Chapter 11

Quaternion algebras over local fields

In this chapter, we classify quaternion algebras over local fields; this generalizes the classification of quaternion algebras over $\mathbb{R}$.

11.1 Local quaternion algebras

Having spent the first part of this book exploring the properties of quaternion algebras, we now seek to classify them over a nice class of fields. Over any field F we have the matrix ring $\mathrm{M}_2(F)$, and if F is a finite field or an algebraically closed field F, then any quaternion algebra over F is isomorphic to the matrix ring. The 'first' quaternion algebra, of course, was the division ring $\mathbb{H}$ of Hamiltonians, and this ring is the only division quaternion ring over $\mathbb{R}$ up to isomorphism.

In this section, we will classify quaternion algebras over a field F that is in some sense similar to $\mathbb{R}$. We will insist that the field F is equipped with a topology compatible with the field operations in which F is Hausdorff and locally compact (every element of F has a compact neighborhood). To avoid trivialities, we will insist that this topology is not the discrete topology (where every subset of F is open): such a topological field is called a *local field*.

For purposes of illustration, we consider local fields F that contain the rational numbers $\mathbb{Q}$ as a dense subfield. Such a field F is the completion of $\mathbb{Q}$ with respect to an absolute value $|\,|$, so is obtained as the set of equivalence classes of Cauchy sequences, and has a topology induced by the metric $d(x, y) = |x - y|$. By a theorem of Ostrowski, such an absolute value is equivalent to either the usual archimedean absolute value or a p-*adic absolute value*, defined by $|0|_p = 0$ and

$$|c|_p = p^{-\operatorname{ord}_p(c)} \quad \text{for } c \in \mathbb{Q}^\times,$$

where $\operatorname{ord}_p(c)$ is the power of p occurring in c in its unique factorization (taken to be negative if p divides the denominator of c written in lowest terms).

Just as elements of $\mathbb{R}$ can be thought of infinite decimals, an element of $\mathbb{Q}_p$ can be

thought of in its p-adic expansion

$$a = (\dots a_3 a_2 a_1 a_0 . a_{-1} a_{-2} \cdots a_{-k})_p = \sum_{n=-k}^{\infty} a_n p^n$$

where each $a_i \in \{0, \dots, p-1\}$ are the *digits* of a. We continue "to the left" because a decimal expansion is a series in the base $1/10 < 1$ and instead we have a base $p > 1$. Inside $\mathbb{Q}_p$ is the ring $\mathbb{Z}_p$ of *p-adic integers*, the completion of $\mathbb{Z}$ with respect to $|\ |_p$: the ring $\mathbb{Z}_p$ consists of those elements of $\mathbb{Q}_p$ with $a_n = 0$ for $n < 0$. The ring $\mathbb{Z}_p$ might be thought of intuitively as $\mathbb{Z}/p^\infty\mathbb{Z}$, if this made sense: they were first defined in this context by Hensel, who wanted a uniform language for when a Diophantine equation has a solution modulo p^n for all n.

By construction, the ring $\mathbb{Z}_p$ and the field $\mathbb{Q}_p$ come equipped with a topology arising from its metric $d_p(x, y) = |x - y|_p$. With respect to this topology, in fact $\mathbb{Z}_p$ is compact and $\mathbb{Q}_p$ is locally compact. It is easiest to see this by viewing $\mathbb{Z}_p$ as a projective limit with respect to the natural maps $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$:

$$\begin{aligned} \mathbb{Z}_p &= \varprojlim_n \mathbb{Z}/p^n\mathbb{Z} \\ &= \left\{ x = (x_n)_n \in \prod_{n=0}^{\infty} \mathbb{Z}/p^n\mathbb{Z} : x_{n+1} \equiv x_n \pmod{p^n} \text{ for all } n \geq 0 \right\}. \end{aligned} \tag{11.1.1}$$

In other words, each element of $\mathbb{Z}_p$ is a compatible sequence of elements in $\mathbb{Z}/p^n\mathbb{Z}$ for each n. The equality (11.1.1) is just a reformulation of the notion of Cauchy sequence for $\mathbb{Z}$, and so for the purposes of this introduction it can equally well be taken as a definition. As for the topology in (11.1.1), each factor $\mathbb{Z}/p^n\mathbb{Z}$ is given the discrete topology, the product $\prod_{n=0}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ is given the product topology, and $\mathbb{Z}_p$ is given the restriction topology. Since each $\mathbb{Z}/p^n\mathbb{Z}$ is compact (it is a finite set!), by Tychonoff's theorem the product $\prod_{n=0}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ is compact; and $\mathbb{Z}_p$ is closed inside this product (a convergent limit of Cauchy sequences is a Cauchy sequence), so $\mathbb{Z}_p$ is compact. The set $\mathbb{Z}_p$ is a neighborhood of 0, indeed, it is the closed ball of radius 1 around 0:

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |a|_p \leq 1\}.$$

In a similar way, the disc of radius 1 around any $a \in \mathbb{Q}_p$ is a compact neighborhood of a homeomorphic to $\mathbb{Z}_p$, so $\mathbb{Q}_p$ is locally compact.

As is evident from this argument, although $\mathbb{Q}_p$ is Hausdorff and locally compact, it has a rather strange topology, akin to a Cantor set: $\mathbb{Q}_p$ is *totally disconnected* (the largest connected subsets consist of single points). Nevertheless, being able to make topological arguments like the one above is the whole point of looking at local fields like $\mathbb{Q}_p$: our understanding of algebraic objects is informed by the topology.

In particular, we have a result for quaternion algebras over $\mathbb{Q}_p$ that is quite analogous to that over $\mathbb{R}$.

Theorem 11.1.2. *There is a unique division quaternion algebra B over $\mathbb{Q}_p$, up to isomorphism. In fact, if $p \neq 2$, then B is given by*

$$B \simeq \left(\frac{e, p}{\mathbb{Q}_p} \right)$$

where $e \in \mathbb{Z}$ is a quadratic nonresidue modulo p.

We approach this theorem in two ways in this section. The first way is using the language of quadratic forms, and for that we use the classification of isomorphism classes of quaternion algebras in terms of similarity classes of ternary quadratic forms. The following proposition then implies Theorem 11.1.2.

Proposition 11.1.3. *There is a unique ternary anisotropic quadratic form Q over $\mathbb{Q}_p$, up to similarity. If $p \neq 2$, then $Q \sim \langle 1, -e, -p \rangle$ where e is a quadratic nonresidue modulo p.*

This proposition can be proved using some rather direct manipulations with quadratic forms. On the other hand, it has the defect that quadratic forms behave differently in characteristic 2, and so one may ask for a more uniform proof. This is the second way that we approach the proof of Theorem 11.1.2: we extend the absolute value on $\mathbb{Q}_p$ to one on a division quaternion algebra B, and use this extension to show that B is unique by direct examination of its valuation ring and two-sided maximal ideal. While it requires a bit more theory, this method of proof also can be used to classify central division algebras over $\mathbb{Q}_p$ in much the same manner.

