Quaternion algebras over fields

Definitions and first results

Let K be a field and $L \mid K$ a quadratic extension. Let $\theta \in K$.

Definition: $H := L \oplus Lu$ with $u \in H$ such that $u^2 = \theta$ and $u\lambda = \overline{\lambda}u$ for all $\lambda \in L$, with $^{-} : L \longrightarrow L$ the non-trivial automorphism from L to L.

Notation: $H := (L, ^{-}, \theta)$

Remark: H is a central simple algebra over K. A quaternion algebra is a central simple algebra of dimension 4 over K.

We also introduce a second

Definition: Let $a, b \in K^*$ and $H := (\frac{a,b}{K})$ be the algebra generated by i, j with the relations $i^2 = a, j^2 = b, ij = -ji = k$. We have $k^2 = -ab$. As K-vectorspace H is generated by the elements $\{1, i, j, k\}$.

Remark: For $L = K(i), \theta = b, u = j, i^2 = a$ we get: $L \oplus Lu \cong (\frac{a,b}{K})$. The elements $a, b \in K^*$ as well as L, θ are not unique, because of: $(\frac{a,b}{K}) \cong (\frac{b,a}{K}) \cong (\frac{a,-ab}{K}) \cong (\frac{ac^2,b}{K})$.

For a field extension $M \mid K$ we have: $M \otimes_K (\frac{a,b}{K}) \cong (\frac{a,b}{M})$, respectivly: $M \otimes_K (L, ^{-}, \theta) \cong (M \otimes_K L, ^{-}, \theta)$

Definition: Let $h = \alpha + i\beta + j\gamma + k\delta \quad \in H$ with $\alpha, \beta, \gamma, \delta \in K$. $\bar{h} := \alpha - i\beta - j\gamma - k\delta$, respectivly: for $h = \lambda_1 + \lambda_2 u$ define: $\bar{h} = \lambda_1 - \lambda_2 u$. $^{-} : H \longrightarrow H$ is an involution, extending the non-trivial K-automorphism $^{-} : L \longrightarrow L$, called conjugation. This conjugation is additive and anti-communtative.

For $h \in H$ we define $n(h) := h \cdot \bar{h}, \quad t(h) := h + \bar{h}$. This is the reduced norm and the reduced trace. The reduced norm defines a quadratic form on H

Also define: $H \times H \longrightarrow K$ given by: $(h_1, h_2) \mapsto < h_1, h_2 > := t(h_1 \cdot h_2)$.

Lemma

- $h \in H$ is invertible $\Longleftrightarrow n(h) \neq 0$
- $<, >$ defines a K-linear, non-degenerate bilinearform.

Remark: Let $H \longrightarrow End_K(H), \quad h \mapsto l_h : a \mapsto h \cdot a$ be the left regular representation. Then it holds: $2t(h) = Tr(l_h)$ and $n(h)^2 = det(l_h)$.

Definition: Let $F \mid K$ be an extension. F is called splitting field for $H \iff H_F := F \otimes_K H \cong M_2(F)$. A F-representation is an inclusion $H \longrightarrow M_2(F)$.

Examples:

1. $M_2(K) \cong (\frac{1,-1}{K})$. Let $L = K(i)$ with $i^2 = -1$ and $j^2 = 1$. Consider the matrices $e_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, e_i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, e_j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, e_{ij} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. This gives an K-algebra-isomorphism:
$$e_1 \mapsto 1, \quad e_i \mapsto i, \quad e_j \mapsto j, \quad e_{ij} \mapsto ij$$

2. $\mathbb{H} := (\frac{-1,-1}{\mathbb{R}})$ the real quaternions have a $\mathbb{C}$-representation:
$$\mathbb{H} = \{\begin{pmatrix} z_1 & z_2 \\ -\bar{z_2} & \bar{z_1} \end{pmatrix} \in M_2(\mathbb{C})\}$$
$\mathbb{H} = \mathbb{R}(i) \oplus \mathbb{R}(i)j$ with $i^2 = -1, \quad j^2 = -1$. We have: $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$ with $\mathbb{H} \ncong M_2(\mathbb{R})$.

