Moufang-féle síkok, oktávalgebrák

Vendégtanári előadás
a Sapientia Erdélyi Magyar Tudományegyetem
szervezésében

Előadó: Dr. Nagy Gábor, SZTE Bolyai Intézet

2002. december 1.

Tartalomjegyzék

1. Absztrakt síkok

A mi tárgyalásunkban **absztrakt síkon** egy $(\mathscr{P}, \mathscr{L}, \mathrm{I})$ halmazokból álló hármast értünk, ahol $\mathscr{P}$ és $\mathscr{L}$ diszjunkt halmazok, az $\mathrm{I} \subset \mathscr{P} \times \mathscr{L}$ pedig a $\mathscr{P}$ és $\mathscr{L}$ halmazokon értelmezett reláció. $\mathscr{P}$ elemeit a sík *pontjainak*, $\mathscr{L}$ elemeit a sík *egyeneseinek* nevezzük, $P \in \mathscr{P}$, $\ell \in \mathscr{L}$, $P \,\mathrm{I}\, \ell$ esetén pedig azt mondjuk, hogy a P pont *illeszkedik* az ℓ egyenesre. Használatos még a *P az ℓ egyenesen fekszik,* illetve a *P az ℓ egyenes pontja* szófordulat.

Ha az ℓ illeszkedik a P és Q pontokra, akkor azt is mondjuk, hogy *összeköti* a két pontot. Amennyiben egyetlen P-t és Q-t összekötő egyenes van, akkor azt PQ-val jelöljük. Két egyenes közös pontjait *metszéspontoknak* is nevezzük. Ha P az egyetlen olyan pont, amely illeszkedik az ℓ és m egyenesekre, akkor a $P = \ell \cap m$ jelölés használatos. Két egyenest *párhuzamosnak* mondunk, ha megegyeznek vagy nincs közös pontjuk; ennek jele $\ell \parallel m$. A $P_1, \ldots, P_k$ pontokat *kollineárisnak* nevezzük, ha létezik egy mindegyikre illeszkedő egyenes. A $P_1, \ldots, P_k$ pontokat *általános helyzetűnek* mondjuk, ha közölük semelyik három nem kollineáris.

Az absztrakt sík fogalma sokkal általánosabb a hétköznapi síkfogalomnál. Az alábbi definíciók már közelebb visznek bennünket ehhez.

1.1. Definíció. *A $\Pi = (\mathscr{P}, \mathscr{L}, \mathrm{I})$ absztrakt síkot* **affin síknak** *nevezzük, ha teljesülnek az alábbi tulajdonságok (axiómák).*

(A1) Két különböző ponthoz egyetlen összekötő egyenes létezik.

(A2) Két különböző egyenesnek legfeljebb egy közös pontja van.

(A3) Adott P ponthoz és ℓ egyeneshez pontosan egy P-re illeszkedő, ℓ-el párhuzamos egyenes létezik. (Párhuzamossági axióma.)

(A4) Létezik három, nem egy egyenesre illeszkedő pont.

1.2. Definíció. *A $\Pi = (\mathscr{P}, \mathscr{L}, \mathrm{I})$ absztrakt síkot* **projektív síknak** *nevezzük, ha teljesülnek az alábbi tulajdonságok (axiómák).*

(P1) Két különböző ponthoz egyetlen összekötő egyenes létezik.

(P2) Két különböző egyenesnek pontosan egy közös pontja van.

(P3) Létezik négy általános helyzetű pont.

Röviden elmagyarázzuk azt a módszert, amely kapcsolatot teremt affin és projektív síkok között.

Legyen $\Pi = (\mathscr{P}, \mathscr{L}, \mathrm{I})$ projektív sík és rögzítsünk egy tetszőleges ℓ_∞ egyenest. Definiáljuk a $\mathscr{P}^* = \mathscr{P} \setminus \{P \mid P \,\mathrm{I}\, \ell\}$, $\mathscr{L}^* = \mathscr{L} \setminus \{\ell_\infty\}$ halmazokat és legyen I^* az I megszorítása $\mathscr{P}^* \times \mathscr{L}^*$-ra. Ekkor $\Pi^* = (\mathscr{P}^*, \mathscr{L}^*, \mathrm{I}^*)$ affin sík. Valóban, két Π^*-beli egyenes akkor és csak akkor párhuzamos, ha Π-beli metszéspontjuk illeszkedik ℓ_∞-re.

Ezen eljárás megfordítása az alábbi. Legyen $\Pi = (\mathscr{P}, \mathscr{L}, \mathrm{I})$ affin sík. Mint minden affin síkon, a párhuzamosság itt is ekvivalencia-reláció $\mathscr{L}$-en, nevezzük a párhuzamossági osztályokat *végtelen távoli pontoknak*, jelölje ezek halmazát ℓ_∞. Legyen $\mathscr{P}^* = \mathscr{P} \cup \ell_\infty$ és $\mathscr{L}^* = \mathscr{L} \cup \{\ell_\infty\}$. Értelmezzük az I^* illeszkedési relációt az alábbi módon

$$P \,\mathrm{I}^*\, \ell \iff \begin{cases} P \in \mathscr{P}, \ell \in \mathscr{L}, P \,\mathrm{I}\, \ell; \\ P \in \ell_\infty, \ell \in \mathscr{L}, \ell \in P; \\ P \in \ell_\infty, \ell = \ell_\infty. \end{cases}$$

Ekkor $\Pi^* = (\mathscr{P}^*, \mathscr{L}^*, \mathrm{I}^*)$ projektív sík. Ezt a Π *projektív lezártjának* is hívjuk. Az ℓ_∞ egyenest *végtelen távoli egyenesnek*, ennek pontjait pedig *végtelen távoli pontoknak* nevezzük.

Ezekkel a műveletekkel lényegében megfeleltethetjük egymásnak a projektív és az affin síkok osztályait, de szem előtt kell tartanunk, hogy míg a projetív lezárás egyértelmű, addig az inverz függ az ℓ_∞ egyenes megválasztásától.

Tekintsünk példákat affin és projektív síkra. Mindkét esetben igaz, hogy az egyeneseket azonosíthatjuk a rájuk illeszkedő pontok halmazával, azaz feltehetjük, hogy $\mathscr{L} \subset 2^{\mathscr{P}}$ és $P \,\mathrm{I}\, \ell \Leftrightarrow P \in \ell$.

Rögzítsük a tetszőleges K testet és definiáljuk az alábbi halmazokat.

$$\begin{aligned}
&\mathscr{P}_a = \mathsf{K} \times \mathsf{K}, \\
&\mathscr{L}_a = \{\{(x,y) \in \mathsf{K}^2 \mid y = mx + b\} \mid m, b \in \mathsf{K}\} \cup \{\{(c,y) \mid y \in \mathsf{K}\} \mid c \in \mathsf{K}\},
\end{aligned}$$

valamint

$$\begin{aligned}
&\mathscr{P}_{\text{proj}} = \{(x:y:z) \mid x,y,z \in \mathsf{K}, (x,y,z) \neq (0,0,0)\}, \\
&\mathscr{L}_{\text{proj}} = \{\{(x:y:z) \mid ax + by + cz = 0\} \mid a,b,c \in \mathsf{K}, (a,b,c) \neq (0,0,0)\},
\end{aligned}$$

ahol $(x:y:z) = \{\lambda(x,y,z) \mid \lambda \in \mathsf{K} \setminus \{0\}\}$ az $(x,y,z) \neq (0,0,0)$ hármas által meghatározott *homogén számhármas.* Ekkor $\Pi_a = (\mathscr{P}_a, \mathscr{L}_a, \in)$, valamint $\Pi_{\text{proj}} = (\mathscr{P}_{\text{proj}}, \mathscr{L}_{\text{proj}}, \in)$ a K *testre épített affin* illetve *projektív síkok.* Π_a projektív lezártja Π_{proj}, ebben pedig bármely végtelen távoli egyenes kijelölése esetén a fenti eljárás Π_a-val izomorf affin síkot eredményez.

2. Osztásgyűrűk, algebrák

A testre épített affin sík konstrukciójában az axiómák ellenőrzésekor messze nem használjuk ki az összes testtulajdonságot. A következő definíció a test foglamát általánosítja, bár megjegyezzük, hogy ebben a jegyzetben nem célunk a legnagyobb általánosság tárgyalása.

