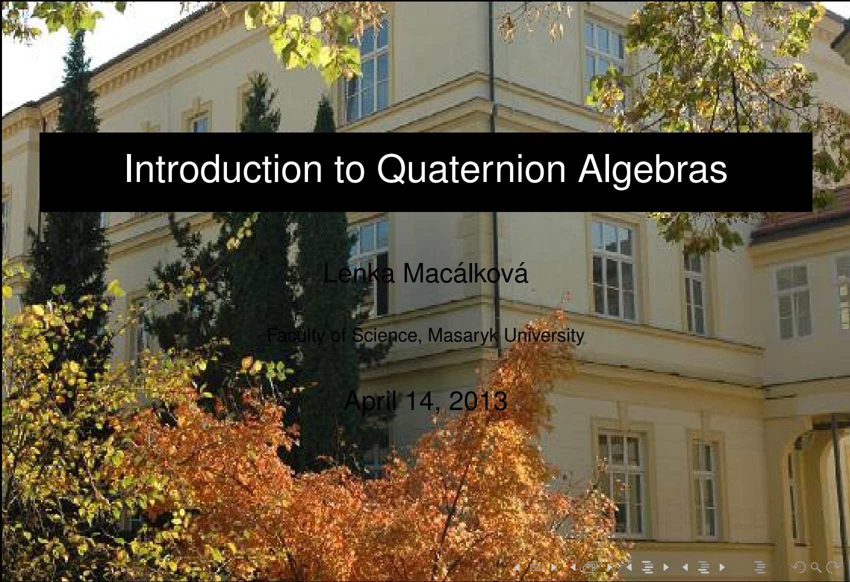

Introduction to Quaternion Algebras

Lenka Macálková

Faculty of Science, Masaryk University

April 14, 2013

Definition of Quaternion Algebra

Let F is a field, char $F \neq 2$. A *quaternion algebra* $\mathcal{A}$ over F is a four-dimensional F-space with basis $1, i, j, k$. Multiplication on $\mathcal{A}$ is defined by following rules:

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

where $a, b \in F^*$. We will denote this quaternion algebra by $(\frac{a,b}{F})$.

Hamilton quaternions

$$\mathcal{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$$

Let $x = 1 + i + 2j, y = -3 + 2i - j - k$, then

$$\begin{aligned}
x + y &= (1 + i + 2j) + (-3 + 2i - j - k) = \\
&= -2 + 3i + j - k \\
x \cdot y &= (1 + i + 2j) \cdot (-3 + 2i - j - k) = \\
&= -3 - 3i - 6j - 6k \\
y \cdot x &= (-3 + 2i - j - k) \cdot (1 + i + 2j) = \\
&= -3 + i - 8j + 4k
\end{aligned}$$

History of Hamilton quaternions

William Rowan Hamilton(1805-1865)

- Irish mathemetician, physicist and astronomer
- inventor of quaternions

Lemma

Let $\mathcal{A} = \left(\frac{a,b}{F}\right)$.

1. $\left(\frac{a,b}{F}\right) \cong \left(\frac{ax^2,by^2}{F}\right)$ for any $a, b, x, y \in F^*$
2. The center of $\mathcal{A}$ is F (i.e., $\mathcal{A}$ is central)
3. $\mathcal{A}$ has no proper two-sided ideal (i.e., $\mathcal{A}$ is simple).

Norm and trace

Definition

Let $\mathcal{A}_0$ be subspace of quaternion algebra $\mathcal{A}$ spanned by i, j, k. Then elements of $\mathcal{A}_0$ are called the *pure quaternions* in $\mathcal{A}$.

Each element x of quaternion algebra $\mathcal{A}$ has a unique decomposition as $x = a + \alpha$, where $a \in F$ and $\alpha \in \mathcal{A}_0$. We can define *conjugate* $\overline{x}$ of x by $\overline{x} = a - \alpha$.

Definition

For $x \in \mathcal{A}$ the *reduced norm* and *reduced trace* are defined as follows $n(x) = x\overline{x}$ and $tr(x) = x + \overline{x}$.

Examples

Let $\mathcal{A} = \left(\frac{-1,5}{\mathbb{Q}}\right)$, $x = \frac{1}{5} + i - j - k$, then

$$\begin{aligned} tr(x) &= (\frac{1}{5} + i - j - k) + (-\frac{1}{5} - i + j + k) = \frac{2}{5} \\ n(x) &= (\frac{1}{5} + i - j - k) \cdot (-\frac{1}{5} - i + j + k) = -\frac{224}{25} \end{aligned}$$

This quaternion algebra has zero divisors, e.g. $1 + 2i + k$.

Hamilton quaternions are division algebra.

Examples

Quaternion algebra $(\frac{-a,a}{F})$ is not division algebra, element $a+k$ is zero divisor.

For any field we have $\left(\frac{1,1}{F}\right) \cong \mathrm{Mat}_{2\times 2}(F)$. Isomorphism is given by

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

Classification

Skolem-Noether Theorem

Let $\mathcal{A}$ is a simple central algebra over F and $\mathcal{B}$ is a simple algebra over F. If $\varphi, \psi : \mathcal{B} \to \mathcal{A}$ are homomorphisms, then exists an invertible element $c \in \mathcal{A}$ such that $\varphi(b) = c^{-1}\psi(b)c$ for all $b \in \mathcal{B}$.

Lemma

If $\mathcal{A} = \left(\frac{a,b}{F}\right)$ is quaternion algebra over F, then $\mathcal{A}$ is either division algebra or $\mathcal{A}$ is isomorphic to $\mathrm{Mat}_{2\times 2}(F(\sqrt{a}))$.

