Kvaternióalgebrák és kvadratikus alakok

Az alábbi jegyzetben bemutatjuk a kvaternióalgebrák és a kvadratikus alakok kapcsolatát, majd belátjuk, hogy minden 4-dimenziós K-algebra, melynek centruma csak K, egy alkalmas kvaternióalgebrával izomorf.

1. Definíció. *Legyen K egy test, $0 \neq a, b \in K$, és tegyük fel, hogy* $\mathrm{char}(K) \neq 2$. *A $K(a,b)$ kvaternióalgebra egy K-feletti 4-dimenziós egységelemes asszociatív algebra, melynek $1, i, j, k \in K(a,b)$ egy bázisa K feletti vektortérként, és a szorzás teljesíti az $i^2 = a$, $j^2 = b$, $ij = k$, $ji = -k$ azonosságokat. Az A egységelemes asszociatív K-algebrát (K feletti) kvaternióalgebrának nevezzük, ha van olyan $a, b \in K^\times$, melyre $A \cong K(a,b)$.*

Egyszerű számolás mutatja, hogy a disztributív és asszociatív szabály szerint a fenti szorzás tetszőleges $a, b \in K^\times$ esetén egyértelműen kiterjeszthető $K(a,b)$-re úgy, hogy $K(a,b)$ egy egységelemes asszociatív K-algebra legyen. Pl. $ik = i(ij) = (i^2)j = aj = -ki$, $jk = -j^2 i = -bi = -kj$, illetve $k^2 = ijij = -i^2 j^2 = -ab$. K természetes módon résztest $K(a,b)$-ben: az egységelem skalárszorosai K-val izomorf résztestet alkotnak, melyet a továbbiakban azonosítunk K-val.

2. Példa. *A szokásos kvaterniók $\mathbb{H}$ gyűrűje izomorf az $\mathbb{R}(-1,-1)$ gyűrűvel. Továbbá ha K tetszőleges test, akkor $K(1,b) \cong M_2(K)$ (2×2-es mátricgyűrű). Az izomorfizmust az $i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$ leképezés adja meg.*

Vegyük észre, hogy $K(ac^2, b) \cong K(a,b) \cong K(b,a)$ tetszőleges $a, b, c \in K^\times$ esetén. Valóban, ha $(ci)^2 = ac^2$ teljesül $K(a,b)$-ben, ezért a $K(ac^2, b) \to K(a,b)$ leképezés, melyre $i \mapsto ci$, $j \mapsto j$, egy izomorfizmus. Másrészt a $K(a,b) \to K(b,a)$, $i \mapsto j$, $j \mapsto i$ is izomorfizmust ad. Továbbá ha $K \leq F$ egy testbővítés, akkor $F \otimes_K K(a,b) \cong F(a,b)$ természetes módon. Speciálisan $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathbb{C}(-1,-1) \cong \mathbb{C}(1,-1) \cong M_2(\mathbb{C})$, hiszen $-1 = i^2 \in (\mathbb{C}^\times)^2$.

A kvaternióalgebrák esetében alapvető kérdés, hogy egy $K(a,b)$ kvaternióalgebra mikor izomorf egy másik, $K(c,d)$ kvaternióalgebrával. Ennek eldöntéséhez segítségünkre lesznek a kvadratikus alakok (szimmetrikus bilineáris függvények).

3. Definíció. *Egy $z = \alpha + \beta i + \gamma j + \delta k \in K(a,b)$ kvaternió konjugáltján a $\overline{z} = \alpha - \beta i - \gamma j - \delta k$ kvaterniót értjük. A z kvaternióról azt mondjuk, hogy tisztán képzetes, ha $\alpha = 0$. A tisztán képzetes kvaterniók halmazát (alterét) $K(a,b)^0$-lal jelöljük. A $z \in K(a,b)$ kvaternió normája $N(z) = z\overline{z} = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2 \in K$, nyoma* $\mathrm{Tr}(z) = z + \overline{z} = 2\alpha \in K$.

4. Lemma. *$\overline{zw} = \overline{w}\ \overline{z}$. Speciálisan $N(zw) = N(z)N(w)$.*

Bizonyítás. Mivel a $f(z,w) = \overline{zw} - \overline{w}\ \overline{z}$ függvény lineáris a z és a w változóban is, ezért az állítást elég belátni, ha $z, w \in \{1, i, j, k\}$. Ezekre viszont az állítás nyilvánvaló a szorzás és a konjugálás definíciójából. A második állításhoz $N(zw) = zw\overline{zw} = zN(w)\overline{z} = N(z)N(w)$. □

A $N(z)$-re úgy tekintünk, mint egy kvadratikus alakra. Mivel $\mathrm{char}(K) \neq 2$, ezért ehhez egyértelműen tartozik egy $B(z,w)$ bilineáris függvény. Valóban,

$$B(z,w) = \frac{N(z+w) - N(z) - N(w)}{2} = \frac{z\overline{w} + w\overline{z}}{2} = \frac{\mathrm{Tr}(z\overline{w})}{2}\ .$$

Legyen $\varphi\colon K(a,b) \to K(c,d)$ egy izomorfizmus (művelettartó bijekció) a két kvaternióalgebra között. Ezalatt azt értjük, hogy φ nemcsak gyűrűizomorfizmus, hanem K-algebra izomorfizmus is, azaz egy K-lineáris leképezés, mely bijektív, és megtartja a szorzást.