2.1. Definíció. *A két darab bináris művelettel felruházott $R = (R, +, \cdot)$ halmazt* **osztásgyűrűnek** *nevezzük, ha az alábbiak teljesülnek.*

(D1) $(R, +)$ *Abel-csoport* $0 \in R$ *neutrális elemmel.*

(D2) *Mindkét oldalon teljesül a disztributivitás, azaz minden $x, y, z \in R$ esetén fennáll $x(y+z) = xy + xz$ és $(x+y)z = xz + yz$.*

(D3) *Tetszőleges $a \in R \setminus \{0\}$, $b \in R$ esetén az $ax = b$ és $ya = b$ egyenletek egyértelműen megoldhatók R-ben x-re és y-ra.*

2.2. Állítás. *Legyen R osztásgyűrű. Ekkor a $\mathscr{P} = R^2$, $\mathscr{L} = \{\{(x,y) \in R^2 \mid y = mx + b\} \mid m, b \in R\} \cup \{\{(c,y) \mid y \in R\} \mid c \in R\}$ választással a $\Pi(R) = (\mathscr{P}, \mathscr{L}, \in)$ hármas affin síkot alkot.* $\square$

A $\Pi(R)$ síkot *az R osztásgyűrűvel koordinátázott affin síknak* nevezzük. Itt azonnal felmerül az R gyűrű algebrai tulajdonságai és a sík geometriai tulajdonságai között fennálló kapcsolatra vonatkozó kérdés. Mielőtt ezt tárgyalnánk, adunk néhány igen fontos, klasszikusnak nevezhető példát osztásgyűrűre. Ezen példák közös vonása, egyben vektorterek a valós számtest felett, és a vektortér struktúra összhangban van az osztásgyűrű struktúrájával.

2.3. Definíció. *A K test feletti A vektorteret* K **feletti algebrának** *vagy röviden csak* K**-algebrának** *nevezzük, ha értelmezve van benne a szorzásnak nevezett bilineáris $(x,y) \mapsto x\cdot y = xy$ művelet.*

2.4. Definíció. *Az A K-algebrát* **osztásalgebrának** *hívjuk, ha minden $a,b \in A$, $a \neq 0$ elemekre az $ax = b$, $ya = b$ egyenletek egyértelműen megoldhatók x-re és y-ra.*

Nyilván minden osztásalgebra egyben osztásgyűrű is. Az is világos, hogy a K test bármely L (kommutatív) testbővítése tekinthető K feletti osztásalgebrának. Eszerint a legkézenfekvőbb példa osztásalgebrára a **komplex számok** $\mathbb{C}$ teste. Ezt követi a **kvaterniók** $\mathbb{H}$ ferdetestje.

Tekintsük az $\mathbb{R}$ feletti 4-dimenziós $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ vektorteret. Értelmezzük a szorzásműveletet a $\{1,i,j,k\}$ bázison az alábbi táblázat alapján, majd terjesszük ki a teljes térre bilineáris módon:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Azonnal látszik, hogy 1 egységeleme $\mathbb{H}$-nak, az asszociativitás pedig számolással leellenőrizhető.

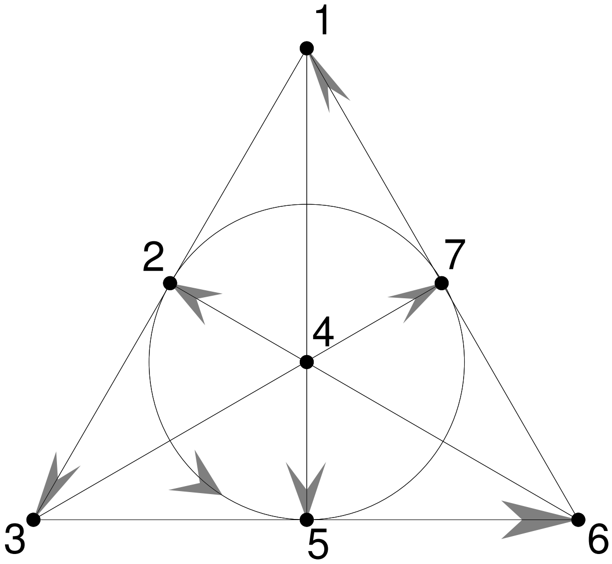
Megjegyzés. Az asszociativitás feltételezése mellett a művelet az $i^2 = j^2 = k^2 = ijk = -1$ relációkkal is megadható.

Definiáljuk a $\mathbb{H} \to \mathbb{H}$,

$$z = x_0 + x_1 j + x_2 j + x_3 k \mapsto \overline{z} = x_0 - x_1 j - x_2 j - x_3 k$$

$\mathbb{R}$-lineáris leképezést, ekkor nyilván $\overline{\overline{z}} = z$ teljesül minden $z \in \mathbb{H}$ esetén. Ezt a leképezést – a komplex számtest analógiájára – *konjugálásnak* nevezzük. Könnyen megmutatható az is, hogy tetszőleges $z_1, z_2 \in \mathbb{H}$ elemekre $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ és $\overline{z_1 \cdot z_2} = \overline{z_2} \cdot \overline{z_1}$ áll fenn, azaz a konjugálás a $\mathbb{H}$ algebra *antiautomorfizmusa*.

Végezetül vegyük észre, hogy minden $z = x_0 + x_1 j + x_2 j + x_3 k \in \mathbb{H}$ elem esetén $N(z) = z\overline{z} = x_0^2 + x_1^2 + x_2^2 + x_3^2$ nem-negatív valós szám, ami csakis a $z = 0$ esetben



1. ábra. Az oktávok „szorzótáblája”.

nulla. Mivel a konjugálás antiautomorfizmus, az $\mathbb{R}$ elemei pedig bármely más elemmel felcserélhetők, ezért tetszőleges $z_1, z_2 \in \mathbb{H}$-ra

$$N(z_1 z_2) = z_1 z_2 \overline{z_1 z_2} = z_1 N(z_2) \overline{z_2} = N(z_1) N(z_2)$$

áll fenn. Az $N : \mathbb{H} \to \mathbb{R}$ leképezést *normának* nevezzük, az utóbbi tulajdoságról pedig azt mondjuk, hogy az N norma *multiplikatív*.

Tekintsünk most egy tetszőleges 0-tól különböző $z \in \mathbb{H}$ elemet. Ekkor $N(z) \neq 0$ valós szám és a $z' = \overline{z}/N(z)$ a $\mathbb{H}$ egy jól meghatározott eleme, amelyre teljesül $zz' = z'z = 1$. A $\mathbb{H} \setminus \{0\}$ halmaz tehát a szorzásra nézve egy nem-kommutatív csoportot alkot, ami azt jelenti, hogy $\mathbb{H}$ ferdetest.

Megjegyzés. Ugyanezekkel a tulajdonságokkal rendelkezik a $z \to \overline{z}$ komplex konjugálás és az $N(z) = z\overline{z}$ komlpex norma is, azzal a különbséggel, hogy a szorzásművelet kommutativitása miatt a konjugálás automorfizmus. Triviális, de fontos észrevétel, hogy $\mathbb{R}, \mathbb{C} = \mathbb{R} + \mathbb{R}i$ a $\mathbb{H}$ részalgebrái.

Vegyük észre, hogy a valós számokból kiindulva, az egyes lépésekben a dimenzió megkétszeresével konstruálunk új osztásalgebrákat. Ennek ára mindkét esetben egy „szép” tulajdonság elvesztése: először a test teljes rendezése, majd a szorzásművelet kommutativitása megy veszendőbe. Mint látni fogjuk, a lépésünket ismételten megtehetjük, ekkor azonban már a szorzásművelet asszociativiásától is el kell búcsúznunk.

Legyen $\{1, e_1, \ldots, e_7\}$ az $\mathbb{R}$ feletti 8-dimenziós vektortér egy bázisa. Az 1. ábra segítségével definiáljuk a báziselemek szorzatait az alábbi módon. $1^2 = 1$, $1e_i = e_i 1 = e_i$, $e_i^2 = -1$ és $e_i e_j = -e_j e_i = e_k$ azon (i, j, k) hármasokra, amelyek az 1. ábrán egy megfelelően irányított blokkot határoznak meg. Például $e_4 e_6 = e_1$, míg $e_7e_6 = -e_1$. Ezt a szorzásműveletet a teljes térre bilineárisan kiterjesztve kapjuk az **oktávok osztásalgebráját.** Ennek jele az irodalomban $\mathbb{O}$.

