H(A\boldsymbol{z}) : \boldsymbol{z}^t A\boldsymbol{x} = 0$ leképezés egy olyan szimmetrikus polaritást határoz meg, melynek abszolút ponthalmaza épp Q. □

A projektív kvadrikák egyik legalapvetőbb geometriai tulajdonsága az egyenesekkel vett metszeteiket érinti. Tekintsük ugyanis a $Q = \boldsymbol{x}^t A\boldsymbol{x} = 0$ kvadrikát és a $P(\boldsymbol{y})$, $R(\boldsymbol{z})$ pontokat összekötő egyenest. Ez utóbbi pontjai pontosan az $S(\lambda\boldsymbol{y} + \mu\boldsymbol{z})$ alakú pontok, ahol λ és μ nem lehet egyszerre nulla. $S \in Q$ akkor és csak akkor, ha

$$0 = (\lambda\boldsymbol{y} + \mu\boldsymbol{z})^t A(\lambda\boldsymbol{y} + \mu\boldsymbol{z}) = \lambda^2(\boldsymbol{y}^t A\boldsymbol{y}) + 2\lambda\mu(\boldsymbol{y}^t A\boldsymbol{z}) + \mu^2(\boldsymbol{z}^t A\boldsymbol{z}), \qquad (6.7)$$

ami egy homogén másodfokú polinom λ és μ változókban. Ha ez a polinom nem azonosan nulla, akkor lehet neki nulla, egy vagy kettő megoldása attól függően, hogy irreducibilis, teljes négyzetté alakítható, vagy

$$(a_1\lambda - b_1\mu)(a_2\lambda - b_2\mu), \qquad (a_1 : b_1) \neq (a_2 : b_2)$$

szorzatra bomlik. Ha a polinom azonosan nulla, akkor nyilván minden $(\mu : \lambda)$ megoldás, azaz a PR egyenes minden pontja Q-ban van. Egyébként az egyenes 0, 1 vagy 2 pontban metszi Q-t.

6.21. Definíció. *Azt mondjuk, hogy az e egyenes* kitérő *a Q kvadrikához, ha $|e \cap Q| = 0$,* metsző, *ha $|e \cap Q| = 2$, és* érintő, *ha $|e \cap Q| = 1$ vagy $e \subset Q$.*

A PR egyenes tehát akkor és csak akkor érintő, ha a (6.7) egyenletben szereplő polinom teljes négyzet vagy azonosan nulla, ami pedig ekvivalens azzal, hogy a diszkriminánsa nulla, azaz

$$(\boldsymbol{y}^t A\boldsymbol{z})^2 - (\boldsymbol{y}^t A\boldsymbol{y})(\boldsymbol{z}^t A\boldsymbol{z}) = 0. \tag{6.8}$$

6.22. Definíció. *A Q kvadrika P pontja* szinguláris, *ha minden P-re illeszkedő egyenes érinti Q-et.*

6.23. Állítás. *Az $Q : \boldsymbol{x}^t A\boldsymbol{x} = 0$ kvadratikus felület akkor és csak akkor nemelfajuló, ha nincs szinguláris pontja.*

Bizonyítás. Ha Q elfajuló, akkor $\det(A) = 0$, ami ekvivalens azzal, hogy valamilyen, nullától különböző $\boldsymbol{y}$ vektorra $\boldsymbol{0} = A\boldsymbol{y} = \boldsymbol{y}^t A$. Ekkor nyilván $P(\boldsymbol{y}) \in Q$; megmutatjuk, hogy ekkor P szinguláris. Egy tetszőleges $R(\boldsymbol{z})$ pont esetén ugyanis a (6.8) diszkrimináns nulla lesz, tehát a PR egyenes érintő.

