

**SOLUTIONS TO PROBLEMS 3.5, 3.9.5, 3.11, 3.13.5**

KATE THOMPSON

3.5 Let  $p$  be an odd prime number, and let  $u \in \mathbb{Z}$  be a quadratic nonresidue modulo  $p$ . Then  $[\mathbb{Q}_p^\times : \mathbb{Q}_p^{\times 2}] = 4$ , and a set of coset representatives is  $1, p, u, pu$ .

*Solutions:* First, we intend to use Hensel's Lemma for this proof; given that, we feel obligated to state which version we will use.

**Lemma.** (*Hensel's Lemma*) Let  $(K, v)$  be a Henselian (e.g. complete) valued field with valuation ring  $R$  and residue field  $k$ . Let  $f \in R[t]$ . If there exists an  $\alpha \in R$  such that  $v(f(\alpha)) > 2v(f'(\alpha))$ , then there exists a  $\beta \in R$  with  $f(\beta) = 0$  and  $v(\alpha - \beta) > v(f'(\alpha))$ .

Let  $P(X) = X^2 - a$  for a  $p$ -adic integer. It is clear that there is a root in  $\mathbb{Z}_p$  only if

$$v(a) = v(x^2) = 2v(x)$$

is even. Then, by dividing  $a$  by an appropriate power of  $p^{2m}$ , we can reduce to the case  $v(a) = 0$ , or  $a \in \mathbb{Z}_p^\times$ .

Now we claim that if  $a \in \mathbb{Z}_p^\times$  is a  $p$ -adic unit and if there exists  $\alpha$  such that  $\alpha^2 \equiv a \pmod{p\mathbb{Z}_p}$ , then  $a$  is a square of an element in  $\mathbb{Z}_p^\times$ . To see this, apply Hensel's lemma to  $X^2 - a$ . Since  $p \neq 2$  and  $a \in \mathbb{Z}_p^\times$ , we are guaranteed to have  $2\alpha \not\equiv 0 \pmod{p}$  so we're fine.

Next, we claim that  $x \in \mathbb{Q}_p$  is a square if and only if  $x = p^{2n}y^2$  for  $n \in \mathbb{Z}$ , and  $y \in \mathbb{Z}_p^\times$  a  $p$ -adic unit. One direction is obvious. The second direction is also fairly obvious—just refer to the previous case, and also note that  $p$  is itself NOT a square in  $\mathbb{Q}_p$  (since if it had a square root, then that square root would have valuation  $\frac{1}{2}$ ). We can conclude then that  $[\mathbb{Q}_p^\times : \mathbb{Q}_p^{\times 2}] = 4$ , and is given by  $\{1, p, u, pu\}$  for  $u$  a quadratic non-residue in  $\mathbb{Z}_p^\times$ . Referring to the text below this Exercise in the course notes, we can moreover conclude that

$$\mathbb{Q}_p^\times / (\mathbb{Q}_p^{\times 2}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

3.9.5 A very special and important quadratic form is  $q_{\mathbb{H}}(x_1, x_2) = x_1x_2$ , the so-called **hyperbolic plane**.

a) Let  $K$  be any field of characteristic different from 2. Give an explicit change of variables that diagonalizes  $q_{\mathbb{H}}$ .

*Solutions:* Short answer: let

$$P = \begin{bmatrix} 1 & -1 \\ 2^{-1} & 2^{-1} \end{bmatrix}$$

Why does this definitely work? Since the characteristic of our field is not 2, we can represent the quadratic form  $x_1x_2$  as the following symmetric matrix:

$$M = \begin{bmatrix} 0 & 2^{-1} \\ 2^{-1} & 0 \end{bmatrix}$$

Thus, using matrix theory, we claim that  $P$  works. To confirm, we compute:

$$\begin{aligned} \begin{bmatrix} 1 & 2^{-1} \\ -1 & 2^{-1} \end{bmatrix} \begin{bmatrix} 0 & 2^{-1} \\ 2^{-1} & 0 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 2^{-1} & 2^{-1} \end{bmatrix} &= \begin{bmatrix} 2^{-2} & 2^{-1} \\ 2^{-2} & -2^{-1} \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 2^{-1} & 2^{-1} \end{bmatrix} \\ &= \begin{bmatrix} 2^{-1} & 0 \\ 0 & -2^{-1} \end{bmatrix} \end{aligned}$$

Last, note that since the characteristic of a field is NOT 2,  $2^{-1}$  exists.

b) Show by brute force that  $q_{\mathbb{H}}$  cannot be diagonalized over  $\mathbb{F}_2$ .