5. Állítás. *A φ izomorfizmus tisztán képzetes kvaterniót tisztán képzetes kvaternióba visz: $\varphi(K(a,b)^0) = K(c,d)^0$.*

Bizonyítás. Az állítás bizonyításához a tisztán képzetes kvaterniókat le kell írnunk algebrai módon, csak a $K(a,b)$ K-algebra műveleteit használva. Ezt a következőképpen lehet megtenni: $0 \neq z \in K(a,b)$ pontosan akkor tisztán képzetes, ha $z \notin K$, de $z^2 \in K$. Valóban, $(\beta i + \gamma j + \delta k)^2 = a\beta^2 + b\gamma^2 - ab\delta^2 \in K$, viszont ha $\alpha \neq 0$ és $\beta i + \gamma j + \delta k \neq 0$, akkor

$$(\alpha + \beta i + \gamma j + \delta k)^2 = \alpha^2 + (\beta i + \gamma j + \delta k)^2 + 2\alpha(\beta i + \gamma j + \delta k) \notin K \ ,$$

hiszen $\alpha^2 + (\beta i + \gamma j + \delta k)^2 \in K$, de $2\alpha(\beta i + \gamma j + \delta k) \notin K$. Vegyük észre, hogy mivel φ izomorfizmus, ezért az 1-et az 1-be képezi, így az 1 skalárszorosait, azaz K-t is K-ba. Speciálisan, ha $0 \neq z \in K(a,b)^0$, akkor $\varphi(z) \notin K$, de $\varphi(z)^2 = \varphi(z^2) \in K$. Tehát $\varphi(z) \in K(c,d)^0$. □

Vegyük észre, hogy a tisztán képzetes kvaterniók pontosan azok, melyeknek nyoma 0, vagyis a konjugáltja a -1-szerese.

6. Következmény. *$\varphi(\overline{z}) = \overline{\varphi(z)}$ minden $z \in K(a,b)$-re.*

Bizonyítás. Írjuk z-t $z = \alpha + z_0$ alakba, ahol $z_0 \in K(a,b)^0$. Ekkor $\overline{z} = \alpha - z_0$. Tehát $\varphi(\overline{z}) = \varphi(\alpha - z_0) = \alpha\varphi(1) - \varphi(z_0) = \alpha - \varphi(z_0) = \overline{\alpha + \varphi(z_0)} = \overline{\varphi(z)}$, hiszen $\varphi(z_0)$ tisztán képzetes. □

Speciálisan a φ izomorfizmus megtartja a normát (és a nyomot) is. Ennek az észrevételnek a pontosabb megértéseként kapjuk a következő tételt.

7. Tétel. *A $K(a,b)$ és $K(c,d)$ ($0 \neq a,b,c,d \in K$) kvaternióalgebrák pontosan akkor izomorfak, ha a*

$$-ax^2 - by^2 + abz^2 \quad \text{és a} \quad -cx^2 - dy^2 + cdz^2$$

kvadratikus alakok ekvivalensek (K fölött).

Bizonyítás. Az egyik irányhoz tegyük fel, hogy $\varphi\colon K(a,b) \to K(c,d)$ egy izomorfizmus. Láttuk, hogy φ a tisztán képzetes kvaterniókat tisztán képzetesbe viszi, és azt is, hogy normatartó. Tehát φ megszorítása $K(a,b)^0$-ra egy ekvivalenciát indukál a két kvadratikus alak között. Valóban, ha φ mátrixa S az i,j,k bázisban (mindkét kvaternióalgebrában), akkor S lesz az áttérési mátrix a két kvadratikus alak között.

Visszafelé, jelöljük B-vel a norma által meghatározott bilineáris függvényt $K(a,b)$-n, illetve B'-vel $K(c,d)$-n. Ha a két kvadratikus alak ekvivalens, akkor létezik egy $\varphi_0\colon K(a,b)^0 \to K(c,d)^0$ lineáris bijekció, melyre $B'(\varphi_0(z), \varphi_0(w)) = B(z,w)$. Speciálisan

$$\begin{aligned} \varphi_0(i)^2 = -N(\varphi_0(i)^2) = -B'(\varphi_0(i),\varphi_0(i)) = -B(i,i) = i^2 = a \ , \\ \varphi_0(j)^2 = -B'(\varphi_0(j),\varphi_0(j)) = -B(j,j) = j^2 = b \ , \text{ és} \\ 0 = B(i,j) = B'(\varphi_0(i),\varphi_0(j)) = \frac{\varphi_0(i)\overline{\varphi_0(j)} + \varphi_0(j)\overline{\varphi_0(i)}}{2} = \frac{-\varphi_0(i)\varphi_0(j) - \varphi_0(j)\varphi_0(i)}{2} \ . \end{aligned}$$