Fordítva, ha $P(\boldsymbol{y}) \in Q$ szinguláris, akkor minden $R(\boldsymbol{z})$ pontra a (6.8) diszkriminánsnak nullának kell lennie, ami $\boldsymbol{y}^t A\boldsymbol{y} = 0$ miatt azt jelenti, hogy minden $\boldsymbol{z}$ vektor esetén $\boldsymbol{y}^t A\boldsymbol{z} = 0$. Ez nyilván másként nem lehetséges, csak ha az $\boldsymbol{y}^t A$ vektor nulla. De mivel $P(\boldsymbol{y})$ projektív pont, így $\boldsymbol{y}$ nem a nullvektor, tehát $A\boldsymbol{y} = \boldsymbol{0}$ csak $\det(A) = 0$ esetén állhat fenn; vagyis ekkor Q elfajuló. □

Megjegyzés. Ha az alaptestünk a $\mathbb{T} = \mathbb{C}$ komplex számtest, vagy bármelyik más *algebrailag zárt test*, akkor nem fordulhat elő, hogy a (6.7) egyenletben szereplő polinom irreducibilis, annak mindig van legalább egy megoldása. Geometriailag ez azt jelenti, hogy ilyen alaptest esetén a kvadrikáknak nincs kitérő egyenesük.

Az alfejezet hátralévő részében a kvadrikák

$$a_0 x_0^2 + \ldots + a_n x_n^2 = 0 \tag{6.9}$$

normál alakját vizsgáljuk meg tüzetesebben, mint látni fogjuk, ezekben a vizsgálatokban alaposan ki fogjuk használni a $\mathbb{T}$ alaptest speciális tulajdonságait.

1. eset: $\mathbb{T} = \mathbb{C}$

A legkönnyebb helyzet a $\mathbb{T} = \mathbb{C}$ komplex számok teste esetén áll elő. Ekkor ugyanis minden a_i együttható előáll, mint egy $b_i \in \mathbb{C}$ komplex szám négyzete: $a_i = b_i^2$. Az $y_0 = b_0 x_0, \ldots, y_n = b_n x_n$ helyettesítéssel bármely nem-elfajuló kvadrika

$$x_0^2 + \ldots + x_n^2 = 0$$

alakra hozható. Az elfajuló esetben a kvadrika alakja $x_0^2 + \ldots + x_k^2 = 0$, $k < n$ lesz. Ez azt is jelenti, hogy a $PG(n, \mathbb{C})$ térben bármely két nem-elfajuló kvadrikához létezik egy projektív lineáris transzformáció, amely az egyiket a másikba viszi.

2. eset: $\mathbb{T} = \mathbb{R}$

Kicsivel bonyolultabb a $\mathbb{T} = \mathbb{R}$ valós számok esete. Ekkor a változók felcserélésével először elérjük, hogy $a_0, \ldots, a_k > 0$, $a_{k+1}, \ldots, a_n < 0$ teljesüljön, majd az

$$y_0 = \sqrt{a_0}x_0, \ldots, y_k = \sqrt{a_k}x_n, \qquad y_{k+1} = \sqrt{-a_{k+1}}x_0, \ldots, y_n = \sqrt{-a_n}x_n$$

helyettesítés az

$$y_0^2 + \ldots + y_k^2 - y_{k+1}^2 - \ldots - y_n^2 = 0 \tag{6.10}$$

normálalakot eredményezi. A $\min\{k+1, n-k\}$ pozitív egész számot a kvadrika *szignatúrájának* nevezzük.

6.24. Állítás (Sylvester tétele). *A $PG(n, \mathbb{R})$ projektív tér $Q_1 : \boldsymbol{x}^t A_1 \boldsymbol{x} = 0$, $Q_2 : \boldsymbol{x}^t A_2 \boldsymbol{x} = 0$ nem-elfajuló kúpszeletei akkor és vihetők át egymásba projektív lineáris transzformációval, ha szignatúrájuk megegyezik.*

Bizonyítás. Tegyük először fel, hogy Q_1, Q_2 szignatúrája megegyezik, ekkor léteznek U_1, U_2 mátrixok által indukált lineáris transzformációk, melyre Q_1, Q_2 alakja (6.10), azaz

$$U_1^t A_1 U_1 = U_2^t A_2 U_2 = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & -1 \end{pmatrix}$$

teljesül. Ez azt jelenti, hogy az $U_2 U_1^{-1}$ mátrix által indukált transzformáció Q_1-et Q_2-be viszi át.

A fordított állítás bizonyítása technikaibb jellegű. Tételezzük most fel, hogy Q_i áttranszformálható egy Q_i' kvadrikába, melynek egyenelete (6.10) alakú ($i = 1, 2$), valamint Q_1 és Q_2 egymásba is áttranszformálhatóak. Ekkor Q_1' és Q_2' egymásba is áttranszformálható lesz, azaz létezik egy U mátrix, melyre $U^t C_1 U = C_2$, ahol C_1, C_2 diagonális mátrixok, melyek főátlójában először csupa 1, majd csupa -1 áll.

