KVATERNIONSKE ALGEBRE

SIMON GRAD

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

V članku so predstavljene kvaternionske algebre. Številni koncepti, kot so algebre z deljenjem, razcepna polja in kvadratne razširitve, se v članku pojavijo v konkretnem in elementarnem kontekstu. Drug pomemben koncept, ki ga predstavimo, je stožnica, povezana s kvaternionsko algebro. Članek zaključimo s klasičnim izrekom iz tridesetih let 20. stoletja, imenovanim Wittov izrek, ki pravi, da pridružena stožnica definira kvaternionsko algebro do izomorfizma natančno.

QUATERNION ALGEBRAS

In this paper, we present our main object of study, that of quaternion algebras. Many concepts such as division algebras, splitting fields or quadratic extensions appear here in a concrete and elementary context. Another important notion we shall introduce is that of the conic associated with quaternion algebra. In the end, we mention a classic theorem from 1930 called Witt's theorem asserting that the associated conic determines a quaternion algebra up to isomorphism.

1. Uvod

V tem članku bomo obravnavali končnorazsežne algebre nad poljem $\mathbb{F}$, ki bodo vedno vsebovale enoto za množenje, pri čemer pa množenje ne bo nujno komutativno.

Primer nekomutativne algebre, kateri se bomo bolj posvetili, je leta 1843 odkril W. R. Hamilton. Ta primer je algebra *kvaternionov* nad poljem realnih števil, ki jo označujemo s $\mathbb{H}$. Z njimi je Hamilton nadaljeval inkluzijo razširitev

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}.$$

2. Osnovne lastnosti

Definicija 1. *Algebra kvaternionov* je 4-dimenzionalna algebra z bazo $\{1, i, j, k\}$ nad poljem $\mathbb{R}$ z definiranim množenjem:

$$i^2 = -1, \quad j^2 = -1, \quad ij = -ji = k.$$

Označimo jo s $\mathbb{H}$.

Zgled 1. Seštejmo in zmnožimo kvaterniona $q = 2i + j - 5k$ in $r = 3 + 5j$.

$$q + r = 3 + 2i + 6j - 5k$$

$$\begin{aligned} q \cdot r &= 2i \cdot r + j \cdot r - 5k \cdot r \\ &= 6i + 10ij + 3j + 5jj - 15k - 25kj \\ &= 6i + 10k + 3j - 5 - 15k + 25i \\ &= -5 + 31i + 3j - 5k \end{aligned}$$

Vredno je omeniti, da je množenje kvaternionov asociativna operacija, zato po definiciji velja; $kj = (ij)j = i(jj) = i(-1) = -i$. Opazimo, da je enota za seštevanje 0 in enota za množenje 1 ter da množenje ni komutativno.

V naslednjih definicijah α_i označuje poljubno realno število.

Definicija 2. *Kvaternion* q je element kvaternionske algebre in je oblike

$$q = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k.$$

Definicija 3. *Konjugirani element* q definiramo kot

$$\overline{q} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k.$$

Definicija 4. *Normo* q pa kot

$$N(q) = q\overline{q} = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2.$$

Osnovne lastnosti kvaternionov so bolj podrobno zapisane v [1].

Definicija 5. A je algebra z deljenjem natanko tedaj, ko za vsak neničelni element a iz A obstaja tak $x \in A$, da velja $ax = xa = 1$. Element x je inverz a.

Ta trditev velja zgolj za asociativne algebre. To so algebre, na katerih je množenje asociativna operacija. Pri nas bodo take vse algebre.

Najbolj znan zgled algebre z deljenjem so realna števila.

Trditev 1. $\mathbb{H}$ *je algebra z deljenjem.*

Dokaz:[Hamilton] Dokazati moramo, da za vsak $q \in \mathbb{H}\backslash\{0\}$ obstaja tak $q^{-1} \in \mathbb{H}$, da $qq^{-1} = q^{-1}q = 1$. Tak element obstaja in ga lahko definiramo kot:

$$q^{-1} = \frac{1}{N(q)}\overline{q}.$$

Element q^{-1} je dobro definiran, če velja $N(q) \neq 0$. Iz Definicije 4 opazimo, da bo $N(q) = 0$ natanko tedaj, ko bo $q = 0$. Torej je q^{-1} inverzni element q in posledično je $\mathbb{H}$ algebra z deljenjem. ∎

Izrek 2 (Frobeniusov izrek). *Vsaka končnorazsežna algebra z deljenjem nad* $\mathbb{R}$ *je izomorfna eni od naslednjih algeber* $\mathbb{R}$*,* $\mathbb{C}$ *ali* $\mathbb{H}$*.*

Frobeniusov izrek nam veliko pove o algebrah z deljenjem nad $\mathbb{R}$. Naravno vprašanje, ki se postavlja je, kaj lahko povemo o algebrah z deljenjem nad poljubnim poljem $\mathbb{F}$.