11.2 Local fields

Definition 11.2.1. A *topological ring* is a ring A equipped with a topology such that the ring operations (addition, negation, and multiplication) are continuous. A *homomorphism* of topological rings is a ring homomorphism that is continuous. A *topological field* is a field that is also a topological ring in such a way that division by a nonzero element is continuous.

A very natural way to equip a ring with a topology that occurs throughout mathematics is by way of an absolute value; to get started, we consider such notions first for fields. Throughout, let F be a field.

Definition 11.2.2. An *absolute value* on F is a map

$$|\,| : F \to \mathbb{R}_{\geq 0}$$

such that:

(i) $|x| = 0$ if and only if $x = 0$;

(ii) $|xy| = |x|y$ for all $x, y \in F$; and

(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in F$ (*triangle inequality*).

An absolute value $|\,|$ on F gives F the structure of a topological field by the metric $d(x, y) = |x - y|$. Two absolute values $|\,|, \|\,\|$ on F are *equivalent* if there exists $c > 0$ such that $|x| = \|x\|^c$ for all $x \in F$; equivalent absolute values induces the same topology on F.

Definition 11.2.3. An absolute value is *nonarchimedean* if $|x+y| \leq \sup\{|x|, |y|\}$ for all $x, y \in F$ (*ultra metric inequality*), and *archimedean* otherwise.

Example 11.2.4. The fields $\mathbb{R}$ and $\mathbb{C}$ are topological fields with respect to the usual archimedean absolute value.

Remark 11.2.5. A field is archimedean if and only if it satisfies the *archimedean property*: for all $x \in F^\times$, there exists $n \in \mathbb{Z}$ such that $|nx| > 1$. In particular, a field F equipped with an archimedean absolute value has $\operatorname{char} F = 0$.

Example 11.2.6. Every field has the *trivial* (nonarchimedean) absolute value, defined by $|0| = 0$ and $|x| = 1$ for all $x \in F^\times$; the trivial absolute value induces the discrete topology on F.

A nonarchimedean absolute value on a field F arises naturally by way of a valuation, as follows.

Definition 11.2.7. A *valuation* of a field F is a map $v : F \to \mathbb{R} \cup \{\infty\}$ such that:

(i) $v(x) = \infty$ if and only if $x = 0$;

(ii) $v(xy) = v(x) + v(y)$ for all $x, y \in F$; and

(iii) $v(x+y) \geq \min(v(x), v(y))$ for all $x, y \in F$.

A valuation is *discrete* if the *value group* $v(F^\times)$ is discrete in $\mathbb{R}$ (has no accumulation points).

Here, we set the convention that $x + \infty = \infty + x = \infty$ for all $x \in \mathbb{R} \cup \{\infty\}$. By (ii), the value group $v(F^\times)$ is indeed a subgroup of the additive group $\mathbb{R}$, and so although an absolute value is multiplicative, a valuation is additive.

Example 11.2.8. For $p \in \mathbb{Z}$ prime, the the map $v(x) = \operatorname{ord}_p(x)$ is a valuation on $\mathbb{Q}$.

Example 11.2.9. Let k be a field and $F = k(t)$ the field of rational functions over k. For $f(t) = g(t)/h(t) \in k(t) \setminus \{0\}$, define $v(f(t)) = \deg g(t) - \deg h(t)$ and $v(0) = \infty$. Then v is a discrete valuation on F.

Given the parallels between them, it should come as no surprise that a valuation gives rise to an absolute value on F by defining $|x| = c^{-v(x)}$ for any $c > 1$; the induced topology on F is independent of the choice of c. By condition (iii), the absolute value associated to a valuation is nonarchimedean.

Example 11.2.10. The *trivial* valuation is the valuation v satisfying $v(0) = \infty$ and $v(x) = 0$ for all $x \in F^\times$. The trivial valuation gives the trivial absolute value on F.

Two valuations v, w are *equivalent* if there exists $a \in \mathbb{R}_{>0}$ such that $v(x) = aw(x)$ for all $x \in F$; equivalent valuations give the same topology on a field. A nontrivial discrete valuation is equivalent after rescaling (by the minimal positive element in the value group) to one with value group $\mathbb{Z}$, since a nontrivial discrete subgroup of $\mathbb{R}$ is cyclic; we call such a discrete valuation *normalized*.

Given a field F with a nontrivial discrete valuation v, we have the *valuation ring* $R = \{x \in F : v(x) \geq 0\}$. We have $R^\times = \{x \in F : v(x) = 0\}$ since $v(x) + v(x^{-1}) = v(1) = 0$ for all $x \in F^\times$. The valuation ring is a local ring with unique maximal ideal

$$\mathfrak{p} = \{x \in F : v(x) > 0\} = R \setminus R^\times.$$

An element $\pi \in \mathfrak{p}$ with smallest valuation is called a *uniformizer*, and comparing valuations we see that $\pi R = (\pi) = \mathfrak{p}$. Since $\mathfrak{p} \subsetneq R$ is maximal, the quotient $k = R/\mathfrak{p}$ is a field, called the *residue field* of R (or of F).

Recall that a topological space is *locally compact* if each point has a compact neighborhood.

Definition 11.2.11. A *local field* is a Hausdorff, locally compact topological field with a nondiscrete topology.

In a local field, we can hope to understand its structure by local considerations in a compact neighborhood, hence the name.

Local fields have a very simple classification as follows.

Theorem 11.2.12. *Every local field F is isomorphic as a topological field to one of the following:*

- *F is archimedean, and $F \simeq \mathbb{R}$ or $F \simeq \mathbb{C}$;*
- *F is nonarchimedean with $\operatorname{char} F = 0$, and F is a finite extension of $\mathbb{Q}_p$ for some prime p; or*
- *F is nonarchimedean with $\operatorname{char} F = p$, and F is a finite extension of $\mathbb{F}_p((t))$ for some prime p; in this case, there is a (non-canonical) isomorphism $F \simeq \mathbb{F}_q((t))$ where q is a power of p.*

We have the following equivalent characterization of nonarchimedean local fields.

Lemma 11.2.13. *A field is a nonarchimedean local field if and only if it is complete with respect to a nontrivial discrete valuation $v : F \to \mathbb{R} \cup \{\infty\}$ with finite residue field.*

Although a local field is only locally compact, the valuation ring is itself compact, as follows.