3. Let $a, b \in K^*$. Consider:
$$I = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, \quad J = \begin{pmatrix} \sqrt{b} & 0 \\ 0 & -\sqrt{b} \end{pmatrix}, \quad E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
Then it holds: $I^2 = aE_2, \quad J^2 = bE_2, \quad IJ = -JI = \begin{pmatrix} 0 & -\sqrt{b} \\ a\sqrt{b} & 0 \end{pmatrix}$
For $\alpha, \beta, \gamma, \delta \in K^*$ one gets:
$$\alpha E_2 + \beta I + \gamma J + \delta IJ = \begin{pmatrix} \alpha + \gamma\sqrt{(b)} & \beta - \delta\sqrt{b} \\ a(\beta + \delta\sqrt{b}) & \alpha - \gamma\sqrt{(b)} \end{pmatrix}$$
With $\lambda_s \in L = K(\sqrt{b})$ for $s = 1, 2$, we obtain:
$$(\frac{a, b}{K}) \cong \{\begin{pmatrix} \lambda_1 & \lambda_2 \\ a\bar{\lambda}_2 & \bar{\lambda}_1 \end{pmatrix} \in M_2(K(\sqrt{b}))\}$$
and recover the splitting field as $K(\sqrt{b})$.

Remark: Let H be a quaternion algebra over K.
Then $B(h_1, h_2) := \frac{1}{2}t(h_1 \cdot \bar{h_2}) \in K$ gives a symmetric, non-degenerate, bilinearform. We get $B(h, h) = n(h)$.

For pure quaternions $H_0 = \{h \in H \mid h = \beta i + \gamma j + \delta ij\}$ the set $\{i, j, ij\}$ forms an orthogonal basis. K is orthogonal to the span of this set, so that (H, B) as quadratic space, has $\{1, i, j, ij\}$ as orthogonal basis.

We have the following

Proposition: For $H = (\frac{a,b}{K})$ and $H' = (\frac{c,d}{K})$ with $a, b, c, d \in K$ the following statements are equivalent:

1. H and H' are isomorphic K-algebras
2. H and H' are isometric as quadratic spaces
3. H_0 and H_0' are isometric as quadratic spaces

Proof: done in the seminar

Corollary: $(\frac{a,a}{K}) \cong (\frac{a,-1}{K})$ because of their isometric normforms.

Theorem: For $H = (\frac{a,b}{K})$ the following statements are equivalent:

1. $H = (\frac{1,-1}{K}) \cong M_2(K)$
2. H is not a division algebra
3. H is isotrop as quadratic space
4. $a \in Norm_{F|K}(F)$ with $F = K(\sqrt{b})$

Proof: done in the seminar

Corollary: Let $a \in K^*$, then $(\frac{a,-a}{K}) \cong (\frac{1,a}{K}) \cong M_2(K)$. If $a \neq 0, 1$ then $(\frac{a,1-a}{K}) \cong M_2(K)$.

Remark: For a finite field K, not of characteristic 2, we get: $(\frac{a,b}{K}) \cong M_2(K)$ for all $a, b \in K$

The Skolem-Noether-Theorem

Lemma: $\varphi : H \otimes_K H \longrightarrow End_K(H), \quad h_1 \otimes_K h_2 \mapsto (h \mapsto h_1 \cdot h \cdot h_2)$ is a K-algebra isomorphism.

Proof: done in the seminar

Theorem: Let $L \mid K$ be a quadratic extension contained in H. $\tau : L \longrightarrow L$ the non-trivial K-automorphism of L. Then there exists a K-algebra-automorphism $\sigma : H \longrightarrow H$ which extends τ, and is of the form: $\sigma(h) = a \cdot h \cdot a^{-1}$ for an $a \in H^*$. Every K-automorphism $\sigma : H \longrightarrow H$ is an inner automorphism.

Proof: done in the seminar

Corollary: Let $L \mid K$ be a quadratic extension contained in H. Then there exists $\theta \in K^*$ such that $H \cong (L, \bar{\ }, \theta)$. θ depends on the non-trivial automorphism $\tau : L \longrightarrow L$.

Proof: done in the seminar

Remark: Let $Aut(H \mid K)$ be the group of K-automorphisms of H. Then $Aut(H \mid K) \cong H^*/K^*$.

Proposition: Let $H = (L, \bar{\ }, \theta)$. Then it holds: $H \cong M_2(K) \Longleftrightarrow \theta \in n(L)$.

Proof: $\Longrightarrow$: If H is not a division algebra then there exists an element $h \neq 0 \in H$ with $n(h) = 0$. Let h be written in the form $h = \lambda + \mu u$ with $u^2 = \theta \in K^*$. Then it follows: $0 = n(h) = \lambda \cdot \bar{\lambda} - \mu \cdot \bar{\mu} \cdot \theta$ with $\lambda, \mu \neq 0$. This gives $\theta = n(\frac{\lambda}{\mu}) \in n(L)$.

$\Longleftarrow$: $\theta \in n(L) \Longleftrightarrow \theta = \lambda \cdot \bar{\lambda}$ for a $\lambda \in L$. Consider $h := \lambda + u \neq 0 \in H$. For this element we get: $n(h) = 0$. So H is not a division algebra.

