Quadratic forms and Hasse's local-global principle

Bachelor's thesis

Duco van de Schepop
June 2024

Supervisor: Dr. R. van Dobben de Bruyn

Department of Mathematics

Universiteit Utrecht

Contents

Abstract

In this thesis we will discuss the topic of quadratic forms and we will prove Hasse's local-global principle. This is a theorem that allows us to determine if a quadratic form with coefficients in $\mathbb{Q}$ has a nontrivial zero. Firstly, we will define quadratic forms and prove some basic properties. Then, we define the p-adic field $\mathbb{Q}_p$ and explore this field thoroughly to learn a lot about its structure and its elements. Finally, we will prove the local-global principle.

Introduction

If a polynomial $f(x) \in \mathbb{Z}[x]$ has a root $a \in \mathbb{Z}$, then the reduced polynomial $\bar{f}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ has a corresponding root $\bar{a} \in \mathbb{Z}/p\mathbb{Z}$ for every prime p. In other words, if f has a 'global' zero, then it has a 'local' zero everywhere. The converse is not true. For example, the polynomial:

$$(x^2 - 2)(x^2 - 3)(x^2 - 6),$$

has a zero in $\mathbb{Z}/p\mathbb{Z}$ everywhere, but none in $\mathbb{Z}$. So, in this case, it is not necessarily true that a local zero everywhere implies a global zero. A local-global principle is a statement that asserts that a certain property is true globally if and only if it is true everywhere locally. Before stating Hasse's local-global principle, we provide an overview of the topics discussed in this thesis.

The first chapter of this thesis is about quadratic forms. A quadratic form on a vector space V over k with $\dim(V) = n$ is a function $f : V \to k$ such that f can be written as:

$$f(x_1, \ldots, x_n) = \sum_i \sum_j a_{ij} x_i x_j,$$

such that $a_{ij} = a_{ji}$. We say that two quadratic forms f on V and g on V' are equivalent if there exists a linear bijection $h : V \to V'$ such that $g \circ h = f$. If this is the case we will write $f \sim g$. The main theorem of this chapter is that every quadratic form f is equivalent to a quadratic form of the form:

$$f \sim a_1 x_1^2 + \ldots + a_n x_n^2.$$

We say that a quadratic form is nondegenerate if $a_i \neq 0$ for all $1 \leqslant i \leqslant n$.

In the second chapter we will define the p-adic field $\mathbb{Q}_p$. Recall, that the field $\mathbb{Q}$ is not complete with respect to te absolute value and that $\mathbb{R}$ can be defined as a completion of $\mathbb{Q}$ using Cauchy sequences. The p-adic field $\mathbb{Q}_p$ is defined similarly. It is defined as a completion of $\mathbb{Q}$, in almost the same way as $\mathbb{R}$, but with respect to another norm. The norm in question is called the p-adic norm. An element $x \in \mathbb{Q}$ is small with respect to this norm if the power of p in the 'prime factorization' of x is high and vice versa.

We will give a decomposition of $\mathbb{Q}_p^\times$, but before we are able to do this we first try to understand what the elements in $\mathbb{Q}_p$ look like. After this we

will do some analysis in $\mathbb{Q}_p$. We will mainly discuss the function $\exp(x)$ and $\log(x)$. These function are important to us because they will allow us the give isomorphism between subsets of $\mathbb{Q}_p$, which in turn allows us to decompose $\mathbb{Q}_p^\times$ and give us criteria when an element in $\mathbb{Q}_p^\times$ is a square.

We will use all this theory to prove bilinearity of the Hilbert symbol. The Hilbert symbol is defined as follows: let $a, b \in \mathbb{Q}_p^\times$. We put:

$$(a,b) = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a solution not equal to 0 in } \mathbb{Q}_p^3. \\ -1 & \text{otherwise.} \end{cases}$$

Bilinearity of the Hilbert symbol means that:

$$(aa', b) = (a, b)(a', b).$$

It is one the the main theorems of this thesis. It is a strong theorem and we will use it a lot to prove the local-global principle, which we will now formally state.

Theorem. A nondegenerate quadratic form f with coefficients in $\mathbb{Q}$ has a nontrivial zero if and only if f has a nontrivialzero in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every prime p.

1 Quadratic forms

1.1 Basic definitions

Definition 1.1.1. Let V be a vector space over a field k. A *quadratic form* on V is a function $Q : V \to k$ that suffices:

1. $Q(ax) = a^2 Q(x)$ for all $a \in k$ and $x \in V$
2. The function $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear function.

We call the pair (V, Q) a *quadratic module*.

In this text, we will limit ourselves to fields k with $char(k) \neq 2$. We also assume that V has finite dimension.

Definition 1.1.2. Let $x, y \in V$. The function $\cdot : V \times V \to R$ defined by:

$$x \cdot y = \frac{1}{2}\big(Q(x + y) - Q(x) - Q(y)\big)$$

is called the *scalar product* associated with Q.

The scalar product has the following important property:

$$x \cdot x = \frac{1}{2}(Q(2x) - 2Q(x)) = Q(x).$$

Proposition 1.1.3. *Define $\mathcal{Q}_V$ as the set of quadratic forms on the vector space V and $\mathcal{B}_V$ as the set of symmetric bilinear functions over the same space. The maps $f : \mathcal{Q}_V \to \mathcal{B}_V$ and $g : \mathcal{B}_V \to \mathcal{Q}_V$ given by:*

$$f(Q)(x, y) := \frac{1}{2}\big(Q(x + y) - Q(x) - Q(y)\big)$$

and

$$g(b)(x) := b(x, x),$$

are well-defined and mutual inverses. We conclude that $\mathcal{Q}_V$ is in bijection with $\mathcal{B}_V$.

Proof. By Definition 1.1.1, the map f sends quadratic forms to symmetric bilinear functions. It is obvious that $g(b)(ax) = b(ax, ax) = a^2 b(x, x) = a^2 g(b)(x)$, so $g(b)$ satisfies the first property of a quadratic form. Because b is bilinear, $g(b)$ also satisfies the second. We prove that f and g are inverses:

$$(f \circ g)(b(x, y)) = \frac{1}{2}\big(b(x + y, x + y) - b(x, x) - b(y, y)\big) = b(x + y)$$

and

$$(g \circ f)(Q(x)) = \frac{1}{2}\big(Q(2x) - 2Q(x)\big) = Q(x). \qquad \square$$

We will now define the matrix of a quadratic form.

Definition 1.1.4. Let (V, Q) be a quadratic module and $B = \{e_1, ..., e_n\}$ be a basis of V. The *matrix of* Q with respect to this basis, is the matrix $A = (a_{ij})$ with $a_{ij} := e_i \cdot e_j$.

If we change the basis by means of an invertible matrix $X = (x_{ij})$, we get a new matrix $A' = (a'_{ij})$ of Q with respect to the new basis $B' = \{Xe_1, ..., Xe_n\}$. We defined $a'_{ij} = (Xe_i \cdot Xe_j)$ and we will show that $A' = X^T AX$:

$$\begin{aligned} Xe_i \cdot Xe_j &= \sum_{k=1}^{n} x_{ki} e_k \cdot \sum_{l=1}^{n} x_{lj} e_l \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} x_{ki} x_{lj} (e_k \cdot e_j) = \left(X^T AX\right)_{ij} \end{aligned}$$

We conclude that $\det(A') = \det(A) \det(X)^2$. The following definition makes sense now.

Definition 1.1.5. The *discriminant* of Q is defined as the determinant of A, it is determined up to multiplication by and element of k^{*^2}. The discriminant is denoted as $d(Q)$.

Example 1.1.6. *Define $Q : \mathbb{R}^n \to \mathbb{R}$ by $Q(x) = x_1^2 + ... + x_n^2$, where we use the usual multiplication and addition in $\mathbb{R}$. We will use the standard basis in this example. If $x, y \in \mathbb{R}^n$, with $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$, then:*

$$\begin{aligned} x \cdot y &= \frac{1}{2}\big(Q(x+y) - Q(x) - Q(y)\big) \\ &= \frac{1}{2}\left(\sum_i (x_i + y_i)^2 - x_i^2 - y_i^2\right) \\ &= \frac{1}{2}\left(\sum_i 2x_i y_i\right) \\ &= x_1 y_1 + x_2 y_2 + ... + x_n y_n. \end{aligned}$$

For the matrix A of Q we see that, with respect to the standard basis, $A = I_n$, where I_n denotes the identity matrix. We also have $d(Q) = 1$.

1.2 Orthogonality

Definition 1.2.1. Let (V, Q) be a quadratic module over k. Two elements $x, y \in V$ are called *orthogonal* if $x \cdot y = 0$. The set of elements orthogonal to a subset $H \subset V$ is denoted by $H^{\perp}$. If V_1 and V_2 are two linear subspaces of V, they are said to be orthogonal if $x \in V_1, y \in V_2$ implies that $x \cdot y = 0$.

Proposition 1.2.2. *Let H be a subset of V, where (V, Q) is a quadratic module. The set $H^{\perp}$, is a linear subspace of V.*

Proof. If $H = \varnothing$, then $H^{\perp} = V$, so suppose that $H \neq \varnothing$. Since $x \cdot 0 = 0$ for all $x \in V$, we have $0 \in H^{\perp}$ and $H^{\perp} \neq \varnothing$. Suppose that v_1, v_2 are elements of $H^{\perp}$ and k_1, k_2 are elements of k. It is sufficient to show that $k_1 v_1 + k_2 v_2 \in H^{\perp}$. Now, for every $v \in H$ we have:

$$(k_1 v_1 + k_2 v_2) \cdot v = k_1(v_1 \cdot v) + k_2(v_2 \cdot v) = 0,$$

by bilinearity of the scalar product. □

Definition 1.2.3. The orthogonal complement $V^{\perp}$ of V itself, is called the *radical* of V, denoted $\mathrm{rad}(V)$. Its codimension is called the *rank* of Q. If $V^{\perp} = \{0\}$, we say that Q is *nondegenerate*.

Let's take a look at $Q : \mathbb{R}^2 \to \mathbb{R}$ defined by $Q(x) = x_1^2 + 2x_1x_2 + x_2^2$, where $x = (x_1, x_2)$. If $y = (y_1, y_2) \in \mathbb{R}^2$, then the scalar product for this quadratic form is:

$$x \cdot y = x_1y_1 + x_1y_2 + y_1x_2 + x_2y_2.$$

Using the standard basis for $\mathbb{R}^2$, it is easy to see that all the entries of the matrix A of Q are given by $a_{ij} = 1$. This means that $d(Q) = \det(A) = 0$ and there exists $k_1, k_2 \in \mathbb{R}$ such that for the column vectors v_1, v_2 of A, we have $k_1v_1 + k_2v_2 = 0$. Since $v_1 = v_2$ we choose $k_1 = -k_2 = 1$. Now, for any $x \in \mathbb{R}^2$ we have:

$$\begin{bmatrix} 1 \\ -1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = x_1 + x_2 - x_1 - x_2 = 0.$$

We conclude that Q is degenerate. The next proposition generalizes this phenomenon.

