Quaternion algebras over local fields

Nuno Arala

A fundamental result in the theory of quadratic forms over local fields is the following:

Theorem 1. *Let F be a local field. Then there is a unique (up to isomorphism) quaternion division algebra over F, namely,*

$$D = \left(\frac{\pi, u}{F}\right)$$

where π is a uniformizer of F and u is such that $F(\sqrt{u})$ is the unique unramified quadratic extension of F.

This is relatively easy to prove when F is nondyadic, i.e., the residue class field k_F has characteristic different from 2. In fact, if F is nondyadic, the statement of Theorem 1 can be made simpler: u can be taken to be any non-square unit in $\mathcal{O}_F$. Only in the dyadic case the unique unramified extension of F needs to be brought into play in order to specify a "special" non-square u. A proof of the general case is given in [1], Section VI.2. I found the argument presented there to be quite sketchy at some points, and hence I decided to write another version of the same proof with some more details whose addition I thought would be welcome.

Example 2 ($F = \mathbb{Q}_2$)**.** Let's compute the unique quaternion division algebra over the field of 2-adic numbers $\mathbb{Q}_2$. The unique quadratic extension of the residue class field $\mathbb{F}_2$ is $\mathbb{F}_4 = \mathbb{F}_2(\varphi)$ where $\varphi^2 + \varphi + 1 = 0$. The polynomial $x^2 + x + 1 \in \mathbb{F}_2[x]$ lifts to the polynomial $X^2 - X - 1 \in \mathbb{Q}_2[X]$, whence the unique unramified quadratic extension L of $\mathbb{Q}_2$ is $\mathbb{Q}_2(\gamma)$ where $\gamma^2 - \gamma - 1 = 0$. This equality implies $\gamma = \frac{1 \pm \sqrt{5}}{2}$, and hence $L = \mathbb{Q}_2(\gamma) = \mathbb{Q}_2(\sqrt{5})$. Theorem 1 then implies that

$$\left(\frac{2, 5}{\mathbb{Q}_2}\right)$$

is the unique quaternion division algebra over $\mathbb{Q}_2$.

Proof of Theorem 1

Let E be a quaternion division algebra over F. Keeping the notation used so far, the goal is to prove that $E \cong \left(\frac{\pi, u}{F}\right)$. Let furthermore v be the normalized valuation of F, $A = \mathcal{O}_F$ the ring of integers, $\mathfrak{p}$ its maximal ideal and $k_F = A/\mathfrak{p}$ the residue field. We split the proof into several steps.

Step 1 *(E as a discretely valued skew-field)*. We make E into some sort of "non-commutative discretely valued field". For this we define

$$w'(x) := v(\mathrm{N}(x))$$

for $x \in E \setminus \{0\}$, where N is the norm form of E. The image of w' is some additive subgroup of $\mathbb{Z}$; let it be $d\mathbb{Z}$, for some positive integer d. We have $2 = v(\pi^2) = v(\mathrm{N}(\pi)) = w'(\pi) \in d\mathbb{Z}$, whence $d \in \{1, 2\}$. Define now $w(x) = \frac{w'(x)}{d}$, and set $w(0) = \infty$.

We claim that w behaves like a valuation (we only don't call it a valuation because the underlying division ring E is not commutative). By this we mean that

(i) $w(xy) = w(x) + w(y)$ for any $x, y \in E$;

(ii) $w(x + y) \geq \min\{w(x), w(y)\}$ for any $x, y \in E$.

Property (i) is obvious. For property (ii), recall from the theory of local fields that if K is a finite extension of F then $u : K \to \mathbb{Z}$ defined by $u(x) = v(\mathrm{N}_{K/F}(x))$ defines a valuation on E. The only reason we cannot apply this directly is that E is not commutative, but there is a way to remedy that. Fix $x, y \in E$. If one of x, y is 0 then (ii) is clear. Otherwise, divide both sides by $w(y)$, and it suffices to prove that

$$w\left(\frac{x}{y} + 1\right) \geq \min\left\{w\left(\frac{x}{y}\right), w(1)\right\}. \tag{1}$$

But $\frac{x}{y}$ is contained in a quadratic extension of F, which is a (commutative) subfield of E. Furthermore, in this subfield the norm $\mathrm{N}_{F\left(\frac{x}{y}\right):F}$ coincides with the quaternion norm N. The inequality (1) now follows, by applying the previously mentioned blackbox to the field extension $F\left(\frac{x}{y}\right) : F$.