Lemma 11.2.14. *Suppose F is nonarchimedean. Then F is totally disconnected and the valuation ring $R \subset F$ is a compact, totally disconnected topological ring.*

Proof. To see that F is totally disconnected (so too R is totally disconnected), by translation it suffices to show that the only connected set containing 0 is $\{0\}$. Let $x \in F^\times$ with $|x| = \delta > 0$. The image $|F^\times| \subseteq \mathbb{R}_{>0}$ is discrete, so there exists $0 < \epsilon < \delta$ so that $|y| < \delta$ implies $|y| \leq \delta - \epsilon$ for all $y \in F$. Thus an open ball is a closed ball

$$D(0, \delta) = \{y \in F : |y| < \delta\} = \{y \in F : |y| \leq \delta - \epsilon\} = D[0, \delta - \epsilon];$$

since $x \in F^\times$ and $\delta > 0$ were arbitrary, the only connected subset containing 0 is $\{0\}$.

Next, we show R is compact. We have a natural continuous ring homomorphism

$$\phi : R \to \prod_{n=1}^{\infty} R/\mathfrak{p}^n$$

where each factor $R/\mathfrak{p}^n$ is equipped with the discrete topology and the product is given the product topology. The map ϕ is injective, since $\bigcap_{n=1}^{\infty} \mathfrak{p}^n = \{0\}$ (every nonzero element has finite valuation). The image of ϕ is obviously closed. Therefore R is homeomorphic onto its closed image. But by Tychonoff's theorem, the product $\prod_{n=1}^{\infty} R/\mathfrak{p}^n$ of compact sets is compact, and a closed subset of a compact set is compact, so R is compact. $\square$

One key property of local fields we will use is Hensel's lemma: it is the nonarchimedean analogue of Newton's method.

Lemma 11.2.15 (Hensel's lemma)**.** *Let F be a nonarchimedean local field with valuation v and valuation ring R, and let $f(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ with $n \geq 1$. Suppose that $a = (a_i)_i \in R^n$ satisfies*

$$k = v(f(a_1, \ldots, a_n)) > 2v(f'(a_1, \ldots, a_n)) \geq 0.$$

Then there exists $\widetilde{a} = (\widetilde{a}_i)_i \in R^n$ such that $f(\widetilde{a}) = 0$ and

$$\widetilde{a}_i \equiv a_i \pmod{\mathfrak{p}^k}$$

for all $i = 1, \ldots, n$.

11.3 Unique division ring, first proof

We now seek to classify quaternion algebras over local fields. First, suppose F is archimedean. When $F = \mathbb{C}$, the only quaternion algebra over $\mathbb{C}$ up to isomorphism is $B \simeq \mathrm{M}_2(\mathbb{C})$. When $F = \mathbb{R}$, by the theorem of Frobenius (Corollary 3.5.5), there is a unique quaternion division algebra over $\mathbb{R}$. The classification of quaternion algebras over nonarchimedean local fields is quite analogous to the classification over $\mathbb{R}$; indeed, we have the following.

Theorem 11.3.1. *Let $F \neq \mathbb{C}$ be a local field. Then there is a unique division quaternion algebra B over F up to F-algebra isomorphism.*

To prove this theorem, from the first paragraph of this section we may assume F is a nonarchimedean local field with discrete valuation v.

We approach the proof of Theorem 11.3.1 from two vantage points. In this section, we give a proof using quadratic forms (which excludes the case where $\operatorname{char} F = 2$); in the next section, we give another proof by extending the valuation (including all characteristics).

By Theorems 4.4.5 and 4.5.5, to prove Theorem 11.3.1 it is equivalent to prove the following proposition.

Proposition 11.3.2. *Let $F \neq \mathbb{C}$ be a local field. Then there is a unique nonsingular anisotropic ternary quadratic form over F up to similarity.*

So our task becomes a hands-on investigation of ternary quadratic forms over F. The theory of quadratic forms over F is linked to that over its residue field k, so we first need to examine isotropy of quadratic forms over a finite field.

Lemma 11.3.3. *A quadratic space V over a finite field with $\dim_F V \geq 3$ is isotropic.*

This statement is elementary (Exercise 11.1).

Lemma 11.3.4. *Suppose $\operatorname{char} k \neq 2$. Let $Q : M \to R$ be a nonsingular quadratic form over R. Then the reduction $Q \bmod \mathfrak{p} : M \otimes_R k \to k$ of Q modulo $\mathfrak{p}$ is nonsingular over k; moreover, Q is isotropic over R if and only if $Q \bmod \mathfrak{p}$ is isotropic.*

Lemma 11.3.4 is a consequence of Hensel's lemma (Lemma 11.2.15). Combining these two lemmas, we obtain the following.

Proposition 11.3.5. *Suppose $\operatorname{char} k \neq 2$. Let $Q : M \to R$ be a nonsingular quadratic form over R with M of rank ≥ 3. Then Q is isotropic.*

Considering valuations, we also deduce the following from Lemma 11.3.4.

Lemma 11.3.6. *Suppose $\operatorname{char} k \neq 2$. Then $\#F^\times/F^{\times 2} \simeq (\mathbb{Z}/2\mathbb{Z})^2$ and is represented by the classes of $1, e, \pi, e\pi$ where $e \in R^\times$ is any element which reduces modulo $\mathfrak{p}$ to a nonsquare in k.*

We first consider the case $\operatorname{char} k \neq 2$.

Proof of Proposition 11.3.2 ($\operatorname{char} k \neq 2$). Let $Q \simeq \langle a, -b, -c\rangle$ be a nonsingular, anisotropic ternary quadratic form over F. Rescaling the basis elements by a power of the uniformizer, we may assume that $v(a), v(b), v(c) \in \{0, 1\}$. Then, by the pigeonhole principle on this set of valuations, we may rescale the form and permute the basis to assume that $a = 1$ and $0 = v(b) \leq v(c)$. If $v(b) = v(c) = 0$ then the quadratic form modulo $\mathfrak{p}$ is nonsingular, so by Lemma 11.3.3 it is isotropic and by Lemma 11.3.4 we conclude Q is isotropic, a contradiction.

We are left with the case $v(b) = 0$ and $v(c) = 1$. By Lemma 11.3.6, we may assume $b = 1$ or $b = e$ where e is a nonsquare in k. If $b = 1$, then the form is obviously isotropic, so we have $b = e$. Similarly, we have $c = \pi$ or $c = e\pi$. In fact, the latter case is similar to the former: scaling by e we have

$$\langle 1, -e, -e\pi\rangle \sim \langle -1, e, -\pi\rangle$$

and since $\langle -1, e\rangle \simeq \langle 1, -e\rangle$ (Exercise 11.2), we have $Q \sim \langle 1, -e, -\pi\rangle$.