Proposition 1.2.4. *A quadratic form Q is nondegenerate if and only if $d(Q) \neq 0$.*

Proof. Let A be the matrix of Q. Denote for $v_1, ..., v_n$ the column vectors of A. We have that $\det(A) = 0$ if and only if $k_1v_1 + ... + k_nv_n = 0$ for some $k_1, ..., k_n \in k$ not all equal to zero or since $v_i = (a_{1i}, \ldots, a_{ni})$:

$$\sum_j k_j a_{ij} = 0 \text{ for all } 1 \leqslant i \leqslant n \ .$$

For arbitrary $x \in V$ with $x = \sum_i x_i e_i$ we have:

$$\begin{aligned}\sum_i x_i e_i \cdot \sum_j k_j e_j &= \sum_i x_i (e_i \cdot \sum_j k_j e_j) \\ &= \sum_i x_i \sum_j k_j (e_i \cdot e_j) = 0.\end{aligned}$$

So, there exists $(k_1, \ldots, k_n) \neq 0 \in V^\perp$ if and only if $d(Q) = 0$. □

Definition 1.2.5. Let $U_1, \ldots, U_m$ be linear subspaces of V. One says that V is the *orthogonal direct sum* of the U_i if they are pairwise orthogonal and if V is the direct sum of them. One writes then:

$$V = U_1 \perp \ldots \perp U_m.$$

Proposition 1.2.6. *Suppose (V, Q) is a quadratic module. We can decompose (V, Q) as:*

$$V = \mathrm{rad}(V) \perp U$$

where $Q|_U$ is nondegenerate.

Proof. If U is any subspace of V then $\mathrm{rad}(V)$ and U are orthogonal. By Proposition 1.2.2 we know that $\mathrm{rad}(V)$ is a subspace of V. Every subspace of a vector space has a complement, i.e. there exists U such that:

$$V = \mathrm{rad}(V) \oplus U \text{ and } U \cap \mathrm{rad}(V) = \{0\}.$$

Now, U must be nondegenerate. If $x \in \mathrm{rad}(U)$, $v \in \mathrm{rad}(V)$ and $u \in U$, we have $x \cdot (v + u) = x \cdot v + x \cdot u = 0$, so $x \in \mathrm{rad}(V)$ and $x = 0$. □

Definition 1.2.7. Given any vector space V over a field k, the *dual space* V^* is defined as the set of all linear maps $\phi : V \to k$. The dual space V^* becomes a vector space over k and $\dim(V) = \dim(V^*)$ if V is finite-dimensional. Elements of the dual space are called *linear forms.*

Lemma 1.2.8. *Let U be a linear subspcae of V, and let U^* be the dual of U. Let $q_U : V \to U^*$ be defined by $q_U(x) = x \cdot -$.*

1. *The kernel of q_U is $U^\perp$.*
2. *The quadratic form Q is nondegenerate if and only if $q_V : V \to V^*$ is an isomorphism.*

Proof. Let $x \in \ker(q_U)$. We have $q_U(x)(u) = x \cdot u = 0$ for all $u \in U$, so $x \in U^\perp$. Now, let $x \in U^\perp$, so for all $u \in U$ we have $q_U(x)(u) = x \cdot u = 0$, so $x \in \ker(q_U)$. This proves 1. Suppose Q is nondegenerate. We have that q_V is injective, since $\ker(q_V)$ must be trivial. We know that q_V is a linear map and injective, so from this we can conclude that a set of independent vectors gets mapped to independent linear forms, using $\dim(V^*) = \dim(V)$ we conclude that q_V is surjective. Suppose that q_V is an isomorphism. Injectivity implies that q_V has trivial kernel. This proves 2. □

Definition 1.2.9. A *metric isomorphism* between quadratic modules (V, Q) and (V', Q') is a linear bijection $f : V \to V'$ such that $Q' \circ f = Q$.

The linearity of a metric isomorphism implies that $f(x) \cdot f(y) = x \cdot y$ for all $x, y \in V$.

Proposition 1.2.10. *Suppose (V, Q) is nondegenerate, then:*

1. *For all linear subspaces U of V, we have*

$$(U^\perp)^\perp = U, \dim(U) + \dim(U^\perp) = \dim(V), \mathrm{rad}(U) = \mathrm{rad}(U^\perp) = U \cap U^\perp.$$

2. *The quadratic module U is nondegenerate if and only if $U^\perp$ is. If this is the case, then $V = U \oplus U^\perp$.*

Proof. By Lemma 1.2.8, the map $q_V : V \to V^*$ is an isomorphism, which implies that $q_U : V \to U^*$ is surjective. The rank-nullity theorem and Lemma 1.2.8 give us:

$$\dim(U^\perp) + \dim(U^*) = \dim(V).$$

Note that $\dim(U) = \dim(U^*)$, so this proves the second equation. By definition, $(U^\perp)^\perp = \{x \in V : x \cdot y = 0, \forall y \in U^\perp\}$, so for arbitrary $u \in U$ we see that $u \in (U^\perp)^\perp$ so $U \subset (U^\perp)^\perp$. By the second equation we have $\dim(U^\perp) + \dim(U) = \dim(V)$ and $\dim((U^\perp)^\perp) + \dim(U^\perp) = \dim(V)$, so $\dim((U^\perp)^\perp) = \dim(U)$. Note that the inclusion is a linear and injective map from U to $(U^\perp)^\perp$, we have seen that we can conclude that the inclusion is now surjective. This proves the first equation. Now, it is easy to see that $\mathrm{rad}(U) = U \cap U^\perp$, so $\mathrm{rad}(U^\perp) = U^\perp \cap (U^\perp)^\perp$ and using the first equation we see $\mathrm{rad}(U) = \mathrm{rad}(U^\perp) = U \cap U^\perp$, which proves 1. We conclude from the last statement of 1, the first statement of 2 and $U \cap U^\perp = \{0\}$. We also know that $\dim(V) = \dim(U) + \dim(U^\perp)$. If we now combine the two bases of U and $U^\perp$ we have a basis for V. We can't express elements from one basis in terms of the other, because we have $U \cap U^\perp = \{0\}$. This proves 2. □

1.3 Isotropic vectors

Definition 1.3.1. An element x of a quadratic module (V, Q) is called *isotropic* if $Q(x) = 0$. A subspace U of V is called *isotropic* if all its elements are isotropic.

Proposition 1.3.2. *Let (V, Q) be a quadratic module and $U \subset V$ be a linear subspace. The following statements are equivalent.*

1. *U is isotropic.*
2. *$U \subset U^{\perp}$.*
3. *$Q|_U = 0$.*

Proof. Suppose U is isotropic and let $x \in U$. Now for all $y \in U$ we have that $x + y \in U$, because U is a subspace of V. We have:

$$x \cdot y = \frac{1}{2}\big(Q(x+y) - Q(x) - Q(y)\big) = \frac{1}{2}(0 - 0 - 0) = 0,$$

so $x \in U^{\perp}$ and we conclude $U \subset U^{\perp}$. Suppose $U \subset U^{\perp}$ and $x \in U$, this means $x \in U^{\perp}$ and we have $Q(x) = x \cdot x = 0$, so $Q|_U = 0$. If $Q|_u = 0$, then it is clear that U is isotropic. We conclude that $1 \implies 2 \implies 3 \implies 1$, so we are done. □

Definition 1.3.3. A quadratic module having a basis formed of two isotropic elements x, y such that $x \cdot y \neq 0$ is called a *hyperbolic plane*.

Let's take a look at the function $Q : \mathbb{R}^2 \to \mathbb{R}$ defined by $Q(x_1, x_2) = 4x_1x_2$. If $x = (x_1, x_2)$ and $y = (y_1, y_2)$, then the scalar product corresponding to Q is:

$$x \cdot y = \frac{1}{2}\big(4(x_1 + y_1)(x_2 + y_2) - 4x_1x_2 - 4y_1y_2\big) = 2(x_1y_2 + y_1x_2).$$

For the standard basis vectors e_1, e_2, we see that $Q(e_i) = 0$ and $e_1 \cdot e_2 = 2$. We conclude that this quadratic module $(\mathbb{R}^2, Q)$ is a hyperbolic plane. Now, let's multiply e_2 by $(e_1 \cdot e_2)^{-1} = \frac{1}{2}$. This gives $e_1 \cdot \frac{1}{2}e_2 = 1$ and the matrix of Q with respect to e_1 and $\frac{1}{2}e_2$ will become $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. The following lemma will generalize this phenomenon.

Lemma 1.3.4. *Suppose (V, Q) is a hyperbolic plane with basis formed by x, y. After multiplying y by $(x \cdot y)^{-1}$ we can suppose that $x \cdot (x \cdot y)^{-1}y = 1$. Then the matrix of Q with respect to x and $(x \cdot y)^{-1}y$ is the matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.*

Proof. We use bilinearity of the scalar product to deduce:

$$x \cdot (x \cdot y)^{-1} y = (x \cdot y)^{-1}(x \cdot y) = 1.$$

For the matrix A of Q we see that $a_{11} = x \cdot x = Q(x) = 0$. For a_{12} and a_{21}, we get $a_{12} = a_{21} = x \cdot (x \cdot y)^{-1} y = 1$ and finally

$$a_{22} = Q((x \cdot y)^{-1} y) = (x \cdot y)^{-2} Q(y) = 0. \qquad \square$$

Proposition 1.3.5. *Let $x \neq 0$ be an isotropic element of a nondegenerate quadratic module (V, Q). Then there exists a subspace $U \subset V$ which contains x and which is a hyperbolic plane.*

Proof. Since Q is nondegenerate, there exists z such that $x \cdot z \neq 0$. Now define $t := (x \cdot z)^{-1} z$ with $x \cdot t = 1$. Also define $y = 2t - (t \cdot t)x$. We calculate:

$$\begin{aligned} Q(y) &= y \cdot y \\ &= (2t - (t \cdot t)x) \cdot (2t - (t \cdot t)x) \\ &= 4(t \cdot t) - 4(t \cdot t)(x \cdot t) + (t \cdot t)^2 (x \cdot x) \\ &= 4(t \cdot t) - 4(t \cdot t) + (t \cdot t)^2 Q(x) = 0. \end{aligned}$$

So y is isotropic and $x \cdot y = (x \cdot 2t) - (x \cdot (t \cdot t)x) = 2$. We also see that x and y are linearly independent, because if they weren't, $x \cdot y = 0$ would follow from the fact x and y are isotropic. Now the subspace $U = kx \oplus ky$ has the desired property. $\square$

Corollary 1.3.6. *If (V, Q) is nondegenerate and contains a nonzero isotropic element, then $Q : V \to k$ is surjective.*

Proof. Suppose $a \in k$. By Proposition 1.3.5, there exists a subspace $U \subset V$ which is a hyperbolic plane. Now, by Lemma 1.3.4, we can assume that x, y form a basis of U with x, y isotropic and $x \cdot y = 1$. We conclude:

$$Q\big(x + \frac{a}{2}y\big) = \big(x + \frac{a}{2}y\big) \cdot \big(x + \frac{a}{2}y\big) = Q(x) + a(x \cdot y) + \frac{a^2}{4} Q(y) = a. \qquad \square$$

1.4 Orthogonal bases

In this section we will take a look at what it means for a quadratic module (V, Q) to have an orthogonal basis and we will define what it means for two bases to be contiguous.