$\mathbb{F}$ bo od tu naprej vedno polje s karakteristiko, ki ni enaka 2. (To pomeni, da $1 + 1 \neq 0$.)

Definicija 6. $\mathbb{F}^\times$ označuje *multiplikativno grupo* polja $\mathbb{F}$. Kot množica je to $\mathbb{F}$ brez 0.

Definicija 7. $\mathbb{F}^{\times 2}$ je podgrupa $\mathbb{F}^\times$, ki ima obliko

$$\mathbb{F}^{\times 2} = \{u_1^2 u_2^2 \dots u_k^2 | u_i \in \mathbb{F}^\times\}.$$

Definicija 8. Za vsaka $a, b \in \mathbb{F}^\times$ definiramo *(posplošeno) kvaternionsko algebro* (a, b) kot 4-dimenzionalno $\mathbb{F}$ algebro z bazo $\{1, i, j, ij\}$ in množenjem definiranim z:

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

Definicija 9. Množici $\{1, i, j, ij\}$ pravimo *kvaternionska baza* (a, b).

Pripomba 1. 1. Če imamo $u, v \in \mathbb{F}^\times$, bo s preslikavo, ki preslika $i \mapsto ui$ in $j \mapsto vj$, definiran izomorfizem med (a, b) in (u^2a, v^2b).

2. Če nastavimo $i \mapsto abj$ in $j \mapsto abi$, potem je

$$(a, b) \cong (a^2b^3, a^3b^2) \cong (b, a).$$

3. Preslikava iz $(a, b) \mapsto (a, b)$ podana s predpisom $q \mapsto \overline{q}$, je *antiavtomorfizem* algebre (a, b), saj je $\overline{q_1 \cdot q_2} = \overline{q_2} \cdot \overline{q_1}$. Velja tudi $\overline{\overline{q}} = q$. Antiavtomorfizem, za katerega velja $(a, b) \cong (b, a)$, se imenuje *involucija*.

4. Norma $q = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 ij$ kvaterniona je tudi v posplošeni kvaternionski algebri definirana kot:

$$N(q) = q\overline{q} = \alpha_0^2 - a\alpha_1^2 - b\alpha_2^2 + ab\alpha_3^2.$$

Torej je norma kot preslikava $N\colon (a, b) \to \mathbb{F}$ neizrojena kvadratna forma. To pomeni, da ne obstaja $q \neq 0$, za katerega je $N(q) = 0$. Norma je tudi multiplikativna preslikava, saj velja:

$$\begin{aligned} N(q_1q_2) &= q_1q_2\overline{q_1q_2} = q_1N(q_2)\overline{q_1} \\ &= N(q_2)N(q_1) \end{aligned}$$

Lema 3. *Kvaternion q iz kvaternionske algebre (a, b) ima inverz natanko tedaj, ko ima neničelno normo. Torej sledi:*

Algebra (a, b) je algebra z deljenjem natanko tedaj, ko ne obstaja neničelni element, ki bi imel ničelno normo.

Definicija 10. Kvaternion q je *čisti*, če zanj velja, da $q \notin \mathbb{F}$ in $q^2 \in \mathbb{F}$.

Pripomba 2. Dokažemo lahko, da je q čisti kvaternion natanko tedaj, ko je $\alpha_0 = 0$. Torej lahko poljubni kvaternion $q = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 ij$ zapišemo kot:

$$q = q_0 + q_1,$$

kjer je $q_0 \in \mathbb{F}$ in q_1 je čisti kvaternion. Norma čistega kvaterniona je

$$N(q_1) = -q_1^2.$$

Zgled 2. Znana algebra je tudi algebra 2×2 matrik $M_2(\mathbb{F})$, ki jo povežemo s kvaternionsko algebro oblike $(1, b)$. To naredimo s pomočjo preslikave, ki preslika

$$i \mapsto I = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad j \mapsto J = \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}.$$

Velja, da je $(1, b)$ izomorfno $M_2(\mathbb{F})$, saj je $\{Id, I, J, IJ\}$ kvaternionska baza in

$$I^2 = 1 \cdot Id \quad J^2 = \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} = b \cdot Id \quad IJ = -JI.$$

Definicija 11. Kvaternionski algebri nad $\mathbb{F}$ rečemo *razcepna*, če je izomorfna $M_2(\mathbb{F})$ algebri.

