O KVATERNIONOVÝCH ALGEBRÁCH

LENKA MACÁLKOVÁ

ABSTRAKT. V tomto článku jsou prezentovány dvě ekvivalentní definice kvaternionových algeber a uvedeny některé příklady. Cílem je seznámit čtenáře se základními pojmy. Více podrobností lze nalézt v [1].

ÚVOD

V první části se seznámíme s pojmem kvaternionové algebry. Uvedeme dvě základní definice a ukážeme, že jsou ekvivalentní. Dále definujeme stopu a normu prvku. V další části poskytneme charakterizaci kvaternionových algeber. Inspirací pro tento článek byly příklady z knihy [1]. Jejich prostřednictvím se budeme čtenáři snažit problematiku alespoň částečně přiblížit.

1. DEFINICE KVATERNIONOVÝCH ALGEBER

Nejprve uvedeme dvě definice kvaternionové algebry nad tělesem F. V první definici je třeba zvlášť ošetřit případ, kdy je těleso charakteristiky 2. Po zavedení dalších potřebných pojmů a uvedení potřebných tvrzení ukážeme, že jsou spolu ekvivalentní. V dalším textu budeme pak vycházet z obou definic a používat tu, která bude v danou chvíli pro naše potřeby vhodnější.

Definice 1.1 (První definice kvaternionové algebry)**.** Případ char $F \neq 2$: *Kvaternionovou algebrou* A nad tělesem F rozumíme vektorový prostor dimenze čtyři s bázovými vektory $1, i, j, k$, kde neutrálním prvkem vzhledem k operaci násobení na A je 1 a dále platí, že

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

kde $a, b \in F^*$.
Případ char $F = 2$: *Kvaternionovou algebrou* A nad F rozumíme, jako v předchozím případě, čtyřdimenzionální vektorový prostor s bází $1, i, j, k$, kde $1 \in F$ je neutrální prvek vzhledem k násobení. Narozdíl od prvního případu, zavedeme operaci násobení následujícím způsobem:

$$i^2 + i = a, \quad j^2 = b, \quad ij = j(1 + i) = k,$$

kde $a \in F, b \in F^*$.

2010 *MSC.* Primární 11R52.
Klíčová slova. kvaternionová algebra, norma, stopa.
Práce byla podporována projektem A-Math-Net – Síť pro transfer znalostí v aplikované matematice (CZ.1.07/2.4.00/17.0100).

Kvaternionovou algebru označujeme symbolem $\left(\frac{a,b}{F}\right)$ (tzv. *Hilbertův symbol*).

Poznámka 1.2. V dalším textu budeme uvažovat pouze tělesa, která nemají charakteristiku 2.

Než uvedeme druhou definici kvaternionové algebry, připomeneme pojmy, které se v definici budou vyskytovat.

Definice 1.3. Nechť R je okruh s jedničkou.

1. *Centrum* okruhu R je množina $Z(R) = \{a \in R | ra = ar, \ \forall r \in R\}$.
2. R-*algebra* A je okruh s jedničkou spolu s homomorfismem $f : R \longrightarrow A$, kde $f(1_R) = 1_A$ a $f(R) \subseteq Z(A)$.
3. A je *centrální* R-*algebra*, jestliže $f(R) = Z(A)$.
4. A je *jednoduchá* R-*algebra*, jestliže nemá žádné netriviální oboustranné ideály.

Poznámka 1.4. V dalším textu budeme v R-algebře A ztotožňovat okruh R s jeho obrazem $f(R)$.

Definice 1.5. Nechť F je těleso, $\overline{F}$ je jeho algebraický uzávěr a A je komutativní F-algebra. Pak A se nazývá *separabilní* K-*algebra*, jestliže $A \cong F[x]/(f(x))$, kde $f(x)$ je polynom s různými kořeny v $\overline{F}$.

Poznámka 1.6. Mějme těleso F a F-algebru A. Máme-li automorfismus ϕ na A, pro který platí, že ϕ zúženo na F je identita, budeme jej nazývat F-automorfismem.

Definice 1.7. *Konjugací* na F-algebře L, rozumíme zobrazení $m \mapsto \overline{m}$, $\forall m \in L$, které je netriviálním F-automorfismem nad L.