Jelölje $0, \ldots, k$ illetve $0, \ldots, \ell$ azokat az i indexeket, amelyekre $(C_1)_{ii} = 1$ illetve $(C_2)_{ii} = 1$. Legyen továbbá $\boldsymbol{f}^{(i)} = U\boldsymbol{e}^{(i)}$ ($i = 0, \ldots, n$). Ekkor fennáll

$$(\boldsymbol{e}^{(i)})^t C_1 \boldsymbol{e}^{(j)} = \begin{cases} 1 & \text{ha } 0 \le i = j \le k \\ -1 & \text{ha } k+1 \le i = j \le n \\ 0 & \text{ha } i \ne j \end{cases}$$

és

$$(\boldsymbol{f}^{(i)})^t C_1 \boldsymbol{f}^{(j)} = (\boldsymbol{e}^{(i)})^t U^t C_1 U \boldsymbol{e}^{(j)} = (\boldsymbol{e}^{(i)})^t C_2 \boldsymbol{e}^{(j)} = \begin{cases} 1 & \text{ha } 0 \le i = j \le \ell \\ -1 & \text{ha } \ell+1 \le i = j \le n \\ 0 & \text{ha } i \ne j \end{cases}$$

Szimmetria okoból nyilván feltehető $k \ge \ell$, a tétel bizonyításához azt kell belátnunk, hogy a szignatúrák megegyeznek, azaz $k = \ell$. Belátjuk, hogy az $\boldsymbol{e}^{(0)}, \ldots, \boldsymbol{e}^{(k)}, \boldsymbol{f}^{(\ell+1)}, \ldots, \boldsymbol{f}^{(n)}$ vektorok lineárisan függetlenek, ebből a tér dimenziója miatt azonnal adódni fog, hogy $k + 1 + (n - \ell) \le n + 1$, azaz $k \le \ell$, s így kész lesz a bizonyítás.

És csakugyan, az $\boldsymbol{e}^{(0)}, \ldots, \boldsymbol{e}^{(k)}, \boldsymbol{f}^{(\ell+1)}, \ldots, \boldsymbol{f}^{(n)}$ vektorok lineáris függősége azt jelentené, hogy nem csupa nulla $\lambda_0, \ldots, \lambda_k, \lambda_{\ell+1}, \ldots, \lambda_n \in \mathbb{R}$ valós számokra

$$\lambda_0 \boldsymbol{e}^{(0)} + \ldots + \lambda_k \boldsymbol{e}^{(k)} + \lambda_{\ell+1} \boldsymbol{f}^{(\ell+1)} + \ldots + \lambda_n \boldsymbol{f}^{(n)} = \boldsymbol{0}.$$

Ez más formában

$$\boldsymbol{z} = \lambda_0 \boldsymbol{e}^{(0)} + \ldots + \lambda_k \boldsymbol{e}^{(k)} = -\lambda_{\ell+1} \boldsymbol{f}^{(\ell+1)} - \ldots - \lambda_n \boldsymbol{f}^{(n)} \ne \boldsymbol{0},$$

ahonnan a fentiek ismeretében a $\boldsymbol{z}^t C_1 \boldsymbol{z}$ valós számra azt kapjuk, hogy