Könnyen meggondolható, hogy ha az $\{i, j, k\}$ hármas egy az 1. ábrán szereplő blokkot határoz meg, akkor $\mathbb{R}+\mathbb{R}e_i+\mathbb{R}e_j+\mathbb{R}e_k$ altér egy $\mathbb{H}$-val izomorf részalgebra $\mathbb{O}$-ban.

Az $z = x_0 + x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4 + x_5e_5 + x_6e_6 + x_7e_7$ elem konjugáltja definíció szerint

$$\bar{z} = x_0 - x_1e_1 - x_2e_2 - x_3e_3 - x_4e_4 - x_5e_5 - x_6e_6 - x_7e_7,$$

míg a normája

$$N(z) = z\bar{z} = x_0^2 + x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 + x_7^2.$$

Közvetlen számolással adódik, hogy a konjugálás ismét antiautomorfizmus, a norma pedig multiplikatív. Ha most a és b nullától különböző $\mathbb{O}$-beli elemek, akkor $N(a)$ és $N(b)$ pozitív valós számok, s így $N(ab) = N(a)N(b)$ és ab sem lehet nulla. Ez azt jelenti, hogy $\mathbb{O}$ nullaosztómentes, vagyis az $L_a : x \mapsto ax$ leképezés injektív $\mathbb{R}$-lineáris transzformáció $\mathbb{O}$-n. Mivel $\mathbb{O}$ véges dimenziós vektortér $\mathbb{R}$ felett, így L_a invertálható, azaz az $ax = b$ egyenlet egyetlen megoldása $x = L_a^{-1}(b)$. Hasonlóan megmutatható $ya = b$ egyértelmű megoldhatósága, tehát $\mathbb{O}$ osztásalgebra. Végezetül, $(e_1e_2)e_4 = e_7$, $e_1(e_2e_4) = -e_7$ mutatja, hogy $\mathbb{O}$ nem asszociatív.

A legtöbb ember számára szokatlan nem asszociatív bináris műveletekkel dolgozni. Néhány própálkozás meggyőzhet bennünket arról, hogy számos korábban használt módszer sikertelen lesz. Szerencsére az oktávok esetén az asszociativitás helyére annak egy gyengébb változata kerül, ami azonban megfelelő módszerekkel majdnem olyan hasznossá tehető.

2.5. Definíció. *Az R nem feltételenül asszociatív gyűrűt* **alternáló gyűrűnek** *nevezzük, ha az*

$$(xx)y = x(xy), \qquad (xy)x = x(yx), \qquad (xy)y = x(yy) \tag{1}$$

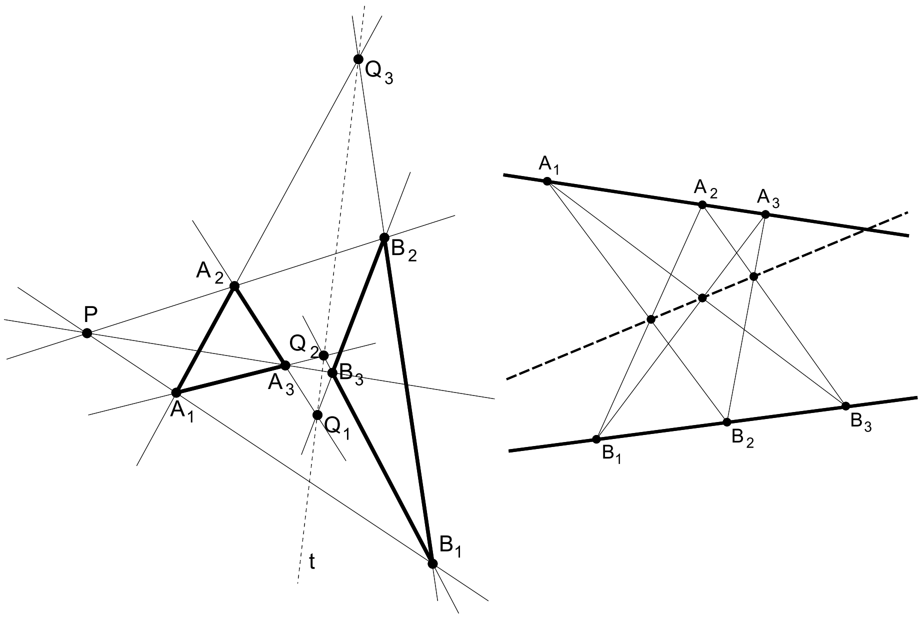
azonosságok teljesülnek minden $x, y \in R$ elemre.

A R gyűrűn értelmezzük az $[x,y,z] = (xy)z - x(yz)$ **asszociátor-zárójelet.** Ez a disztributivitás miatt minden változójába additív, algebra esetén pedig trilineáris is.

Ennek az észrevételnek segítségével az alternáló tulajdonságot az $[x,x,y] = [x,y,x] = [x,y,y] = 0$ egyenlőségek fejezik ki. Ezek nem additív (lineáris) azonosságok, azonban egy *polarizálásnak* nevezett trükkel additívvá (lineárissá) tehetők:

$$0 = [x+y, x+y, z] = [x,x,z] + [x,y,z] + [y,x,z] + [y,y,z] = [x,y,z] + [y,x,z],$$

vagyis $[x,y,z] = -[y,x,z]$. Hasonlóan, $[x,y,z] = -[z,y,x] = -[x,z,y]$, amiből pedig $[x,y,z] = [y,z,x] = [z,x,y]$ is következik. Ez indokolja az „alternáló” elnevezést. Könnyen meggondolható az is, hogy a definícióban szereplő három azonosság közül bármelyik kettő maga után vonja a harmadikat.



2. ábra. A Desargues-féle (P,t) és a Pappusz-féle tulajdonság.

3. Konfigurációk a projektív síkon

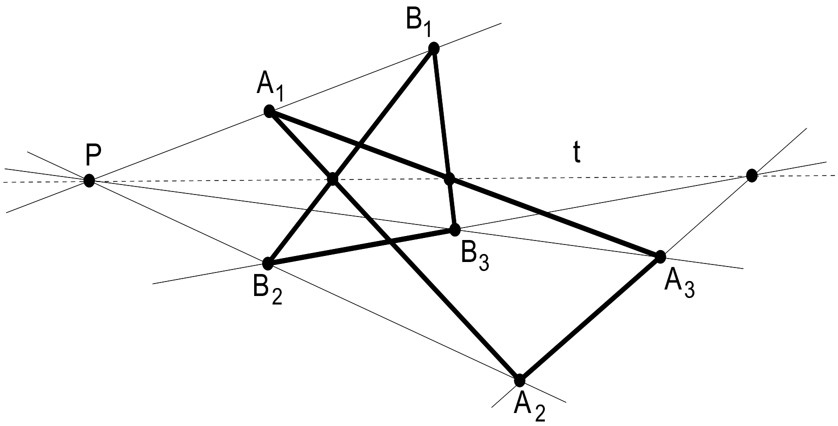
Ebben a fejezetben a definíciók és állítások nagy része a projektív síkon értelmes, ezért ha affin síkról van szó, akkor ilyen esetekben annak a projektív lezártjára kell gondolni. A tipikus eset Desargues és Pappusz jól ismert tételei (ld. a 2. ábrát), ezeket a valós testre épített projektív síkon legegyszerűbben közvetlen számolással tudjuk bebizonyítani. Ezzel szemben az absztrakt esetben ezeket axiómaként fogalmazzuk meg.

3.1. Definíció. *Azt mondjuk, hogy a* Π *sík* **Pappusz-féle,** *ha az* A_1, A_2, A_3 *és* B_1, B_2, B_3 *kollineáris ponthármasok esetén az* $A_1B_2 \cap A_2B_1$, $A_1B_3 \cap A_3B_1$, $A_2B_3 \cap A_3B_2$, *pontok is kollineárisak.*

3.2. Definíció. *Rögzítsük a* Π *sík* P *pontját és* t *egyenesét. Legyenek* A_1, A_2, A_3, B_1, B_2, B_3 *tetszőleges olyan pontok, melyekre* P, A_i, B_i *kollineárisak* $i = 1,2,3$ *esetén. Definiáljuk a* $Q_i = A_jA_k \cap B_jB_k$ *pontokat,* $\{i, j, j\} = \{1,2,3\}$. *Azt mondjuk, hogy* Π*-n teljesül a* **Desargues-féle** (P,t) **tulajdonság,** *ha valahányszor* Q_1, Q_2, Q_3 *közül kettő* t*-re esik, akkor a harmadik is.*

3.3. Definíció. *Azt mondjuk, hogy a* Π *sík* **Desargues-féle,** *ha minden* P *pont és* t *egyenes esetén teljesül a Desargues-féle* (P,t) *tulajdonság. Azt mondjuk, hogy a* Π **Moufang-féle sík,** *ha minden* $P \mathrm{I} t$ *esetben teljesül a Desargues-féle* (P,t) *tulajdonság.*

Megjegyzés. A $P \mathrm{I} t$ esetben *kis Desargues-konfigurációról* beszélünk, ld. a 3. ábrát.