Define now

$$B := \{x \in E : w(x) \geq 0\} \text{ and } \mathfrak{P} := \{x \in E : w(x) > 0\}$$

which behave as the ring of integrs and maximal ideal of the "discretely valued skew-field" E. In fact it is clear that B is a subring of E and $\mathfrak{P}$ is an ideal of B. We assemble together some related observations.

(a) $B \cap F = A$ and $\mathfrak{P} \cap A = \mathfrak{p}$. These are obvious.

(b) The (two-sided) ideals of B are precisely (apart from the zero ideal)

$$\{x \in E : w(x) \geq m\}$$

for non-negative integers m. It is clear that sets of this form are indeed ideals. Conversely, let $\mathfrak{a}$ be a nonzero ideal of B, and let $m = \min\{w(x) : x \in \mathfrak{a}\}$; suppose $m = w(r)$ where $r \in \mathfrak{a}$. Then clearly $\mathfrak{a} \subseteq \{x \in E : w(x) \geq m\}$. On the other hand, if $w(x) \geq m$, then

$$w\left(xr^{-1}\right) = w(x) - w(r) = w(x) - m \geq 0$$

and hence $\frac{x}{r} \in B$. Since $x = (xr^{-1}) \cdot r$ it follows that $x \in \mathfrak{a}$. This establishes $\mathfrak{a} = \{x \in E : w(x) \geq m\}$.

(c) The ideal $\{x \in E : w(x) \geq m\}$ of B can also be written as $\mathfrak{P}^m$. In fact, it is clear that $\mathfrak{P}^m \subseteq \{x \in E : w(x) \geq m\}$. Conversely, let x be such that $w(x) \geq m$, and take $\tau \in E$ such that $w(\tau) = 1$ (which exists, because by construction w is surjective). Then $w(\tau^{-m}x) = w(x) - m \geq 0$, and hence $\tau^{-m}x \in B$ and $x = \tau^m(\tau^{-m}x) \in \mathfrak{P}^m$, since $\tau \in \mathfrak{P}$. This proof also shows that

$$\mathfrak{P}^m = \{y\tau^m : y \in B\}.$$

(d) The quotient ring $B/\mathfrak{P}$ is a division ring. In fact, let $x+\mathfrak{P}$ be an element of the quotient ring, where $x \in B$. If $x + \mathfrak{P}$ is different from 0, then x is not in $\mathfrak{P}$ and $w(x) = 0$. This implies $w(x^{-1}) = 0$, hence $x^{-1} \in B$ and

$$(x + \mathfrak{P})(x^{-1} + \mathfrak{P}) = (x^{-1} + \mathfrak{P})(x + \mathfrak{P}) = 1 + \mathfrak{P}$$

establishing the fact that $x + \mathfrak{P}$ is invertible.

Step 2 *(Structure of B as A-module).* By definition, N maps B into A. The bilinear form T associated with the quadratic form N maps $(x, y) \in B \times B$ to

$$\mathrm{N}(x + y) - \mathrm{N}(x) - \mathrm{N}(y)$$

and it follows that T maps $B \times B$ into A. Let now $(\beta_1, \beta_2, \beta_3, \beta_4)$ be an arbitrary F-basis of E such that each β_i is in B (just take any F-basis of E and multiply its elements by suitable powers of τ so that we get elements of B). It is then clear that

$$\bigoplus_{i=1}^{4} A\beta_i \subseteq B. \tag{2}$$

On the other hand, since the bilinear form T is non-degenerate, there exists an F-basis $(\gamma_1, \gamma_2, \gamma_3, \gamma_4)$ of E such that

$$T(\gamma_i, \beta_j) = \begin{cases} 1, \text{ if } i = j \\ 0, \text{ if } i \neq j. \end{cases}$$

Now take an arbitrary $x \in B$ and write it as $x_1\gamma_1 + x_2\gamma_2 + x_3\gamma_3 + x_4\gamma_4$ with $x_1, x_2, x_3, x_4 \in F$. Then, for $i = 1, 2, 3, 4$,

$$T(x, \beta_i) = T(x_1\gamma_1 + x_2\gamma_2 + x_3\gamma_3 + x_4\gamma_4, \beta_i) = x_i$$

and since x and β_i are in E it follows that $x_i \in A$. We obtain

$$B \subseteq \bigoplus_{i=1}^{4} A\gamma_i. \tag{3}$$

Now observe that, since A is a discrete valuation ring, it is in particular a PID. Since B is clearly a torsion-free A-module, by the structure theorem of modules over PID's we get that B is a free A-module. By (2) and (3) its rank is both ≥ 4 and ≤ 4, respectively, and thus B is a free A-module of rank 4.