To conclude, we show that the form $\langle 1, -e, -\pi\rangle$ is anisotropic. Suppose that $x^2 - ey^2 = \pi z^2$ with $x, y, z \in F^3$ not all zero. By homogeneity, we may assume $x, y, z \in R$ and at least one of $x, y, z \in R^\times$. Reducing modulo $\mathfrak{p}$ we have $x^2 \equiv ey^2 \pmod{\mathfrak{p}}$ so since e is a nonsquare we have $v(x), v(y) \geq 1$. But this implies that $v(z) = 0$ and so $v(\pi z^2) = 1 = v(x^2 - ey^2) \geq 2$, a contradiction. $\square$

Now suppose that $\operatorname{char} k = 2$. Recall the issues with inseparability in characteristic 2 (Paragraph 5.1.2). Let $\wp(k) = \{z + z^2 : z \in k\}$ be the *Artin-Schreier group* of k. The polynomial $x^2 + x + t$ is reducible if and only if $t \in \wp(k)$, and since k is finite, we have $k/\wp(k) \simeq \mathbb{Z}/2\mathbb{Z}$ (Exercise 11.3). Let $t \in R$ represent the nontrivial class in $k \setminus \wp(k)$.

Proof of Proposition 11.3.2 ($\operatorname{char} k = 2$*).* By nonsingularity and scaling, we may assume that $Q \sim [1, b] \perp \langle c \rangle$ with $b, c \in R$. If $v(b) > 0$, then $[1, b]$ is isotropic modulo $\mathfrak{p}$ and hence Q is isotropic, a contradiction. So $v(b) = 0$, and for the same reason b in the same class as $t \in k \setminus \wp(k)$. Scaling, we may assume $v(c) = 0, 1$. If $v(c) = 0$, then either c or $t + c$ belongs to $\wp(k)$ and so again we have a contradiction. Thus $v(c) = 1$ and $c = u\pi$ for some $u \in R^\times$; but then $[u, tu] \simeq [1, t]$ so $Q \sim [1, t] \perp \langle \pi \rangle$. To conclude, we verify that this form is indeed anisotropic, applying the same argument as in the last paragraph in the proof when $\operatorname{char} k \neq 2$ to the quadratic form $x^2 + xy + ty^2 = \pi z^2$. $\square$

In mixed characteristic where $\operatorname{char} F = 0$ and $\operatorname{char} F = 2$, the extension $K = F[x]/(x^2 + x + t)$ for t nontrivial in $k/\wp(k)$ is the unramified quadratic extension of F, and we can complete the square to obtain $K = F(\sqrt{e})$ with $e \in F^\times \setminus F^{\times 2}$—it is just no longer the case that e is nontrivial in $k^\times/k^{\times 2}$. Putting these cases together, we have the following corollary.

Corollary 11.3.7. *Let $F \neq \mathbb{C}$ be a local field and B be a quaternion algebra over F. Then B is a division quaternion algebra if and only if*

$$B \simeq \left(\frac{K, \pi}{F}\right)$$

where K is the unramified quadratic extension of F. In particular, if $\operatorname{char} k \neq 2$*, then B is a division algebra if and only if*

$$B \simeq \left(\frac{e, \pi}{F}\right), \text{ where } e \text{ is nontrivial in } k^\times/k^{\times 2}$$

and if $\operatorname{char} F = \operatorname{char} k = 2$*, then B is a division algebra if and only if*

$$B \simeq \left[\frac{t, \pi}{F}\right), \text{ where } t \text{ is nontrivial in } k/\wp(k).$$

11.4 Local Hilbert symbol

Recall the definition of the Hilbert symbol (Section 4.7). In this section, we compute the Hilbert symbol over a local field F with $\operatorname{char} k \neq 2$. Let $a, b \in F^\times$.

We begin with the case where F is archimedean. If $F = \mathbb{C}$, then the Hilbert symbol is identically 1. If $F = \mathbb{R}$, then

$$(a, b)_{\mathbb{R}} = \begin{cases} 1, & \text{if } a > 0 \text{ or } b > 0; \\ -1, & \text{if } a < 0 \text{ and } b < 0. \end{cases}$$

Lemma 11.4.1. *The Hilbert symbol over a nonarchimedean local field F is bimultiplicative, i.e.*

$$(a, bc)_F = (a, b)_F(a, c)_F \quad \textit{and} \quad (ab, c)_F = (a, c)_F = (b, c)_F$$

for all $a, b, c \in F^\times$.

Remark 11.4.2. The bimultiplicativity property of the local Hilbert symbol is a special property and does not extend to a general field!

Proof. This will follow from the direct computation below (11.4.3), but it is helpful to know this fact independently.

We appeal to Theorem 4.5.5(vi): we have $(a, b)_F = 1$ if and only if $b \in \mathrm{N}_{K/F}(K^\times)$ where $K = F[x]/(x^2 - a)$. If K is not a field, then $(a, b)_F = 1$ identically, so it is certainly multiplicative. Otherwise, $F^\times/\mathrm{N}_{K/F}(K^\times) \simeq \mathbb{Z}/2\mathbb{Z}$: when $\operatorname{char} k \neq 2$, this follows from Lemma 11.3.6, but it is true in general. Multiplicativity is then immediate. □

Since the Hilbert symbol is well-defined up to squares, the symbol $(a, b)_F$ is determined by the values with $a, b \in \{1, e, \pi, e\pi\}$ where e is a nonsquare in $k^\times$. Let $s = (-1)^{(\#k-1)/2}$, so that $s = 1, -1$ according as -1 is a square in k. Then we have:

$(a, b)_F$	1	e	π	$e\pi$
1	1	1	1	1
e	1	1	-1	-1
π	1	-1	s	$-s$
$e\pi$	1	-1	$-s$	s

(11.4.3)

The computation of this table is Exercise 11.7.

11.4.4. The following criteria follow from 11.4.3:

(a) If $v(ab) = 0$, then $(a, b)_F = 1$.

(b) If $v(a) = 0$ and $v(b) = v(\pi)$, then

$$(a, b)_F = \left(\frac{a}{\pi}\right) = \begin{cases} 1 & \text{if } a \in k^{\times 2}; \\ -1 & \text{if } a \in k^\times \setminus k^{\times 2}. \end{cases}$$

11.4.5. The computation of the Hilbert symbol for local fields with $\operatorname{char} F \neq 2$ but $\operatorname{char} k = 2$ is significantly more involved. We provide in Exercise 11.11 a way to understand this symbol for a general F. In this paragraph, we compute the Hilbert symbol for $F = \mathbb{Q}_2$.

To begin, the group $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ is generated by $-1, -3, 2$, so representatives are $\{\pm 1, \pm 3, \pm 2, \pm 6\}$. The extension $\mathbb{Q}_2(\sqrt{-3}) \supset \mathbb{Q}_2$ is the unique unramified extension.

We recall Hilbert's criterion: $(a, b)_F = 1$ if and only if $ax^2 + by^2 = 1$ has a solution with $x, y \in F$.