See part (c) for a less forceful method. ☹

c) Show that  $q_{\mathbb{H}}$  cannot be diagonalized over any field of characteristic 2.

*Solutions:* Suppose that it can be diagonalized. This means that for some  $a, b, c, d \in F$ ,  $ad - bc \neq 0$ , we have

$$\begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$$

Working this out, we see that we have:

$$\begin{aligned} \begin{bmatrix} a & c \\ b & d \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} &= \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \\ &= \begin{bmatrix} ac & ad \\ bc & bd \end{bmatrix} \end{aligned}$$

This means that  $ad = bc = 0$ ; however, that would contradict our assumption that  $ad - bc = 0$ .

This actually ‘kills’ both this part of the problem, as well as part (b).

3.11 Let  $K$  be any field of characteristic different from 2. Show that  $u(K) = 1$  iff  $K$  is quadratically closed.

*Solutions:* Assume that  $K$  is a field of characteristic other than 2. Moreover, suppose  $K$  is quadratically closed. This means that for all  $k \in K$ ,  $k = \ell^2$  for some  $\ell \in K$ . We intend to show that  $u(K) = 1$ . Certainly, there is at least one one-dimensional anisotropic form over  $K$ —take  $q(x) = x^2$  (since  $K$  is a field  $q(x) = 0 \Leftrightarrow x = 0$ ). Now we must show that every quadratic form over  $K$  in 2 or more variables is isotropic. Without loss of generality, take a quadratic form in 2 variables,  $q(x, y)$ . Using the fact that  $\text{char}(K) \neq 2$ , we can write  $q(x, y)$  as the diagonal matrix

$$M_{q(x,y)} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$$

for  $a, b \in K$ . If  $a = b = 0$ , all vectors are isotropic. If (wlog)  $a = 0, b \neq 0$ , take  $(b, 0)$  to be our isotropic vector. Last, if  $a, b \neq 0$ , then  $(x, y)$  is an anisotropic vector where  $x^2 = b$  and  $y^2 = -a$ .

Now assume that  $u(K) = 1$ . This means that every quadratic form in more than one variable is isotropic. This means for all  $a, b \in K$  there exist  $(x, y) \neq (0, 0)$  so that  $ax^2 + by^2 = 0$ . Assuming for example that  $a$  and  $b$  are not 0, this happens if and only if  $ax^2 = -by^2$  or  $\frac{a}{-b} = \left(\frac{x}{y}\right)^2$ . This means that  $K$  is quadratically closed. (take  $b = -1$  and let  $a \in K$  be arbitrary)

3.13.5 The goal is “simple”: we aim to show that  $u(\mathbb{Q}_2) = 4$ . This means we hope to show that there exists an anisotropic quadratic form in four variables over  $\mathbb{Q}_2$  AND that all quadratic forms in five or more variables over  $\mathbb{Q}_2$  are isotropic.

First, some background information on quaternion algebras:

**Definition.** Let  $a, b \in F^\times$ . Define the quaternion algebra  $A = \left(\frac{a, b}{F}\right)$  to be the  $F$ -algebra on the generators  $i, j$  which satisfy

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

Note that for  $k = ij \in A$ , we immediately have

$$k^2 = (ij)(ij) = -i^2j^2 = -ab \in F^\times$$

and the properties

$$ik = -ki = aj \text{ and } kj = -jk = bi$$

**Example.** With  $F = \mathbb{R}$ ,  $a = b = -1$ ,  $A = \left(\frac{-1, -1}{\mathbb{R}}\right)$  is the “usual division ring of quaternions over the reals” and is denoted by  $\mathcal{H}$ .