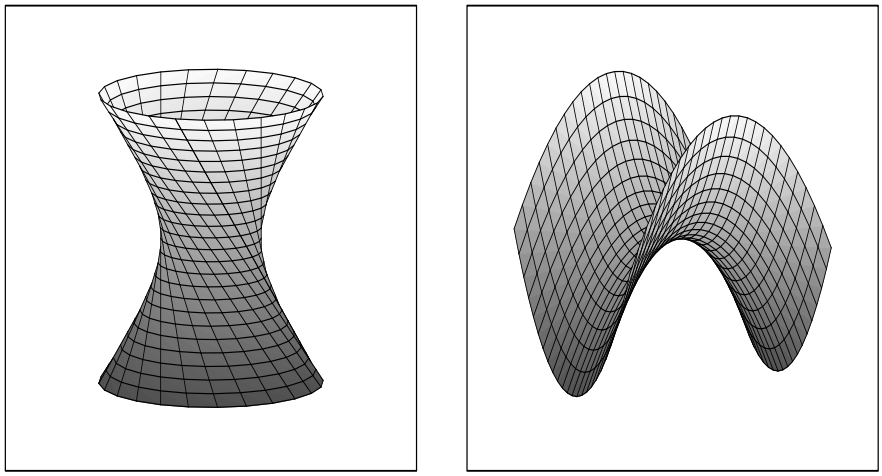
$$\begin{aligned} \boldsymbol{z}^t C_1 \boldsymbol{z} &= (\lambda_0 (\boldsymbol{e}^{(0)})^t + \ldots + \lambda_k (\boldsymbol{e}^{(k)})^t) C_1 (\lambda_0 \boldsymbol{e}^{(0)} + \ldots + \lambda_k \boldsymbol{e}^{(k)}) \\ &= \lambda_0^2 + \ldots + \lambda_k^2 \\ &= (-\lambda_{\ell+1} (\boldsymbol{f}^{(\ell+1)})^t - \ldots - \lambda_n (\boldsymbol{f}^{(n)})^t) C_1 (-\lambda_{\ell+1} \boldsymbol{f}^{(\ell+1)} - \ldots - \lambda_n \boldsymbol{f}^{(n)}) \\ &= -\lambda_{\ell+1}^2 - \ldots - \lambda_n^2. \end{aligned}$$

Ezek összevetéséből $\lambda_0^2 + \ldots + \lambda_k^2 + \lambda_{\ell+1}^2 + \ldots + \lambda_n^2 = 0$ adódik, ellentmondván annak a feltételezésünknek, hogy nem minden λ_i nulla. □

Megjegyzés. Megfigyelhettük, hogy a valós projektív térben kvadrikának tekintjük az $x_0^2 + \ldots + x_n^2 = 0$ egyenlettel meghatározott ponthalmazt, jóllehet az üres! Ezzel együtt az állításunk szerint az n-dimenziós valós projektív térben a lényegesen különböző (azaz egymásba át nem transzformálható) kvadrikák száma $n/2$ illetve $(n-1)/2$, attól függően, hogy n páros illetve páratlan.

Tanulságos konkrétan is megvizsgálni a 3-dimenziós valós projektív tér nem-elfajuló kvadrikáit. Az imént említett *üres halmaz* egyenlete $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 0$, ennek szignatúrája 0. A *gömb* affin térbeli egyenlete $x_1^2 + x_2^2 + x_3^2 = 1$, ami a projektív térben $x_0^2 - x_1^2 - x_2^2 - x_3^2 = 0$ alakra módosul. Más szóval a gömb szignatúrája 1.

2 szignatúrájú kvadrikára példa a *nyeregfelület*, ennek affin alakja $x_1 = x_2 x_3$, projektív egyenlete pedig $x_0 x_1 - x_2 x_3 = 0$. Projektíven ezzel ekvivalens az $x_0^2 + x_1^2 - x_2^2 - x_3^2 = 0$ alak, aminek viszont az affin változata



6.1. ábra. Az egyköpenyű hiperboloid és a nyeregfelület.

$-x_1^2 + x_2^2 + x_3^2 = 1$. Ezt a felületet megkaphatjuk oly módon is, hogy az x_1x_2 -síkbeli $-x_1^2 + x_2^2 = 1$ hiperbolát megforgatjuk az x_2-tengely körül, ezért nevezzük őt *forgási* vagy *egyköpenyű hiperboloidnak* is. (Ld. a 6.1 ábrát.)

A nyeregfelület és a forgási hiperboloid projektíven egymásba transzformálhatók, de a valós affin térben ezek két lényegesen különböző kvadrika. A különbséget a végtelen távoli síkkal vett metszetük adja, a nyeregfelület azt két egyenesben, míg az egyköpenyű hiperboloid egy nemelfajuló kúpszeletben metszi.

3. eset: $\mathbb{T} = \mathbb{F}_q$, q páratlan

A legérdekesebb számolással a véges testek esetében találkozunk, s azzal mindjárt az elején. A továbbiakban q páratlan prímhatvány.