If $a, b \in \mathbb{Z}$ are odd, then

$$\begin{aligned} ax^2 + by^2 = z^2 &\text{ has a nontrivial solution in } \mathbb{Q}_2 \\ \iff \quad & a \equiv 1 \pmod 4 \text{ or } b \equiv 1 \pmod 4; \end{aligned}$$

by homogeneity and Hensel's lemma, it is enough to check for a solution modulo 4. This deals with all of the symbols with a, b odd.

By the determination above, we see that $(-3, b) = -1$ for $b = \pm 2, \pm 6$ and $(2, 2)_{\mathbb{Q}_2} = (-1, 2)_{\mathbb{Q}_2} = 1$ the latter by Hilbert's criterion, as $-1 + 2 = 1$; knowing multiplicativity (Lemma 11.4.1), we have uniquely determined all Hilbert symbols. It is still useful to compute several of these symbols individually, in the same manner as (11.4.5) (working modulo 8): see Exercise 11.10. We summarize the results here:

$(a,b)_{\mathbb{Q}_2}$	1	-3	-1	3	2	-6	-2	6
1	1	1	1	1	1	1	1	1
-3	1	1	1	1	-1	-1	-1	-1
-1	1	1	-1	-1	1	1	-1	-1
3	1	1	-1	-1	-1	-1	1	1
2	1	-1	1	-1	1	-1	1	-1
-6	1	-1	1	-1	-1	1	-1	1
-2	1	-1	-1	1	1	-1	-1	1
6	1	-1	-1	1	-1	1	1	-1

(11.4.6)

[[Unramified square symbol.]]

11.5 Unique division ring, second proof

We now proceed to give a second proof of Theorem 11.3.1; we will extend the valuation v to one uniquely on a division quaternion algebra. For this, we will need to rely a bit more heavily on the theory of local fields. We retain our assumption that F is a nonarchimedean local field with valuation ring R, residue field k, and maximal ideal $\mathfrak{p}$ generated by a uniformizer π.

Let $K \supseteq F$ be a finite extension of fields. Then there exists a unique valuation w on K such that $w|_F = v$, and we say that w *extends* v: this valuation is defined by

$$w(x) = \frac{v(\mathrm{N}_{K/F}(x))}{[K : F]}; \tag{11.5.1}$$

in particular, K is also a nonarchimedean local field. (The only nontrivial thing to check is condition (iii), and this can be derived from the fact that

$$v(\mathrm{N}_{K/F}(x)) \geq 0 \Rightarrow v(\mathrm{N}_{K/F}(x+1)) \geq 0$$

for $x \in K$ and this follows by a direct examination of the minimal polynomial of x.)

Lemma 11.5.2. *The integral closure of R in K is the valuation ring $S = \{x \in K : w(x) \geq 0\}$, and S is an R-order in K.*

A finite extension K/F is *unramified* if a uniformizer π for F is also a uniformizer for K. There is a unique unramified extension of F of any degree $f \in \mathbb{Z}_{\geq 1}$ and such a field corresponds to the unique extension of the residue field k of degree f. In an unramified extension K/F of degree $[K : F] = f$, we have $N_{K/F}(K^\times) = R^\times \pi^{f\mathbb{Z}}$, so $b \in \mathrm{N}_{K/F}(K^\times)$ if and only if $f \mid v(b)$.

11.5.3. If $\operatorname{char} k \neq 2$, then by Hensel's lemma, the unramified extension of degree 2 is given by adjoining a square root of the unique nontrivial class in $k^\times/k^{\times 2}$; if $\operatorname{char} k = 2$, then the unramified extension of degree 2 is given by adjoining a root of the polynomial $x^2 + x + t$ where t is a nontrivial class in the Artin-Schreier group $k/\wp(k)$.

Let $K \supseteq F$ be a finite separable extension of fields. We say K/F with $e = [K : F]$ is *totally ramified* if a uniformizer π_K has the property that π_K^e is a uniformizer for F. For any finite separable extension K/F of degree n, there is a (unique) maximal unramified subextension K_{un}/F, and the extension K/K_{un} is totally ramified.

$$\begin{tikzcd}
 & & K \\
 & K_{\text{un}} \arrow[ur, dash, "e"] & \\
F \arrow[ur, dash, "f"] & &
\end{tikzcd}$$

We say that $e = [K : K_{\text{un}}]$ is the *ramification degree* and $f = [K_{\text{un}} : F]$ the *inertial degree*, and we have the fundamental equality

$$n = [K : F] = ef. \tag{11.5.4}$$

We now seek to generalize these theorems to the noncommutative case. Let D be a central simple *division* algebra over F with $\dim_F D = [D : F] = n^2$. We extend the valuation v to a map

$$\begin{aligned} w : D &\to \mathbb{R} \cup \{\infty\} \\ \alpha &\mapsto \frac{v(\mathrm{N}_{D/F}(\alpha))}{[D : F]} = \frac{v(\operatorname{nrd}(\alpha))}{n}, \end{aligned}$$

where the equality follows from the fact that $\mathrm{N}_{D/F}(\alpha) = \operatorname{nrd}(\alpha)^n$ (see Section 6.7).

Lemma 11.5.5. *The map w defines a valuation on D, i.e., the following hold:*

(i) $w(\alpha) = \infty$ *if and only if* $\alpha = 0$.

(ii) $w(\alpha\beta) = w(\alpha) + w(\beta) = w(\beta\alpha)$ *for all* $\alpha, \beta \in D$.

(iii) $w(\alpha + \beta) \geq \min(w(\alpha), w(\beta))$ *for all* $\alpha, \beta \in D$.

(iv) $w(D^\times)$ *is discrete in* $\mathbb{R}$.

Proof. Statement (i) is clear (note it already uses that D is a division ring). Statement (ii) follows from the multiplicativity of nrd and v. To prove (iii), we may assume $\beta \neq 0$ and so $\beta \in D^\times$. We have

$$w(\alpha + \beta) = w((\alpha\beta^{-1} + 1)\beta) = w(\alpha\beta^{-1} + 1) + w(\beta).$$

But the restriction of w to $F(\alpha\beta^{-1})$ is a discrete valuation, so $w(\alpha\beta^{-1} + 1) \geq \min(w(\alpha\beta^{-1}), w(1))$ so by (ii) $w(\alpha + \beta) \geq \min(w(\alpha), w(\beta))$, as desired. Finally, (iv) holds since $w(D^\times) \subseteq v(F^\times)/n$ and the latter is discrete. □

From Lemma 11.5.5, we say that w is a *discrete valuation* on D since it satisfies the same axioms as for a field. It follows from Lemma 11.5.5 that the set

$$\mathcal{O} = \{\alpha \in D : w(\alpha) \geq 0\}$$

is a ring, called the *valuation ring* of D.