The following is a general proposition (which we will state primarily out of interest—only items 3–5 will be needed, and not until the end):

**Proposition.** (1) For any  $a, b, x, y \in F^\times$

$$\left(\frac{a, b}{F}\right) = \left(\frac{ax^2 + by^2}{F}\right)$$

(2)  $\left(\frac{-1, 1}{F}\right) \cong \mathbb{M}_2(F)$  (i.e., the set of  $2 \times 2$  matrices with coefficients in  $F$ )

(3) The center of  $\left(\frac{a, b}{F}\right)$  is  $F$  (or  $F \cdot 1$ )

(4)  $\left(\frac{a, b}{F}\right)$  is a simple algebra (that is, it has no nontrivial ideals).

(5) For  $a, b, c \in F^\times$ , we have

$$\left(\frac{a, b}{F}\right) \otimes \left(\frac{a, c}{F}\right) \cong \left(\frac{a, bc}{F}\right) \otimes \left(\frac{c, -a^2c}{F}\right) \cong \left(\frac{a, bc}{F}\right) \otimes \mathbb{M}_2(F)$$

We will need later the following proposition (stated without proof):

**Proposition.** For  $A = \left(\frac{a, b}{F}\right)$ , the following statements are equivalent:

(1)  $A \cong \left(\frac{-1, 1}{F}\right) \cong \mathbb{M}_2(F)$

(2)  $A$  is NOT a division algebra

(3)  $A$  is isotropic as a quadratic space.

(4)  $A$  is hyperbolic as a quadratic space.

(5)  $a \in N_{E/F}(E)$ , where  $E = F(\sqrt{b})$  and  $N_{E/F}$  is the field norm.

Note that (at least for now, assuming  $\text{char}(F) \neq 2$ ), we can take a quaternion algebra and see it as a quadratic space. To do that, consider an arbitrary element

$$x = \alpha + \beta i + \gamma j + \delta k$$

We first define the conjugate  $\bar{x}$  of  $x$  by

$$\bar{x} = \alpha - (\beta i + \gamma j + \delta k)$$

**Definition.** For an arbitrary quaternion  $x \in A$ , define its norm  $N(x)$  and trace  $T(x)$  by

$$\begin{aligned} N(x) &= x\bar{x} \\ T(x) &= x + \bar{x} \end{aligned}$$

Using this, we can associate to  $A$  a symmetric bilinear form

$$B(x, y) = \frac{x\bar{y} + y\bar{x}}{2} = \frac{T(x\bar{y})}{2} \in F$$

We then will refer to  $(A, B)$  as a quadratic space over  $F$ .

Note that using this notation, the quadratic form associated with  $B$  sends

$$x \mapsto B(x, x) = \frac{T(x\bar{x})}{2} = x\bar{x} = N(x)$$

Some “facts” (meaning, items that will be stated without proof) regarding the quadratic space  $(A, B)$  (as well as arbitrary quaternions  $x \in A$ ):

- (1)  $(A, B)$  has orthogonal basis  $\{1, i, j, k\}$ .
- (2)  $(A, B)$  is a regular quadratic space and is isometric to

$$\langle 1, -a, -b, ab \rangle \cong \langle 1, -a \rangle \otimes \langle 1, -b \rangle$$

(which can be verified by noting

$$N(1) = 1, N(i) = -a, N(j) = -b, \text{ and } N(k) = ab$$

- (3) Any quaternion  $x \in A$  satisfies a quadratic polynomial equation over a base field  $F$ . Specifically

$$x^2 - (T(x))x + (N(x)) = 0$$

- (4) Last, it is taken as fact that  $\langle 1, -a, -b, ab \rangle$  (for  $a, b \in F^\times$ ) are precisely the four-dimensional quadratic forms  $q$  over  $F$  such that  $d(q) = 1$  (i.e., the determinant of the matrix associated with  $q$  is 1), and  $1 \in D_F(q)$  (i.e.,  $q$  represents 1).

We now move closer to our particular question by discussing quaternion algebras over local fields; specifically we hope to prove that there exists a unique quaternion division algebra over any local field. But first:

**Definition.** A complete discrete valued field  $F$  is called a local field if the residue class field  $\bar{F}$  is finite. In this case,  $|\bar{F}|$  is denoted by  $\mathbb{N}\mathfrak{p}$ . We will also (while we're at it) define  $U = \{x \in F^\times : v(x) = 0\}$ .