Tehát $\varphi_0(i), \varphi_0(j), \varphi_0(i)\varphi_0(j)$ egy ortonormált bázist alkot $K(c,d)^0$-ben, melyben a kvadratikus alak $N(x\varphi_0(i) + y\varphi_0(j) + z\varphi_0(i)\varphi_0(j) = -ax^2 - by^2 + abz^2$. Speciálisan a

$$\begin{array}{rcl} \varphi\colon K(a,b) & \to & K(c,d) \\ \alpha + \beta i + \gamma j + \delta k & \mapsto & \alpha + \beta\varphi_0(i) + \gamma\varphi_0(j) + \delta\varphi_0(i)\varphi_0(j) \end{array}$$

leképezés egy művelettartó bijekció $K(a,b)$ és $K(c,d)$ között. □

Ahhoz, hogy a fenti tételt még effektívebbé tegyük, szükségünk lesz az alábbi lineáris algebrai tételre:

8. Tétel (Witt egyszerűsítési-)**.** *Legyen β egy nemelfajuló szimmetrikus bilineáris függvény egy K fölötti végesdimenziós V vektortéren, $U, U' \leq V$ pedig alterek V-ben. Tegyük fel, hogy $\varphi\colon U \to U'$ egy olyan bijektív lineáris leképezés, melyre $\beta(\varphi(u), \varphi(v)) = \beta(u,v)$ minden $u, v \in U$-ra. Ekkor φ kiterjed egy $\tilde{\varphi}\colon V \to V$ β-t megtartó izomorfizmussá, azaz $\tilde{\varphi}_{|U} = \varphi$ és $\beta(\tilde{\varphi}(u), \tilde{\varphi}(v)) = \beta(u,v)$ minden $u, v \in V$-re.*

Bizonyítás. Rekurzívan bizonyítunk: minden lépésben U-ról egy eggyel nagyobb dimenziós altérre terjesztjük ki a φ izometriát (β-tartó lineáris leképezést). Két esetet különböztetünk meg aszerint, hogy a β megszorítása az U altérre elfajuló-e.

1. eset: A $\beta_{|U}$ megszorítás elfajuló. Ez azt jelenti, hogy van olyan $0 \neq x \in U$ vektor, melyre $\beta(x,u) = 0$ minden $u \in U$-ra. Viszont mivel β nemelfajuló az egész V téren a feltevés szerint, ezért van olyan $y \in V$ vektor, melyre $\beta(x,y) \neq 0$, sőt, megfelelő konstanssal megszorozva y-t azt is feltehetjük, hogy $\beta(x,y) = 1$. Nyilván $y \notin U$, hiszen $x \in U^\perp$. Sőt, vegyük észre, hogy tetszőleges $c \in K$-ra $\beta(y - cx, x) = \beta(y,x) - c\beta(x,x) = \beta(y,x) = 1$, tehát y-t lecserélhetjük $y - cx$-re. Ekkor $\beta(y - cx, y - cx) = \beta(y,y) - 2c\beta(x,y) + \beta(x,x) = \beta(y,y) - 2c$. Speciálisan $c = \beta(y,y)/2$ választással feltehetjük, hogy $\beta(y,y) = 0$. Elég kiterjesztenünk a $\varphi\colon U \to U'$ izometriát az y és U által generált altérre. Ehhez vizsgáljuk meg, milyen tulajdonságokkal kell rendelkezzen a $z = \tilde{\varphi}(y) \in V$ vektor. Ahhoz, hogy $\tilde{\varphi}$ is izometria legyen, az kell, hogy

$$\begin{array}{c} 0 = \beta(y,y) = \beta(\tilde{\varphi}(y), \tilde{\varphi}(y)) = \beta(z,z) \text{ és} \\ \beta(y,u) = \beta(\tilde{\varphi}(y), \tilde{\varphi}(u)) = \beta(z, \varphi(u)) \end{array} \tag{1}$$

teljesüljön minden $u \in U$-ra. Vegyük észre, hogy az $\varphi(u) \mapsto \beta(y,u)$ leképezés egy $f_y\colon U' \to K$ lineáris függvény, azaz az U'^* duális tér egy eleme. Mivel β nemelfajuló, ezért a

$$\begin{array}{rcl} \tilde{\beta}\colon V & \to & V^* \\ v & \mapsto & (\tilde{\beta}(v)\colon u \in V \mapsto \beta(u,v) \in K) \end{array}$$

leképezés injektív, de mivel $\dim_K V = \dim_K V^*$, ezért szürjektív is. Sőt, minden $U' \to K$ lineáris leképezés kiterjeszthető V-re (pl. U' egy bázisának V bázisává való kiegészítésével, és az új bázisvektorokon 0-val értelmezve). Ez valójában azt jelenti, hogy a természetes megszorítás, mint $V^* \to U'^*$ lineáris leképezés szürjektív. Speciálisan a megszorításnak a $\tilde{\beta}$-mal vett kompozíciója is szürjektív, azaz van egy olyan $z_0 \in V$ vektorunk, melynek képe épp $f_y \in U'^*$. Ez pedig pont azt jelenti, hogy $\beta(z_0, \varphi(u)) = \beta(y,u)$ minden $u \in U$-ra. Továbbá a fentiekhez hasonlóan $z = z_0 - \frac{\beta(z_0,z_0)}{2}\varphi(x)$ az (1) feltételt is teljesíti. Ha pedig már van egy ilyen z vektorunk, akkor a $\tilde{\varphi}\colon \langle U, y\rangle \to \langle U', z\rangle$ leképezést a $\tilde{\varphi}(u + \lambda y) = \varphi(u) + \lambda z$ képlettel definiáljuk. A (1) azonosságok miatt ez egy φ-t kiterjesztő izometria.