Proposition 11.5.6. *$\mathcal{O}$ is the unique maximal R-order in D, consisting of all elements of D that are integral over R.*

Proof. First, we prove that

$$\mathcal{O} = \{\alpha \in D : \alpha \text{ is integral over } R\}.$$

In one direction, suppose $\alpha \in D$ is integral over R. Since R is integrally closed, by Lemma 8.3.10 the coefficients of the minimal polynomial $f(x) \in F[x]$ of α belong to R. Since D is a division ring, $f(x)$ is irreducible and hence the reduced characteristic polynomial $g(x)$ is a power of $f(x)$ and thus has coefficients in R. The reduced norm is the constant coefficient of $g(x)$, so $\alpha \in \mathcal{O}$.

Now suppose $\alpha \in \mathcal{O}$, so that $w(\alpha) \geq 0$, and let $K = F(\alpha)$. Let $f(x) \in F[x]$ be the minimal polynomial of α. We want to conclude that $f(x) \in R[x]$ knowing that $w(\alpha) \geq 0$. But the restriction of w to K is the unique extension of v to K, and so this is a statement about the extension K/F of local fields and therefore follows from the theory in the commutative case. For completeness, we give the proof. Let L be a splitting field of $f(x)$ containing K. Then v extends to a unique valuation w_L on L. At the same time, the norm w on D restricts to a discrete valuation on K and hence by equivalence of valuations, we have $w_L(\alpha) \geq 0$. But now if $f(x) = \prod_{i=1}^n (x - \alpha_i) = x^n + \cdots + a_0 \in F[x]$ with $\alpha_i \in L$, then $w_L(\alpha_i) = a_0 = w(\alpha) \geq 0$. Thus the coefficients of f (symmetric functions in the α_i) belong to R, and so α is integral over R.

We can now prove that $\mathcal{O}$ is an R-order. Scaling any element $\alpha \in D^\times$ by an appropriate power of π gives it positive valuation, so $\mathcal{O}F = D$. So to conclude we must show that $\mathcal{O}$ is finitely generated as an R-module. For this purpose, we may assume that D is central over F, since the center $K = Z(D)$ is a field extension of F of finite degree and the integral closure of R in K is finitely generated as an R-module (Lemma 11.5.2). A central division algebra is separable, so we may apply Lemma 8.4.1: every $\alpha \in \mathcal{O}$ is integral over R and $\mathcal{O}$ is a ring, so the lemma implies that $\mathcal{O}$ is an R-order.

Finally, it follows immediately that $\mathcal{O}$ is a maximal R-order: by Corollary 8.3.9, every element of an R-order is integral over R, and $\mathcal{O}$ contains all such elements. □

Remark 11.5.7. For a quaternion division algebra D, we can argue more directly in the proof of Proposition 11.5.6 using the reduced norm: see Exercise 11.14.

It follows from Proposition 11.5.6 that $\mathcal{O}$ is a finitely generated R-submodule of D. But R is a PID (every ideal is a power of the maximal ideal $\mathfrak{p}$) so in fact $\mathcal{O}$ is free of rank $[D : F]$ over R. We have

$$\mathcal{O}^\times = \{\alpha \in D : w(\alpha) = 0\} \tag{11.5.8}$$

since $w(\alpha^{-1}) = -w(\alpha)$ and $\alpha \in \mathcal{O}^\times$ if and only if $\mathrm{nrd}(\alpha) \in R^\times$. Consequently,

$$P = \{\alpha \in D : w(\alpha) > 0\} = \mathcal{O} \setminus \mathcal{O}^\times$$

is the unique maximal two-sided ideal of $\mathcal{O}$. Therefore $\mathcal{O}$ is a *noncommutative local ring*, a ring with a unique maximal left (or right) ideal.

We are now prepared to give the second proof of the main result in this chapter (Theorem 11.3.1). By way of analogy, we consider the commutative case: for an extension L of F of degree $[L : F] = n$, we have a ramification degree e and an inertial degree f with $ef = n$ (11.5.4). The same will be true when B is a division quaternion algebra: we will show that $\mathcal{O}/P$ is a quadratic field extension of k and hence that B contains an unramified separable quadratic extension K of F (extending the analogy, that $f = 2$); and then computing with valuations we will conclude that $P^2 = \pi\mathcal{O}$ (and $e = 2$) from which the result follows.

Proof of Theorem 11.3.1. Suppose that $v : F \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ is normalized and let $j \in P$ have minimal (positive) valuation $w(j) \geq 1/2$. Then for any $0 \neq \alpha \in P$ we have $w(\alpha j^{-1}) = w(\alpha) - w(j) \geq 0$ so $\alpha j^{-1} \in \mathcal{O}$ so $\alpha \in \mathcal{O}j$. Thus $P = \mathcal{O}j = j\mathcal{O} = \mathcal{O}j\mathcal{O}$, since P is a two-sided ideal. Arguing in the same way, since

$$w(j) \leq w(\pi) = v(\pi^2) = 1 \leq w(j^2),$$

we conclude that $P \supseteq \pi\mathcal{O} \supseteq P^2 = j^2\mathcal{O}$. The map $\alpha \mapsto \alpha j$ yields an isomorphism $\mathcal{O}/P \xrightarrow{\sim} P/P^2$ of k-vector spaces, so

$$4 = \dim_k \mathcal{O}/\pi\mathcal{O} \leq \dim_k \mathcal{O}/P + \dim_k P/P^2 = 2\dim_k \mathcal{O}/P \tag{11.5.9}$$

and thus $\dim_k \mathcal{O}/P \geq 2$; in particular, $\mathcal{O}/P \neq k$.

Since $\mathcal{O} \setminus P = \{x \in \mathcal{O} : w(x) = 0\} = \mathcal{O}^\times$, the ring $\mathcal{O}/P$ is a division algebra over k and hence a finite division ring. But then by Wedderburn's theorem (Exercises 3.12 and 5.11, or Exercise 6.17), the ring $\mathcal{O}/P$ is a field. Thus, there exists $i \in \mathcal{O}$ such that $\mathcal{O}/P = k(i)$, since k is a finite field. Then $K = F(i)$ is an unramified separable quadratic extension of F and consequently $\dim_k \mathcal{O}/P = f = 2$. Therefore equality holds in (11.5.9), and so $P^2 = \pi\mathcal{O}$.