Trditev 4. *Za kvaternionsko algebro (a, b) so naslednje trditve ekvivalentne.*

1. *Algebra (a, b) je razcepna.*
2. *Algebra (a, b) ni algebra z deljenjem.*

3. Norma $N\colon (a,b) \to \mathbb{F}$ ima netrivialno ničlo.

4. Element b je element norme iz razširitve polja $\mathbb{F}(\sqrt{a})|\mathbb{F}$.

Pripomba 3. Ker smo že pokazali, da velja $(a,b) \cong (b,a)$, lahko vlogi a-ja in b-ja v (4.) točki trditve zamenjamo. Nova oblika točke (4.) pravi: "Element a je element norme iz razširitve polja $\mathbb{F}(\sqrt{b})|\mathbb{F}$."

Da bi bolje razumeli točko (4.) Trditve 4 in znali trditev dokazati, si oglejmo nekaj osnovnih pojmov iz teorije polj, ki jih potrebujemo tudi v nadaljevanju.

Definicija 12. Če je $\mathbb{F}$ podpolje polja E, rečemo, da je E *razširitev polja* $\mathbb{F}$, in zapišemo $E|\mathbb{F}$ (beri: razširitev E nad poljem $\mathbb{F}$).

Definicija 13. E je *enostavna razširitev* polja $\mathbb{F}$, če obstaja tak $a \in E$, da velja:

$$E = \mathbb{F}(a) = \{f(a)g(a)^{-1} | f(X), g(X) \in \mathbb{F}[X], g(a) \neq 0\}.$$

Elementu a pravimo *primitivni element*.

Zgled 3. Eden izmed najbolj preprostih zgledov enostavne razširitve polja je razširitev polja $\mathbb{Q}$. Razširimo ga z željo, da bi znali v novem razširjenem polju rešiti enačbo $x^2 - 2 = 0$. Pri tem dobimo normalno razširitev druge stopnje $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$. Primitivno število je tu $\sqrt{2}$ in premore eno konjugirano število $-\sqrt{2}$. Galoisova grupa $G(\mathbb{Q}(\sqrt{2})|\mathbb{Q}) = \{Id, \sigma\}$, kjer je σ avtomorfizem, ki preslika $\sqrt{2}$ v $-\sqrt{2}$. V tem primeru je

$$N_{\mathbb{Q}(\sqrt{2})|\mathbb{Q}}(a + b\sqrt{2}) = \underbrace{(a + b\sqrt{2})}_{\text{Dobimo iz } Id.} \underbrace{(a - b\sqrt{2})}_{\text{Dobimo iz } \sigma.}.$$

Definicija 14. Če vsebuje $Ker(\mathbb{F}[X] \to \mathbb{F}[a])$ od nič različne polinome, je a *algebraični element* nad $\mathbb{F}$.

Definicija 15. $E|\mathbb{F}$ je *algebraična razširitev*, če je vsak $a \in E$ algebraičen nad $\mathbb{F}$.

Definicija 16. Algebraična razširitev E polja $\mathbb{F}$ je *normalna*, če vsak nerazcepen polinom $f(X) \in \mathbb{F}[X]$, ki ima v polju E vsaj eno ničlo, razpade v E na same linearne faktorje.

Definicija 17. Grupa vseh $\mathbb{F}$ avtomorfizmov končne normalne razširitve $E|\mathbb{F}$ se imenuje *Galoisova grupa*.

Definicija 18. Naj bo E končna razširitev polja $\mathbb{F}$. Funkcija

$$m_\alpha\colon E \to E \quad m_\alpha(x) = \alpha x$$

je linearna transformacija na vektorskem prostoru E.

Norma polja $N_{E|\mathbb{F}}(\alpha)$ je determinanta te linearne transformacije. Le to lahko izračunamo po formuli:

$$N_{E|\mathbb{F}}(\alpha) = \prod_{\sigma \in G(E|\mathbb{F})} \sigma(\alpha).$$

Galvajeve grupe in razširitve polj so bolj podrobno razložene v [4]. Vrnimo se nazaj na Trditev 4 in jo dokažimo.