Definition 1.4.1. A basis $(e_1, ..., e_n)$ of a quadratic module (V, Q) is called *orthogonal* if its elements are pairwise orthogonal, i.e. if $e_i \cdot e_j = 0$ for $i \neq j$ and $(\{e_1, ..., e_n\}) = V$.

Define $a_i = e_i \cdot e_i$. It is now easy to see that $d(Q) = a_1 \dots a_n$. If we assume that our quadratic module (V, Q) is nondegenerate, then $d(Q) \neq 0$ and $a_i \neq 0$ for all i.

Proposition 1.4.2. *Every quadratic module (V, Q) has an orthogonal basis.*

Proof. We will prove this by induction on the dimension of V. If $\dim(V) = 0$, then this statement is trivial, because a vector space with $\dim(V) = 0$ will have the empty set as basis. Assume the proposition holds for $\dim(V) = n$. Suppose $\dim(V) = n + 1$, if V is isotropic all bases of V are orthogonal. So suppose V is non isotropic and choose $e_1 \in V$ such that $e_1 \cdot e_1 \neq 0$. Define $W = ke_1$. By Proposition 1.2.10:

$$\dim(W) + \dim(W^\perp) = n + 1,$$

or $\dim(W^\perp) = n$. Using the induction hypothesis we find a basis $(e_2, ..., e_{n+1})$ for $W^\perp$. Note that e_1 does not belong to $W^\perp$. We conclude that $(e_1, e_2, ..., e_{n+1})$ forms an orthogonal basis over V. □

Definition 1.4.3. Two orthogonal bases B and B' of V are called *contiguous* if $B \cap B' \neq \varnothing$.

Lemma 1.4.4. *Assume that (V, Q) is a nondegenerate quadratic module with $\dim(V) \geqslant 3$. Let $B = \{e_1, ..., e_n\}$ and $B' = \{e'_1, ..., e'_n\}$ be two orthogonal bases of V. If $(e_1 \cdot e_1)(e'_i \cdot e'_i) = (e_1 \cdot e'_i)^2$ for $i = 1, 2$, then there exists $x \in k$ such that $e_x = e'_1 + xe'_2$ is nonisotropic and $ke_1 \oplus ke_x$ is a nondegenerate plane.*

Proof. By bilinearity of the scalar product and the fact that B' is an orthogonal basis, we have $e_x \cdot e_x = e'_1 \cdot e'_1 + x^2(e'_2 \cdot e'_2)$. We want that $Q(e_x) = e_x \cdot e_x \neq 0$. This means that x^2 should not be equal to $-(e'_1 \cdot e'_1)/(e'_2 \cdot e'_2)$. We also want $ke_1 \oplus ke_x$ to be nondegenerate. This is equivalent to saying that the discriminant is not equal to zero, or $(e'_1 \cdot e'_1)(e_x \cdot e_x) - (e_1 \cdot e_x)^2 \neq 0$. We have:

$$\begin{aligned}
(e_1 \cdot e_1)(e_x \cdot e_x) - (e_1 \cdot e_x)^2 &= (e_1 \cdot e_1)((e'_1 \cdot e'_1) + x^2(e'_2 \cdot e'_2)) - (e_1 \cdot e_x)^2 \\
&= (e_1 \cdot e_1)(e'_1 \cdot e'_1) + x^2(e_1 \cdot e_1)(e'_2 \cdot e'_2) - (e_1 \cdot e_x)^2 \\
&= (e_1 \cdot e'_1)^2 + x^2(e_1 \cdot e'_2)^2 - (e_1 \cdot e_x)^2 \\
&= -2x(e_1 \cdot e'_1)(e_2 \cdot e'_2) \neq 0
\end{aligned}$$

So, x should not be equal to zero. If k has at least 4 elements, we can find x such that $x \neq 0$ and $x^2 \neq -(e'_1 \cdot e'_1)/(e'_2 \cdot e'_2)$. Now, since $char(k) \neq 2$ we only have to look at $\mathbb{F}_3$. In $\mathbb{F}_3$, we have $1^1 = 1$ and $2^2 = 1$ so, $(e_1 \cdot e_1)(e'_i \cdot e'_i) = 1$ for $i = 1, 2$. We conclude that $x^2 \neq -1 = 2$ and $x \neq 0$ give us the solution $x = 1$. □

Proposition 1.4.5. *Let (V, Q) be a nondegenerate quadratic module with $dim(V) \geqslant 3$, and let $B = \{e_1, ..., e_n\}$ and $B' = \{e'_1, ..., e'_n\}$ be two orthogonal bases of V. There exists a finite sequence $B_0, ..., B_m$ of orthogonal bases of V such that $B_0 = B$, $B_m = B'$ and B_i is contiguous with B_{i+1} for $0 \leqslant i < m$.*

Proof. We consider three cases.

1. If $(e_1 \cdot e_1)(e'_1 \cdot e'_1) - (e_1 \cdot e'_1)^2 \neq 0$, then there doesn't exist $a \in k$ such that $e'_1 = ae_1$, because if it did we would have $(e_1 \cdot e_1)(ae_1 \cdot ae_1) - (e_1 \cdot ae_1)^2 = 0$ by bilinearity of the scalar product. By the definition of the matrix associated to the a quadratic module, we can also conclude that in this case, the quadratic module $P = ke_1 \oplus ke'_1$ is nondegenerate. We know that $e_1 \cdot e_1 \neq 0$ and $e'_1 \cdot e'_1 \neq 0$. Using the same argument as in the proof of Proposition 1.4.2, there exists ϵ_2, ϵ'_2 such that:

   $$P = ke_1 \oplus\!\!\!\!- \, k\epsilon_2 = ke'_1 \oplus\!\!\!\!- \, k\epsilon'_2.$$

   We have $V = P \oplus\!\!\!\!- \, P^{\perp}$ by Proposition 1.2.10. By Proposition 1.4.2, there exists an orthogonal basis $\{e''_3, ..., e''_n\}$ of $P^{\perp}$. The sequence:

   $$B, \{e_1, \epsilon_2, e''_3, ..., e''_n\}, \{e'_1, \epsilon'_2, e''_3, ..., e''_n\}, B'$$

   suffices.

2. If $(e_1 \cdot e_1)(e'_2 \cdot e'_2) - (e_1 \cdot e'_2)^2 \neq 0$, then the proof is similar to case 1, replacing e'_1 by e'_2.

3. If $(e_1 \cdot e_1)(e'_i \cdot e'_i) - (e_1 \cdot e'_i)^2 = 0$ for $i = 1, 2$, then by Lemma 1.4.4, there exists $x \in k$ such that $e_x = e'_1 + xe'_2$ is non isotropic and generates with e_1 a nondegenerate plane. Since e_x is non isotropic, there exists ϵ''_2 such that e_x and ϵ''_2 form an orthogonal basis of the plane $ke'_1 \oplus\!\!\!\!- \, ke'_2$. Then $B'' = \{e_x, \epsilon''_2, e'_3, ..., e'_n, \}$ is an orthogonal basis of V, since $\{e'_3, .., e'_n\}$ forms an orthogonal basis of the orthogonal complement of $ke'_1 \oplus\!\!\!\!- \, ke'_2$. Since $ke_1 \oplus ke_x$ is a nondegenerate plane, we have seen in the first case that there exists a chain from B to B'' and because B'' and B' are contiguous we conclude that B and B' are contiguous. This proves the proposition. □

1.5 Reformulation of statements

Suppose that (k^n, f) is a quadratic module and that the matrix $A = (a_{ij})$ is the matrix assosciated to f.

Definition 1.5.1. Two quadratic forms f and f' are called *equivalent* if the corresponding modules are isomorphic. We then write $f \sim f'$.

Remember that two quadratic modules (k^n, f) and (k^n, f') are isomorphic if there exists a linear bijective map $g : k^n \to k^n$ such that $f' \circ g = f$. Note that a linear bijective map can be represented by an invertible matrix, so this is equivalent to saying that there exists a invertible matrix C such that $f'(Cx) = f(x)$.

Example 1.5.2. *We define two quadratic forms:*

$$f(x_1, x_2) = x_1^2 - x_2^2 \text{ and } f'(x_1, x_2) = x_1 x_2.$$

We also define a linear map $g(x_1, x_2) = (x_1 - x_2, x_1 + x_2)$. *It is clear that* $f' \circ g = f$. *We conclude that* $x_1 x_2 \sim x_1^2 - x_2^2$.

We can now see that the following translation of Lemma 1.3.3 makes sense.

Definition 1.5.3. A quadratic form $(k^2, f(x_1, x_2))$ is *hyperbolic* if we have:

$$f \sim x_1 x_2 \sim x_1^2 - x_2^2.$$

Suppose $f(x_1, \ldots, x_n)$ and $g(x_1, \ldots, x_m)$ are two quadratic forms. It is easy to see that $f(x_1, \ldots, x_n) + g(x_{n+1}, \ldots, x_{n+m})$ is also a quadratic form. From now on we will write $f + g$ for this sum.

Definition 1.5.4. An element $a \in k$ is *represented* by a quadratic form $f(x_1, \ldots, x_n)$ if there exists $(x_1, \ldots, x_n) \neq 0 \in k^n$, with $f(x_1, \ldots, x_n) = a$.

We can now translate Proposition 1.3.5 and its corollary.