Step 3 *(Structure of $B/\mathfrak{P}$ as k_F-vector space).* It is clear that, from the A-module structure of B, the quotient ring $B/\mathfrak{p}B$ inherits a structure of an $A/\mathfrak{p}$-module; simply define the scalar multiplication by $(a+\mathfrak{p})(b+\mathfrak{p}B) = ab+\mathfrak{p}B$. In a similar way, We claim that its dimension over the field $k_F = A/\mathfrak{p}$ is 4. For this, observe the following:

- If (e_1, e_2, e_3, e_4) is a basis of B over A, then clearly $e_1 + \mathfrak{p}B, e_2 + \mathfrak{p}B, e_3 + \mathfrak{p}B, e_4 + \mathfrak{p}B$ generate $B/\mathfrak{p}B$ as a k_F-vector space. Thus $\dim_{k_F}(B/\mathfrak{p}B) \leq 4$.

- If $(f_1+\mathfrak{p}B, \ldots, f_n+\mathfrak{p}B)$ is a basis of $B/\mathfrak{p}B$ as a k_F-vector space, let B' be the A-submodule of B spanned by $f_1, \ldots, f_n$. Given any $b \in B$, we know we can write

  $$b + \mathfrak{p}B = (b_1 + \mathfrak{p})(f_1 + \mathfrak{p}B) + \cdots + (b_n + \mathfrak{p}B)(f_n + \mathfrak{p}B)$$

  which means that $b - b_1 f_1 - \cdots - b_n f_n \in \mathfrak{p}B$. Since b is arbitrary, this proves that $B = B' + \mathfrak{p}B$. Since A is a local ring with maximal ideal $\mathfrak{p}$, Nakayama's Lemma implies that $B' = B$. Thus B is generated by $f_1, \ldots, f_n$ as an A-module, which implies that $n \geq 4$, in view of the fact that B is a free A-module of rank 4. Thus $\dim_{k_F}(B/\mathfrak{p}B) \geq 4$.

This establishes that $\dim_{k_F}(B/\mathfrak{p}B) = 4$. What we are really interested in, though, is the structure of $B/\mathfrak{B}$; this can also be seen as a k_F-module, with scalar multiplication defined by $(a + \mathfrak{p})(b + \mathfrak{P}) = ab + \mathfrak{P}$. Now we see two cases, according to the value of d.

- If $d = 2$, then $w(\pi) = \frac{w'(\pi)}{d} = 1$, and hence we can take $\tau = \pi$ in Observation (b) of Step 2. Therefore

  $$\mathfrak{p}B = \pi B = \tau B = \mathfrak{P}$$

  according to the same observation. It follows that $B/\mathfrak{P} = B/\mathfrak{p}B$. Hence in this case $\dim_{k_F}(B/\mathfrak{P}) = \dim_{k_F}(B/\mathfrak{p}B) = 4$.

- If $d = 1$, then $w(\pi) = 2$, and according to Observation (b) of Step 2 π is a generator of the ideal $\{x \in B : w(x) \geq 2\} = \mathfrak{P}^2$ of B. Hence $\mathfrak{p}B = \mathfrak{P}^2$. We now observe that we have a short exact sequence of k_F-vector spaces given by

  $$0 \longrightarrow \mathfrak{P}/\mathfrak{P}^2 \longrightarrow B/\mathfrak{P}^2 \longrightarrow B/\mathfrak{P} \longrightarrow 0$$

  which implies $4 = \dim_{k_F}(B/\mathfrak{p}B) = \dim_{k_F}(B/\mathfrak{P}^2) = \dim_{k_F}(\mathfrak{P}/\mathfrak{P}^2) + \dim_{k_F}(B/\mathfrak{P})$. But we have an isomorphism between $B/\mathfrak{P}$ and $\mathfrak{P}/\mathfrak{P}^2$, given by

  $$b + \mathfrak{P} \mapsto \tau b + \mathfrak{P}^2.$$

  (To check that this is injective, we must check that $\tau b \in \mathfrak{P}^2$ implies $b \in \mathfrak{P}$; but if $\tau b \in \mathfrak{P}^2$, then $w(\tau b) \geq 2$, implying $w(b) \geq 1$, which is what we wanted.) Therefore our previous equality can be rewritten as $4 = 2\dim_{k_F}(B/\mathfrak{P})$, implying that in this case $\dim_{k_F}(B/\mathfrak{P}) = 2$.