**Proposition.** A local field  $F$  has a unique unramified quadratic extension  $K$ .

*Proof.* Let  $\Omega$  denote the algebraic closure of  $F$ . Let  $K \subset \Omega$  be the splitting field of  $X^{(\mathbb{N}\mathfrak{p})^2} - X$  over  $F$ . We note that  $\bar{K} = (\mathbb{N}\mathfrak{p})^2$ , and consequently  $[\bar{K} : \bar{F}] = 2$ . Moreover, we note that  $X^{(\mathbb{N}\mathfrak{p})^2} - X \in \bar{K}[x]$  has distinct roots. Thus, by Hensel's lemma, there exists a primitive root  $\alpha$  of  $X^{(\mathbb{N}\mathfrak{p})^2-1} - 1$  in  $K$  such that  $K = F(\alpha)$ . The discriminant of  $X^{(\mathbb{N}\mathfrak{p})^2-1} - 1$  is not divisible by  $\mathfrak{p}$ , and thus we see that  $K/F$  is unramified.

On the other hand, if  $K/F$  is a quadratic unramified extension, then  $\bar{K}$  is the unique quadratic extension of  $\bar{F}$  and we are done.  $\square$

We actually know quite a bit more than that, however. Specifically:

**Proposition.** Let  $F$  be a local field and let  $K$  be its unique unramified quadratic extension. Then, there exists  $u \in U$  such that  $K = F(\sqrt{u})$  (the square class of  $u$  in  $F$  is uniquely determined)

*Proof.* Suppose  $K = F(\alpha)$ , and  $[K : F] = 2$ . Suppose moreover that  $K$  is unramified. We will show that  $K = F(\sqrt{u})$ . Since  $F$  is a field of characteristic zero

$$\alpha^2 + b\alpha + c = 0$$

for some  $b, c \in F$ . Using the quadratic formula that means we really have

$$\alpha^2 + c' = 0$$

for some  $c' \in F^\times$ . We then can write  $c' = \pi^r u$  for  $\pi$  a uniformizer and  $u$  an element of valuation 0; to see this, consider the map

$$\psi : F^\times \rightarrow \mathbb{Z} \times \mathcal{O}_F^\times$$

given by

$$\psi(a) \mapsto \left( \text{ord}_{\mathfrak{p}} a, \frac{a}{\pi^{\text{ord}_{\mathfrak{p}} a}} \right).$$

This means that  $\alpha^2 = \pi^r u$  for some  $r \in \mathbb{Z}$ . Because  $\pi$  is still a uniformizer for  $K$ , and  $u$  is still a unit in  $K$ , we see that  $\alpha^2 = \pi^r u \in K$  implies  $r$  is even; more specifically, this will use the assumption that  $K$  is unramified, for that tells us

$$\begin{aligned} \alpha^2 &= \pi^r u \Rightarrow \\ 2\text{ord}_{\mathfrak{p}}(\alpha) &= r \quad \mathbf{AND} \\ \text{ord}_{\mathfrak{p}}(\alpha) &= \text{ord}_{\mathfrak{p}}(\alpha) \in \mathbb{Z} \end{aligned}$$

Now that we know  $r$  is even, we see  $K = F(\sqrt{\pi^r u}) = F(\pi^{r/2} \sqrt{u}) = F(\sqrt{u})$ .  $\square$

We have one other (quick) item to note: in our particular case, the valuation  $v : F^\times \rightarrow \mathbb{Z}$  is extended by  $v' : K^\times \rightarrow \mathbb{Z}$ . If we let  $\sigma$  be the  $F$  automorphism of  $K$  that sends  $\sqrt{u}$  to  $-\sqrt{u}$ , we see that for any  $z \in K^\times$ ,  $v'(z) = v'(z^\sigma)$ . This implies

$$\begin{aligned} v(N_{K/F}(z)) &= v(z z^\sigma) \\ &= v'(z) + v'(z^\sigma) \\ &= 2v'(z) \end{aligned}$$

This implies that  $\pi$ , which has valuation 1 is not a norm from  $K = F(\sqrt{u})$ .