2. eset: A β megszorítása U-ra nemelfajuló. Az alapötlet a következő: vesszük az U és U' alterek „szögfelezőjét", és arra tükrözzük az egész V vektorteret. A probléma az, hogy csak akkor lehet tükrözni, ha a β megszorítása a „szögfelezőre" nemelfajuló. A szerencse viszont az, hogy két „szögfelező" is van: az $u+\varphi(u)$ alakú elemek által generált altér, illetve az $u-\varphi(u)$ alakú elemek által generált altér – ezek közül valamelyiket mindig tudjuk használni. A precíz bizonyítás $\dim U$ szerinti indukcióval történik.

Ha $\dim U = 1$, akkor $U = \langle x\rangle$ valamilyen $x \in U$ elemre. Sőt, mivel feltettük, hogy $\beta_{|U}$ nemelfajuló, ezért $\beta(x,x) \neq 0$. Ekkor

$$\beta(x \pm \varphi(x), x \pm \varphi(x)) = \beta(x,x) + \beta(\varphi(x)\varphi(x)) \pm 2\beta(x,\varphi(x)) = 2(\beta(x,x) \pm \beta(x,\varphi(x)) \ .$$

Tehát $\beta(x+\varphi(x), x+\varphi(x))$ és $\beta(x-\varphi(x), x-\varphi(x))$ közül nem lehet mindkettő 0, hiszen $\mathrm{char}(K) \neq 2$, és $\beta(x,x) \neq 0$. Legyen $z = x+\varphi(x)$ vagy $z = x-\varphi(x)$ úgy, hogy $\beta(z,z) \neq 0$. Ekkor $z \notin \langle z\rangle^\perp$, azaz $V = \langle z\rangle \oplus \langle z\rangle^\perp$, hiszen $\langle z\rangle^\perp$ egy $(\dim V - 1)$-dimenziós altér. Speciálisan minden $v \in V$ elem egyértelműen felírható $v = w + \lambda z$ alakban, ahol $w \in \langle z\rangle^\perp$. Definiáljuk a $\tilde\varphi\colon V \to V$ leképezést a következőképpen:

$$\tilde\varphi(w+\lambda z) := \begin{cases} v - \lambda z \ , & \text{ha } z = x - \varphi(x) \\ -v + \lambda z \ , & \text{ha } z = x + \varphi(x) \end{cases} .$$

Vegyük észre, hogy a fenti leképezés izometrikus, hiszen izometrikus mind a $\langle z\rangle$, mind a $\langle z\rangle^\perp$ altéren, tehát ezek ortogonális direkt összegén is. Sőt, $\tilde\varphi(x) = \varphi(x)$, hiszen

$$\beta(x+\varphi(x), x-\varphi(x)) = \beta(x,x) - \beta(\varphi(x),\varphi(x)) = 0 \ ,$$

azaz x felírása $\langle z\rangle$-beli és $\langle z\rangle^\perp$-beli vektorok összegeként $x = \frac{x+\varphi(x)}{2} + \frac{x-\varphi(x)}{2}$. Tehát $\tilde\varphi$ definíciója szerint $\tilde\varphi(x) = \frac{x+\varphi(x)}{2} - \frac{x-\varphi(x)}{2} = \varphi(x)$.

Tegyük fel végül, hogy $\dim U > 1$ és persze $\beta_{|U}$ nemelfajuló. A Gram-Schmidt-féle ortogonalizációs eljárással alkalmas bázisban β mátrixa diagonális. Speciálisan (a bázisvektorokat két nemüres halmaz uniójára bontva) U-t felírhatjuk nemtriviális $U_1, U_2 \leq U$ alterek ortogonális direkt összegeként: $U_1 \perp U_2$ és $U_1 \oplus U_2 = U$. Sőt, ekkor β megszorítása U_1-re, ill. U_2-re sem elfajuló, hiszen β mátrixa ezeken az altereken is egy diagonális mátrix, 0-tól különböző elemekkel a főátlóban. Továbbá nyilván $V = U_1 \oplus U_1^\perp$ és $U_2 \leq U_1^\perp$. Jelöljük φ_j-vel a φ megszorítását U_j-re $(j = 1,2)$. Az indukciós feltevés szerint van egy olyan $\tilde\varphi_1\colon V \to V$ izometria, melynek megszorítása U_1-re épp φ_1. Ekkor $\tilde\varphi_1^{-1} \circ \varphi$ értelmes és izometrikus U-n, és U_1-en identikus. Szintén az indukciós feltevés szerint a $\tilde\varphi_1^{-1} \circ \varphi\colon U_2 \to U_1^\perp$ leképezést ki tudjuk terjeszteni az $U_2 \leq U_1^\perp$ altérről egy $\tilde\varphi_2\colon U_1^\perp \to U_1^\perp$ izometriává, sőt $V_1 = U_1 \oplus U_1^\perp$-re is úgy, hogy U_1-en pedig identikus legyen. Ekkor $\tilde\varphi := \tilde\varphi_1 \circ \tilde\varphi_2$ jó kiterjesztés lesz. Egyrészt ez két izometria kompozíciója, azaz megtartja β-t. Másrészt U_1-re való megszorítása $\varphi_1 \circ \mathrm{id} = \varphi_1$, U_2-re való megszorítása pedig $\tilde\varphi_1 \circ \tilde\varphi_1^{-1} \circ \varphi_2 = \varphi_2$. □