By Exercise 6.14, there exists $b \in F^\times$ such that $B \simeq \left(\frac{K, b}{F}\right)$. But B is a division ring if and only if $b \in F^\times \setminus N_{K/F}(K^\times)$ by Theorems 4.5.5 and 5.3.8. Since K/F is unramified we have $N_{K/F}(K^\times) = R^\times \pi^{2\mathbb{Z}}$, so we may take $b = \pi$ (Exercise 5.3) and $B \simeq \left(\frac{K, \pi}{F}\right)$ is the unique division quaternion algebra over F. $\square$

Corollary 11.5.10. *If F is nonarchimedean and $B = \left(\frac{K, b}{F}\right)$, then $B \simeq \mathrm{M}_2(F)$ if K is unramified over F (so v is split or inert in K) and $v(b) = 0$.*

Remark 11.5.11. Let $B \simeq \left(\frac{K, \pi}{F}\right)$ be a division quaternion algebra over F, so that K is a separable quadratic subfield and $j^2 = \pi$. As above, in analogy with the case of field extensions, we define the *ramification degree* of B over F as $e(B/F) = 2$ and the *inertial degree* of B over F as $f(B/F) = 2$ and note the equality $e(B/F)f(B/F) = 4 = [B : F]$, as in the commutative case. This equality carries over more generally to division algebras; see Exercise 11.17.

11.6 Topology

In this section, we conclude with some discussion about the topology of algebras over local fields. [[More on topological groups?]]

Let F be a local field. Then F is locally compact (by definition) but is not itself compact. The subgroup $F^\times = F \setminus \{0\}$ is equipped the subspace topology; it is open in F so $F^\times$ is locally compact—this is quite visible when $F = \mathbb{R}, \mathbb{C}$ is archimedean. If F is nonarchimedean, with valuation ring R and valuation v, then $F^\times$ is totally disconnected and further $R^\times = \{x \in R : v(x) = 0\} \subset R$ is closed so is a topological abelian group that is compact (and totally disconnected).

Now let B be a finite-dimensional F-algebra. Then as a vector space over F, it has a unique topology compatible with the topology on F, as any two norms on a topological vector F-space (extending the norm on F) are equivalent (the sup norm is equivalent to the sum of squares norm, etc.). Two elements are close in the topology on B if and only if their coefficients are close with respect to a (fixed) basis: for example, two matrices in $\mathrm{M}_n(F)$ are close if and only if all of their coordinate entries are close. Consequently, B is locally compact topological ring (take a compact neighborhood in each coordinate). It is also true that $B^\times$ is a locally compact topological group: the norm $\mathrm{N}_{B/F} : B^\times \to F^\times$ is a continuous map, so $B^\times$ is open in B, and an open subset of a Hausdorff, locally compact space is locally compact in the subspace topology.

Example 11.6.1. If $B = \mathrm{M}_n(F)$, then $B^\times = \mathrm{GL}_n(F)$ is locally compact: any closed, bounded neighborhood that avoids the locus of matrices with determinant 0 is a compact neighborhood. When F is archimedean, this is quite visual: any matrix of nonzero determinant is at some finite distance away from the determinant zero locus! Note however that $\mathrm{GL}_n(F)$ is not itself compact since $F^\times = \mathrm{GL}_1(F)$ is not compact.

Now suppose F is nonarchimedean with valuation v and valuation ring R. Then R is the maximal compact subring of F. Indeed, $x \in F$ lies in a compact subring if and only if $v(x) \geq 0$ if and only if x is integral over R. The only new implication here is the statement that if $v(x) < 0$ then x does not lie in a compact subring, and that is because the sequence $x_n = x^n$ does not have a convergent subsequence as $|x_n| \to \infty$.

Next, let $\mathcal{O}$ be an R-order in B. Then $\mathcal{O} \simeq R^n$ is a free R-module of finite rank. Choosing a basis, the above argument shows that $\mathcal{O}$ is compact as the Cartesian power of a compact set. The group $\mathcal{O}^\times$ is therefore also compact because it is closed: for

$\gamma \in \mathcal{O}$, we have $\gamma \in \mathcal{O}^\times$ if and only if $\mathrm{N}_{B/F}(\gamma) \in R^\times \subset R$ and $R^\times = \{x \in R : v(x) = 0\} \subseteq R$ is closed.

Example 11.6.2. For $R = \mathbb{Z}_p \subseteq F = \mathbb{Q}_p$ and $B = \mathrm{M}_n(\mathbb{Q}_p)$, the order $\mathcal{O} = \mathrm{M}_n(\mathbb{Z}_p)$ is compact (neighborhoods can be taken coordinatewise) and the subgroup $\mathcal{O}^\times = \mathrm{GL}_n(\mathbb{Z}_p)$ is compact: there is no way to run off to infinity, either in a single coordinate or via the determinant.

11.6.3. Suppose $B = D$ is a division ring. Then the valuation ring $\mathcal{O}$ is the maximal compact subring of B, for the same reason as in the commutative case. In this situation, the unit group $\mathcal{O}^\times$ is a pro-solvable group! We have a filtration $\mathcal{O} \supset P \supset P^2 \supset \dots$ giving rise to a filtration

$$\mathcal{O}^\times \supset 1 + P \supset 1 + P^2 \supset \dots.$$

As in the second proof of Theorem 11.3.1, the quotient $\mathcal{O}/P$ is a finite extension of the finite residue field k, so $(\mathcal{O}/P)^\times$ is a cyclic abelian group. The maximal two-sided ideal P is principal, generated by an element j of minimal valuation, and multiplication by j^n gives an isomorphism $\mathcal{O}/P \xrightarrow{\sim} P^n/P^{n+1}$ of k-vector spaces (or abelian groups) for all $n \geq 1$.

Furthermore, for each $n \geq 1$, we have an isomorphism of groups

$$\begin{aligned} P^n/P^{n+1} &\xrightarrow{\sim} (1 + P^n)/(1 + P^{n+1}) \\ \alpha &\mapsto 1 + \alpha. \end{aligned} \tag{11.6.4}$$

Therefore, $\mathcal{O}^\times = \varprojlim_n (\mathcal{O}/P^n)^\times$ is an inverse limit of solvable groups.

11.6.5. We will also want to consider norm 1 groups; for this, we assume that B is a semisimple algebra. Let

$$B^1 = \{\alpha \in B : \mathrm{nrd}(\alpha) = 1\}.$$

Then B^1 is a closed subgroup of $B^\times$, since the reduced norm is a continuous function. If B is a divison ring and F is nonarchimedean, then B has a valuation ring $\mathcal{O}$, and $B^1 = \mathcal{O}^1$ is compact. If B is a division ring and F is archimedean, then $B \simeq \mathbb{H}$ and $B^1 \simeq \mathbb{H}^1 \simeq \mathrm{SU}(2)$ is compact (it is identified with the 3-sphere in $\mathbb{R}^4$). Finally, if B is not a division ring, then either B is the product of two algebras or B is a matrix ring over a division ring, and correspondingly B is not compact by considering the subgroup $(\pi, 1/\pi)$ or a unipotent subgroup.

[[Classification of *connected* locally compact division rings]]
[[topology on division D is the same as given by the vector space topology]]

11.7 Splitting fields

Proposition 11.7.1. *Let B be a division quaternion ring over F, and let L be a separable field extension of F of finite degree. Then L is a splitting field for B if and only if $[L : F]$ is even.*

Proof. We have $B \simeq \left(\frac{K,\pi}{F}\right)$ where K is the unramified quadratic extension of F. Let e, f be the ramification index and inertial degree of L. Then $[L : F] = n = ef$, so n is even if and only if e is even or f is even.