Dokaz: (1) ⇒ (2) : Vemo, da obstajajo neničelne matrike, ki imajo determinanto enako 0. Te pa niso obrnljive. *(2) ⇒ (3) :* Sledi neposredno iz Leme 3. *(3) ⇒ (4) :* Po (3) vemo, da obstaja tak neničelni q, da $N(q) = 0$. Izraziti želimo b iz $N(q) = \alpha_0^2 - a\alpha_1^2 - b\alpha_2^2 + ab\alpha_3^2 = 0$. Torej dobimo

$$b = N_{\mathbb{F}(\sqrt{a})|\mathbb{F}}(\alpha_0 + \sqrt{a}\alpha_1)N_{\mathbb{F}(\sqrt{a})|\mathbb{F}}(\alpha_2 - \sqrt{a}\alpha_3)^{-1} \in N_{\mathbb{F}(\sqrt{a})|\mathbb{F}},$$

saj je norma multiplikativna funkcija. S tem smo pokazali, da je b element norme iz razširitve polja $\mathbb{F}(\sqrt{a})|\mathbb{F}$. *(4) ⇒ (1) :* Dokažemo, da $(a, b) \cong (1, 4a^2)$, od tu pa kot v Zgledu 2 sledi (1). Predpostaviti smemo, da a ni kvadrat v $\mathbb{F}$. Če je b norma iz $\mathbb{F}(\sqrt{a})$, potem je tudi b^{-1}. Po (4) in naši predpostavki za a najdemo $r, s \in \mathbb{F}$, ki zadoščata enačbi $b^{-1} = r^2 - as^2$. Če definiramo $u = rj + sij$ in $v = (1 + a)i + (1 - a)ui$ opazimo, da velja, da so $\{1, u, v, uv\}$ baza, $u^2 = 1$, $v^2 = 4a^2$ in $uv = -vu$. Zato je res $(a, b) \cong (1, 4a^2)$. ∎

3. Razcep nad kvadratno razširitvijo polja

Poglavje pred nami je povzeto po [2]. Za začetek se spomnimo definicije centra algebre.

Definicija 19. *Center algebre* A nad $\mathbb{F}$ je definiran kot:

$$Z(A) = \{x \in A | xy = yx; \forall y \in A\}.$$

Očitno je, da je $Z(A) \subseteq A$ in po predpostavki, da je $\mathbb{F}$ polje, je $\mathbb{F} \subseteq Z(A)$.

Definicija 20. Če je $\mathbb{F}$ enak $Z(A)$, je A *centralna algebra* nad $\mathbb{F}$.

Trditev 5. *Če je A algebra z deljenjem, sledi da je center algebre polje.*

Trditev 6. *Če je D centralna 4-dimenzionalna algebra z deljenjem, je izomorfna kvaternionski algebri.*

Lema 7. *Če je D centralna 4-dimenzionalna algebra z deljenjem in vsebuje komutativno podalgebro (nad $\mathbb{F}$), ki je izomorfna ne trivialni kvadratni razširitvi polja $\mathbb{F}(\sqrt{a})|\mathbb{F}$, potem je D izomorfna kvaternionski algebri (a, b) za ustrezen $b \in \mathbb{F}^\times$.*

Dokaz: [Leme 7] Recimo, da je $A \subseteq D$ komutativna podalgebra in $A \cong \mathbb{F}(\sqrt{a})|\mathbb{F}$. Torej v A obstaja tak $q \in A$, da $q^2 = a$. Iz tega sledi, da je $q^2 \in \mathbb{F}$ in $q \notin Z(D)$, saj $q = \sqrt{a}$. To pa pomeni, da $q \notin \mathbb{F}$, ki pa je enak $Z(D)$. Od tu sledi, da ima notranji avtomorfizem $(x \mapsto q^{-1}xq)$ red točno 2. Kot $\mathbb{F}$-linearni avtomorfizem od D, ima ta preslikava lastno vrednost -1. To pomeni, da obstaja tak $r \in D$, da