3. ábra. A kis Desargues-konfiguráció.

Az alábbi két tétel és az őket követő állítás bizonyítása megtalálható Radó Ferenc és Orbán Béla *A geometria mai szemmel* c. könyvében.

3.4. Tétel (Hessenberg). *Bármely Pappusz-féle projektív sík Desargues-féle projektív sík.* □

3.5. Tétel. *A Π sík akkor és csak akkor Pappusz-féle, ha izomorf egy K test feletti $\Pi(\mathsf{K})$ síkhoz. A Π sík akkor és csak akkor Desargues-féle, ha izomorf egy F ferdetest feletti $\Pi(\mathsf{F})$ síkhoz.* □

Mindkét utóbbi tétel bizonyításában központi szerepet játszik az alábbi állítás.

3.6. Állítás. *A (P,t) tulajdonság ekvivalens azzal, hogy minden $Q,Q' \neq P$ pontpárhoz, melyek P-vel kollineárisak és nem illeszkednek t-re, létezik pontosan egy kollineáció, amely P-t és t pontjait fixen hagyja és amely Q-t Q'-be viszi.* □

A kis Desargues-féle projektív síkok jellemzését Ruth Moufang német matematikusnő adta meg.

3.7. Tétel (Moufang). *A Π sík akkor és csak akkor Moufang-féle, ha izomorf egy R alternáló osztásgyűrű feletti $\Pi(R)$ síkhoz.* □

A tétel bizonyítása helyett megelégszünk azzal, hogy az utolsó fejezetben megmutatjuk, hogy az $\mathbb{O}$-ra épített sík Moufang-féle.

4. Kompozícióalgebrák

A továbbiakban A $\mathbb{R}$ feletti egységelemes véges dimenziós algebrát jelöl.

4.1. Definíció. *Azokat az A algebrákat nevezzük* **kompozícióalgebrának**, *amelyeken értelmezve van egy $N : A \to \mathbb{R}$ nem-elfajuló multiplikatív kvadratikus alak, azaz $N(xy) = N(x)N(y)$ minden $x, y \in A$ esetén.*

4.2. Definíció. *Az A algebrát* **kvadratikus algebrának** *nevezzük, ha minden $x \in A$ elemhez léteznek $\alpha, \beta, \gamma \in \mathbb{R}$ valós számok, melyekre $\alpha x^2 + \beta x + \gamma = 0$.*

A $\mathbb{C}$ komplex számtest, a kvaterniók $\mathbb{H}$ ferdeteste és az oktávok $\mathbb{O}$ osztásalgebrája az $N(z) = z\bar{z}$ normával példát szolgáltatnak $\mathbb{R}$ feletti kompozícióalgebrára. Az $\mathbb{R}$ feletti 2×2 mátrixok vektortere a mátrixszorzásra és a determinánsra, mint normára nézve egy további példa. Ez azonban a többivel ellentétben rendelkezik nullaosztókkal, azaz nem osztásalgebra.

Tetszőleges A kompozícióalgebra esetén definiálhatjuk az alábbi fogalmakat: A normához kapcsolódó *belső szorzat* $f(x,y) = \frac{1}{2}(N(x+y) - N(x) - N(y))$, a $z \in A$ elem *nyoma* $t(z) = 2f(1,z)$, a z elem *konjugáltja* $\bar{z} = t(z) - z$. Nyilván a $z \mapsto t(z)$, $z \mapsto \bar{z}$ leképezések $\mathbb{R}$-lineárisak.

4.3. Tétel. *Minden kompozícióalgebra alternáló kvadratikus algebra.*

Bizonyítás. Legyen A tetszőleges kompozícióalgebra. Az $N(xy) = N(x)N(y)$ egyenlőségbe y helyére $y + w$-t írva, azaz y szerinti polarizálással, valamint a belső szorzat definíciójának felhasználásával kapjuk, hogy

$$N(x)f(y,w) = f(xy,xw). \tag{2}$$

Tovább polarizálva a (2) egyenlőséget x szerint, az

$$2f(x,z)f(y,w) = f(xy,zw) + f(zy,xw) \tag{3}$$

egyenlőség következik. Ebbe $z = 1$-et és $y = xu$-t helyettesítve kapjuk, hogy

$$t(x)f(xu,w) = f(x(xu),w) + f(xu,xw). \tag{4}$$

Használjuk fel a (2) azonosságot és f bilinearitását arra, hogy a (4) egyenletet

$$0 = f(x(xu) - t(x)xu + N(x)u, w). \tag{5}$$

alakra hozzuk. Mivel (5) teljesül minden w-re és f nem-elfajuló, az

$$x(xu) - t(x)xu + N(x)u = 0 \tag{6}$$

egyenlet teljesül minden x, u-ra. $u = 1$ helyettesítés adja, hogy minden x teljesíti az

$$x^2 - t(x)x + N(x) = 0 \tag{7}$$

azonosságot, ami bizonyítja, hogy A kvardatikus algebra.

Végezetül (7)-et jobbról u-val szorozva, majd (6)-ből kivonva kapjuk az $x(xu) - x^2u = 0$ egyenlőséget. Hasonlóan, a (3) egyenlőségbe $w = 1$-et és $x = vy$-t helyettesítve

$$(vy)y - t(y)vy + N(y)v = 0 \tag{8}$$

majd $(vy)y - vy^2 = 0$ adódik, azaz A alternáló algebra. □

A nyom linearitása miatt

$$\begin{aligned}(x+y)^2 &= t(x+y)(x+y) - N(x+y)\\ &= t(x)x - N(x) + t(y)y - N(y) + t(x)y + t(y)x - f(x,y)\\ &= x^2 + y^2 + t(x)y + t(y)x - f(x,y),\end{aligned}$$

vagyis

$$xy + yx = t(x)y + t(y)x - f(x,y). \tag{9}$$

4.4. Állítás. *A konjugálás a kompozícióalgebra antiautomorfizmusa. Teljesül továbbá* $\overline{\overline{x}} = x$.

Bizonyítás. Tudjuk, hogy $N(\alpha x) = \alpha^2 N(x)$ és $N(1) = N(1)^2$. Ha $N(1) = 0$ lenne, akkor $N(x) = N(1)N(x) = 0$ lenne minden $x \in A$ esetén, ami kizárt. Így $N(1) = 1$ és $t(1) = 2f(1,1) = 2$, de ekkor minden $\alpha \in \mathbb{R}$ esetén $t(\alpha) = 2\alpha$. Ezért aztán

$$\overline{\overline{x}} = t(t(x) - x) - t(x) + x = 2t(x) - 2t(x) + x = x.$$

A konjugálást illetően csak azt kell megmutatnunk, hogy $\overline{xy} = \overline{y}\,\overline{x}$. A (9) egyenlőség és t definíciója szerint

$$\begin{aligned}\overline{y}\,\overline{x} - \overline{xy} &= t(y)t(x) - t(x)y - t(y)x + xy + yx - t(xy)\\ &= t(y)t(x) - f(x,y) - t(xy)\\ &= f(1,x)f(1,y) - f(x,y) - f(1,xy).\end{aligned}$$

Itt azonban az utolsó rész 0, amit a (3) egyenletből kapunk $z = w = 1$ helyettesítéssel. □

A fejezetet két fontos észrevétellel zárjuk.

4.5. Lemma. *Az A egységelemes kompozícióalgebra tetszőleges x, y elemiere az x, y és $\overline{x}$ elemekből képzett asszociátor nulla.*

Bizonyítás. Az x elem $\overline{x} = t(x) - x$ konjugáltjára teljesül

$$[\overline{x}, x, y] = [t(x) - x, x, y] = t(x)[1, x, y] - [x, x, y] = 0,$$

mivel $(1x)y = 1(xy)$ és $x^2y = x(xy)$. Az asszociátor-zárójel alternálása miatt ekkor az összes asszociátor értéke nulla. □

Legyen B az A kompozícióalgebra olyan részalgebrája, amely tartalmazza az 1 egységelemet és amelyen az $f(x,y)$ belső szorzat nem-elfajuló. (Azaz minden $x \in B$-ra létezik $y \in B$, hogy $f(x,y) \neq 0$.) Jelölje $B^{\perp}$ a B f-re vonakozó

$$B^{\perp} = \{y \in A \mid f(x,y) = 0 \text{ minden } x \in A \text{ esetén } \}$$

ortogonális kiegészítő alterét. A belső szorzat bilinearitása miatt $B^{\perp}$ $\mathbb{R}$-lineáris altér.