Now that we are (hopefully) done with introductions and background material, we proceed to the following “meaty” theorem:

**Theorem.** *Let  $F$  be an arbitrary local field.  $F$  has a unique quaternion division algebra, namely  $D = \left( \frac{\pi, u}{F} \right)$ .*

*Proof.* Since we have observed that  $\pi$  is not a norm from  $K = F(\sqrt{u})$ , it follows from before-mentioned propositions that  $D$  is indeed a division algebra. Conversely, let  $E$  be any quaternion division algebra over  $F$ . We will show that  $E \cong D$ .

– Step 1: Define a homomorphism  $w' : E \setminus \{0\} \rightarrow \mathbb{Z}$  by  $w'(x) = v(N(x))$ , where  $N$  denotes the (anisotropic) norm form of  $E$ . Let  $d$  be the unique positive integer such that  $w'(E \setminus \{0\}) = d\mathbb{Z}$ . Since

$$w'(\pi) = v(N(\pi)) = v(\pi^2) = 2,$$

$d$  must be either 2 or 1. We may “normalize”  $w'$  by setting  $w(x) = w'(x)/d$  for  $x \in E \setminus \{0\}$ , and (by convention)  $w(0) = \infty$ . Let  $B = \{x \in E : w(x) \geq 0\}$ , which is a subring of  $E$ , and let  $\mathfrak{P} = \{x \in E : w(x) \geq 1\}$ , which is a 2-sided ideal in  $B$ . First, we see that we have

$$\begin{aligned} B \cap F &= \{x \in E : v(N(x))/d \geq 0\} \cap \{x \in F\} \\ &= \{x \in F : 2v(x) \geq 0\} \\ &= \{x \in F : v(x) \geq 0\} \\ &= A \end{aligned}$$

and

$$\begin{aligned} \mathfrak{P} \cap A &= \{x \in A : v(N(x)) \geq d\} \\ &= \{x \in A : v(x) \geq d/2\} \\ &= \{x \in F : v(x) \geq 1\} \\ &= \mathfrak{p} \text{ (by definition)} \end{aligned}$$

- Step 2: We have  $E = F \cdot B$ . In fact, if  $x \in E$ , then  $N(\pi^m x) = \pi^{2m} N(x)$  (note: this uses the fact that  $\pi$  is not a norm from  $K = F(\sqrt{u})$ ). If  $m$  is sufficiently large, then  $N(\pi^m x) \in A$ , which implies that  $\pi^m x \in B$ , or  $x \in (1/\pi^m) \cdot B$ .
- Step 3: Since  $N$  maps  $B$  into  $A$ , the inner product associated with  $N$  clearly maps  $B \times B$  into  $A$ . By a dual basis argument, we see that  $B$  is contained in a finitely generated  $A$ -submodule of  $E$ . Since  $A$  is a discrete valuation ring, this shows that  $B$  must be a free (left)  $A$ -module (of rank 4, by Step 2). [For slightly more specificity to this ‘claim,’ since  $E = F \cdot B$ , we see that we have a basis  $\{x_1, \dots, x_4\}$  of  $E$  with  $x_i \in B$ . Since the quadratic form associated to  $E$  is regular, we in fact have a dual basis  $\{x_1^*, \dots, x_4^*\}$ . Thus for  $x \in B$ , we can write  $x = \sum a_i x_i^*$ . Using last the fact that  $N(B) \in A$  we get  $A[x_1, \dots, x_4] \subset B \subset A[x_1^*, \dots, x_4^*]$ ] Setting  $e = w(\pi) = 2/d$ , we have

$$\begin{aligned} \mathfrak{p}B &= \pi B \text{ (since } \pi \text{ is a generator for } \mathfrak{p}\text{)} \\ &= \mathfrak{P}^e \end{aligned}$$

To see this last equality, we will have the following two cases:

Case 1:  $d = 1$  and  $e = 2$ . Then we have:

$$\begin{aligned} \mathfrak{P}^2 &= \{x \in E : v(N(x)) \geq 1\}^2 \\ &= \{x \in E : v(N(x)) \geq 2\} \\ &= \pi B \end{aligned}$$

Case 2:  $d = 2$  and  $e = 1$ . Then we have:

$$\begin{aligned} \mathfrak{P} &= \{x \in E : \frac{v(N(x))}{2} \geq 1\} \\ &= \{x \in E : v(N(x)) \geq 2\} \\ &= \pi B \end{aligned}$$

So now, let  $f$  be the  $\overline{F}$ -dimension of  $B/\mathfrak{P}$ . Then

$$\begin{aligned} 4 &= \dim_{\overline{F}}(B/\mathfrak{P}^e) \\ &= e \cdot \dim_{\overline{F}}(B/\mathfrak{P}) \\ &= ef \end{aligned}$$

Since  $d$  equals 1 or 2,  $e = \frac{2}{d} = 1$  or 2, and thus  $f$  is either 2 or 4.