9. Következmény. *Legyen β egy nemelfajuló szimmetrikus bilineáris függvény a V vektortéren, és $U, U' \leq V$ alterek. Ha U és U' izometrikusan izomorfak (azaz létezik közöttük β-tartó bijektív lineáris leképezés), akkor $U^\perp$ és $U'^\perp$ is izometrikusan izomorf.*

Bizonyítás. Valóban, a $\varphi\colon U \to U'$ izometriát Witt egyszerűsítési tétele alapján (8. Tétel) kiterjeszthetjük egy $\tilde\varphi\colon V \to V$ izometriává, melynek megszorítása $U^\perp$-re egy $\tilde\varphi_{|U^\perp}\colon U^\perp \to U'^\perp$ izometria. □

A leggyakoribb alkalmazása Witt fenti tételének a következő:

10. Következmény. *Ha az* $a_0x_0^2 + \sum_{i=1}^n a_ix_i^2$ *és az* $a_0x_0^2 + \sum_{i=1}^n c_ix_i^2$ *kvadratikus alakok ekvivalensek és nemelfajulók* ($a_0, a_1, \ldots, a_n \neq 0$)*, akkor a* $\sum_{i=1}^n a_ix_i^2$ *és* $\sum_{i=1}^n c_ix_i^2$ *kvadratikus alakok is ekvivalensek.*

Bizonyítás. A fenti két kvadratikus alak ekvivalenciája azt jelenti, hogy van egy olyan β szimmetrikus bilineáris függvény egy V vektortéren, melynek mátrixa egy $b_0, b_1, \ldots, b_n$ bázisban

$$\begin{pmatrix} a_0 & 0 & \cdots & 0 \\ 0 & a_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & a_n \end{pmatrix},$$

az $e_0, e_1, \ldots, e_n$ bázisban pedig

$$\begin{pmatrix} a_0 & 0 & \cdots & 0 \\ 0 & c_1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & c_n \end{pmatrix}.$$

Az állítás következik a 9. Következményből az $U = \langle b_0 \rangle$ és $U' = \langle e_0 \rangle$ választással. □

Láttuk, hogy $\mathbb{C}$ fölött az egyetlen kvaternióalgebra az $M_2(\mathbb{C})$ mátrixgyűrű. A valós számok $\mathbb{R}$ teste fölött is csak két kvaternióalgebra van izomorfia erejéig: $\mathbb{H}$ és $M_2(\mathbb{R})$. Sőt, nem nehéz belátni, hogy a p-adikus számok $\mathbb{Q}_p$ teste fölött is pontosan két nemizomorf kvaternióalgebra van (még $p = 2$ esetén is!): az egyik persze a mátrixgyűrű, a másik pedig egy ferdetest. $\mathbb{Q}$ fölött azonban jóval bonyolultabb a helyzet: végtelen sok páronként nemizomorf kvaternióalgebra létezik. Ennek oka a következő: $\mathbb{R}$, $\mathbb{C}$, és $\mathbb{Q}_p$ fölött van *analízis*, melynek segítségével a legtöbb számból tudunk négyzetgyököt vonni (egész pontosan $\mathbb{C}$-ben minden számnak van négyzetgyöke). Ugyanis approximálhatjuk a négyzetgyököt, és a sorozat a teljesség miatt konvergálni fog egy $\mathbb{R}$, $\mathbb{C}$, ill. $\mathbb{Q}_p$-beli számhoz. A precíz állítás az, hogy $|\mathbb{C}^\times : (\mathbb{C}^\times)^2| = 1$, $|\mathbb{R}^\times : (\mathbb{R}^\times)^2| = 2$, $|\mathbb{Q}_p^\times : (\mathbb{Q}_p^\times)^2| = 4$ (ha $p > 2$ prím), végül $|\mathbb{Q}_2^\times : (\mathbb{Q}_2^\times)^2| = 8$. Ezzel szemben $|\mathbb{Q}^\times : (\mathbb{Q}^\times)^2| = \infty$, hiszen például a prímszámok osztályai mind különbözők.