Definice 1.8 (Druhá definice kvaternionové algebry)**.** Nechť F je těleso. *Kvaternionová algebra* A s centrem F je centrální algebra A dimenze 4 nad F taková, že existuje separabilní algebra L dimenze 2 nad F a $\theta \in F^*$ tak, že $A = L + Lu$, kde $u \in A$ splňuje

$$u^2 = \theta, \quad um = \overline{m}u$$

pro všechna $m \in L$, kde $m \mapsto \overline{m}$ je konjugace na L. Tuto konjugaci rozšíříme na celou kvaternionovou algebru předpisem $\overline{u} = -u$.

Definice 1.9. Pomocí konjugace (viz definice 1.7) definujeme *normu* prvku $\mathrm{n}(x)$ a *stopu* $\mathrm{tr}(x)$ jako

$$\mathrm{n}(x) = x\overline{x}, \quad \mathrm{tr}(x) = x + \overline{x}.$$

Příklad 1.10. Prvky kvaternionové algebry A můžeme vnořit do okruhu matic nad $F(\sqrt{a})$. Je-li char $F \neq 2$, stačí například uvážit vnoření:

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad j \mapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}.$$

Normu můžeme v tomto případě chápat jako determinant matice a stopu jako stopu matice.

Příklad 1.11. Nejznámějším příkladem kvaternionové algebry jsou tzv. *Hamiltonovy kvaterniony* $\mathcal{H}$. Jedná se o případ, kdy $F = \mathbb{R}$ a $i^2 = j^2 = k^2 = -1$, tj. $\mathcal{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$.

Mezi další příklady patří např. $A = \left(\frac{-2,3}{\mathbb{Q}}\right)$. Zde je $i^2 = a = -2$, $j^2 = b = 3$, $k^2 = -ab = 6$. Podívejme se nyní na násobení, normu a stopu v této algebře. Nechť $x = a_0 + a_1 i + a_2 j + a_3 k$, $y = b_0 + b_1 i + b_2 j + b_3 k$ jsou prvky algebry A. Pak

$$\begin{aligned} x \cdot y &= a_0 b_0 - 2a_1 b_1 + 3a_2 b_2 + 6a_3 b_3 + (a_0 b_1 + a_1 b_0 - 3a_2 b_3 + 3a_3 b_2)i + \\ &\quad +(a_0 b_2 - 2a_1 b_3 + a_2 b_0 + +2a_3 b_1)j + (a_0 b_3 + a_1 b_2 - a_2 b_1 + b_3 b_0)k. \end{aligned}$$

Tedy například

$$(1 + 2i - j + 3k)(1 - i + 2j + k) = 17 + 22i - 9j + 7k.$$

Pro výpočet stopy a normy budeme využívat konjugaci definovanou jako $\overline{x} = a_0 - a_1 i - a_2 j - a_3 k$. Potom

$$\begin{aligned} \mathrm{tr}(x) &= x + \overline{x} = 2a_0 \\ \mathrm{n}(x) &= x\overline{x} = a_0^2 + 2a_1^2 - 3a_2^2 - 6a_3^2. \end{aligned}$$

Například pro $x = 1{+}2i{-}j{+}3k$ je $\mathrm{tr}(x) = 2$, $\mathrm{n}(x) = -48$. Prvky této kvaternionové algebry můžeme reprezentovat maticemi následujícím způsobem:

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i \mapsto \begin{pmatrix} \sqrt{-2} & 0 \\ 0 & -\sqrt{-2} \end{pmatrix} \quad j \mapsto \begin{pmatrix} 0 & 3 \\ 1 & 0 \end{pmatrix}.$$

Poznámka 1.12. Pro libovolné těleso F platí, že $M_2(F) \equiv \left(\frac{1,1}{F}\right)$. Pro izomorfismus stačí zvolit

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Příklad 1.13. Nechť A je kvaternionová algebra nad tělesem F. Mějme prvek $x = a_0 + a_1 i + a_2 j + a_3 k \in A \setminus F$. Nechť char $F \neq 2$. Pak snadno spočteme, že

$$x^2 = a_0^2 - aa_1^2 - ba_2^2 + aba_3^2 + 2a_0(a_1 i + a_2 j + a_3 k).$$

Tedy prvek $x \in A \setminus F$ je kořenem kvadratického polynomu $x^2 - x \cdot \mathrm{tr}(x) + \mathrm{n}(x)$.

Než ukážeme ekvivalenci definic 1.1 a 1.8, dokážeme některá pomocná tvrzení, která v důkazu využijeme.