6.25. Lemma. *Egy $\mathbb{F}_q$ véges test minden nullától különböző eleme előáll $x^2 + y^2$ $(x, y \in \mathbb{F}_q)$ alakban.*

Bizonyítás. Jelöljük N-nel a $\mathbb{F}_q$-beli nullától különböző négyzetek halmazát. Először megmutatjuk, hogy létezik $a \in \mathbb{F}_q^* \setminus N$ elem, amely előáll $y^2 + 1$ alakban. Tegyük fel ugyanis ennek az ellenkezőjét és tekintsük az

$$X = \{(x, y) \in \mathbb{F}_q^2 : x^2 = y^2 + 1\}$$

halmazt. Az indirekt feltétel szerint minden $y \in \mathbb{F}_q$ esetén megoldható x-ben az $x^2 = y^2 + 1$ egyenlet, ráadásul legfeljebb két eset kivételével két különböző megoldásunk van, nevezetesen x és $-x$. A két kivétel $y^2 = -1$ esetén léphet fel. Ez azt jelenti, hogy az X halmaznak legalább $2q - 2$ eleme van: $|X| \geq 2q - 2$.

Másrészről definiálhatjuk az $f : X \to \mathbb{F}_q^*$, $(x, y) \mapsto x - y$ leképezést. ($x = y$ nyilván nem lehetséges $x^2 = y^2 + 1$ esetén.) Megmutatjuk, hogy f injektív. Valóban, az $a = x - y \neq 0$ érték az $x^2 = y^2 + 1$ feltétel mellett egyértelműen meghatározza az $x + y = 1/(x - y) = a^{-1}$ összeg értékét is. Így kapjuk, hogy

$$x = \frac{a + a^{-1}}{2}, \qquad y = \frac{-a + a^{-1}}{2}$$

kell teljesüljön, azaz (x, y) egyértelműen meg van határozva. Injektív leképezés esetén az értelmezési tartomány számossága legfeljebb akkora, mint a képhalmazé, azaz $|X| \leq q - 1$. A fentivel összevetve $2q - 2 \leq q - 1$, azaz $q \leq 1$ adódik, ami lehetetlenség.

Rögzítsünk most egy fentiek szerint létező $a = y^2 + 1 \neq 0$, $a \notin N$ elemet. Nyilván minden $b = c^2 \in N$ előáll két négyzetszám összegeként: $b = c^2 + 0^2$. Abban az esetben, ha $b \notin N$, $b \neq 0$, $b = g^{2k+1}$ alakban írható, ahol q az $\mathbb{F}_q^*$ ciklikus multiplikatív csoport generátoreleme, lásd a 3.6 tételt. Hasonlóan, az a nem-négyzet előáll, mint $a = g^{2\ell+1}$. Ebből adódik, hogy $c = g^{k-\ell}$ elemre $a^{-1}b = c^2 \in N$. Ebből megkapjuk a b elem

$$b = ac^2 = (y^2 + 1)c^2 = (yc)^2 + c^2$$

felírását két elem négyzetösszegeként. □

6.26. Lemma. *Rögzítsünk egy olyan $a \in \mathbb{F}_q$ elemet, amely egyetlen $\mathbb{F}_q$-beli elemnek sem a négyzete és legyenek k, ℓ egész számok, amelyekre $2|\ell$ és $0 \leq \ell \leq 2k$. Ekkor az*

$$Q : x_0^2 + \ldots + x_\ell^2 + ax_{\ell+1}^2 + \ldots + ax_{2k}^2 = 0$$

kvadrika lineáris transzformációval

$$\pm x_0^2 - x_1^2 - \ldots - x_k^2 + x_{k+1}^2 + \ldots + x_{2k}^2 = 0$$

alakra hozható.

Bizonyítás. A 6.25 lemma szerint léteznek $b, c \in \mathbb{F}_q$ elemek, amelyre $a = b^2 + c^2$, és $b, c \neq 0$, mert a nem négyzet. A

$$(b^2 + c^2)(x_{2i+1}^2 + x_{2i+2}^2) = (bx_{2i+1} + cx_{2i+2})(cx_{2i+1} - bx_{2i+2})$$