Proposition 1.5.5. *If f represents 0 and is nondegenerate, then one has $f \sim f_2 + g$, where f_2 is hyperbolic. Moreover, f represents all elements of k.*

Corollary 1.5.6. *Let $g = g(x_1, \ldots, x_{n-1})$ be a nondegenerate quadratic form and let $a \in k^\times$. The following properties are equivalent:*

1. *The form g represents a.*
2. *One has $g \sim h + ax_{n-1}^2$, where h is a form in $n-2$ variables.*

3. *The form* $f = g - ax_n^2$ *represents 0.*

Proof. If g represents a, then there exists $x \in k^{n-1}$ with $g(x) = x \cdot x = a$. If H denotes the orthogonal complement to x, we have $k^n = H \oplus kx$. So, we have $g \sim h + ax_{n-1}^2$, where h denotes the quadratic form attached to a basis of H. The converse is clear. If $f = g - ax_n^2$ has a nontrivial zero $(x_1, \ldots, x_{n-1}, x_n)$, then we have two cases. If $x_n = 0$, then g represents 0 and since g is nondegenerate, g also represents a. If $x_n \neq 0$, then $g(x_1/x_n, \ldots, x_{n-1}/x_n) = a$. The converse is clear, so we are done. □

Corollary 1.5.7. *Let* g *and* h *be two nondegenerate forms of rank* $\geqslant 1$*, and let* $f = g - h$*. The following properties are equivalent:*

1. *The form* f *represents* 0*.*
2. *There exists* $a \in k^\times$ *which is represented by* g *and* h*.*
3. *There exists* $a \in k^\times$ *such that* $g - az^2$ *and* $h - az^2$ *represent* 0*.*

Proof. If f represents 0, then we write the zero as (x, y) with $g(x) = h(y)$. If the element $a = g(x) = g(y) \neq 0$, then 2 is true. If $a = 0$, then g and h represent all elements of k, so we conclude that 1 implies 2. The converse is clear. The second and third statement are equivalent by the previous corollary. □

We finish this section by giving a translation of Proposition 1.4.2.

Proposition 1.5.8. *Let* f *be a quadratic form in* n *variables. There exist* $a_1, \ldots, a_n \in k$ *such that* $f \sim a_1x_1^2 + \ldots + a_nx^n$*.*

2 The p-adics numbers

2.1 Basic definitions

Recall that $\mathbb{Q}$ is incomplete, i.e. there exists a Cauchy sequence in $\mathbb{Q}$ that diverges. As the reader might know, the real numbers $\mathbb{R}$ are defined as the completion of $\mathbb{Q}$, with respect to the absolute value norm. The p-adics can be defined as a completion of the rational numbers with respect to another norm, that is dependent on a prime number. Before we are able to define the p-adics, we first define the p-adic absolute value. It is easy to see that the following definition is well-defined, because every integer has a unique prime factorization.

Definition 2.1.1. Fix a prime $p \in \mathbb{N}$. The *p-adic valuation* on $\mathbb{Z}$ is the function:

$$v_p : \mathbb{Z} - \{0\} \to \mathbb{R}$$

defined as follows: for each integer $n \in \mathbb{Z}$, $n \neq 0$, let $v_p(n)$ be the unique postive integer satisfying

$$n = p^{v_p(n)} n' \text{ with } p \nmid n'.$$

We extend v_p to $\mathbb{Q}$ as follows: if $x = \frac{a}{b} \in \mathbb{Q}^\times$, then $v_p(x) = v_p(a) - v_p(b)$.

It will be convenient to set $v_p(0) = +\infty$. The reasoning behind this is that any prime number devides zero as many times as we like.

Lemma 2.1.2. *For all x and y in $\mathbb{Q}$, we have:*

1. $v_p(xy) = v_p(x) + v_p(y)$.
2. $v_p(x + y) \geqslant \min\{v_p(x), v_p(y)\}$.

Proof. If $x = 0$ then:

$$v_p(xy) = v_p(0) = \infty = \infty + v_p(y) = v_p(x) + v_p(y),$$

and

$$v_p(x + y) = v_p(y) = \min\{v_p(x), v_p(y)\}$$

for all $y \in \mathbb{Q}$. If $y = 0$, then the proof is similar. We now assume that $x \neq 0$ and $y \neq 0$. We can write:

$$x = p^i \frac{a}{b} \text{ and } y = p^j \frac{c}{d},$$

such that $i, j \in \mathbb{Z}$ and $p \nmid a, b, c, d$. The first property is immediate and the second follows from the fact that common powers of p, can be factored out from a sum. □

Definition 2.1.3. For any nonzero $x \in \mathbb{Q}$, we define the *p-adic absolute value* of x by:

$$|x|_p = p^{-v_p(x)}.$$

We extend this to all of $\mathbb{Q}$ by defining $|0|_p = 0$. We will also write $|\ |_\infty$ for the usual absolute value on $\mathbb{Q}$.

Note that the extension to $\mathbb{Q}$ makes sense, because we defined $v_p(0) = \infty$.

Proposition 2.1.4. *The function $|\ |_p$ is an absolute value on $\mathbb{Q}$ and:*

$$|x + y|_p \leqslant \max\{|x|_p, |y|_p\}.$$

Proof. For $x \in \mathbb{Q}$ we have that $|x|_p \geqslant 0$ by the definition of $|\ |_p$. It also follows from the definition that $|x|_p = 0$ if and only if $v_p(x) = \infty$ if and only if $x = 0$. By Lemma 2.1.2 the following holds:

$$|xy|_p = p^{-v_p(xy)} = p^{-v_p(x)}p^{-v_p(y)} = |x|_p|y|_p$$

and

$$|x + y|_p = p^{-v_p(x+y)} \leqslant p^{-\min\{v_p(x),v_p(y)\}} \leqslant p^{-v_p(x)} + p^{-v_p(y)} = |x|_p + |y|_p.$$

This proves the first claim. Assume without loss of generality that $|x|_p \geqslant |y|_p$, so $v_p(x) \leqslant v_p(y)$. We conclude that:

$$|x + y|_p = p^{-v_p(x+y)} \leqslant p^{-\min\{v_p(x),v_p(y)\}} = p^{-v_p(x)}$$

Lemma 2.1.5. *If $x, y \in \mathbb{Q}$ and $|x|_p \neq |y|_p$, then $|x + y|_p = \max\{|x|_p, |y|_p\}$.*

Proof. Without loss of generality, assume $|x|_p > |y|_p$. By Proposition 2.1.4:

$$|x + y|_p \leqslant |x|_p = \max\{|x|_p, |y|_p\}.$$

Using the proposition again and the fact that $x = (x + y) - y$, we have:

$$|x|_p \leqslant \max\{|x + y|_p, |y|_p\}.$$

Because $|x|_p > |y|_p$ it must hold that: $\max\{|x + y|_p, |y|_p\} = |x + y|_p$. We showed that $|x + y|_p \leqslant |x|_p \leqslant |x + y|_p$, so we conclude that $|x + y|_p = |x|_p$. This proves the lemma. □

Definition 2.1.6. We define the *trivial absolute value* on $\mathbb{Q}$ as $|x| = 1$ if $x \neq 0$ and $|x| = 0$ if $x = 0$.

This clearly is an absolute value on $\mathbb{Q}$. We now defined lots of different absolute values. The following definition will let us compare them.

Definition 2.1.7. We call two absolute values $|\ |_1$ and $|\ |_2$ *equivalent* if for any Cauchy sequence (x_n) in $\mathbb{Q}$ we have $x_n \to a$ with respect to $|\ |_1$ if and only if $x_n \to a$ with respect to $|\ |_2$.

The following two theorems are proven in [2, p.56] and [2, p.63].

Theorem 2.1.8. *Every non-trivial absolute value on $\mathbb{Q}$ is equivalent to one of the absolute values $|\ |_p$, where p is a prime number or $p = \infty$.*

Theorem 2.1.9. *The field $\mathbb{Q}$ of rational numbers is not complete with respect to any of its non-trivial absolute values.*

These theorems tell us that it actually makes sense to find a completion of $\mathbb{Q}$ with respect to the p-adic absolute value.

Definition 2.1.10. We denote by $\mathcal{C}_p(\mathbb{Q})$, or $\mathcal{C}$ if the context is clear, the set of all Cauchy sequences of elements of $\mathbb{Q}$:

$$\mathcal{C}_p(\mathbb{Q}) = \{(x_n) : (x_n) \text{ is a Cauchy sequence with respect to } |\ |_p\}.$$

Proposition 2.1.11. *Defining:*

$$(x_n) + (y_n) = (x_n + y_n) \text{ and } (x_n)(y_n) = (x_n y_n),$$

makes $\mathcal{C}_p(\mathbb{Q})$ a commutative ring with unity.

Proof. We first check that the sequences on the right-hand side are Cauchy. We know that for every Cauchy sequence (x_n), there exists M such that $|x_m|_p \leqslant M$. For all $\epsilon > 0$ there exists $N_1 \in \mathbb{N}$ such that if $n, m \geqslant N_1$, then $|x_m - x_n| < \frac{\epsilon}{2M}$. Similarly, there exists $N_2 \in \mathbb{N}$ such that if $n, m \geqslant N_2$, then $|y_m - y_n| < \frac{\epsilon}{2M}$. Now, let $N = \max\{N_1, N_2\}$. For $n, m \geqslant N$, we have:

$$\begin{aligned} |x_m y_m - x_n y_n|_p &= |x_m(y_m - y_n) + y_n(x_m - x_n)|_p \\ &\leqslant |x_n|_p |y_m - y_n|_p + |y_n|_p |x_m - x_n|_p \\ &< M(\frac{\epsilon}{2M} + \frac{\epsilon}{2M}) = \epsilon. \end{aligned}$$

This proves that $(x_n y_n)$ is Cauchy. The argument for $(x_n + y_n)$ is similar. We conclude that the operations are well-defined. We know that $\mathbb{Q}$ is a field, so it is easy to see that $\mathcal{C}_p(\mathbb{Q})$ is a commutative ring with unity $(x_n) = (1)$, since it is a subring of $\prod_{n\in\mathbb{N}} \mathbb{Q}$. □

Definition 2.1.12. We define $\mathcal{N} \subset \mathcal{C}$ to be the set of Cauchy sequences that tend to zero with respect to $|\ |_p$:

$$\mathcal{N} = \{(x_n) : \lim_{n\to\infty} |x_n|_p = 0\}.$$

We will now identify sequences that differ by elements of $\mathcal{N}$. In other words, we identify Cauchy sequences that have the same limit. Note that it is easy to see that $\mathcal{N}$ is an ideal. We will define the p-adic field by taking the quotient of $\mathcal{C}$ by $\mathcal{N}$.