$$qr + rq = 0.$$

Elementi $\{1, q, r, qr\}$ so linearno neodvisni nad $\mathbb{F}$, saj bi v nasprotnem primeru levo množenje s q pokazalo, da $qr = -rq$ leži v $Lin\{1, q\}$, ampak potem bi komutiral s q. To pa ni res, saj je antikomutativna preslikava. Relacija $qr + rq = 0$ implicira, da $\mathbb{F}$-linearni avtomorfizem $x \mapsto r^{-1}xr$ pusti vse 4 bazne elemente fiksne in posledično pusti vse elemente fiksne. Torej $r^2 \in Z(D)$ po predpostavki $Z(D) = \mathbb{F}$ je potem $r^2 \in \mathbb{F}$. Lema velja, če razglasimo $r^2 = b \in \mathbb{F}$. ∎
Dokaz:[Trditve 6] Naj bo $d \in D \setminus \mathbb{F}$. Ker je D končen, je $\{1, d, d^2, d^3, \cdots\}$ linearno neodvisna. Torej obstaja $f \in \mathbb{F}[x]$ da $f(d) = 0$. Ker je D algebra z deljenjem, nima deliteljev niča in lahko sklepamo, da je f nerazcepen. To pomeni $\mathbb{F}[x]/(f) \to D$ je homomorfizem in $\mathbb{F}(d)$ je podalgebra D. Sledi, da stopnja $[\mathbb{F}(d) \colon \mathbb{F}]$ ni enaka 1, saj $d \notin \mathbb{F}$ in ker D ni komutativna stopnja, ni enaka 4. Torej je $[\mathbb{F}(d) \colon \mathbb{F}] = 2$. Od tu pa iz leme vemo, da je $D \cong (a, b)$. ∎

Trditev 8. *Naj bo A kvaternionska algebra nad $\mathbb{F}$ in $a \in \mathbb{F}^\times \setminus \mathbb{F}^{\times 2}$. Naslednje trditve so ekvivalentne.*

1. *A je izomorfna kvaternionski algebri (a, b) za nek $b \in \mathbb{F}^\times$.*
2. *Algebra $A \otimes \mathbb{F}(\sqrt{a})$ je razcepna.*
3. *A vsebuje komutativno podalgebro izomorfno $\mathbb{F}(\sqrt{a})$.*

Da bomo bolje razumeli zapis $A \otimes \mathbb{F}(\sqrt{a})$ in lažje dokazali trditev, si oglejmo, kaj pomeni in kako pridemo do njega.

Definicija 21. Preslikavi $f\colon X \times Y \to \mathbb{F}$, kjer sta X in Y vektorski polji nad poljem $\mathbb{F}$, rečemo *bilinearna*, če velja:

- $f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y)$,
- $f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2)$,
- $f(\alpha x, y) = \alpha f(x, y)$ in
- $f(x, \alpha y) = \alpha f(x, y)$.

Pripomba 4. Če je x v bilinerarni preslikavi konstanten, ta preslikava ustreza pogojem linearne preslikave za y. To velja tudi, če sta vlogi x-a in y-a obrnjeni.

Najprej si oglejmo, kako je s tenzorji v primeru vektorskih prostorov. X in Y sta vektorska prostora. *Tenzor* definiramo na podlagi ideje, da bi $X \times Y$ nadomestili z neko množico $(X \otimes Y)$. Tako bi naša bilinearna preslikava postala linearna preslikava $X \otimes Y \to Z$. Kako se konstruira tenzorje si ne bomo pogledali natančneje. Ogledali pa si bomo določena pravila, ki jih moramo upoštevati ob računanju s tenzorji. V naslednjih lastnostih tenzorjev bo $x_i \in X$, $y_i \in Y$ in $\alpha \in \mathbb{F}$.

Elementi v $X \otimes Y$ so vsote $x_i \otimes y_j$ takih elementov, ki imajo lastnosti:

- $x \otimes (y_1 + y_2) = x \otimes y_1 + x \otimes y_2$,
- $(x_1 + x_2) \otimes y = x_1 \otimes y + x_2 \otimes y$ in
- $(\alpha x) \otimes y = \alpha(x \otimes y) = x \otimes (\alpha y)$.

Če sta A in B algebri nad $\mathbb{F}$, *tenzorski produkt* $A \otimes_{\mathbb{F}} B$ tudi sam postane algebra nad $\mathbb{F}$.