4.6. Lemma. *Ha B az A kompozícióalgebra nem-elfajuló részalgebrája, akkor minden $d \in B^{\perp}$ elemre $dB \subseteq B^{\perp}$.*

Bizonyítás. Azt kell megmutatni, hogy tetszőleges $b, c \in B$ elemre $f(c, db) = 0$. A (3) egyenlet szerint

$$f(c1, db) = 2f(c,d)f(1,b) - f(d1, cb) = 0,$$

hiszen $d \perp b, c, cb \in B$. $\square$

5. A Cayley-Dickson eljárás

Ebben a fejezetben A $\mathbb{R}$ feletti véges dimenziós, egységelemes kompozícióalgebrát jelöl N nem-elfajuló multiplikatív normával. Az N-hez tartozó belső szorzatot $f(x,y)$ a nyomot $t(x)$ jelöli. Ekkor x kielégíti az $x^2 - t(x)x + N(x) = 0$ egyenletet és a konjugálás művelete antiautomorfizmus. Teljesül továbbá $N(x) = x\overline{x}$.

A Cayley-Dickson eljárás néven ismert módszer segítségével A és egy tetszőleges $\alpha \in \mathbb{R}$ szám felhasználásával egy új $\mathbb{R}$-algebrát konstruálhatunk. Definiáljuk a $B = A \oplus A$ vektortéren az alábbi bilineáris szorzásműveletet:

$$(a_1, a_2)(b_1, b_2) = (a_1 b_1 - \alpha b_2 \overline{a_2}, \overline{a_1} b_2 + b_1 a_2).$$

Triviális számolással adódik, hogy $(1,0)$ egységelem B-ben és az $a \mapsto (a,0)$ leképezés A beágyazása B-be. Ilyen formán A-t és $\mathbb{R}$-t B részalgebrájának tekinthetjük. Mivel pedig a $v = (0,1)$ elemre $v^2 = -\alpha$, az új algebrát $B = A + vA$ alakba írhatjuk.

Megjegyzés. Az $\mathbb{R}$ valós számtestből az $\alpha = 1$ választással a Cayley-Dickson eljárás a $\mathbb{C}$ komplex számtestet hozza létre.

Terjesszük most ki a konjugálás műveletét B-re az $\overline{(a_1, a_2)} = (\overline{a_1}, -a_2)$ definícióval. Ekkor $x = (a_1, a_2) \in B$ esetén

$$\begin{aligned} t_B(x) &= x + \overline{x} = (a_1 + \overline{a_1}, 0) = t(a_1) \in \mathbb{R}, \\ N_B(x) &= x\overline{x} = \overline{x}x = (a_1\overline{a_1} + \alpha a_2 \overline{a_2}, 0) = N(a_1) + \alpha N(a_2) \in \mathbb{R} \end{aligned}$$

és x eleget tesz az

$$x^2 - t(x)x + N(x) = x^2 - (x + \overline{x})x + x\overline{x} = 0$$

$\mathbb{R}$ feletti másodfokú egyenletnek, azaz B kvadratikus algebra. Végezetül megmutatjuk, hogy a konjugálás B antiautomorfizmusa:

$$
\begin{aligned}
(\overline{b_1}, -b_2)(\overline{a_1}, -a_2) &= (\overline{b_1}\,\overline{a_1} - \alpha a_2 \overline{b_2}, -b_1 a_2 - \overline{a_1} b_2) \\
&= \overline{(a_1 b_1 - \alpha b_2 \overline{a_2}, -(\overline{a_1} b_2 + b_1 a_2))} \\
&= \overline{(a_1, a_2)(b_1, b_2)}.
\end{aligned}
$$

A Cayley-Dickson eljárás tehát egy kvadratikus algebrát hoz létre. A következő állítás megmutatja, hogy mely esetekben lesz B kompozícióalgebra.

5.1. Állítás. *Tekintsük az A kompozícióalgebrából és az $\alpha \in \mathbb{R}$ elemből a Cayley-Dickson eljárással megkonstruált B algebrát. Ekkor a következő állítások ekvivalensek.*

(i) *B kompozícióalgebra.*

(ii) *B alternáló algebra.*

(iii) *A asszociatív algebra.*

Bizonyítás. Elsőként azt látjuk be, hogy N nem-elfajuló kvadratikus alak; ebből a 4.3 és 7.3 tételek szerint következik (i) és (ii) ekvivalenciája. Már láttuk, hogy $N_B(a_1, a_2) = N(a_1) + \alpha N(a_2)$, amiből adódik az

$$f_B((a_1, a_2), (b_1, b_2)) = f(a_1, b_1) + \alpha f(a_2, b_2)$$

belső szorzat. Tegyük fel, hogy $x = (a_1, a_2) \in B$ elemre $f_B(x, y) = 0$ teljesül minden $y = (b_1, b_2) \in B$ esetén, ez csak úgy lehetséges, ha $f(a_1, b_1) = f(a_2, b_2) = 0$ áll fenn minden $b_1, b_2 \in A$-ra. Mivel azonban N nem-elfajuló A-n, így ez utóbbi feltétel implikálja $a_1 = a_2 = 0$-t és $x = 0$-t. Ez pontosan azt jelenti, hogy N_B nem-elfajuló kvadratikus alak B-n.

Tekintsük most az $x = (a_1, a_2)$, $y = (b_1, b_2)$ B-beli elemeket és a 4.5 lemma segítségével számítsuk ki az $x^2 y - x(xy)$ különbséget.

$$
\begin{aligned}
x^2 y &= (a_1^2 - \alpha a_2 \overline{a_2}, a_1 a_2 + \overline{a_1} a_2)(b_1, b_2) \\
&= (a_1^2 b_1 - \alpha(a_2 \overline{a_2}) b_1 - \alpha b_2 \overline{a_2}(a_1 + \overline{a_1}), \\
&\qquad (\overline{a_1})^2 b_2 - \alpha(a_2 \overline{a_2}) b_2 + b_1 (a_1 + \overline{a_1}) a_2),
\end{aligned}
$$

$$
\begin{aligned}
x(xy) &= (a_1, a_2)(a_1 b_1 - \alpha b_2 \overline{a_2}, \overline{a_1} b_2 + b_1 a_2) \\
&= (a_1^2 b_1 - a_1(b_2 \overline{a_2}) - \alpha(\overline{a_1} b_2)\overline{a_2} - \alpha b_1 (a_2 \overline{a_2}), \\
&\qquad (\overline{a_1})^2 b_2 + \overline{a_1}(b_1 a_2) + (a_1 b_1) a_2 - \alpha b_2 (\overline{a_2} a_2))
\end{aligned}
$$

Mivel $a_1 + \overline{a_1}, a_2 \overline{a_2} \in \mathbb{R}$, ezért fennáll $\alpha b_2 \overline{a_2}(a_1 + \overline{a_1}) = \alpha((a_1 + \overline{a_1}) b_2)\overline{a_2}$ és $(a_2 \overline{a_2}) b_1 = b_1 (a_2 \overline{a_2})$, így az első komponensek különbségére

$$a_1(b_2 \overline{a_2}) - (a_1 b_2)\overline{a_2} = -[a_1, b_2, \overline{a_2}]$$

adódik. A második komponenseknél hasonlóan járunk el, az $(a_2\overline{a_2})b_2 = b_2(\overline{a_2}a_2)$ és $b_1(a_1+\overline{a_1})a_2 = ((a_1+\overline{a_1})b_1)a_2$ egyenlőségeket használva kapjuk, hogy a különbség

$$(\overline{a_1}b_1)a_2 - \overline{a_1}(b_1a_2) = [\overline{a_1}, b_1, a_2].$$

Tehát

$$[x,x,y] = (-[a_1,b_2,\overline{a_2}], [\overline{a_1}, b_1, a_2]),$$

vagyis B akkor és csak akkor elégíti ki az $x^2y = x(xy)$ azonosságot, ha A asszociatív. Ez bizonyítja (ii)$\Longrightarrow$(iii)-t.