Example

Any quaternion algebra $\left(\frac{a,b}{F}\right)$ is subalgebra of $\mathrm{Mat}_{2\times 2}(F(\sqrt{a}))$. We consider mapping

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

Theorem

Every four-dimensional simple central algebra over F of characteristic $\neq 2$ is a quaternion algebra.

Proof

Let $\mathcal{A}$ be four-dimensional simple central algebra over F. If $\mathcal{A}$ is isomorphic to $\mathrm{Mat}_{2\times 2}(F)$, it is quaternion algebra, so by lemma we can assume then $\mathcal{A}$ is a division algebra. For $w \notin Z(\mathcal{A})$, subalgebra $F(w)$ is commutative, thus $F(w)$ is field.
Because $\mathcal{A}$ is central, $F(w) \neq \mathcal{A}$. Consider $u \in \mathcal{A} \setminus F(w)$. Elements $1, u, w, uw$ are independent over F, thus form basis of $\mathcal{A}$. Thus

$$w^2 = a_0 + a_1 w + a_2 u + a_3 uw, \quad a_i \in F.$$

Since $u \notin F(w)$, $w^2 = a_0 + a_1 w$. Thus $F(w)$ is quadratic extension of F. Choose $y \in F(w) \setminus F$ such that $y^2 = a \in F$, so $F(w) = F(y)$.

The automorphism on $F(y)$ induced by $y \mapsto -y$ be induced by conjugation by invertible $z \in \mathcal{A}$ (by Skolem-Noether Theorem), thus $zyz^{-1} = -y$. Since $1, y, z, yz$ are independed over F, clearly $z \notin F(y)$. Since $z^2yz^{-2} = y$ so that $z^2 \in Z(\mathcal{A})$ (i.e., $z^2 = b \in F$). So $\{1, y, z, yz\}$ is basis of $\mathcal{A}$ and $\mathcal{A} \cong \left(\frac{a,b}{F}\right)$.

Theorem

For $\mathcal{A} = (\frac{a,b}{F})$, the following are equivalent:

1. $\mathcal{A} \cong \mathrm{Mat}_{2\times 2}(F(\sqrt{a}))$.
2. $\mathcal{A}$ is not a division algebra.
3. $\mathcal{A}$ is isotropic as a quadratic space with the norm form.
4. $\mathcal{A}_0$ is isotropic as a quadratic space with the norm form.
5. The quadratic form $ax^2 + by^2 = 1$ has solution in F.
6. If $E = F(\sqrt{b})$, then $a \in N_{E|F}(E)$.

Proof – part 1

$1 \Leftrightarrow 2$ We have isomorphism

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

The ring of matrices is not division ring, thus $\mathcal{A}$ is not division ring too.

$2 \Leftrightarrow 3$ It follows since $x \in \mathcal{A}^\times \Leftrightarrow n(x) \in F^\times$.

$3 \Rightarrow 4$ Let $0 \neq x = a_0 + a_1 i + a_2 j + a_3 k \in \mathcal{A}, n(x) = 0$. If $tr(x) = 0$, we are done. Otherwise, we can assume $a_1 \neq 0$. Then $n(x) = 0 \Rightarrow a_0^2 - ba_2^2 = a(a_1^2 - ba_3^2)$. We consider $y = b(a_0 a_3 + a_1 a_2)i + a(a_1^2 - a_3^2)j + (a_0 a_1 + ba_2 a_3)k$, using brutal power gives $n(y) = 0$. For contradiction we assume $\mathcal{A}_0$ is anisotropic. Thus $y = 0$ and $-aa_1^2 + aba_3^2 = 0$. Thus $n(a_1 i + a_3 k) = 0$, and if $\mathcal{A}_0$ is anisotropic, $a_1 = 0$ and we get contradiction.

Proof – part 2

$4 \Rightarrow 5$ Let $0 \neq x \in \mathcal{A}_0$, $x = a_1 i + a_2 j + a_3 k, n(x) = 0$, thus at least two of a_1, a_2, a_3 are non-zero. If $a_3 \neq 0$, then $a\left(\frac{a_2 a}{a_3}\right)^2 + b\left(\frac{a_1}{ba_3}\right)^2 = 1$ and 5) holds. Otherwise $a\left(\frac{1+2a}{2a}\right)^2 + b\left(\frac{a_2(1-a)}{2aa_1}\right)^2 = 1$ and we are done.

$5 \Rightarrow 6$ Let $ax_0^2 + by_0^2 = 1$. If $x_0 = 0$, then $\sqrt{b} \in F$ and result is obvious. If $x \neq 0$ then $n\left(\frac{1}{x_0} + \frac{\sqrt{b}y_0}{x_0}\right) = a$.

$6 \Rightarrow 2$ Let $\sqrt{b} = c \in F$ then $j^2 = b = c^2$. So $(c-j)(c+j) = 0$ and $\mathcal{A}$ has zero divisors. Now let $\sqrt{b} \notin F$, then there exist $x_1, y_1 \in F$, such that $a = x_1^2 - by_1^2$. Then $n(x_1 + i + y_1 j) = 0$ and $\mathcal{A}$ has non-zero non-invertible element.

SAGE

- open-source mathematics software
- implemented in Python
- online www.sagemath.org
- packages for number theory

SAGE and Quaternion Algebras

- most of functions are implemented for algebras over infinite fields
- working with elements (plus, times, norm, trace)
- classification of quaternion algebras
- discriminants, orders, ...

Thank you for your attention.