Lemma 2.1.13. *The quotient ring $\mathcal{C}/\mathcal{N}$ is a field.*

Proof. We need to show that every sequence that doesn't converge to zero has an inverse. If (x_n) is a Cauchy sequence that doesn't converge to zero, then it is not possible that for all $N \in \mathbb{N}$ there exists n such that $n \geqslant N$ and $x_n = 0$. So there exists $N \in \mathbb{N}$ such that, if $n \geqslant N$, then $x_n \neq 0$. Define the sequence (y_n) as $y_n = x_n$ if $n < N$ an $y_n = 1/x_n$ if $n \geqslant N$. Because (x_n) is Cauchy, the sequence (y_n) is also Cauchy. It is clear that (y_n) is an inverse of (x_n). □

Definition 2.1.14. The *field of the p-adic numbers* is defined as:

$$\mathbb{Q}_p = \mathcal{C}/\mathcal{N}.$$

We now show that any Cauchy sequence with respect to the p-adic norm, that doesn't converge to zero, eventually has constant p-adic valuation. This is a crucial result to extend the p-adic norm to $\mathbb{Q}_p$,

Lemma 2.1.15. *Let $(x_n) \in \mathcal{C}$, $(x_n) \notin \mathcal{N}$. There exists an integer N such that $|x_n|_p = |x_m|_p$ when $m, n \geqslant N$.*

Proof. Since (x_n) is a Cauchy sequence not converging to zero, we can find c and N_1, such that:

$$n \geqslant N_1 \implies |x_n|_p \geqslant c > 0.$$

Using the definition of Cauchy sequences we can also find N_2 such that:

$$n, m \geqslant N_2 \implies |x_m - x_n|_p < c.$$

Set $N = \max\{N_1, N_2\}$. For $n, m \geqslant N$, we have:

$$|x_m - x_n|_p < c \leqslant |x_n|_p \leqslant \max\{|x_m|_p, |x_n|_p\}.$$

By Lemma 2.1.5 it must hold that $|x_n|_p = |x_m|_p$. □

Suppose that the sequences (x_n) and (y_n) don't converge to zero and that they are the same when viewed as element in $\mathbb{Q}_p$. Using the previous lemma we see that, the p-adic norm of both sequences are eventually stationary and equal. This gives rise to the following definition.

Definition 2.1.16. If γ is an element of $\mathbb{Q}_p$, and (x_n) is any Cauchy sequence representing γ, we define:

$$|\gamma|_p = \lim_{n\to\infty} |x_n|_p.$$

Note that the properties we showed in Proposition 2.1.4 extend to $\mathbb{Q}_p$, because they are true for every term in the Cauchy sequence. As example, for $x = (x_n) \in \mathbb{Q}_p$, we have that $|x_n|_p \geqslant 0$ for all n, so $|x|_p = \lim_{n\to\infty} |x_n|_p \geqslant 0$. The following theorems show we have come full circle. They are proven in [2, p.68 - 69].

Theorem 2.1.17. *The image of $\mathbb{Q}$ under the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ is a dense subset of $\mathbb{Q}_p$.*

Theorem 2.1.18. *The p-adic field $\mathbb{Q}_p$ is complete with respect to $|\ |_p$.*

2.2 Exploring $\mathbb{Q}_p$

We have seen that the properties in Proposition 2.1.4 hold in $\mathbb{Q}_p$. If $x, y \in \mathbb{Q}_p$ and $|x|_p, |y|_p \leqslant 1$, then $|xy|_p = |x|_p|y|_p \leqslant 1$ and:

$$|x + y|_p \leqslant \max\{|x|_p, |y|_p\} \leqslant 1.$$

So, the following defintion makes sense.

Definition 2.2.1. The *ring of the p-adic integers* is the ring:

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

Proposition 2.2.2. *The following properties hold.*

1. *The inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ has dense image. Specifically, given $x \in \mathbb{Z}_p$ and $n \geqslant 1$, there exists an $\alpha_n \in \mathbb{Z}$, $0 \leqslant \alpha_n \leqslant p^n - 1$, such that $|x - \alpha_n|_p \leqslant p^{-n}$. The integer α_n with these properties is unique.*

2. *For any $x \in \mathbb{Z}_p$, there exists a Cauchy sequence (α_n) converging to x, of the following type:*

   - *$\alpha_n \in \mathbb{Z}$ satisfies $0 \leqslant \alpha_n \leqslant p^n - 1$*
   - *for every $n \geqslant 2$ we have $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$*

   The sequence (α_n) with these properties is unique.

Proof. Choose $x \in \mathbb{Z}_p$ and $n \geqslant 1$. Theorem 2.1.17 gives us that we can choose $a/b \in \mathbb{Q}$, reduced to lowest terms, as close to x as we like:

$$\left|x - \frac{a}{b}\right|_p \leqslant p^{-n} \leqslant 1.$$

Using Proposition 2.1.4 and $|x|_p \leqslant 1$, we also have:

$$\left|\frac{a}{b}\right|_p = \left|x - \left(x - \frac{a}{b}\right)\right|_p \leqslant \max\left\{|x|_p, \left|x - \frac{a}{b}\right|_p\right\} \leqslant 1.$$

We conclude that p does not divide b. So there exists $a', b' \in \mathbb{Z}$ such that $a'p^n + b'b = 1$ or $b'b \equiv 1 \pmod{p^n}$. This implies:

$$\left|\frac{a}{b} - ab'\right|_p = \left|\frac{(1 - b'b)a}{b}\right|_p = \left|\frac{a}{b}\right|_p |(1 - b'b)|_p \leqslant p^{-n}.$$

Note that b' is unique mod p^n, since congruence is an equivalence relation and p does not devide b. We define α_n as the unique integer such that:

$$0 \leqslant \alpha_n \leqslant p^n - 1 \text{ and } \alpha_n \equiv ab' \pmod{p^n}.$$

Note that:

$$\begin{aligned} |x - \alpha_n|_p &= \left|x - \frac{a}{b} + \frac{a}{b} - ab' + ab' - \alpha_n\right|_p \\ &\leqslant \max\left\{\left|x - \frac{a}{b}\right|_p, \left|\frac{a}{b} - ab'\right|_p, |ab' - \alpha_n|_p\right\} \leqslant p^{-n}. \end{aligned}$$

This proves 1. To prove 2, we just make a Cauchy sequence using α_n from 1. Note that for $n \geqslant 2$ we have:

$$|\alpha_n - \alpha_{n-1}|_p \leqslant \max\{|x - \alpha_n|_p, |x - \alpha_{n-1}|_p\} \leqslant p^{-(n-1)},$$

This implies that $\alpha_n \equiv \alpha_{n-1} \pmod{p^{n-1}}$. For uniqueness, notice that at each step in 1 our choices were unique mod p^n. □

We will now show a way to represent the elements of $\mathbb{Q}_p$ as power series in p. Let's begin with a p-adic integer $x \in \mathbb{Z}_p$. We have seen in the previous proposition that we can find a Cauchy sequence (α_n), converging to x, with the property that for $n \geqslant 1$:

$$\alpha_{n+1} \equiv \alpha_n \pmod{p^n} \text{ and } 0 \leqslant \alpha_n \leqslant p^n - 1.$$

The (α_n) are integers so we can write them in base p. What we get is:

$$\alpha_n = \sum_{i=0}^{n-1} b_i p^i \quad \text{and} \quad \alpha_{n+1} = \sum_{i=0}^{n} b_i p^i,$$

where $0 \leqslant b_i \leqslant p - 1$.

Lemma 2.2.3. *Given any $x \in \mathbb{Z}_p$, the series:*

$$\sum_{i=0}^{\infty} b_i p^i,$$

obtained as above, converges to x.

Proof. By definition a series converges if an only if it's sequence of partial sums converges. The partial sums of our series are α_n, which we constructed to converge to x. □

We conclude that:

Corollary 2.2.4. *Every $x \in \mathbb{Z}_p$ can be written as:*

$$x = \sum_{i=0}^{\infty} b_i p^i,$$

where $0 \leqslant b_i \leqslant p-1$. This representation is unique.

Proof. We only need to check uniqueness. Notice that all α_n are unique, and this implies that all b_i are too, because they give the base p representation of α_n. □

We will now show that any sum $\sum_{i=0}^{\infty} b_i p^i$ with $0 \leqslant b_i \leqslant p-1$ also converges to an element in $\mathbb{Z}_p$.

Lemma 2.2.5. *A sequence (α_n) in $\mathbb{Q}_p$ is a Cauchy sequence if and only if:*

$$\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0.$$

Proof. If (α_n) is Cauchy, then we choose $m = n+1$ to see that the limit $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$. Conversely, we see that if $m > n$:

$$\begin{aligned} |\alpha_m - \alpha_n|_p &= |\alpha_m - \alpha_{m-1} + \alpha_{m-1} - \alpha_{m-2} + \ldots + \alpha_{n+1} - \alpha_n|_p \\ &\leqslant \max\{|\alpha_m - \alpha_{m-1}|_p, \ldots, |\alpha_{n+1} - \alpha_n|_p\}. \end{aligned}$$

It is clear that (α_n) is Cauchy if $\lim_{n\to\infty} |a_{n+1} - a_n|_p = 0$.. □

This lemma gives us an easier way to check when an infinite series in $\mathbb{Q}_p$ is convergent. Remember when we work in $\mathbb{R}$, if a series $\sum_n a_n$ converges, then $\lim_{n\to\infty} a_n = 0$. In $\mathbb{Q}_p$, the converse is also true.

Corollary 2.2.6. *An infinite series $\sum_n a_n$ with $a_n \in \mathbb{Q}_p$ is convergent if and only if:*

$$\lim_{n\to\infty} a_n = 0.$$

Proof. By definition a series converges if an only if it's sequence of partial sums converges. If we can show that the sequence of partial sums is a Cauchy sequence, then it converges, since $\mathbb{Q}_p$ is complete. Denote (s_n) for the sequence of partial sums and notice that $s_n - s_{n-1} = a_n$. By the previous lemma, (s_n) is a Cauchy sequence if and only if $\lim_{n\to\infty} |a_n|_p = 0$. □

Corollary 2.2.7. *A sum $\sum_{i=0}^{\infty} b_i p^i$ with $0 \leqslant b_i \leqslant p-1$ converges to an element in $\mathbb{Z}_p$.*

Proof. By Corollary 2.2.6 it suffices to show that:

$$\lim_{i\to\infty} b_i p^i = 0,$$

to prove convergence in $\mathbb{Q}_p$. We need to show that for all $\epsilon > 0$ there exists $N \in \mathbb{N}$ such that if $i \geqslant N$, then $|b_i p^i|_p < \epsilon$. We have that $|b_i p^i|_p = p^{-i}$ or $|b_i p^i|_p = 0$ if $b_i = 0$, so N obviously exists. Note that $v_p(\sum_{i=0}^{\infty} b_i p^i) \geqslant 0$, so the sum converges to an element in $\mathbb{Z}_p$. □

If $x \in \mathbb{Z}_p$, then $|x|_p \leqslant 1$ and if $x^{-1} \in \mathbb{Z}_p$, then $|x|_p^{-1} = |x^{-1}|_p \leqslant 1$. We conclude that $|x|_p = |x^{-1}|_p = 1$. If we write x as $\sum_i b_i p^i$, then this is equivalent to saying that $b_0 \neq 0$.