11. Következmény. $\mathbb{Q}$ *fölött végtelen sok nemizomorf kvaternióalgebra van.*

Bizonyítás. Belátjuk, hogy a $\mathbb{Q}(-1, -p)$ kvaternióalgebrák páronként nemizomorfak, ha p végigfut a $4k-1$ alakú prímeken. Tegyük fel indirekten, hogy $p \neq q$ két $4k-1$ alakú prím, melyre $\mathbb{Q}(-1, -p) \cong \mathbb{Q}(-1, -q)$. A 7. Tétel szerint ekkor az $x^2 + py^2 + pz^2$ és az $x^2 + qy^2 + qz^2$ kvadratikus alakok ekvivalensek $\mathbb{Q}$ fölött. Ez viszont a 10. Következmény szerint azt jelenti, hogy a $py^2 + pz^2$ és a $qy^2 + qz^2$ kvadratikus alakok is ekvivalensek. Node a p előáll $py^2 + pz^2$ alakban (jelesül $y = 1$, $z = 0$), de nem áll elő $qy^2 + qz^2$ alakban. Valóban, mivel a -1 kvadratikus nemmaradék modulo p (hiszen $p \equiv -1 \pmod 4$), ezért p csak páros kitevőn szerepelhet $qy^2 + qz^2$ prímtényezős felbontásában: A közös nevező négyzetével beszorozva p kitevőjének a paritása nem változik, tehát feltehetjük, hogy $y, z \in \mathbb{Z}$ és relatív prímek (le is oszthatunk a legnagyobb közös osztó négyzetével). Speciálisan legalább az egyik nem osztható p-vel, amikoris $p \nmid q(y^2 + z^2)$, hiszen ellenkező esetben -1-ből lehetne négyzetgyököt vonni modulo p. Például ha $p \nmid y$, akkor $(z/y)^2 \equiv -1 \pmod p$. □

A következő tételben azt látjuk be, hogy egy kvaternióalgebra mindig vagy ferdetest, vagy mátrixgyűrű. Sőt, a kvadratikus alakról le is lehet olvasni viszonylag könnyen, hogy melyik eset áll fenn.

12. Tétel. *Egy $K(a,b)$ kvaternióalgebrára a következők ekvivalensek:*

(*i*) $K(a,b) \cong M_2(K)$*;*

(*ii*) $K(a,b)$ nem *nullosztómentes;*

(*iii*) $K(a,b)$ nem *ferdetest;*

(*iv*) *Az $N\colon K(a,b) \to K$ kvadratikus alaknak van izotróp eleme (azaz olyan $0 \neq z \in K(a,b)$, melyre $N(z) = 0$);*

(*v*) *Az $N\colon K(a,b)^0 \to K$ kvadratikus alaknak van izotróp eleme, azaz van olyan $0 \neq z$* tisztán képzetes *kvaternió, melyre $N(z) = 0$;*

(*vi*) *Az $ax^2 + by^2 = 1$ egyenletnek van megoldása K-ban.*

Bizonyítás. Az $(i) \Rightarrow (ii) \Rightarrow (iii)$ irányok nyilvánvalóak.

A $(iii) \Rightarrow (iv)$ irányhoz tegyük fel indirekten, hogy $z \neq 0$ esetén $N(z) \neq 0$. Ekkor az $\frac{1}{z} = \frac{\overline{z}}{N(z)}$ elem z inverze, tehát $K(a,b)$ ferdetest a (iii) feltevéssel ellentétben.

A $(iv) \Rightarrow (v)$ irányhoz vegyünk egy $0 \neq z \in K(a,b)$ elemet, és tegyük fel, hogy $N(z) = 0$, de z nem tisztán képzetes, azaz $\mathrm{Tr}(z) \neq 0$. Legyen $U = \langle 1, z\rangle$ az 1 és z elemek által generált altér $K(a,b)$-ben. U szükségképpen kétdimenziós, hiszen z nem lehet K-beli, ugyanis $z\overline{z} = N(z) = 0$. Vegyünk egy $0 \neq y \in U^\perp$ elemet. Ilyen van, hiszen $\dim U = 2$, ezért $\dim U^\perp = \dim K(a,b) - \dim U = 2$. Ekkor $z \perp y$ és $1 \perp y$ miatt $\mathrm{Tr}(y\overline{z}) = 2B(y,z) = 0 = \mathrm{Tr}(y)$. Sőt, $\mathrm{Tr}(z)\cdot 1 - z = \overline{z} \in \langle 1, z\rangle$, ezért $2B(y,\overline{z}) = \mathrm{Tr}(yz) = 0$. Továbbá yz és $y\overline{z}$ közül nem lehet mindkettő 0, hiszen akkor összegük $y(z+\overline{z}) = \mathrm{Tr}(z)y$ is 0 lenne, holott $0 \neq \mathrm{Tr}(z) \in K$ és $y \neq 0$. Másrészt $N(yz) = N(y\overline{z}) = N(y)N(z) = 0$, azaz találtunk egy 0-tól különböző kvaterniót (jelesül yz és $y\overline{z}$ közül azt, amelyik $\neq 0$), melynek normája és nyoma is 0, speciálisan tisztán képzetes.