- Step 4 We now will use the finiteness of  $\overline{F}$ . We begin by stating Wedderburn’s Little Theorem:

**Theorem.** *All finite division rings are finite fields.*

Thus, Wedderburn tells us that  $B/\mathfrak{P}$  must be a commutative field, and therefore an extension of  $\overline{F}$ . Choose  $s \in B$  such that the residue class of  $s$  generates  $B/\mathfrak{P}$  over  $\overline{F}$ . The field  $L = F(s)$  is a quadratic extension of  $F$ . This claim results from the following:

**Lemma.** *If the quaternion algebra  $E$  over  $F$  is a division algebra and  $s \notin Z(E)$ , then  $L = F(s)$  is a quadratic field extension of  $F$  and  $n|_L = N_{L/F}$ .*

Assuming for now that the lemma holds, we see that the quadratic minimal polynomial of  $s$  over  $F$  necessarily has coefficients in  $A$ , since  $N(s) = N_{L/F}(s) \in A$ . Thus,  $e = \dim_{\overline{F}}(B/\mathfrak{P})$  must be 2 (so  $e = 2$  and  $d = 1$ ).

Note also  $L$  is a local field, with valuation ring  $L \cap B$ , and residue class field  $\overline{L} = (L \cap B)/(L \cap \mathfrak{P})$ . Since  $\overline{L}$  contains the residue class of  $s$ , we conclude that  $\dim_{\overline{F}} \overline{L} = 2$ ; i.e.,  $L$  is unramified over  $F$ .

Last, for future references and hopeful notation simplification, let  $L = F(\beta)$ , where  $\beta = \sqrt{u}$ , and  $u$  is as before.

- Step 5 We begin by stating the Skolem-Noether Theorem:

**Theorem.** *Let  $A$  be a finite-dimensional central simple algebra over  $F$  and let  $B$  be a finite-dimensional simple algebra over  $F$ . If  $\phi, \psi : B \rightarrow A$  are algebra homomorphisms, then there exists an invertible element  $c \in A$  such that  $\phi(b) = c^{-1}\psi(b)c$  for all  $b \in B$ .*

Now, let  $\sigma$  denote the  $F$ -automorphism of  $L$  taking  $\beta$  to  $\beta^\sigma = -\beta$ . Skolem-Neother tells us that there exists  $\alpha \in E$  such that  $z^\sigma = \alpha^{-1}z\alpha$  for every  $z \in L$ . Since  $\sigma^2 = Id_L$ ,

$$\begin{aligned} z &= (z^\sigma)^\sigma \\ &= \alpha^{-1}(z^\sigma)\alpha \\ &= \alpha^{-1}(\alpha^{-1}z\alpha)\alpha \\ &= \alpha^{-2}z\alpha^2 \end{aligned}$$

and hence  $\alpha^2$  commutes with  $L$ . But  $E = L \oplus L \cdot \alpha$ , so  $\alpha^2$  lies in the center of  $E$ ; that is,  $\alpha^2 \in F^\times$  (see our very first proposition).