Step 4 *(Finding $\beta \in E$ such that $\beta^2 = u$).* Now recall that the residue class field k_F is a finite field, and since the division ring $B/\mathfrak{P}$ is a finite-dimensional vector space over k_F it must also be finite. By Wederburn's Little Theorem $B/\mathfrak{P}$ is a finite field extension of k_F. Choose $s \in B$ so that the residue class $s + \mathfrak{B}$ generates $B/\mathfrak{P}$ over k_F. Now s, as any element of a quaternion algebra, satisfies a quadratic equation over F, say $s^2 + bs + c = 0$ (where $c = \mathrm{N}(s)$). If this polynomial is not irreducible, then s is in F, and hence in $F \cap B = A$. This implies that the extension $k_F(s + \mathfrak{P})$ of k_F is trivial, which is absurd since we know it has degree 2 or 4. Therefore $X^2 + bX + c \in F[x]$ is not irreducible. It is a well-known consequence of Hensel's Lemma that in a monic irreducible polynomial over a local field the coefficient with minimal valuation is either the first or the last. Since in this case the first coefficient has valuation 0 and

$v(c) = v(\mathrm{N}(s)) = dw(s) \geq 0$, we have $v(b) \geq 0$, i.e., $b \in A$. However the equality $s^2 + bs + c = 0$ now implies that $s + \mathfrak{P}$ satisfies a quadratic equation with coefficients in k_F. This implies that $B/\mathfrak{P}$ has degree at most 2 as an extension of k_F, and, since we know this degree is either 2 or 4, it must be 2.

Let $L = F(s)$. Then L is a degree 2 extension of F, and, since the residual extension $F(s+\mathfrak{p})$ also has degree 2, we conclude that L is the unramified quadratic extension of F. Then $L = F(\beta)$ for some β with $\beta^2 = u$, with u defined as in the beginning.

Step 5 *(Finding $\alpha \in E$ such that $\alpha^2 \in F^\times$).* Let σ denote the only non-trivial element of $\mathrm{Gal}(L/F)$, which maps β to $-\beta$. By the Skolem-Noether Theorem applied to the embeddings of the field $F(\sqrt{u})$ into the central simple algebra E, we know that σ is induced by an inner automorphism of E, i.e., there exists $\alpha \in E$ such that

$$\sigma(z) = \alpha^{-1} z \alpha$$

for every $z \in L$. The above equality with $z = \beta$ yields

$$\alpha\beta = -\beta\alpha.$$

Moreover, we have $\sigma^2(z) = \alpha^{-2} z \alpha^2$ for $z \in L$, implying that conjugation by α^2 acts as the identity on L, i.e., α^2 commutes with all elements of L. However, since α is obviously not in L (or conjugation by α would act as the identity on L), the F-vector spaces L and $L\alpha$ of L are two 2-dimensional subspaces of E whose intersection contains only 0, hence $E = L \oplus L\alpha$. Since α^2 commutes elementwise with L it follows that α commutes elementwise with E, i.e., $\alpha^2 \in Z(E)$. Since quaternion algebras are central it follows that $\alpha^2 \in F$.

Now write $\alpha^2 = \pi^m x$, with x a unit in A. Then α and β satisfy the relations

$$\alpha^2 = \pi^m x \quad \beta^2 = u, \quad \alpha\beta = -\beta\alpha$$

and moreover it is clear from $L = F(\beta)$ and $E = L \oplus L\alpha$ that α and β generate E, whence

$$E \cong \left(\frac{\pi^m x, u}{F}\right).$$

In the Brauer group $B(F)$ of F, we have the equality

$$\left(\frac{\pi^m x, u}{F}\right) = \left(\frac{\pi^m, u}{F}\right)\left(\frac{x, u}{F}\right) = \left(\frac{\pi^m, u}{F}\right)$$

where the second equality follows from the fact that x is a norm from L, according to Proposition VI.2.9 of [1], implying that the quaternion algebra $\left(\frac{x,u}{F}\right)$ splits. Since $\left(\frac{\pi^m x,u}{F}\right)$ and $\left(\frac{\pi^m x,u}{F}\right)$ are both 4-dimensional, the Brauer-equivalence actually implies that these two are isomorphic, i.e.,

$$E \cong \left(\frac{\pi^m, u}{F}\right).$$

Since by assumption E is not split, π^m is not a square, implying that m is odd and that $\pi^m = \pi$ in $F^\times/(F^\times)^2$. Therefore we have $E \cong \left(\frac{\pi,u}{F}\right)$, and we are done.

References

[1] T. Y. Lam, *Quadratic Forms over Fields*, Graduate Studies in Mathematics, 2005