Az $(v) \Rightarrow (vi)$ irányhoz legyen $0 \neq z = \beta i + \gamma j + \delta k$ egy 0 normájú elem, azaz $N(z) = -a\beta^2 - b\gamma^2 + ab\delta^2 = 0$. Először is ha $\delta \neq 0$, akkor $x = \frac{\gamma}{a\delta}$ és $y = \frac{\beta}{b\delta}$ megoldása az $ax^2 + by^2 = 1$ egyenletnek. Ha viszont $\delta = 0$, akkor mivel $z \neq 0$ és $a, b \neq 0$, ezért $\beta, \gamma \neq 0$, tehát $b = -a\frac{\beta^2}{\gamma^2}$. Így ebben az esetben az

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

megoldás.

A $(vi) \Rightarrow (i)$ irányhoz legyen $x_0, y_0 \in K$ olyan, hogy $ax_0^2 + by_0^2 = 1$. Először találunk egy olyan $z \in K(a,b)^0$ tisztán képzetes kvaterniót, melynek normája $N(z) = -1$. Ehhez legyen $w = by_0 i + ax_0 j + k$. Ekkor $N(w) = -ab^2y_0^2 - ba^2x_0^2 + ab = 0$, de persze $w \neq 0$. Mivel a B szimmetrikus bilineáris függvény nemelfajuló $K(a,b)^0$-n (mátrixának determinánsa $a^2b^2 \neq 0$), ezért van olyan $u_1 \in K(a,b)^0$ tisztán képzetes kvaternió, melyre $B(u_1, w) = \frac{1}{2}$. Sőt, $u = u_1 - B(u_1,u_1)w$ választással $B(u,u) = B(u_1,u_1) - 2B(u_1,u_1)B(u_1,w) + B(u_1,u_1)^2B(w,w) = 0$

és $B(u,w) = B(u_1,w) = \frac{1}{2}$, hiszen $B(w,w) = N(w) = 0$. Legyen $z = u - w$. Ekkor $N(z) = B(u-w, u-w) = B(u,u) + B(w,w) - 2B(u,w) = -1$.

A Gram-Schmidt féle ortogonalizációs eljárással z-t egészítsük ki $K(a,b)^0$ egy B-ortogonális bázisává. Speciálisan ebben a bázisban B mátrixa

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & d \end{pmatrix}$$

alakú. Viszont ennek determinánsa $-cd$, B mátrixának determinánsa az eredeti bázisban pedig $a^2b^2 = \det(S)^2(-cd)$, ha $S \in \mathrm{GL}_3(K)$ az áttérési mátrix. Tehát $0 \neq -cd$ egy négyzetelem K-ban, ezért az utolsó bázisvektort az $\frac{ab}{d\det(S)} \neq 0$ számmal beszorozva elérhetjük, hogy $d = -c$. Így a 7. Tétel miatt $K(a,b) \cong K(1,-c) \cong M_2(K)$. □

A következő tételben belátjuk, hogy minden olyan 4-dimenziós egységelemes K-algebra, melynek centruma K, izomorf egy kvaternióalgebrával. Ezek a legkisebb nemtriviális *centrális egyszerű algebrák*. Egy D végesdimenziós K-algebrát centrális egyszerűnek nevezünk, ha centruma K, és egyszerű, azaz nincs nemtriviális kétoldali ideálja. Ezekről bővebben az [1] könyvben lehet olvasni: fontos alkalmazásaik vannak az algebrai számelméletben.

13. Tétel. *Legyen D egy 4-dimenziós egységelemes asszociatív K-algebra (*$\mathrm{char}(K) \neq 2$*). Ekkor a következők ekvivalensek:*

(*i*) *D kvaternióalgebra;*

(*ii*) *$Z(D) = K$ és D egyszerű gyűrű (azaz nincs nemtriviális kétoldali ideálja);*

(*iii*) *$\overline{K} \otimes_K D \cong M_2(K)$;*

(*iv*) *$D \cong M_2(K)$ vagy D olyan ferdetest, melyre $Z(D) = K$.*

Bizonyítás. (*i*) $\Rightarrow$ (*iii*) a fenti megjegyzéshez hasonlóan következik, hiszen a-nak van egy c négyzetgyöke $\overline{K}$-ban, ezért $\overline{K}(a,b) \cong \overline{K}(c^2,b) \cong \overline{K}(1,b) \cong M_2(\overline{K})$.

(*iii*) $\Rightarrow$ (*ii*): Vegyük észre, hogy $M_2(\overline{K})$ centruma 1-dimenziós (mint $\overline{K}$ feletti vektortér), és tartalmazza $\overline{K} \otimes_K Z(D)$-t. Tehát $Z(D)$ is maximum 1 dimenziós lehet csak K felett, de K-t tartalmazza, így $Z(D) = K$. Továbbá ha $I \lhd D$ ideál, akkor $\overline{K} \otimes_K I \lhd \overline{K} \otimes_K D \cong M_2(\overline{K})$. Viszont $M_2(\overline{K})$ egyszerű gyűrű, így D is az.