Definition 2.2.8. The *p-adic units* are the invertible elements of $\mathbb{Z}_p$. We will denote the set of all such element by $\mathbb{Z}_p^\times$:

$$\mathbb{Z}_p^\times = \{x \in \mathbb{Q}_p : |x|_p = 1\}.$$

We will now show that every element in $\mathbb{Q}_p$ can be written as a power series in p.

Lemma 2.2.9. *For every $x \in \mathbb{Q}_p^\times$ there exists an $n \in \mathbb{Z}$ such that $p^n x \in \mathbb{Z}_p^\times$.*

Proof. If $v_p(x) = 0$ then $x \in \mathbb{Z}_p^\times$. Otherwise:

$$v_p(p^{-v_p(x)}x) = v_p(p^{-v_p(x)}) + v_p(x) = 0.$$

So, $|p^{-v_p(x)}x|_p = 1$ and $p^{-v_p(x)}x \in \mathbb{Z}_p^\times$. □

Corollary 2.2.10. *Every $x \neq 0 \in \mathbb{Q}_p$ can be written in the form:*

$$x = \sum_{i\geqslant -m}^{\infty} b_i p^i,$$

where $0 \leqslant b_i \leqslant p-1$ and $-m = v_p(x)$ and $b_{-m} \neq 0$. This representation is unique.

Proof. By Lemma 2.2.9, we can write $y = p^m x \in \mathbb{Z}_p^\times$. By Corollary 2.2.4 we can write y as:

$$y = \sum_{i=0}^{\infty} b_i p_i$$

then the corollary follows by multiplying by p^{-m}. The representation is unique because the representation of y is. □

By Corollary 2.2.7 we also see that conversely every sum $\sum_{i \geqslant -m}^{\infty} b_i p^i$ with $0 \leqslant b_i \leqslant p-1$ and $b_{-m} \neq 0$ defines an element in $\mathbb{Q}_p$. Elements in $\mathbb{Q}_p$ are sometimes written as: $\ldots b_n \ldots b_2 b_1 b_0 . b_{-1} \ldots b_{-m}$.

2.3 Analysis in $\mathbb{Q}_p$

We will now do some analysis in $\mathbb{Q}_p$. Our goal is to prove results about power series. After, we will use the developed theory to define the exponential and logarithmic in $\mathbb{Q}_p$ and prove their known properties.

Proposition 2.3.1. *Let $f(x) = \sum_n a_n x^n$, and define:*

$$\rho = \frac{1}{\limsup_{n\to\infty} \sqrt[n]{|a_n|_p}},$$

where dividing by zero gives $\rho = \infty$ and dividing by infinity gives $\rho = 0$.

1. *If $\rho = 0$, then $f(x)$ converges only when $x = 0$.*
2. *If $\rho = \infty$, then $f(x)$ converges for every $x \in \mathbb{Q}_p$.*
3. *If $0 < \rho < \infty$ and $\lim_{n\to\infty} |a_n|_p \rho^n = 0$, then $f(x)$ converges if and only if $|x|_p \leqslant \rho$.*
4. *If $0 < \rho < \infty$ and $|a_n|_p \rho^n$ does not tend to zero as n goes to infinity, then $f(x)$ converges if and only if $|x|_p < \rho$.*

Proof. By Corollary 2.2.6, we know that the region of convergence is:

$$\{x \in \mathbb{Q}_p : \lim_{n\to\infty} |a_n x^n|_p = 0\}.$$

It is easy to see that $f(0)$ converges. For all $\epsilon > 0$ there exists N such that $n \geqslant N$ implies that:

$$\Big| \sup_{m \geqslant n} \sqrt[m]{|a_m|_p} - \frac{1}{\rho} \Big| < \epsilon.$$

This in turn means that:

$$\frac{1}{\rho} - \epsilon < \sup_{m \geqslant n} \sqrt[m]{|a_m|_p} < \epsilon + \frac{1}{\rho}.$$

We see that $\sup_{m \geqslant n} \sqrt[m]{|a_m|_p} < \epsilon + (1/\rho)$ for all but finitely many n and thus $|a_n|_p < (\epsilon + 1/\rho)^n$ for all but finitely many n. If $|x|_p < \rho$, then $|x|_p/\rho < 1$ and:

$$|a_n x^n|_p < \left(\epsilon |x|_p + \frac{|x|_p}{\rho}\right)^n \to 0,$$

if we choose ϵ small enough. The case $|x| = \rho$ is clear, because of Corollary 2.2.6. We also see that $\frac{1}{\rho} - \epsilon < \sup_{m \geqslant n} \sqrt[m]{|a_m|_p}$ for infinitely many n and thus $(\frac{1}{\rho} - \epsilon)^n < |a_n|_p$ for infinitely many n. This means that:

$$(1 - \epsilon\rho)^n = (\frac{1}{\rho} - \epsilon)^n \rho^n < |a_n x^n|_p,$$

can't convert to 0 if we choose ϵ small enough. □

Corollary 2.3.2. *The series:*

$$f(x) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{x^n}{n},$$

converges if and only if $|x|_p < 1$.

Proof. We check that $\lim_{n \to \infty} p^{-v_p(n)/n} = 1$. If $v_p(n) = i$, then $p^i \leqslant n$ and $i \leqslant \log_p(n)$. Now, $0 \leqslant v_p(n)/n \leqslant \log_p(n)/n$. By L'Hopital's rule we have $\lim_{n \to \infty} \log_p(n)/n = 0$, so $\lim_{n \to \infty} v_p(n)/n = 0$ and we conclude:

$$\lim_{n \to \infty} p^{-v_p(n)/n} = 1.$$

If a limit exists, then the limit is equal to the limit superior, we conclude that $\rho = 1$. The limit $\lim_{n \to \infty} |1/n|_p$ does not tend to zero. By Proposition 2.3.1, we conclude that the series converges for $|x|_p < 1$. □

Corollary 2.3.3. *The series:*

$$g(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!},$$

converges if and only if $|x|_p < p^{-1/(p-1)}$.

Proof. Before we try to find ρ, we will calculate $v_p(n!)$. Notice that $\lfloor n/p^i \rfloor$ is the amount of numbers in $\{1, 2, \ldots, n\}$ with a factor p^i. This means that:

$$\begin{aligned} v_p(n!) &= v_p(1) + v_p(2) + \ldots + v_p(n) \\ &= \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor < \sum_{i=0}^{\infty} \frac{n}{p^i} = \frac{n}{p-1}. \end{aligned}$$

Now, $|a_n|_p = |1/n!|_p = p^{v_p(n!)} < p^{n/(p-1)}$. We get $\rho \geqslant p^{-1/(p-1)}$, so the series converges for $|x|_p < p^{-1/(p-1)}$. If $|x|_p = p^{-1/(p-1)}$ then $|x^n/n!|_p$ does not tend to zero. To see this set $n = p^m$ for some m, then:

$$v_p(n) = 1 + p + \ldots + p^{m-1} = \frac{p^m - 1}{p-1},$$

and

$$v_p\left(\frac{x^n}{n!}\right) = v_p\left(\frac{x^{p^m}}{p^m!}\right) = \frac{p^m}{p-1} - \frac{p^m - 1}{p-1} = \frac{1}{p-1}.$$

The corollary follows from Corollary 2.2.6 and Proposition 2.3.1. □

We are now able to define the exponential and logarithmic functions in $\mathbb{Q}_p$, using the usual power series for these functions. We will later see that they are each others inverses and that their standard properties, i.e. $e^{a+b} = e^a e^b$ and $\log(ab) = \log(a) + \log(b)$ hold. Moreover, we will use these properties to define a group homomorphism.

Definition 2.3.4. We define the *p-adic logarithm* as the function:

$$\begin{aligned} \log : (1 + p\mathbb{Z}_p) &\to \mathbb{Q}_p \\ \log(x) &= \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(x-1)^n}{n}. \end{aligned}$$

Assume $p > 2$. If $x \in p\mathbb{Z}_p$, then $|x|_p \leqslant p^{-1} < p^{-1/(p-1)}$. If $|x|_p < p^{-1/(p-1)}$, then $v_p(x) > 1/(p-1)$ and $x \in p\mathbb{Z}_p$. This proves that $x \in p\mathbb{Z}_p$ if and only if $|x|_p < p^{-1/(p-1)}$ when $p > 2$. If $p = 2$, then a similar argument shows that $x \in 4\mathbb{Z}_p$ if and only if $|x|_p < p^{-1/(p-1)}$. We will use this in the following definition.

Definition 2.3.5. Define $D_p = \{x \in \mathbb{Z}_p : |x|_p < p^{-1/(p-1)}\}$, if $p = 2$, then $D_p = 4\mathbb{Z}_p$, else $D_p = p\mathbb{Z}_p$. We define the *p-adic exponential* as a function from $D_p \to \mathbb{Q}_p$ defined by:

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

We will now start with some theory on differentiating power series.

Definition 2.3.6. Let $U \subset \mathbb{Q}_p$ be an open set, and let $f : U \to \mathbb{Q}_p$ be a function. We say f is *differentiable* at $x \in U$ if the limit

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h},$$

exists. We say f is differentiable if it is differentiable for all $x \in U$.