összefüggés felhasználával, alkalmazva az

$$\begin{array}{ll} y_i = x_i & \text{ha } i = 0, \ldots, \ell, \\ y_{2i+1} = bx_{2i+1} + cx_{2i+2}, & \\ y_{2i+2} = cx_{2i+1} - bx_{2i+2} & \text{ha } i = \ell/2, \ldots, k-1 \end{array}$$

behelyettesítést, a Q új alakja

$$y_0^2 + \ldots + y_{2k}^2 = 0.$$

Ha -1 négyzet $\mathbb{F}_q$-ban, akkor innen triviálisan megkapható a kívánt alak. Tételezzük fel most, hogy -1 nem négyzet $\mathbb{F}_q$-ban és válasszuk meg az e, f nullától különböző elemeket úgy, hogy $-1 = e^2 + f^2$. Legyen továbbá $s = 1$ ha k páros és $s = 0$ ha k páratlan és tekintsük az alábbi behelyettesítést.

$$\begin{array}{ll} y_{2i+s} = bz_{2i+s} + cz_{2i+s+1}, & \\ y_{2i+s+1} = cz_{2i+s} - bz_{2i+s+1} & \text{ha } i = 0, \ldots, \frac{k-1-s}{2}, \\ y_i = z_i & \text{ha } i = k+1, \ldots, 2k \text{ vagy } i = 0 \text{ és } s = 1. \end{array}$$

Az

$$y_{2i+s}^2 + y_{2i+s+1}^2 = (e^2 + f^2)(z_{2i+s}^2 + z_{2i+s+1}^2) = -z_{2i+s}^2 - z_{2i+s+1}^2$$

egyenlőség miatt a behelyettesítést alkalmazva a Q egyenletére kapott alak

$$\begin{array}{ll} z_0^2 - z_1^2 - \ldots - z_k^2 + z_{k+1}^2 + \ldots + z_{2k}^2 = 0 & \text{ha } k \text{ páros, azaz } s = 1, \\ -z_0^2 - z_1^2 - \ldots - z_k^2 + z_{k+1}^2 + \ldots + z_{2k}^2 = 0 & \text{ha } k \text{ páratlan, azaz } s = 0; \end{array}$$

pontosan a lemmában szereplő állítás szerint. □

6.27. Tétel. *Legyen $Q : \boldsymbol{x}^t A\boldsymbol{x} = 0$ a $PG(n, \mathbb{F}_q)$ projektív tér nem-elfajuló kvadrikája. Ekkor egy lineáris transzformációval Q az alábbi normálalakok egyikére hozható.*

(i) Ha $n = 2k$ páros, akkor

$$Q : x_0^2 + x_1x_2 + \ldots + x_{2k-1}x_{2k} = 0.$$

Ebben az esetben parabolikus kvadrikáról *beszélünk.*

(ii) H $n = 2k + 1$, akkor

$$Q^+ : x_0x_1 + x_2x_3 + \ldots + x_{2k}x_{2k+1} = 0$$

vagy

$$Q^- : f(x_0, x_1) + x_2x_3 + \ldots + x_{2k}x_{2k+1} = 0,$$

ahol $f(x_0, x_1) = ax_0^2 + bx_0x_1 + cx_1^2$ irreducibilis másodfokú polinom a $\mathbb{F}_q$ test felett. A Q^+ esetben hiperbolikus, *a Q^- esetben pedig* elliptikus kvadrikáról *beszélünk.*

Bizonyítás. Tekintsük először az $n = 2k$ esetet. Ekkor a 6.26 lemma közvetlen alkalmazásával és esetleg egy -1-el való szorzás, illetve a változók felcserélésével adódik az

$$x_0^2 - x_1^2 - \ldots - x_k^2 + x_{k+1}^2 + \ldots + x_{2k}^2 = 0$$

alak. Innen az

$$y_0 = x_0,\ y_i = -x_i + x_{k+i},\ y_{k+i} = x_i + x_{k+i},\ i = 1, \ldots, k$$

helyettesítéssel kapjuk az

$$y_0^2 + y_1 y_{k+1} + \ldots + y_k y_{2k} = 0$$

alakot, ami a tételben szereplőtől csak a változók sorrendjében tér el.