Zgled 4. Vzemimo algebro 2×2 matrik. Ta ima bazo $\{E_{11}, E_{12}, E_{21}, E_{22}\}$. Baza $M_2(\mathbb{R}) \otimes \mathbb{R}$ je $\{(E_{11}, 1), (E_{12}, 1), (E_{21}, 1), (E_{22}, 1)\}$. Primeri seštevanja in množenja na tenzorjih so naslednji:

$$(E_{11} \otimes 1) + (E_{12} \otimes 1) = (E_{11} + E_{12}) \otimes 1$$

$$(\begin{bmatrix} 1 & 2 \\ 1 & 1 \end{bmatrix} \otimes 3) \cdot (\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \otimes 2) = (\begin{bmatrix} 1 & 3 \\ 1 & 2 \end{bmatrix} \otimes 6) = (\begin{bmatrix} 6 & 18 \\ 6 & 12 \end{bmatrix} \otimes 1).$$

Kot vidimo lahko vsak tenzor prevedemo na obliko $(A \otimes 1)$, kjer je A 2×2 matrika.

Torej je $M_2(\mathbb{R}) \otimes \mathbb{R}$ izomorfno $M_2(\mathbb{R})$.

Z razumevanjem tenzorjev, dokažemo Trditev 8.

Dokaz: (1) $\Rightarrow$ (2) : Po predpostavki vemo, da $A \otimes \mathbb{F}(\sqrt{a}) = (a, b) \otimes \mathbb{F}(\sqrt{a})$. Ta algebra je definirana nad poljem $\mathbb{F}(\sqrt{a})$ in je nad isto razširitvijo polja kar izomorfna kvaternionski algebri (a, b) . V tem polju je a kvadrat torej $(a, b) \cong (1, b)$, slednja pa je po Zgledu 2 izomorfna 2×2 matrikam nad $\mathbb{F}(\sqrt{a})$. *(3) $\Rightarrow$ (1) :* Sledi iz Leme 7. *(2) $\Rightarrow$ (3) :* Slednje zaradi dolžine ne bomo dokazovali. (Dokaz je zapisan v knjigi [2].) ∎

4. Pridružene stožnice

Invarianta je značilnost matematičnih objektov, ki ostane nespremenjena, ko se izvede določene transformacije na tem objektu.

Definicija 22. *Pridružena stožnica* $C(a,b)$ je pomembna invarianta v kvaternionski algebri (a,b). $C(a,b)$ je projektivna ravninska krivulja s homogeno enačbo

$$ax^2 + by^2 = z^2, \tag{1}$$

kjer so x, y, z homogene koordinate v projektivni ravnini P^2. (Za več glej [3])

Zgled 5. V primeru $(1,1) \cong M_2(\mathbb{F})$ je enačba krožnica

$$x^2 + y^2 = z^2.$$

Pripomba 5. Stožnica $C(a,b)$ je kanonično pridružena na algebro (a,b) in je neodvisna od izbire baze. Da to res drži, si oglejmo preslikavo, ki $x \mapsto by$, $y \mapsto ax$ in $z \mapsto abz$. Dobimo enačbo $ab^2y^2 + ba^2x^2 = a^2b^2z^2$, ki jo delimo z ab.

$$q^2 = ax^2 + by^2 - abz^2 = 0$$
$$q = xi + yj + zij$$

Opazimo, da je q čisti kvaternion. Ti pa so neodvisni od izbire baze.

Ta opomba nam pove, da če sta kvaternionski algebri (a,b) in (c,d) izomorfni kot algebri nad $\mathbb{F}$, od tu sledi, da sta nad $\mathbb{F}$ izomorfni tudi $C(a,b)$ in $C(c,d)$.

Definicija 23. Če obstajajo taki $x_0, y_0, z_0 \in \mathbb{F}$, ki niso vsi naenkrat enaki 0 in zadoščajo enačbi (1), potem ima stožnica $C(a,b)$ v (x_0, y_0, z_0) $\mathbb{F}$-*racionalno točko.*

Trditev 9. *Kvaternionska algebra* (a,b) *je razcepna natanko tedaj, ko stožnica* $C(a,b)$ *ima* $\mathbb{F}$*-racionalno točko.*

Dokaz: (⇐): Če (x_0, y_0, z_0) je $\mathbb{F}$-racionalna točka in $y_0 \neq 0$, potem iz enačbe 1 izpeljemo

$$b = (\frac{z_0}{y_0})^2 - a(\frac{x_0}{y_0})^2.$$

Točki (4) iz Trditve 4 je zadoščeno. Iz tu sledi, da je (a,b) razcepna.