Mivel a konjugálás antiautomorfizmus, teljesül az

$$\begin{aligned}
\overline{[x,y,z]} &= -[\overline{z},\overline{y},\overline{x}] \\
&= -[t(z)-z, t(y)-y, t(x)-x] \\
&= -[-z,-y,-x] \\
&= [z,y,x]
\end{aligned}$$

azonosság. Tegyük ezért fel, hogy A asszociatív, így $[x,x,y] = 0$. Ekkor $[y,x,x] = \overline{[x,x,y]} = \overline{0} = 0$, azaz $(yx)x = yx^2$, vagyis B alternáló algebra. □

5.2. Állítás. *Az A kompozícióalgebrából és az $\alpha \in \mathbb{R}$ elemből a Cayley-Dickson eljárással megkonstruált B algebra akkor és csak akkor asszociatív, ha A kommutatív és asszociatív.*

Bizonyítás. Az 5.1 állítás szerint ha B asszociatív, akkor A is asszociatív és teljesül

$$0 = (0,1)(a,0)\cdot(b,0) - (0,1)\cdot(a,0)(b,0) = (0, ba-ab),$$

vagyis A kommutatív is egyben. Ha pedig A kommutatív és asszociatív, akkor egyszerű közvetlen számolás kiadja B asszociativitását. □

5.3. Állítás. *Az A kompozícióalgebrából és az $\alpha \in \mathbb{R}$ elemből a Cayley-Dickson eljárással megkonstruált B algebra akkor és csak akkor kommutatív, ha* $\dim(A) = 1$.

Bizonyítás. Ha $A = \mathbb{R}$, akkor B asszociatív és $\overline{\alpha} = \alpha$ minden $\alpha \in \mathbb{R}$ esetén. Ebben az esetben a szorzásművelet definíciójából azonnal látszik B kommutativitása. Tegyük fel most, hogy B kommutatív és asszociatív, az 5.2 állítás szerint ekkor A kommutatív. Az $(a,0)(0,1) - (0,1)(a,0) = (0, \overline{a} - a) = 0$ egyenlőség mutatja, hogy a konjugálás identikus leképezés A-n és $t(a) = 2a$. Vagyis $a \in \mathbb{R} = A$. □

Megjegyzés. A bizonyításból az derül ki, hogy $A = \mathbb{R}$ akkor és csak akkor teljesül, ha a konjugálás művelete az identikus leképezés A-n.

A fejezet hátralévő részében a Cayley-Dickson eljárás „természetes előfordulásáról” győződhetünk meg.

5.4. Tétel. *Legyen A a B kompozícióalgebra olyan részalgebrája, amely tartalmazza az* 1 *egységelemet és amelyen* f *nem-elfajuló. Ekkor bármely* $v \in A^{\perp}$ *elem esetén* $v^2 \in \mathbb{R}$ *és a* $B_1 = A + vA$ *olyan részalgebrája* B*-nek, amely izomorf az* A*-ból és* $\alpha = -v^2$*-ből Cayley-Dickson eljárással nyert algebrához.*

Bizonyítás. Mivel $1 \in A$ és $v \in A^{\perp}$, így $t(v) = f(1, v) = 0$ és $v \in V$, tehát $v^2 \in \mathbb{R}$. Igaz továbbá, hogy bármely $a \in A$-ra

$$0 = f(v,a) = v\overline{a} + a\overline{v} = v\overline{a} - av,$$

vagyis $av = v\overline{a}$. A 4.6 lemma szerint minden $b \in A$ esetén $vb \in A^{\perp}$, ezért az előzőhöz hasonlóan

$$(vb)a = \overline{a}(vb).$$

Ebből kiszámíthatjuk a következő különbségeket:

$$\begin{aligned}
(va)b - v(ba) &= (va)b - (vb)a + (vb)a - v(ba) \\
&= (\overline{a}v)b - \overline{a}(vb) + [v,b,a] \\
&= (\overline{a}v)b - \overline{a}(vb) + [a,v,b] \\
&= (\overline{a}v)b - \overline{a}(vb) + (av)b - a(vb) \\
&= ((a+\overline{a})v)b - (a+\overline{a})(vb) \\
&= 0,
\end{aligned}$$

és

$$\begin{aligned}
(va)(vb) - v^2(b\overline{a}) &= (va)(vb) - ((va)v)b + (v(av))b - v(v(b\overline{a})) \\
&= -[va,v,b] + (v(av))b - v((v\overline{a})b) \\
&= [v,\overline{a}v,b] + [v,av,b] \\
&= (a+\overline{a})[v,v,b] \\
&= 0,
\end{aligned}$$

ahol felhasználtuk a korábban bizonyított azonosságokat és azt, hogy B alternáló algebra. Ezekből két B_1-beli elem szorzatára

$$\begin{aligned}
(a_1 + va_2)(b_1 + vb_2) &= a_1b_1 + (va_2)b_1 + (vb_2)\overline{a_1} + (va_2)(vb_2) \\
&= a_1b_1 - v^2(b_2\overline{a_2}) + v(b_1a_2) + v(\overline{a_1}b_2) \\
&= a_1b_1 + \alpha b_2\overline{a_2} + v(\overline{a_1}b_2 + b_1a_2).
\end{aligned}$$

Ez pontosan azt jelenti, hogy B_1 olyan részalgebrája B-nek, amely izomorf az A-ból és $\alpha = -v^2$-ből Cayley-Dickson eljárással nyert algebrához. □

6. Hurwitz tétele

Eddig talán nem hangsúlyoztuk kellőképpen, de remélhetőleg sokak számára eddig is világos volt az a fontos tény, hogy $\mathbb{R}$-ből és az $\alpha = 1$ értékből kiindulva a Cayley-Dickson eljárás rendre a $\mathbb{C}$, $\mathbb{H}$ valamint $\mathbb{O}$ kompozícióalgebrákat szolgáltatja.

6.1. Tétel (Hurwitz). *Minden valós számtest feletti véges dimenziós, nullaosztómentes kompozícióalgebra izomorf a következők valamelyikével:* $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$, $\mathbb{O}$.

Bizonyítás. Legyen B a feltételeknek megfelelő algebra. Legyen f a B normájához tartozó belső szorzat és jelölje $X^{\perp}$ az $X \subseteq B$ halmaz f-re vonatkozó ortogonális kiegészítő alterét. Mint korábban láttuk, hogy bármely $0 \neq v \in \mathbb{R}^{\perp}$ elemre $t(v) = 0$ és $v^2 < 0$. Ha ugyanis $v^2 = c > 0$ állna fenn, akkor $(v - \sqrt{c})(v + \sqrt{c}) = 0$ teljesülne, ami B nullaosztómentessége miatt azt jelentené, hogy $v = \pm\sqrt{c} \in \mathbb{R}$. Ez nem lehetséges.

Ha $\dim(B) = 1$, akkor $B = \mathbb{R}$. Tegyük fel, hogy $\dim(B) > 1$, akkor $A_1 = \mathbb{R}$ valódi részalgebra és $A_1^{\perp} \neq 0$. Választhatunk egy $v_1 \in A_1^{\perp}$ elemet, amelyre $v_1^2 = -1$, és amelyre az 5.4 tétel szerint az $A_2 = A_1 + v_1 A_1$ olyan részalgebrája B-nek, amely izomorf az $\mathbb{R}$-ből és $\alpha = 1$-ből Cayley-Dickson eljárással nyert algebrához, vagyis $A_2 \cong \mathbb{C}$.

Ha $\dim(B) = 2$, akkor $B = A_2 \cong \mathbb{C}$. Tegyük fel, hogy $\dim(B) > 2$, és válasszunk egy $v_2 \in A_2^{\perp}$ úgy, hogy $v_2^2 = -1$. Tekintsük az $A_3 = A_2 + v_2 A_2$ alteret. Az 5.4 tétel szerint ez olyan részalgebra B-ben, amely izomorf a $\mathbb{C}$-ből $\alpha = 1$ választással konstruált algebrához, azaz $\mathbb{H}$-hoz.

Ha $\dim(B) = 4$, akkor $B = A_3 \cong \mathbb{H}$. Ha $\dim(B) > 4$, akkor a fentiekhez hasonlóan választunk egy $v_3 \in A_3^{\perp}$ elemet, amelyre $v_3^2 = -1$, és kapjuk az $\mathbb{O}$-val izomorf $A_4 = A_3 + v_3 A_3$ részalgebrát. Ha $\dim(B) = 8$, akkor $B \cong \mathbb{O}$. Megmutatjuk, hogy $\dim(B) > 8$ nem lehetséges.