Lemma 1.14. *Nechť F je těleso a $A = \left(\frac{a,b}{F}\right)$ je kvaternionová algebra podle definice 1.1. Pak platí*

1. $\left(\frac{a,b}{F}\right) \cong \left(\frac{ax^2,by^2}{F}\right)$ *pro libovolné $x, y \in F^*$.*
2. *A je centrální algebra.*
3. *A je jednoduchá algebra.*

Důkaz. 1. Mějme $A = \left(\frac{a,b}{F}\right)$ s bází $\{1, i, j, k\}$, $A' = \left(\frac{ax^2,by^2}{F}\right)$ s bází $\{1, i', j', k'\}$. Definujme zobrazení $\varphi : A' \longrightarrow A$ s předpisem $\varphi(1) = 1$, $\varphi(i') = xi$, $\varphi(j') = yj$ a $\varphi(k') = xyk$. Protože platí

$$\begin{aligned} (xi)^2 &= ax^2, \\ (yj)^2 &= by^2, \\ (xi)(yj) &= (xy)(ij) = -(xy)(ji) = -(yj)(xi), \end{aligned}$$

jedná se o izomorfismus F-algeber.

2. Nechť $\overline{F}$ je algebraický uzávěr F. Pak zřejmě platí $\left(\frac{a,b}{F}\right) \otimes_F \overline{F} \cong \left(\frac{a,b}{\overline{F}}\right)$. Protože $\overline{F}$ je algebraicky uzavřené, je každý jeho prvek čtvercem. Tedy podle první části tohoto tvrzení dostáváme, že $\left(\frac{a,b}{\overline{F}}\right) \cong \left(\frac{1,1}{\overline{F}}\right) \cong M_2(\overline{F})$. Centrem $M_2(\overline{F})$ je $\overline{F}$, a tudíž centrum $\left(\frac{a,b}{F}\right)$ je F.
3. Mějme nenulový ideál $I \subseteq A$ a nechť $\overline{F}$ opět značí algebraický uzávěr tělesa F. Protože $\left(\frac{a,b}{F}\right) \otimes_F \overline{F} \equiv \left(\frac{a,b}{\overline{F}}\right)$, pak $I \otimes_F \overline{F}$ je nenulový ideál v $M_2(\overline{F})$. Víme, že $M_2(\overline{F})$ je jednoduchá algebra. Navíc I je vektorový prostor nad F, který má dimenzi 4, a tedy $I = A$.

$\square$

Nyní již ukážeme, že definice 1.1 a 1.8 jsou spolu ekvivalentní. Uvažme nejprve kvaternionovou algebru dle definice 1.8. Operaci násobení můžeme rozepsat následujícím způsobem:

$$(l_1 + l_2u)(l_3 + l_4u) = (l_1l_3 + l_2\overline{l_4}\theta) + (l_1l_4 + l_2\overline{l_3})u.$$

Protože L je separabilní algebra dimenze 2, je buď kvadratickým rozšířením tělesa F nebo je izomorfní součinu $F \times F$. V obou případech existují generátory L nad F, označme je $1, y$. Pak za bázi z definice 1.1 stačí zvolit $1, i = y, j = u$, tedy $b = \theta$.

Mějme nyní kvaternionovou algebru podle definice 1.1 s bází $1, i, j, k$. Tato algebra je podle lemmatu 1.14 centrální a jednoduchá. Rozšíření $F(i)$ je zřejmě separabilní, tedy $L = F(i)$. Položíme $u = j$ a ukážeme, že pak $A = L + Lu$ splňuje definici kvaternionové algebry 1.8. Stačí ověřit, že $um = \overline{m}u$ pro všechna $m \in L$.

Pokud je char $F \neq 2$, definujeme zobrazení $^-$ pro libovolné $x \in A$, $x = a_0 + a_1i + a_2j + a_3k$ jako

$$\overline{x} = a_0 - a_1i - a_2j - a_3k.$$

Prvky $m \in L$ jsou tedy ve tvaru $m = a_0 + a_1i$. Pak

$$j(a_0 + a_1i) = a_0j + a_1ji = a_0j - a_1ij = (a_0 - a_1i)j,$$

a tedy požadovaná rovnost platí. Pro char $F = 2$ definujeme

$$\overline{x} = (a_0 + a_1) + a_1i + a_2j + a_3k.$$

Potom dostáváme, že

$$j(a_0 + a_1i) = a_0j + a_1ji = a_0j + a_1j + a_1ij = ((a_0 + a_1) + a_1i)j.$$

2. Klasifikace kvaternionových algeber

Věta 2.1. *Každá kvaternionová algebra* $\left(\frac{a,b}{F}\right)$ *je buď okruh s dělením nebo je izomorfní okruhu matic* $M_2(F(\sqrt{a}))$.