Proposition 2.3.7. *Let $f(x) = \sum_{n=0}^{\infty} a_n x^n$ be a power series with non-zero radius of convergence $\rho > 0$. Let $x \in \mathbb{Q}_p$, such that $f(x)$ converges, then so does $f'(x)$ and we have $f'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1}$.*

Proof. If $x = 0$, then $f(x+h) = f(h)$ converges when $|h|_p < \rho$. When $x \neq 0$ and $|h|_p < |x|_p$, then $|x+h|_p = |x|_p$ by Lemma 2.1.5, so $f(x+h)$ converges. So, when $h \to 0$, there are element such that $f(x+h)$ converges. Using the Binomial Theorem we get that:

$$f(x+h) = \sum_{n=0}^{\infty} a_n (x+h)^n = \sum_{n=0}^{\infty} a_n \sum_{k=0}^{n} \binom{n}{k} x^{n-m} h^m.$$

If we substract $f(x)$, divide by h and take the limit to zero, then we get:

$$f'(x) = \lim_{h \to 0} \sum_{n=1}^{\infty} \sum_{k=1}^{n} a_n \binom{n}{k} x^{n-k} h^{k=1} = \sum_{n=1}^{\infty} n a_n x^{n-1}.$$

If $x = 0$, then it is clear that $f'(x)$ converges. Now suppose that $x \neq 0 \in \mathbb{Q}_p$ and $f(x)$ converges. By Corollary 2.2.6 this means that $|a_n x^n|_p \to 0$. Also:

$$|n a_n x^{n-1}|_p \leqslant |a_n x^{n-1}|_p = \frac{1}{|x|_p} |a_n x^n|_p \to 0,$$

so $f'(x)$ converges. □

We can now prove a Corollary which is a variant to a theorem that states that two power series are equivalent if and only if their coefficients are.

Corollary 2.3.8. *Suppose $f(x)$ and $g(x)$ are power series, and suppose that both series converge for $|x|_p < \rho$. If $f'(x) = g'(x)$ for all $|x|_p < \rho$, then there exists a constant $c \in \mathbb{Q}_p$ such that $f(x) = g(x) + c$ as power series.*

Proof. Suppose $f(x) = \sum_{n=0}^{\infty} a_n x^n$ and $g(x) = \sum_{n=0}^{\infty} b_n x^n$. If $f'(x) = g'(x)$ when $|x|_p \leqslant \rho$, then $f'(0) = g'(0)$ and by the previous proposition $a_1 = b_1$. We can repeat this process by continuing to differentiate to conclude that $a_n = b_n$ for $n \geqslant 1$ and f and g only vary by a constant term. □

We are now finally able to prove the standard properties of the logarithm and exponential.

Proposition 2.3.9. *If $a, b \in 1 + p\mathbb{Z}_p$, we have $ab \in 1 + p\mathbb{Z}_p$ and:*

$$\log(ab) = \log(a) + \log(b).$$

Proof. The first claim is clear. To prove the second, we will write $a = 1 + x$ and $b = 1 + y$. For $x \in p\mathbb{Z}_p$, we define:

$$f(x) = \log(1 + x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n,$$

so f converges if $x \in p\mathbb{Z}_p$. By proposition 2.3.7 we have:

$$f'(x) = \sum_{n=0}^{\infty} (-1)^n x^n = 1/(1 + x).$$

Now, for $y \in p\mathbb{Z}_p$, we define:

$$g(x) = \log((1 + x)(1 + y)) = f(y + (1 + y)x).$$

It is clear that $g(x)$ converges for $x \in p\mathbb{Z}_p$. The Binomial Theorem gives us:

$$\begin{aligned} f(y + (1 + y)x) &= \sum_{n=1}^{\infty} (-1)^{n+1} \frac{((1 + y)x + y)^n}{n} \\ &= \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} \sum_{k=0}^{n} \binom{n}{k} ((1 + y)x)^{n-k} y^k \\ &= \sum_{m=1}^{\infty} \left(\sum_{k=0}^{\infty} \frac{(-1)^{k+m+1}}{k + m} \binom{k + m}{k} y^k \right) ((1 + y)x)^m. \end{aligned}$$

Since $y \in p\mathbb{Z}_p$ we have that $f(y)$ converges which implies:

$$\left| \frac{(-1)^{k+m+1}}{k + m} \binom{k + m}{k} y^k \right|_p \leqslant \left| \frac{(-1)^{k+m+1}}{k + m} y^k \right|_p \to 0 \text{ as } k \to \infty$$

We conclude from this that both $f(x)$ and $g(x)$ are defined as power series that converge when $x \in p\mathbb{Z}_p$. By the chain rule we have $f'(x) = g'(x)$, so by Corollary 2.3.8 we conclude that $g(x) = f(x) + c$ and $c = g(0) = f(y)$. So we have shown that $g(x) = f(x) + f(y)$, but this is what we wanted to show. □

Proposition 2.3.10. *If $a, b \in D_p$, we have $a + b \in D_p$ and:*

$$e^{a+b} = e^a e^b.$$

Proof. The first claim follows from the fact that $D_p = p\mathbb{Z}_p$ if $p \neq 2$ and $D_p = 4\mathbb{Z}_p$. The second claim is proven by a standard argument using the Binomial Theorem. □

The following theorem is proven in [2, p.124 - p.127], we will use it to prove that the exponential and logarithm are inverses.

Lemma 2.3.11. *Let $f(x) = \sum_n a_n x^n$ and $g(x) = \sum_n b_n x^n$ be two power series with $g(0) = 0$, and let $h(x) = f(g(x))$ be their composition. Suppose that:*

1. *$g(x)$ converges,*
2. *$f(g(x))$ converges,*
3. *for every n, $|b_n x^n|_p \leqslant |g(x)|_p$.*

Then $h(x)$ also converges and $f(g(x)) = h(x)$.

Lemma 2.3.12. *If $n \in \mathbb{Z}$ with $n = a_0 + a_1 p + \ldots + a_k p^k$ where $0 \leqslant a_i \leqslant p-1$ and $s = a_1 + \ldots + a_k$, then:*

$$v_p(n!) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{p^i} \right\rfloor = \frac{n-s}{p-1}.$$

Proof. We have already proven the first equivalence in Corollary 2.3.3. We will now prove the second:

$$\begin{aligned}
\sum_{i=1}^{k} \left\lfloor \frac{n}{p^i} \right\rfloor &= \sum_{i=1}^{k} (a_i + a_{i+1} p + \ldots + a_k p^{k-i}) \\
&= \sum_{i=1}^{k} \sum_{j=i}^{k} a_j p^{j-i} \\
&= \sum_{j=0}^{k} a_j \frac{p^j - 1}{p-1} \\
&= \frac{1}{p-1} \sum_{j=0}^{k} a_j (p^j - 1) = \frac{n-s}{p-1}.
\end{aligned}$$

□

Proposition 2.3.13. *Let $x \in \mathbb{Z}_p$, $|x|_p < p^{-1/(p-1)}$, then:*

$$\log(e^x) = x \text{ and } e^{\log(1+x)} = 1 + x$$

Proof. If $x = 0$, then the proposition is obvious, so assume $x \neq 0$. Then:

$$v_p\left(\frac{x^{n-1}}{n!}\right) = (n-1)v_p(x) - v_p(n!) > \frac{n-1}{p-1} - \frac{n-s}{p-1} = \frac{s-1}{p-1} \geqslant 0.$$

It follows that $|x^n/n!|_p < |x|_p$, which in turn implies that $|e^x - 1|_p = |x|_p$, by Lemma 2.1.5. We also have $1 = |e^x|_p > |x|_p > |x^n/n!|_p$ for $n \geqslant 2$, so using Lemma 2.3.11 we conclude that $\log(e^x) = x$. Notice that $|n!|_p \leqslant |n|_p$, so:

$$\left|\frac{x^n}{n}\right|_p \leqslant \left|\frac{x^n}{n!}\right|_p < |x|_p.$$

We get $|\log(1+x)|_p = |x|_p$, so $\log(1+x)$ is in the domain of the exponential and we again use Lemma 2.3.11 to conclude that $e^{\log(1+x)} = 1 + x$. □

Theorem 2.3.14. *Suppose $p \neq 2$. The p-adic logarithm defines an isomorphism of groups:*

$$\log : (1 + p\mathbb{Z}_p) \to p\mathbb{Z}_p,$$

with the exponential function as inverse. In particular:

$$(1 + p\mathbb{Z}_p) \cong p\mathbb{Z}_p \cong \mathbb{Z}_p.$$

Proof. Proposition 2.3.9 says that the logarithm is a homomorphism. Proposition 2.3.10 does the same for the exponential. Proposition 2.3.13 says that the functions are mutual inverses. We have seen that $|x|_p < p^{-1/(p-1)}$ if and only if $x \in p\mathbb{Z}_p$, so we also conclude that the domain and codomain are correct. □

Theorem 2.3.15. *Suppose $p = 2$. The p-adic logarithm defines an isomorphism of groups:*

$$\log : (1 + 4\mathbb{Z}_p) \to 4\mathbb{Z}_p,$$

with the exponential function as inverse. In particular:

$$(1 + 4\mathbb{Z}_p) \cong 4\mathbb{Z}_p \cong \mathbb{Z}_p.$$

Proof. We have seen that $|x|_p < p^{-1/(p-1)}$ if and only if $x \in 4\mathbb{Z}_p$, so we conclude that the domain and codomain are correct. The rest is the same as above. □

2.4 Squares in $\mathbb{Q}_p$

We will begin this section with a proposition which serves as preparation to understand an important theorem better. This theorem is called Hensel's Lemma. Hensel's Lemma will make it easier to show that a given polynomial with coefficients in $\mathbb{Z}_p$ has a zero in $\mathbb{Z}_p$. By reducing the polynomial modulo p^n.

Proposition 2.4.1. *For any $n \geqslant 1$:*

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}.$$

Proof. By Corollary 2.2.4, any element $x \in \mathbb{Z}_p$ can we written as a sum $x = \sum_{i=0}^{\infty} b_i p^i$, where $0 \leqslant b_i \leqslant p-1$. When we view x as element in $\mathbb{Z}_p/p^n\mathbb{Z}_p$ we see that it is equivalent to $\sum_{i=0}^{n-1} b_i p^i$. Moreover, the set:

$$\{b_0 + b_1 p + \ldots + b_{n-1}p^{n-1} : 0 \leqslant b_i \leqslant p-1\},$$

is the complete set of representatives of equivalence classes of $\mathbb{Z}_p/p^n\mathbb{Z}_p$. So, it is obvious that $b_0 = 1$ is a generator of $\mathbb{Z}_p/p^n\mathbb{Z}_p$. We also see that the order of $\mathbb{Z}_p/p^n\mathbb{Z}_p$ is p^n. So $\mathbb{Z}_p/p^n\mathbb{Z}_p$ is a cyclic group of order p^n and thus isomorphic to $\mathbb{Z}/p^n\mathbb{Z}$. □

Theorem 2.4.2 (Hensel's Lemma)**.** *Let $F \in \mathbb{Z}_p[X]$ and $n, k \in \mathbb{Z}$ such that $0 \leqslant 2k < n$. Suppose that there exists a p-adic integer $\alpha_0 \in \mathbb{Z}_p$ such that:*

$$F(\alpha_0) \equiv 0 \pmod{p^n},$$

and

$$v_p(F'(\alpha_0)) = k.$$

Then there exists a unique p-adic integer $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_0 \pmod{p^{n-k}}$ and $F(\alpha) = 0$.