But f is even if and only if L contains an unramified quadratic subextension, necessarily isomorphic to K; but then K splits B so L splits B.

Otherwise, L is linearly disjoint from K so $K \otimes_F L = KL$ is the unramified quadratic extension of L. Therefore $B \otimes_F L \simeq \left(\frac{KL,\pi}{L}\right)$. Let R_L be the valuation ring of L and let π_L be a uniformizer for L. Then $N_{KL/L}(KL^\times) = R_L^\times \pi_L^{2\mathbb{Z}}$. If L/F has ramification index e, then $\pi = u\pi_L^e$ for some $u \in R_L^\times$. Putting these together, we see that $B \otimes_F L$ is a division ring if and only if π is a norm from KL if and only if e is even. $\square$

Corollary 11.7.2. *If K/F is a separable quadratic field extension, then $K \hookrightarrow B$.*

In other words, B contains every separable quadratic extension of F!

11.8 Extensions and further reading

The p-adic numbers were developed by Hensel. In the early 1920s, Hasse used them in the study of quadratic forms and algebras over number fields. At the time, what is now called the "local–global principle" then was called the the p-adic transfer from the "small" to the "large".

Theory of local fields: [Neu99, Corollary V.1.2]. J.-P. SERRE [1] Corps Locaux. Actualites Scientifiques et Industrielles. Hermann Paris (1966), 2e edition.

Weil started this game in his basic number theory.

Theory of local division rings more generally and noncommutative local rings.

11.9 Algorithmic aspects

Computing the Hilbert symbol

Exercises

11.1. Let k be a finite field and let $Q : V \to k$ be a ternary quadratic form. Show that q is isotropic. *[Hint: Reduce to the case of finding a solution to $y^2 = f(x)$ where f is a polynomial of degree 2. Then only the case $\#k$ odd remains; show that f takes on at least $(q+1)/2$ values in k but there are at most $(q-1)/2$ nonsquares in k.]*

Conclude again that there is no division quaternion ring over a finite field k.

11.2. Let k be a finite field with $\operatorname{char} k \neq 2$ and let $e \in k^\times$. Show that there is an isometry $\langle -1, e\rangle \simeq \langle 1, -e\rangle$.

11.3. Let k be a finite field with even cardinality. Show that $\#k/\wp(k) = 2$, where $\wp(k)$ is the Artin-Schreier group.

11.4. Let $F \neq \mathbb{C}$ be a local field and let Q be a nonsingular ternary quadratic form over F. Show that Q is isotropic over any quadratic field extension of F.

11.5. Let B be a division quaternion algebra over a nonarchimedean local field F. Give another proof that the unramified quadratic extension K of F embeds in B as follows.

Suppose it does not: then for all $x \in \mathcal{O}$, the extension $F(x)/F$ is ramified, so there exists $a \in R$ such that $x - a \in P \cap K(x)$; then write $x = x_0 = a + jx_1$, where $P = j\mathcal{O}$, and iterate to conclude that $x = \sum_{n=0}^{\infty} a_n j^n$ with $a_n \in R$. But $F(j)$ is complete so $\mathcal{O} \subseteq F(j)$, a contradiction.

11.6. Let B be a division quaternion algebra over the nonarchimedean local field F.

a) Show that B is a complete, locally compact topological ring and that $\mathcal{O}$ is the maximal compact subring of B.

b) Show that $\mathcal{O}^\times$ and $B^\times/F^\times$ are compact topological groups.

c) Conclude that the smooth, irreducible complex representations of $B^\times$ are finite dimensional, and compare this with the alternative $B \simeq \mathrm{M}_2(F)$.

11.7. Show that the table of Hilbert symbols (11.4.3) is correct.

11.8. Let F be a local field and K the unramified quadratic extension of F. Compute the K-left regular representation of a division quaternion algebra B over F (2.2.8) and identify the maximal order R and the maximal ideal P.

11.9. Prove a descent for the Hilbert symbol, as follows. Let K be a finite extension of the local field F with $\operatorname{char} F \neq 2$ and let $a, b \in F^\times$. Show that $(a, b)_K = (a, N_{K/F}(b))_F$.

11.10. Show that the table of Hilbert symbols (11.4.6) is correct by considering the equation $ax^2 + by^2 \equiv 1 \pmod 8$.

11.11. [[Alternative method for computing the Hilbert symbol.]]

11.12. One can package Paragraph 11.4.4 together with multiplying by squares to prove the following more general criterion. For $a, b \in F^\times$, we have

$$(a, b)_F = (-1)^{v(a)v(b)(q-1)/2} \left(\frac{\overline{a}}{\pi}\right)^{v(b)} \left(\frac{\overline{\overline{b}}}{\pi}\right)^{v(a)}$$

where $a = a_0\pi^{v(a)}$ and $b = b_0\pi^{v(b)}$ (and $v(\pi) = 1$).

11.13. Consider $B = \left(\frac{-1,-1}{\mathbb{Q}_2}\right)$ and let $\mathcal{O} = \mathbb{Z}_2 \oplus \mathbb{Z}_2 i \oplus \mathbb{Z}_2 j \oplus \mathbb{Z}_2(1 + i + j + ij)/2$. Show that B is a division ring. Give an explicit formula for the discrete valuation w on B (extending the valuation v on $\mathbb{Q}_2$) and prove that $\mathcal{O}$ is its valuation ring.

11.14. Let B be a division quaternion algebra over F. Show that $\alpha \in B$ is integral over R if and only if $\mathrm{nrd}(x), \mathrm{nrd}(x+1) \in R$ if and only if $w(x), w(x+1) \geq 0$, where w is the valuation on B.

11.15. Let B be a division quaternion algebra over a nonarchimedean local field F, and let $\mathcal{O}$ be the valuation ring. Show that every one-sided (left or right) ideal of $\mathcal{O}$ is a power of the maximal ideal J and hence is two-sided.

11.16. Let F be a nonarchimedean local field, let $B = \mathrm{M}_2(F)$ and $\mathcal{O} = \mathrm{M}_2(R)$. Show that there are $q+1$ right $\mathcal{O}$-ideals of norm $\mathfrak{p}$ corresponding to the elements of $\mathbb{P}^1(k)$ or to the lines in k^2.

11.17. Let D be a finite-dimensional division algebra over a nonarchimedean local field F of degree $[D : F] = n^2$ with valuation ring $\mathcal{O}$ and two-sided ideal P. Show that $\mathcal{O}/P$ is finite extension of k of degree n and $J^n = \mathcal{O}\pi\mathcal{O}$.

11.18. Show that (11.6.4) is an isomorphism of (abelian) groups.