Důkaz. Důkaz tvrzení pro náročnost není uveden. Lze jej nalézt například v [1] na straně 81. □

Poznámka 2.2. Okruhem s dělením rozumíme nekomutativní okruh, kde ke každému nenulovému prvku existuje prvek inverzní.

Uvažujme nyní kvaternionovou algebru dle definice 1.8.

Věta 2.3. *Nechť* $\mathrm{n}(L) = \{x \in F | x = \mathrm{n}(l) \text{ pro } l \in L\}$. *Pak* A *je izomorfní okruhu matic* $M_2(F(\sqrt{a}))$ *právě tehdy, když* L *není těleso nebo* $\theta \in n(L)$.

Důkaz. Než začneme s důkazem tvrzení, označme $i^2 = a$, $u^2 = \theta$. V prvním a druhém kroku ukážeme implikaci zprava doleva, ve třetím a čtvrtém kroku provedeme důkaz opačné implikace.

1. Nejprve ukážeme, že pokud L není těleso, pak A je izomorfní okruhu matic $M_2(F(\sqrt{a}))$. Nechť L není těleso. Pokud k prvku $a_0+a_1 i \in L$ existuje prvek inverzní, je obecně ve tvaru $(a_0 + a_1 i)^{-1} = \frac{a_0-a_1 i}{a_0^2-aa_1^2}$. Protože L není těleso, existuje nenulový prvek $a_0+a_1 i$, který inverzi nemá, tzn. $a_0^2-aa_1^2 = 0$. To ale znamená, že $a_0^2 = aa_1^2$. Uvážíme-li prvek $h \in A$, $h = (a_0+a_1 i)+(a_0+a_1 i)u$, pak

$$\begin{aligned} \mathrm{n}(h) &= (a_0 + a_1 i + a_0 u + a_1 iu) \cdot (a_0 - a_1 i - a_0 u - a_1 iu) = \\ &= (a_0^2 - aa_1^2) - (a_0^2 - aa_1^2)\theta = 0. \end{aligned}$$

   Prvek h má nulovou normu, a tedy je dělitelem nuly. Protože v A existují dělitelé nuly, je A je podle věty 2.1 izomorfní okruhu matic $M_2(F(\sqrt{a}))$.
2. Nechť nyní L je těleso a $\theta \in \mathrm{n}(L)$. Naším cílem je dokázat, že A je izomorfní okruhu matic. Protože $\theta \in \mathrm{n}(L)$, existuje $m = a_0 + a_1 i \in L$ tak, že $\mathrm{n}(m) = a_0^2 - aa_1^2 = \theta$.

   Pro libovolný prvek $h \in A$ platí, že

$$h^2 = h_0^2 + h_1^2 a + h_2^2\theta - h_3^2 a\theta + 2h_0(h_1 i + h_2 u + h_3 iu).$$

   Nyní ukážeme, že koeficienty h_0, h_1, h_2, h_3 lze zvolit tak, že $h^2 = 1, h \neq \pm 1$. Pokud zvolíme $h_0, h_1 = 0$, pak

$$h^2 = (h_2^2 - h_3^2 a)\theta.$$

   Protože $\mathrm{n}(m) = \mathrm{n}(a_0+a_1 i) = \theta$ a L je těleso, pak $\mathrm{n}(m^{-1}) = \mathrm{n}(\hat{a_0}+\hat{a_1} i) = \frac{1}{\theta}$. Položíme $h_2 = \hat{a_0}, h_3 = \hat{a_1}$, a tím jsme našli vhodný prvek $h \in A$. Pak

$$0 = h^2 - 1 = (h-1)(h+1),$$

   a tím jsme našli netriviální dělitele nuly a podle věty 2.1 je A izomorfní s $M_2(F(\sqrt{a}))$.