A $\dim(B) > 8$ esetben ugyanis az előbbi eljárást folytatva tudnánk egy $v_4 \in A_4^{\perp}$ elemet választani, amelyre $v_4^2 = -1$ és az 5.4 tétel szerint az $A_5 = A_4 + v_4 A_4$ részalgebra izomorf lenne az $\mathbb{O}$-ból és $\alpha = 1$-ből a Cayley-Dickson eljárással megalkotott 16-dimenziós algebrához. Mivel viszont a feltevés szerint B kompozícióalgebra, azaz alternáló, az A_5 részalgebra is alternáló. Ekkor az 5.1 állításból adódóan $\mathbb{O}$-nak asszociatívnak kellene lennie, ami nyilvánvaló ellentmondás. Tehát $\dim(B) \leq 8$ és minden esetben B izomorf a tételben felsorolt $\mathbb{R}$-algebrák valamelyikéhez. $\square$

7. Kvadratikus algebrák

A kvadratikus algebrák osztályának a jelentősége már kitűnhetett az eddigi fejezetekből is. Most részletesebben is megvizsgáljuk ezt az algebraosztályt.

A fejezet során A mindig $\mathbb{R}$ feletti, véges dimenziós, egységelemes kvadratikus algebrát fog jelölni.

7.1. Lemma. *Definiáljuk A alábbi részhalmazát:*

$$V = \{x \in A \setminus \mathbb{R} \mid x^2 \in \mathbb{R}\} \cup \{0\}.$$

Ekkor V lineáris altér A-ban és $A = \mathbb{R} \oplus V$ vektorterek direkt összege, azaz minden $x \in A$ elemhez egyértelműen léteznek $\alpha \in \mathbb{R}$, $u \in V$ elemek, amelyre $x = \alpha + u$.

Bizonyítás. Tetszőleges $x \in A \setminus \mathbb{R}$ elemhez léteznek $b, c \in \mathbb{R}$ elemek, amelyre $x^2 + bx + c = 0$. Ekkor nyilván $x + b/2 \neq \mathbb{R}$ és $(x + b/2)^2 = -c + b^2/4 \in \mathbb{R}$, azaz $x + b/2 \in V$ és x előáll egy $\mathbb{R}$-beli és egy V-beli elem összegeként. Mivel $\mathbb{R} \cap V = \{0\}$, így A direkt felbontásához elegendő megmutatni, hogy V lineáris altér.

Az világos, hogy $\alpha \in \mathbb{R}$ esetén $\alpha V \subseteq V$, hátra van még $V + V \subseteq V$. Rögzítsünk ehhez tetszőleges u, v V-beli elemeket. Ha ezek lineárisan függők, akkor szükségszerűen egyik skalárszorosa a másiknak, de akkor az összegük is skalárszorosa ugyanannak az elemnek, tehát benne van V-ben. Tegyük ezért fel a továbbiakra, hogy u és v lineárisan függetlenek.

Tudjuk, hogy A kvadratikus algebra, így léteznek $a, b, c, d \in \mathbb{R}$ skalárok, amelyekre $(u+v)^2 = a(u+v) + b$ és $(u-v)^2 = c(u-v) + d$. Ezekből $uv + vu$-t kétféleképpen kifejezve kapjuk, hogy

$$uv + vu = au + av + b - u^2 - v^2 = -cu + cv - d + u^2 + v^2,$$

vagyis $a^*u + b^*v + c^* = 0$, ahol $a^* = a + c$, $b^* = a - c$ és $c^* = b + d - 2u^2 - 2v^2$ mind $\mathbb{R}$-beli elemek.

Tegyük most fel, hogy $a^* \neq 0$, ekkor $b^* \neq 0$, mert $u \notin \mathbb{R}$ és $c^* \neq 0$ mert u és v lineárisan függetlenek. Ezért $a^*u + b^*v + c^* = 0$-t átalakíthatjuk $u = b^{**}v + c^{**}$ alakra, ahol $b^{**}c^{**} \neq 0$. Ebből az következne, hogy

$$v = \frac{u^2 - v^2 - (c^{**})^2}{2b^{**}c^{**}} \in \mathbb{R},$$

ami viszont a feltételeink szerint nem igaz. Így tehát szükségszerűen $a^* = 0$, amiből következik $b^* = 0$ is.

Ezzel beláttuk $a + c = a - c = 0$-t, ami azt jelenti, hogy $a = c = 0$ és $(u+v)^2 = b \in \mathbb{R}$. $u + v \in \mathbb{R}$ azt jelentené, hogy $u + v + c^* = 0$ teljesül valamely $c^* \in \mathbb{R}$ elemre, azt azonban az előző bekezdésben láttunk, hogy nem lehetséges. Így tehát $u + v \in V$. $\square$

A továbbiakban gyakran fogunk hivatkozni az $x = \alpha + u$ felbontásra, itt α-t és u-t az x elem *valós* illetve *képzetes részének* fogjuk nevezni. Bevezetjük továbbá a következő jelöléseket: $t(x) = 2\alpha$, $N(x) = \alpha^2 - u^2$. Ekkor $t(x), N(x) \in \mathbb{R}$ és

$$x^2 - t(x)x + N(x) = (\alpha + u)^2 - 2\alpha(\alpha + u) + \alpha^2 - u^2 = 0.$$

Ezeken kívül $u, v \in V$ elemekre definiáljuk az alábbi műveleteket:

$$u \times v = uv \text{ képzetes része}, \qquad (u, v) = -uv \text{ valós része.}$$

Mivel a valós és képzetes rész képzése $\mathbb{R}$-lineáris, ezért $\times$ bilineáris szorzásművelet és $(.,.)$ belső szorzat V-n. A fenti jelöléssel nyilván

$$uv = -(u, v) + u \times v.$$

7.2. Lemma. *Ha A asszociatív kvadratikus algebra, akkor az imént definiált műveletek rendelkeznek az alábbi tulajdonságokkal.*

(i) $u \times v$ *antiszimmetrikus.*

(ii) (u,v) *szimmetrikus.*

(iii) $(u \times v, u) = 0.$

(iv) $(u \times v, w) = (u, v \times w)$. *(Invariancia.)*

(v) $(u \times v) \times v = (u,v)v - (v,v)u$. *(Gyenge kifejtési tétel.)*

(vi) $(u \times v, u \times v) = (u,u)(v,v) - (u,v)^2.$

Bizonyítás. Az $uv + vu = (u+v)^2 - u^2 - v^2 \in \mathbb{R}$ képzetes része $u \times v + v \times u = 0$, ez bizonyítja (i)-t. A alternáló, így $(uv)u = u(vu)$. Ezt kifejtve kapjuk, hogy

$$-(u \times v, u) - (u,v)u + (u \times v) \times u = -(u, v \times u) - (v,u)u + u \times (v \times u).$$

A $\times$ művelet antiszimmetriája miatt $(u \times v) \times u = u \times (v \times u)$ és a két képzetes részre kapjuk, hogy $(u,v)u = (v,u)u$, ami mutatja $(.,.)$ szimmetriáját, azaz (ii)-t. A valós részek összehasonlításából

$$(u \times v, u) = (u, v \times u) = -(u \times v, u) \implies \text{(iii)}.$$

(iv)-t megkapjuk (iii) u szerinti polarizálásával.

Használjuk most az $uv^2 = (uv)v$ azonosságot: egyrészt tudjuk, hogy $uv^2 = -u(v,v)$, másrészt $(uv)v = -(u,v)v - (u \times v, v) + (u \times v) \times v$. $(u \times v, v) = 0$ miatt ezek összevetése (v)-t eredményezi. Végezetül az invariancia és a gyenge kifejtési tétel felhasználásával megkapjuk (vi)-t:

$$\begin{aligned}(u \times v, u \times v) &= ((u \times v) \times u, v) \\ &= -((v,u)u - (u,u)v, v) \\ &= (u,u)(v,v) - (v,u)^2. \qquad \square\end{aligned}$$

A fejezet fő eredménye a következő.