Če je $y_0 = 0$, potem sledi, da $x_0 \neq 0$. Torej je a norma v $\mathbb{F}(\sqrt{b})|\mathbb{F}$.

(⇒): Vemo, da lahko za $r, s \in \mathbb{F}$ zapišemo $b = r^2 - as^2$. Potem je $(s, 1, r)$ $\mathbb{F}$-racionalna točka na $C(a,b)$.

■

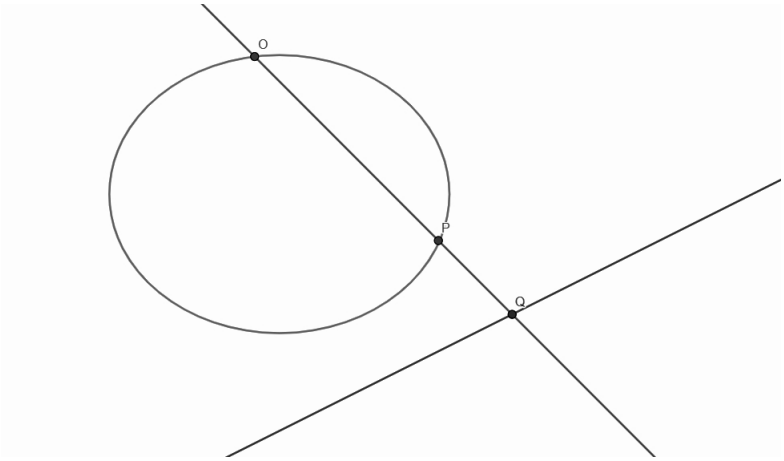
Zgled 6. Za $a \neq 1$ ima stožnica $ax^2 + (1-a)y^2 = z^2$ $\mathbb{F}$-racionalno točko v $(1,1,1)$. Torej je po trditvi kvaternionska algebra (a, 1-a) razcepna.

Pripomba 6. Gladka projektivna stožnica nad $\mathbb{F}$ je izomorfna projektivni premici P^1 nad $\mathbb{F}$ natanko tedaj, ko ima $\mathbb{F}$-racionalno točko.

Izomorfizem je podan tako (glej sliko 1), da se vzame presečišče premice, ki gre skozi $\mathbb{F}$-racionalno točko O in točko na stožnici P in premice P^1, ki je koordinata v P^2.

Na ta način dobimo še en ekvivalenten pogoj za razcepne kvaternionske algebre.

Slika 1. Projekcija stožnice na premico



Zgled 7. $\mathbb{F}$ je končno polje s q elementi (q je lih). Potem je vsaka kvaternionska algebra (a, b) nad $\mathbb{F}$ razcepna.

Da to dokažemo je dovolj po trditvi pokazati, da ima stožnica $C(a, b)$ $\mathbb{F}$-racionalno točko. Našli bomo točko (x_0, y_0, z_0), kjer $z_0 = 1$. Multiplikativna grupa $\mathbb{F}^\times$ je ciklična in reda $(q-1)$. Torej je točno $1 + \frac{q-1}{2}$ kvadratov v $\mathbb{F}$ (vključno z 0). Množici $\{ax^2 | x \in \mathbb{F}\}$ in $\{1 - by^2 | y \in \mathbb{F}\}$ imata obe moč $1 + \frac{q-1}{2}$, torej morata imeti skupni element.

Zgled 8. Poglejmo si polje $\mathbb{Z}_7$ in kvaternionsko algebro $(2, 3)$. $\mathbb{Z}_7^{\times 2} = \{0, 1, 2, 4\}$. Izračunajmo množici $\{ax^2 | x \in \mathbb{F}\}$ in $\{1 - by^2 | y \in \mathbb{F}\}$.

$$\{ax^2 | x \in \mathbb{F}\} = \{0, 1, 2, 4\}$$
$$\{1 - by^2 | y \in \mathbb{F}\} = \{1, 2, 3, 5\}$$

Tako smo našli $\mathbb{F}$-racionalni točki. To sta: $(2, 0, 1)$ ali $(1, 4, 1)$.

Definicija 24. $\mathbb{F}(t)$ polje racionalnih funkcij nad poljem $\mathbb{F}$.

$\mathbb{F}(t)$ je po definiciji definiran kot polje deliteljev kolobarja polinomov $\mathbb{F}[t]$. Če $t \mapsto 0$, potem je $\mathbb{F}(t) \to \mathbb{F}$ homomorfizem, ki mu rečemo *specializacijska preslikava* pridružena t.