3. Ukažme nyní, že pokud A je izomorfní okruhu matic $M_2(F(\sqrt{a}))$ a současně L je tělesem, pak $\theta \in \mathrm{n}(L)$. Libovolný prvek $h \in A$ je tvaru $h = a_0 + a_1 i + (a_2 + a_3 i)u$, kde $a_k \in F$ pro $k = 0, \ldots, 3$. Pro normu platí
$$\mathrm{h}(x) = a_0^2 - a_1^2 a - a_2^2 \theta + a_3^2 a\theta = \mathrm{n}(m_1) - \theta \mathrm{n}(m_2),$$
kde $m_1, m_2 \in L$. Protože A je izomorfní okruhu matic, obsahuje dělitele nuly, a tedy existuje prvek $h \in A$ takový, že $\mathrm{n}(h) = 0$, tzn. $\mathrm{n}(m_1) - (\mathrm{n}(m_2))\theta = 0$. Protože L je těleso, pak $\theta = \frac{\mathrm{n}(m_1)}{\mathrm{n}(m_2)}$. Nyní ukážeme, že θ je normou konkrétního prvku z L. Nechť $m_1 = a_0 + a_1 i$, $m_2 = b_0 + b_1 i$, pak
$$\begin{aligned}\theta &= \frac{a_0^2 - a_1^2 a}{b_0^2 - b_1^2 a} = \\ &= \frac{(a_0 + a_1 i)(a_0 - a_1 i)}{(b_0 + b_1 i)(b_0 - b_1 i)} = \\ &= \underbrace{\left(\frac{a_0 + a_1 i}{b_0 + b_1 i} \cdot \frac{b_0 - b_1 i}{b_0 - b_1 i}\right)}_{m} \underbrace{\left(\frac{a_0 - a_1 i}{b_0 - b_1 i} \cdot \frac{b_0 + b_1 i}{b_0 + b_1 i}\right)}_{\overline{m}} = \\ &= \mathrm{n}(m), \text{ kde } m \in L,\end{aligned}$$
a tedy $\theta \in \mathrm{n}(L)$.
4. Nyní zbývá ukázat, je-li A izomorfní okruhu matic $M_2(F(\sqrt{a}))$ a současně $\theta \notin \mathrm{n}(L)$, pak L není těleso. Budeme postupovat sporem. Předpokládejme, že $A \equiv M_2(F(\sqrt{a}))$, $\theta \notin \mathrm{n}(L)$ a L je těleso. Pak se ale dostáváme do sporu, neboť podle 2. platí implikace
$$A \equiv M_2(F(\sqrt{a})) \text{ a současně } L \text{ je těleso } \Longrightarrow \theta \in \mathrm{n}(L).$$

□

Definice 2.4. Pokud je A kvaternionová algebra nad F izomorfní s $M_2(F(\sqrt{a}))$, pak říkáme, že A *se štěpí nad* F.

Poznámka 2.5. Z Weddeburnovy věty (viz [2] strana 556) víme, že každá konečná algebra s dělením je tělesem. Tedy každá kvaternionová algebra nad konečným tělesem F je izomorfní s $M_2(F)$.

Příklad 2.6. Uvažme nad tělesem $\mathbb{Q}$ dvě následující kvaternionové algebry
$$A = \left(\frac{-2, -3}{\mathbb{Q}}\right), \ A' = \left(\frac{2, 1}{\mathbb{Q}}\right).$$
Algebra A je algebrou s dělením, neboť pro normu prvků platí
$$\mathrm{n}(x) = a_0^2 + 2a_1^2 + 3a_2^2 + 6a_3^2,$$
a tedy jediným prvkem s nulovou normou je 0 a algebra A nemá dělitele nuly.

Algebra A' je izomorfní s $M_2(\mathbb{Q}(\sqrt{2}))$, neboť například $1 + i + j + k$ je dělitelem nuly, protože $\mathrm{n}(1 + i + j + k) = 0$.

Reference

[1] C. Maclachlan, A. W. Reid: *The Arithmetic of Hyperbolic 3-Manifolds*, Springer-Verlag, New York, 2003.
[2] D. S. Dummit, R. M. Foote: *Abstract Algebra*, 3rd ed., John Wiley & Sons, Hoboken, 2004.

Lenka Macálková, Ústav matematiky a statistiky, Přírodovědecká fakulta, Masarykova univerzita v Brně, Kotlářská 2, 611 37 Brno, Česká republika,
e-mail: `macalkoval@gmail.com`