– Step 6 Now we just need to put all the pieces together. Note that  $\alpha, \beta \in E$  satisfy

$$\begin{aligned} \alpha^2 &= \pi^m x \in F^\times \quad (\text{where again } m \in \mathbb{Z} \text{ and } x \in U) \\ \beta^2 &= u \in F^\times \\ \text{and } \alpha\beta\alpha^{-1} &= -\beta, \text{ or } \alpha\beta = -\beta\alpha \end{aligned}$$

Therefore,  $E$  is the quaternion algebra  $\left(\frac{\pi^m x, u}{F}\right)$ . But  $x$  is a norm from  $L = F(\sqrt{u})$ . So then

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

Since  $E$  is a division algebra, we see that  $m$  must be odd (for proof of this: suppose  $m$  is even. Since  $E$  is a division algebra, by a previous proposition we see that  $\langle 1, -\pi^m, -u, \pi^m u \rangle$  must be anisotropic. BUT, if  $m$  is even, then vector  $(0, 0, \pi^{m/2}, 1) \neq (0, 0, 0, 0)$  will be isotropic. Contradiction). Therefore,

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

□

**Corollary.** *The (anisotropic) norm form  $\phi_F := \langle 1, -\pi, -u, \pi u \rangle$  of  $D$  is universal.*

*Proof.* The group  $F^\times$  is generated by  $-\pi$  and all  $x \in U$  (note that we used this fact in the previous proposition). Since  $x$  is a norm from  $L = F(\sqrt{u})$ ,  $\langle 1, -u \rangle$  represents  $x$  and hence  $\phi_F$  represents  $x$ . But the values of  $\phi_F$  form a subgroup of  $F^\times$  so  $\phi_F$  is clearly universal. □

So now that we have successfully shown that there is a anisotropic quadratic form in four variables over  $\mathbb{Q}_p$  for any  $p$  (namely, for  $\mathbb{Q}_2$ ), we use the following “localized” version of Hasse-Minkowski to show that all quadratic forms in five or more variables are isotropic:

**Theorem.** *Let  $F$  be any local field. Then any five-dimensional form  $f$  over  $F$  is isotropic.*

*Proof.* Assume that  $f$  is anisotropic. Scaling  $f$  by an element that it represents, we may assume that  $f \cong \langle 1, a, b, c, d \rangle$ . Since  $\langle 1, a, b \rangle$  is anisotropic, so is  $\langle 1, a, b, ab \rangle$ . We claim that  $\langle 1, -c, -d \rangle$  must be isotropic. Again, assume not. If  $\langle 1, -c, -d \rangle$  is anisotropic, then so is  $\langle 1, -c, -d, cd \rangle$ . Since there is a unique quaternion division algebra over  $F$  (and hence a unique anisotropic quadratic form in four variables over  $F$ ), we get

$$\langle 1, a, b, ab \rangle \cong \langle 1, -c, -d, cd \rangle$$

This however, would imply that

$$\langle a, b, c, d \rangle \cong \langle 1, -1, -ab, cd \rangle$$

which is of course a contradiction. Therefore,  $\langle 1, -c, -d \rangle$  is isotropic, which tells us  $\langle c, d \rangle \cong \langle 1, cd \rangle$  and (more importantly)

$$\langle 1, a, b, c, d \rangle \cong \langle 1, a, b, 1, cd \rangle.$$

We repeat this argument twice more, first to see that  $\langle 1, -a, -b \rangle$  must be isotropic and  $\langle a, b \rangle \cong \langle 1, ab \rangle$ ; second to see that  $\langle 1, -ab, -cd \rangle$  is isotropic and  $\langle ab, cd \rangle \cong \langle 1, abcd \rangle$ . This gives

$$f \cong \langle 1, a, b, 1, cd \rangle \cong \langle 1, 1, ab, 1, cd \rangle \cong \langle 1, 1, 1, 1, abcd \rangle$$

Our previous theorem says there is a unique anisotropic quadratic form in four variables over  $F$ , so we have

$$\langle 1, 1, 1, 1 \rangle \cong \phi_F$$

However, the last corollary told us that  $\phi_F$  (and hence  $\langle 1, 1, 1, 1 \rangle$ ) is universal. Thus  $f$  is actually isotropic.  $\square$

This then, completes the proof that  $u(\mathbb{Q}_2) = 4$ .

#### REFERENCES

- [1] Gouvea, Fernando Q., *p-adic Numbers: An Introduction*, Springer, 2003
- [2] Lam, T.Y., *Introduction to Quadratic Forms over Fields*, American Mathematical Society Graduate Studies in Mathematics Series, Volume 67, 2005
- [3] Maclachlan, C., and Reid, A., *The Arithmetic of Hyperbolic 3-Manifolds*, Springer Graduate Texts in Mathematics, Volume 219, 2003