(*ii*) $\Rightarrow$ (*iv*): Tegyük fel, hogy D nem ferdetest, azaz van olyan $0 \neq x \in D$, ami nem invertálható. Ha pl. bal inverze nincs, akkor az azt jelenti, hogy $x \in Dx \subsetneq D$. Tehát Dx egy nemtriviális balideál D-ben. Legyen $0 \neq I$ egy minimális dimenziójú balideál D-ben. Ekkor a D elemeivel való balszorzás egy K-lineáris leképezés I-n, tehát kapunk egy $\varphi\colon D \to \mathrm{End}_K(I) \cong M_{\dim I}(K)$ K-algebra homomorfizmust. Ráadásul ez injektív, mivel D egyszerű (és $\mathrm{Ker}\varphi \lhd D$). Tehát $1 < \dim_K I < 4$, hiszen $\dim_K I = 1$ esetén $M_1(K) = K$ csak 1-dimenziós, ezért nem képezhető bele a 4-dimenziós D injektíven. Továbbá ha $\dim_K I = 3$ lenne, akkor I lenne az egyetlen nemtriviális balideál D-ben, hiszen $I_1 \neq I_2$ ($\dim_K I_1 = \dim_K I_2 = 3$) nemtriviális balideálok esetén $0 < \dim_K I_1 \cap I_2 < \dim_K I_1 = 3$ lenne, ami ellentmond $\dim I$ minimalitásának. Viszont ekkor I jobbideál is D-ben, mivel $y \in D$ esetén Iy is egy legfeljebb 3-dimenziós balideál D-ben, azaz $Iy = I$ vagy 0, de mindenképp $Iy \subseteq I$. Ez ellentmondás,

hiszen D egyszerű, azaz nincs benne kétoldali ideál. Azt kaptuk tehát, hogy $\dim_K I = 2$, ezért $\dim_K \mathrm{End}_K(I) = 4$, így φ nemcsak injektív, hanem szürjektív is, speciálisan $D \cong M_2(K)$.

$(iv) \Rightarrow (i)$: Azt már láttuk, hogy $M_2(K) \cong K(1,b)$ egy kvaternióalgebra. Legyen tehát D egy 4-dimenziós ferdetest, melyre $Z(D) = K$. Ekkor minden $\alpha \in D$ algebrai K felett (a hatványai lineárisan összefüggők), és $K \leq K(\alpha) \lneq D$, hiszen D nemkommutatív ($Z(D) = K$). Mivel D vektortér $K(\alpha)$ felett is, ezért $|K(\alpha) : K| \mid 4$ (fokszámtétel), ezért minden $\alpha \in D \setminus K$-ra $|K(\alpha) : K| = 2$. Viszont $\mathrm{char}(K) \neq 2$ miatt minden másodfokú bővítés megkapható egy elem négyzetgyökének adjungálásával, ezért van olyan $i \in K(\alpha)$ elem, melyre $i^2 =: a \in K^\times$ és $K(\alpha) = K(i)$. Mivel $i \notin K = Z(D)$, ezért az i-vel való $\varphi_i \colon D \to D$ konjugálás nemtriviális automorfizmusa D-nek, melynek négyzete az $i^2 = a$-val való konjugálás, ami az identitás, hiszen $a \in K = Z(D)$. Tehát φ_i-nek a sajátértékei ± 1, és mivel φ_i nem az identitás (és diagonalizálható, hiszen négyzete az identitás), ezért a -1 is sajátértéke. Tehát van olyan $0 \neq j \in D$, melyre $iji^{-1} = -j$. Ekkor viszont $ij^2i^{-1} = (-j)^2 = j^2$, tehát j^2 felcserélhető i-vel. Viszont az i-vel felcserélhető elemek egy $C_i(D)$ részferdetestet alkotnak D-ben, melyre $K(i) \leq C_i(D) \lneq D$ miatt $C_i(D) = K(i)$ (fokszámtétel). Vagyis $j^2 = b + ci$ alakba írható, ahol $b, c \in K$. Viszont ha $c \neq 0$ lenne, akkor $i = (j^2 - b)/c \in K(j)$ lenne, azaz i és j felcserélhetők lennének, ami ellentmondana $iji^{-1} = -j$-nek.Tehát $c = 0$ és $j^2 = b \in K$, azaz beláttuk, hogy $D \cong K(a,b)$. □

14. Megjegyzés. *A $(ii) \Rightarrow (iv)$ irány a Wedderburn-Artin tételből is következik (nem véletlen, hogy nagyon hasonlítanak a bizonyításaik). Ugyanis ha D egyszerű, akkor* $\mathrm{Jac}(D) = \{0\}$, *hiszen a Jacobson radikál ideál D-ben. Másrészt D nyilván bal-artin, hiszen minden balideál D-ben egy altér, és* $\dim_K D = 4 < \infty$. *Tehát D féligegyszerű, így a Wedderburn-Artin tétel szerint ferdetestek feletti mátrixgyűrűk direkt összege. Node $Z(D)$ egydimenziós, ezért D nem lehet egynél több mátrixgyűrű direkt összege, azaz vagy egy 1×1-es mátrixgyűrű egy ferdetest felett, vagy $M_2(K)$-val izomorf (másképp nem lehetne 4-dimenziós).*

Hivatkozások

[1] Gille, Philippe; Szamuely Tamás, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics **101**, Cambridge University Press, Cambridge, 2006.