Legyen most $n = 2k + 1$ páratlan szám és tételezzük fel, hogy Q-t már $a_0 x_0^2 + \ldots + a_n x_n^2 = 0$ alakra hoztuk. A 6.26 lemma alapján tudjuk, hogy a $PG(n-1, \mathbb{F}_q)$ projektív térnek létezik egy $U = (u_{ij})_{i,j=0}^{n-1}$ mátrix által indukált $\boldsymbol{y} = U\boldsymbol{x}$ lineáris transzformációja, amellyel az $a_0 x_0^2 + \ldots + a_{2k} x_{2k}^2 = 0$ kvadrika

$$\pm x_0^2 - x_1^2 - \ldots - x_k^2 + x_{k+1}^2 + \ldots + x_{2k}^2 = 0$$

alakra hozható. Alkalmazva az

$$y_i = u_{i0} x_0 + \ldots + u_{i,n-1} x_{n-1}, \qquad i = 0, \ldots, n-1, \qquad y_n = x_n$$

majd a

$$z_0 = y_0,\ z_n = y_n,\ z_i = -y_i + y_{k+i},\ z_{k+i} = y_i + y_{k+i},\ i = 1, \ldots, k$$

behelyettesítéseket, Q alakja először az

$$\pm y_0^2 - y_1^2 - \ldots - y_k^2 + y_{k+1}^2 + \ldots + y_{2k}^2 + a_{2k+1} y_{2k+1}^2 = 0,$$

majd a

$$\pm z_0^2 + z_1 z_{k+1} + \ldots + z_k z_{2k} + a_{2k+1} z_{2k+1}^2 = 0$$

alakot veszi fel. A változók felcserélésével ebből megkaphatjuk az

$$a x_0^2 + b x_1^2 + x_2 x_3 + \ldots + x_{2k} x_{2k+1} = 0 \tag{6.11}$$

alakot, ahol $a = \pm 1$ és $b = a_{2k+1}$. Világos, hogy ha $-\frac{a}{b}$ nem négyzetszám, akkor az $a x_0^2 + b x_1^2 = 0$ egyenletnek nincs megoldása az $\mathbb{F}_q$ test felett, azaz $\mathbb{F}_q$ felett irreducibilis. Ekkor megkaptuk az elliptikus kvadrika esetét.

Ha létezik olyan $f \in \mathbb{F}_q$ elem, amelyre $-\frac{a}{b} = f^2$, akkor

$$ax_0^2 + bx_1^2 = ax_0^2 - af^2x_1^2 = (ax_0 - afx_1)(x_0 + fx_1),$$

azaz az

$$y_0 = ax_0 - afx_1,\ y_1 = x_0 + fx_1,\ y_i = x_i,\ i = 2, \ldots, n$$

helyettesítás leszállítja a kívánt

$$y_0y_1 + y_2y_3 + \ldots + y_{n-1}y_n = 0$$

hiperbolikus kvadrika alakot.

Végezetül meg kell még mutatnunk, hogy a páratlan dimenzióban fellépő két normálalak egymásba nem transzformálható át. Mindkét esetet felöleli a (6.11) egyenletben szereplő alak. Ennek mátrixa

$$\begin{pmatrix} a & 0 & & & & & \\ 0 & b & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ & & & & & 1 & 0 \end{pmatrix}$$

melynek determinánsa $ab(-1)^k$. Rögzített dimenzió esetén tehát már a mátrix determinánsa eldönti, hogy $-ab$ négyzet-e vagy sem. Mivel ez utóbbi ekvivalens azzal, hogy $-\frac{a}{b}$ négyzet-e vagy sem, az a tény, hogy a kvadrikát meghatározó mátrix determinánsa négyzet-e, meghatározza, hogy elliptikus vagy hiperbolikus kvadrikáról van-e szó. Lineáris transzformáció esetén pedig a kvadrika mátrixa $A \mapsto U^tAU$ formában tud változni, tehát az a tulajdonság, hogy $\det(A)$ négyzetszám $\mathbb{F}_q$-ban, változatlan marad. Ez azt jelenti, hogy egy elliptikus kvadrika nem transzformálható át hiperbolikus kvadrikába. □

A véges test feletti projektív tér nem-elfajuló kvadrikáiról tehát az alábbit mondhatjuk el. Ha a tér dimenziója páros, akkor bármely két nem-elfajuló kvadrika áttranszformálható egymásba projektív lineáris transzformációval. Ha a tér dimenziója páratlan, akkor a térben két lényegesen különböző nem-elfajuló kvadrika van, és bármely másik áttranszformálható a kettő közül az egyikbe.

Az elliptikus és a hiperbolikus kvadrikákat kiválóan tudjuk szemléltetni a 3-dimenziós valós projektív térben is. Az elliptikus esetet a *gömb*, a hiperbolikusat pedig az *egyköpenyű hiperboloid* szemlélteti, ld. a 6.1 ábrát.