Further results

Proposition (Frobenius): Let D be a finite dimensional division algebra with center $\mathbb{R}$. Then $D \cong \mathbb{H}$ (the real quaternions)

Proof: Let $d \in D - \mathbb{R}$. Then $\mathbb{R}(d) \cong \mathbb{R}(i) \cong \mathbb{C}$ with $i^2 = -1$. So, $\mathbb{R}(d)$ is proper contained in D. Let $\tilde{d} \in D$ be an element such that $\mathbb{R}(\tilde{d}) \cong \mathbb{R}(u)$ with $u^2 = -1$ and $u \notin \mathbb{R}(i)$. The elements i, u do not commute, because otherwise $\mathbb{R}(i, u)$ would be a field extension. But then $u \in \mathbb{R}(i)$. Consider now the element $j := iui + u$. For this we get: $ij = -ji$. Let $\mathcal{H} := \mathbb{R}(i) + \mathbb{R}(i)j \subset D$, and $\tau : i \mapsto -i$ be conjugation in $\mathbb{R}(i)$. Then $\varphi_j : \mathcal{H} \longrightarrow \mathcal{H}$, defined as $x \mapsto j \cdot x \cdot j^{-1}$ extends τ, because of $\varphi_j(i) = -i$. We now claim that $j^2 \in \mathbb{R}$: $j^2 \cdot i = i \cdot j^2$ So, $j^2 \in \mathbb{R}(i)$. $\tau(j^2) = \varphi_j(j^2) = j^2$. So, $j^2 \in \mathbb{R}$ and $j^2 < 0$ because otherwise $j \in \mathbb{R} = center(D)$. But then we would get $jij^{-1} = -i = i$, which is absurd. So we conclude that $\mathcal{H} \cong \mathbb{H} \subset D$. If $\mathbb{H}$ is proper contained in D, we can choose an element $\hat{d} \in D - \mathbb{H}$ such that $\hat{d}i = i\hat{d}$ and $\hat{d}^2 \in \mathbb{R}$. We proceed as done before. But then we get: $\hat{d}ji = \hat{d}(-i)j = i\hat{d}j$, which means that $dj \in \mathbb{R}(i)$. But then $\hat{d} \in \mathbb{H}$ which contradicts our choise. $\Longrightarrow \mathbb{H} \cong D$.

We conclude the section with a remarkable property of quaternion algebras:

Proposition: Let $a, b, c \in K^*$. Then it holds:

$$(\frac{a,b}{K}) \otimes_K (\frac{a,c}{K}) \cong (\frac{a,bc}{K}) \otimes_K M_2(K)$$

Proof: Let $H_1 := (\frac{a,b}{K}) \cong < 1, i_1, j_1, k_1 >_K$ with $i_1^2 = a, \quad j_1^2 = b, \quad k_1^2 = -ab$ and similar $H_2 := (\frac{a,c}{K}) \cong < 1, i_2, j_2, k_2 >_K$. Consider $H_3 :=< 1 \otimes 1, i_1 \otimes 1, j_1 \otimes j_2, k_1 \otimes j_2 >_K =: < \mathbf{1}, I, J, IJ >_K$. This is a 4-dimensional subalgebra of $H_1 \otimes H_2$. We have: $I^2 = a, \quad J^2 = bc, \quad IJ = -JI$. This gives $H_3 \cong (\frac{a,bc}{K})$. Define $H_4 :=< 1 \otimes 1, 1 \otimes j_2, i_1 \otimes k_2, -ci_1 \otimes i_2 >_K =< \mathbf{1}, \tilde{I}, \tilde{J}, \tilde{K} >_K$. We then get: $\tilde{I}^2 = c, \quad \tilde{J}^2 = -a^2c, \quad \tilde{I}\tilde{J} = \tilde{J}\tilde{I}$. This gives: $H_4 = (\frac{c,-a^2c}{K})$. Using the classification by quadratic forms we obtain that $H_4 \cong M_2(K)$. Further more we get that $H_1 \otimes H_2 \cong H_3 \otimes H_4 \cong H_3 \otimes M_2(K)$. This follows from the fact that $\{1, I, J, K\}$ commutes with $\{1, \tilde{I}, \tilde{J}, \tilde{K}\}$ elementwise. Evaluating the two tensorproducts gives the proposition.

Corollary: $\mathbb{H} \otimes \mathbb{H} \cong M_4(\mathbb{R})$.

Proof: $(\frac{-1,-1}{\mathbb{R}}) \otimes_{\mathbb{R}} (\frac{-1,-1}{\mathbb{R}}) \cong (\frac{-1,1}{\mathbb{R}}) \otimes_{\mathbb{R}} M_2(\mathbb{R}) \cong M_2(\mathbb{R}) \otimes_{\mathbb{R}} M_2(\mathbb{R}) \cong M_4(\mathbb{R})$.