7.3. Tétel. *Legyen A véges dimenziós, nullaosztómentes, asszociatív kvadratikus algebra. Ekkor A kompozícióalgebra az imént definiált* $N(\alpha + u) = \alpha^2 - u^2$ *normára nézve.*

Bizonyítás. Minden kvadratikus algebrában definíció szerint N kvadratikus alak. Bármely $x = \alpha + u \neq 0$ A-beli elem esetén $\alpha - u \neq 0$, így az A nullaosztómentessége miatt $N(x) = (\alpha + x)(\alpha - x) \neq 0$, azaz N nem-elfajuló. Meg kell még mutatnunk, hogy multiplikatív. Tudjuk, hogy $x = \alpha + u$ esetén $N(x) = \alpha^2 - u^2 = \alpha^2 + (u,u)$. Továbbá, ha $y = \beta + v$, akkor

$$xy = \alpha\beta - (u,v) + \alpha v + \beta u + u \times v.$$

Eszerint

$$\begin{aligned}
N(xy) &= \alpha^2\beta^2 - 2\alpha\beta(u,v) + (u,v)^2 + \alpha^2(v,v) + \beta^2(u,u) + \\
&\quad (u \times v, u \times v) + 2\alpha\beta(u,v) + 2\alpha(v, u \times v) + 2\beta(u, u \times v) \\
&= \alpha^2\beta^2 + \alpha^2(v,v) + \beta^2(u,u) + (u,v)^2 + (u \times v, u \times v) \\
&= \alpha^2\beta^2 + \alpha^2(v,v) + \beta^2(u,u) + (u,u)(v,v) \\
&= (\alpha^2 + (u,u))(\beta^2 + (v,v)) \\
&= N(x)N(y),
\end{aligned}$$

ahol a második lépésben a 7.2 lemma (iii) pontját, a harmadikban pedig a (vi) pontját használtuk fel. □

8. Frobenius tétele

8.1. Tétel (Frobenius). *A valós számtest feletti véges dimenziós ferdetestek a következők egyikével izomorfak:* $\mathbb{R}$, $\mathbb{C}$ *vagy* $\mathbb{H}$.

Bizonyítás. Legyen B a feltételeknek megfelelő algebra. Elegendő megmutatni, hogy B kvadratikus algebra, hiszen ekkor alkalmazható rá a 7.3 tétel, ami azt jelentené, hogy B kompozícióalgebra. A nullaosztómentesség miatt ekkor Hurwitz tétele szerint B izomorf $\mathbb{R}$-hez, $\mathbb{C}$-hez, $\mathbb{H}$-hoz vagy $\mathbb{O}$-hoz. Mivel $\mathbb{O}$-ban a szorzás nem asszociatív, adódik a tétel állítása.

Legyen most $x \in B$ tetszőleges elem és jelölje $g(X)$ az $\mathbb{R}$ feletti minimálpolinomját. B nullaosztómentessége miatt $g \in \mathbb{R}(X)$ irreducibilis $\mathbb{R}$ felett, azaz $\deg(g) = 1$ vagy 2. Ez pontosan azt jelenti, hogy megfelelő $\alpha, \beta, \gamma \in \mathbb{R}$ számokkal $\alpha x^2 + \beta x + \gamma = 0$ teljesül, vagyis B kvadratikus algebra. □

9. Az oktávsík Moufang-tulajdonsága

Ebben a fejezetben Π_a illetve Π az $\mathbb{O}$ feletti affin síkot, illetve annak projektív lezártját jelöli.

9.1. Állítás. *Tetszőleges* $a, b, c \in \mathbb{O}$ *esetén az alábbi leképezések* Π_a *kollineációját határozzák meg:* $(x,y) \mapsto (x+a, y+b)$, $(x,y) \mapsto (x, y+cx)$.

Bizonyítás. A disztributivitás felhasználásával közvetlen számolással adódik az állítás. □

9.2. Következmény. *Jelölje* ℓ_∞ *a* Π *sík végtelen távoli egyenesét, és legyen* P *ennek egy pontja. Ekkor* Π*-n teljesül a* (P, ℓ_∞) *tulajdonság.*

Bizonyítás. A 3.6 állítás szerint elegendő megmutatni, hogy bármely $Q(u,v)$ és $Q'(u',v')$ affin pontokhoz létezik olyan kollineáció, amely a végtelen távoli pontokat fixen hagyja, Q-t pedig Q'-be viszi. Mivel az $(x,y) \mapsto (x+u-u', y+v-v')$ leképezés a párhuzamossági osztályokat invariánsan hagyja, ez megfelelő lesz. □

Tudjuk, hogy $\mathbb{O}$-ban $\bar{x}(xy) = N(x)y = (yx)\bar{x}$, azaz $x^{-1} = N(x)^{-1}\bar{x}$ helyettesítéssel $x^{-1}(xy) = y = (yx)x^{-1}$ teljesül.

9.3. Állítás. *Az $(x,y) \to (y,x)$ leképezés kollineáció Π_a-n.*

Bizonyítás. Elegendő meggondolnunk, az $Y = mX + b$, $m \neq 0$ alakú egyenesek képe ugyanilyen. Valóban, $(t, mt+b) \mapsto (mt+b, t) = (t', m^{-1}t' - m^{-1}b)$, azaz ezen egyenes képe $Y = m^{-1}X - m^{-1}b$. A számoláskor $x^{-1}(xy) = y$-t és a disztributivitást használjuk. □

9.4. Állítás. *Értelmezzük Π ponthalmazán az alábbi φ leképezést: $x \neq 0$ esetén $(x,y) \mapsto (x^{-1}, yx^{-1})$, $(0,y)$ képe az y meredekségű egyenesek végtelen távoli pontja, a függőleges egyenesek végtelen távoli pontjának a képe pedig önmaga. Ekkor φ a Π projektív sík kollineációja.*

Bizonyítás. Az $Y = mX + b$ alakú egyenesek $(t, mt+b)$ pontjainak képe $(t^{-1}, (mt+b)t^{-1}) = (t', bt'+m)$, amik az $Y = bX + m$ egyenest alkotják. Az $X = 0$ egyenes pontjainak képei a végtelen távoli egyenes pontjai. Az $X = c$, $c \neq 0$ egyenes pontjai az $X = c^{-1}$ egyenesre illeszkednek. Ezzel beláttuk az állítást úgy, hogy a számoláskor a disztributivitáson kívül az $(xy)y^{-1} = x$ azonosságot használtuk. □

9.5. Tétel. *A Π sík kollineációi tranzitívan hatnak az egyenesek halmazán.*

Bizonyítás. Megmutatjuk, hogy bármely affin egyenes elvihető a végtelen távoli egyenesbe kollineációval. Legyen ℓ tetszőleges, a végtelen távoli egyenestől különböző egyenes. Nyilván egy $(x,y) \mapsto (x+a, y+b)$ alakú eltolással ℓ elvihető az origóba. Ha $\ell : Y = kX$, $k \neq 0$ különbözik mindkét tengelytől, akkor az $(x,y) \mapsto (x, y-kx)$ kollineáció elviszi az x-tengelybe. Az x-tengelyt az $(x,y) \mapsto (y,x)$ az y-tengelybe viszi. Tehát bármely egyenes kollineációval elvihető az y-tengelybe, amit viszont az $(x,y) \mapsto (x^{-1}, yx^{-1})$ kollineáció a végtelen távoli egyenesbe visz. □

9.6. Lemma. *Tegyük fel, hogy a Σ projektív síkon valamely P pontra és t egyenesre teljesül a (P,t) tulajdonság. Ekkor a Σ bármely φ kollineációja esetén teljesül a $(\varphi(P), \varphi(t))$ tulajdonság.*

Bizonyítás. Ez könnyen adódik a 3.6 állításból. □

9.7. Tétel. *Az $\mathbb{O}$-ra épített Π projektív sík Moufang-féle.*

Bizonyítás. Legyen $P\,\mathrm{I}\,t$ tetszőleges. A 9.5 tétel szerint létezik olyan φ kollineáció, amely az ℓ_∞ végtelen távoli egyenest t-be viszi. A 9.2 következmény szerint Π teljesíti a $(\varphi^{-1}(P), \ell_\infty)$ tulajdonságot, ami a 9.6 lemma alapján azt jelenti, hogy a (P, t) tulajdonság is teljesül. □

Megjegyzés. Meggondolható, hogy tetszőleges alternáló osztásgyűrűben, a disztributivitás mellett teljesülnek a $x^{-1}(xy) = y = (yx)x^{-1}$ azonosságok is. Mivel a fentiekben $\mathbb{O}$ egyetlen más tulajdonságát sem használtuk ki, a fejezet minden bizonyítása elmondható tetszőleges alternáló osztásgyűrű feletti sík esetén.