Zgled 9. Naj bo (a, b) kvaternionska algebra nad $\mathbb{F}$.

Algebra (a, b) je razcepna nad $\mathbb{F}$ natanko tedaj, ko $(a, b) \otimes \mathbb{F}(t)$ je razcepna nad $\mathbb{F}(t)$.

Predpostavimo, da je podana točka (x_t, y_t, z_t) iz $C(a, b)$ definirana nad $\mathbb{F}(t)$. Ker je enačba 1, ki definira $C(a, b)$, homogena, lahko po množenju z ugodnim elementom iz $\mathbb{F}(t)$ domnevamo, da x_t, y_t, z_t vsi ležijo v $\mathbb{F}[t]$ in vsaj eden izmed njih je neničelna konstanta. Potem specializacijska preslikava poda $\mathbb{F}$-točko $(x_t(0), y_t(0), z_t(0))$ v $C(a, b)$.

Za konec podamo kriterij za razcepne kvaternionske algebre nad $\mathbb{F}(t)$, ki ne pride iz $\mathbb{F}$.

Zgled 10. Za $a \in \mathbb{F}^\times$ je algebra (a, t) nad $\mathbb{F}(t)$ razcepna, natanko tedaj ko je a kvadrat v $\mathbb{F}$.

Ponovimo razmislek $(x_t, y_t, z_t) \in \mathbb{F}(t)$ v $C(a, b)$, kot v prejšnjem primeru lahko sklepamo, da $x_t, y_t, z_t \in \mathbb{F}[t]$. Če bi bila x_t in z_t deljiva s t, potem bi po enačbi 1 isto veljalo tudi za y_t. To pomeni, da lahko enačbo delimo dokler x_t in z_t ne bosta več deljiva s t. Potem lahko nastavimo $t = 0$. Od tu pa vemo, da je $ax_t(0)^2 = z_t(0)^2$ oziroma $a = z_t(0)^2 x_t(0)^{-2}$. Iz zadnje enačbe pa je očitno, da je a kvadrat.

5. Wittov izrek

V zadnjem kratkem poglavju na hitro omenimo še Wittov izrek, ki ga zaradi zahtevnosti ne bomo dokazovali. Dokaz je zapisan v knjigi [2].

Izrek 10 (Wittov izrek). *Naj bosta* $Q_1 = (a_1, b_1)$ *in* $Q_2 = (a_2, b_2)$ *kvaternionski algebri in* $C_i = (a_i, b_i)$ *pridružena stožnica.* Q_1 *in* Q_2 *sta izomorfni nad* $\mathbb{F}$ *natanko tedaj, ko sta polji* $\mathbb{F}(C_1)$ *in* $\mathbb{F}(C_2)$ *izomorfni nad* $\mathbb{F}$.

V algebraični geometriji sta dve gladki krivulji izomorfni natanko tedaj, ko sta njuna funkcijska polja izomorfna. Od tu Wittov izrek lahko zapišemo drugače.

Izrek 11 (Witt 2). *Kvaternionski algebri sta izomorfni natanko tedaj, ko sta pridruženi stožnici izomorfni kot algebraični krivulji.*

6. Zaključek

V članku smo definirali kvaternionske algebre nad poljubnim poljem in pogledali mnoge njihove lastnosti. Drug pomemben koncept, ki smo ga predstavili, je bila stožnica povezana s kvaternionsko algebro. Na koncu smo omenili še Wittov izrek, ki je povezal oba pojma.

Kvaternionske algebre so v matematiki zelo uporaben koncept, ki se uporablja v teoriji števil. Za nekatera polja, vključno s polji algebrskih števil, je vsak element drugega reda lahko predstavljen s kvaternionsko algebro.

LITERATURA

[1] M. Brešar, *Uvod v algebro*, eKnjiga, DMFA - založništvo, Ljubljana, 2018.

[2] P. Gille in T. Szamuely, *Central Simple Algebras and Galois Cohomology*, eKnjiga, Cambridge university press, New York, 2006.

[3] A. Vavpetič, *Afina in projektivna geometrija*, eKnjiga, samozaložba A. Vavpetič, Ljubljana, 2011.

[4] I. Vidav, *Algebra*, 7. izdaja, DMFA - založništvo, Ljubljana, 2017.