Proof. We will construct (α_i) such that for $i \geqslant 0$, we have:

1. $F(\alpha_i) \equiv 0 \pmod{p^{n+i}}$.
2. $\alpha_{i+1} \equiv \alpha_i \pmod{p^{n-k+i}}$.

Such a sequence is Cauchy and for its limit α we have $F(\alpha) = 0$, because of continuity. Moreover, $\alpha \equiv \alpha_0 \pmod{p^{n-k}}$ by construction. We will proof that (α_i) exists by induction. Note that α_0 is given. Suppose that α_i exists,

we will find α_{i+1}. Property 2 requires that $\alpha_{i+1} = \alpha_i + b_i p^{n-k+i}$ for some $b_i \in \mathbb{Z}_p$. Write $F(x) = \sum_j c_j x^j$, then the Binomial Theorem gives:

$$\begin{aligned} F(\alpha_{i+1}) &= \sum_{j=0}^{d} c_j (\alpha_i + b_i p^{n-k+i})^j \\ &= \sum_{j=0}^{d} c_j (\alpha_i^j + j b_i p^{n-k+i} \alpha^{j-1} + \mathcal{O}(p^{2(n-k+i)})) \\ &= F(\alpha_i) + b_i p^{n-k+i} F'(\alpha_i) \pmod{p^{n+i+1}}. \end{aligned}$$

We can simplify this, using that $F(\alpha_i) \equiv 0 \pmod{p^{n+i}}$. We can write $F(\alpha_i) = x p^{n+i}$ for some x. We try to solve that:

$$x + p^{-k} F'(\alpha_i) b_i \equiv 0 \pmod{p}.$$

Also notice that property 2 implies that $\alpha_i \equiv \alpha_0 \pmod{p^{n-k}}$. Which means, $F(\alpha_i) \equiv F(\alpha_0) \pmod{p^{n-k}}$. By assumption, $n > 2k$ and $v_p(F'(\alpha_0)) = k$, which implies that $v_p(F'(\alpha_i)) = k$. Now, we can bring x to the other side and notice that $p^{-k} F'(\alpha_i)$ is invertible:

$$b_i \equiv -x(p^{-k} F'(\alpha_i))^{-1} \pmod{p}.$$

There exists a unique $0 \leqslant b_i \leqslant p-1$ with this property. If we set $\alpha_{i+1} = \alpha_i + b_i p^n$, then α_{i+1} has the stated properties. □

Theorem 2.4.3 (Multivariate Hensel's Lemma)**.** *Let $F \in \mathbb{Z}_p[X_1, \ldots, X_m]$. Suppose that $0 \leqslant 2k < n$ and that there exists $\alpha = (\alpha_1, \ldots, \alpha_m) \in (\mathbb{Z}_p)^m$ such that:*

$$F(\alpha) \equiv 0 \pmod{p^n},$$

and $0 \leqslant j \leqslant m$ such that:

$$v_p\left(\frac{\partial F}{\partial X_j}(\alpha)\right) = k.$$

Then there exists $y = (y_1, \ldots, y_n) \in (\mathbb{Z}_p)^n$ such that $F(y) = 0$ and $y \equiv \alpha \pmod{p^{n-k}}$.

Proof. The case where $m = 1$ is clear. If $m > 1$, then we obtain a polynomial in one variable, $F(\alpha_1, \ldots, X_j, \ldots, \alpha_m)$. We use the one dimensional case (with point α_j). This shows existence of $y_j \equiv \alpha_j \pmod{p^{n-k}}$ such that $F(\alpha_1, \ldots, y_j, \ldots, \alpha_n) = 0$. If we put $y_i = \alpha_i$ for $i \neq j$, then the element $y = (y_1, \ldots, y_m)$ has the desired properties. □

Recall that an element x of a field is an m-th root of unity if $x^m = 1$; it is called a primitive m-th root of unity if in addition $x^n \neq 1$ for $0 < n < m$. For a n-th root of unity $\zeta \in \mathbb{Q}_p$, we have $1 = |\zeta^n|_p = |\zeta|_p^n$, so $|\zeta|_p = 1$ and $\zeta \in \mathbb{Z}_p^\times$. Using Hensel's lemma we can show that $\mathbb{Q}_p$ contains the $(p-1)$-th roots of unity.

Corollary 2.4.4. *The field $\mathbb{Q}_p$ contains the $(p-1)$-th roots of unity.*

Proof. Define $f(x) = x^{p-1} - 1$. By Fermat's little theorem $x^{p-1} \equiv 1 \pmod{p}$ for any prime p and x not divisible by p. These are all elements $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$. We have $v_p((p-1)\alpha^{p-2}) = 0$, so we can apply Hensel's Lemma $p-1$ times, with respect to f, to get $p-1$ unique elements in $\mathbb{Z}_p$, that satisfy $x^{p-1} = 1$. They are unique because for all $\alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$ there exists $x \in \mathbb{Z}_p$ such that $x^{p-1} - 1 = 0$ and $x \equiv \alpha \pmod{p}$. □

Proposition 2.4.5. *If $p \neq 2$, then the roots of unity in $\mathbb{Q}_p$ are exactly the $(p-1)$-th roots of unity.*

Proof. Define $\pi : \mathbb{Z}_p^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ by reducing modulo p. It is clear that π is a homomorphism. Suppose that $\zeta_1, \zeta_2 \in \mathbb{Z}_p^\times$ are two different roots of unity. If $\zeta_1 \equiv \zeta_2 \pmod{p}$, then $\zeta_1\zeta_2^{-1} \equiv 1 \pmod{p}$. They are in the kernel of π and we have $\ker(\pi) = 1 + p\mathbb{Z}_p$. By Theorem 2.3.14 we have that $1 + p\mathbb{Z}_p \cong \mathbb{Z}_p$. If $x \in \mathbb{Z}_p$ and $|nx|_p = 0$, then $|n|_p = 0$ or $|x|_p = 0$, so we conclude that $\mathbb{Z}_p$ and $1 + p\mathbb{Z}_p$ have no torsion. However, $\zeta_1\zeta_2^{-1} \in 1 + p\mathbb{Z}_p$, which means that $\zeta_1 = \zeta_2$. We conclude that different roots of unity are different modulo p, so there are at most $p-1$ unique roots of unity. □

A similar statement is true in $\mathbb{Q}_2$. The proof is identical.

Proposition 2.4.6. *If $p = 2$, then the roots of unity in $\mathbb{Q}_p$ are exactly $\{\pm 1\}$.*

Proof. Define $\pi : \mathbb{Z}_p^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$ by reducing modulo 4. It is clear that π is a homomorphism. Theorem 2.3.15 gives us that $1 + 4\mathbb{Z}_p \cong \mathbb{Z}_p$ is torsion-free. A similar argument as in the proof of the previous proposition gives us that different roots of unity are different modulo 4. We know that $\pm 1 \in \mathbb{Q}_p$, so we conclude the proposition. □

We are now able to decompose $\mathbb{Z}_p^\times$, which in turn will allow us to give a decomposition of $\mathbb{Q}_p^\times$. We use μ_n to denote the group of n-th roots of unity in $\mathbb{Q}_p$.

Lemma 2.4.7. *If $p \neq 2$, then $\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)$, where $(1 + p\mathbb{Z}_p) \cong \mathbb{Z}_p$. If $p = 2$, then $\mathbb{Z}_2^\times \cong \mu_2 \times (1 + 4\mathbb{Z}_2)$, where $(1 + 4\mathbb{Z}_2) \cong \mathbb{Z}_2$.*

Proof. If $p \neq 2$ and $x \in \mathbb{Z}_p^\times$, then we can choose $\zeta \in \mu_{p-1}$ such that $x \equiv \zeta \pmod{p}$. Now we have that $\zeta^{-1}x \in 1 + p\mathbb{Z}_p$, because if not, then $x \not\equiv \zeta \pmod{p}$. This means that $x = \zeta \cdot \zeta^{-1}x$ and $\mathbb{Z}_p \cong V \times (1 + p\mathbb{Z}_p)$. The case $p = 2$ is similar. □

Theorem 2.4.8. *The group $\mathbb{Q}_p^\times$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ if $p \neq 2$ and to $\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z}$ if $p = 2$.*

Proof. Every element $x \in \mathbb{Q}_p^\times$ can be uniquely written in the form $x = p^n u$ with $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. So $\mathbb{Q}_p \cong \mathbb{Z} \times \mathbb{Z}_p^\times$. The theorem follows from Lemma 2.4.7 and the fact that $\mu_{p-1} \cong \mathbb{Z}/(p-1)\mathbb{Z}$ if $p \neq 2$ and $\mu_2 \cong \mathbb{Z}/2\mathbb{Z}$ if $p = 2$. □

Theorem 2.4.9. *Suppose $p \neq 2$ and let $x = p^n u$ be and element of $\mathbb{Q}_p^\times$, with $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Now, x is a square if and only if n is even and u mod p is a square.*

Proof. By the previous theorem we can decompose u into $u = u'v$ where $u' \in (1 + p\mathbb{Z}_p)$ and $v \in \mu_{p-1}$. Notice that:

$$\frac{1}{1+p} = 1 - p + p^2 - p^3 + p^4 - \ldots \in \mathbb{Z}_p,$$

so $1/2$ is also in $\mathbb{Z}_p$, which means that every element in $\mathbb{Z}_p$ is square. Since $(1+p\mathbb{Z}_p) \cong \mathbb{Z}_p$, all elements in $(1+p\mathbb{Z}_p)$ are squares. We have $u \equiv v \pmod{p}$ and we know that $\mu_{p-1} \cong (\mathbb{Z}/p\mathbb{Z})^\times$, so the theorem follows. □

Theorem 2.4.10. *An element $x = 2^n u$ of $\mathbb{Q}_2^\times$ is square if and only if n is even and $u \equiv 1 \pmod{8}$.*

Proof. The decomposition $\mathbb{Z}_2^\times = \{\pm 1\} \times (1 + 4\mathbb{Z}_p)$ shows that u is square if and only if u belongs to $(1 + 4\mathbb{Z}_p)$ and is a square in this group. Suppose $x \in (1 + p^2\mathbb{Z}_p)$ with $x = 1 + p^2 + \ldots$. If there exists y with $x = y^2$, then $y^2 \equiv 5 \mod 8$, but no such y exists. This means that squares of $(1 + 4\mathbb{Z}_p)$ are elements in $(1 + 8\mathbb{Z}_p)$. If $x \in (1 + 8\mathbb{Z}_p)$, then $x - y^2 = 0 \pmod{2^3}$ has solution $y = 1$. The derivative of $x - y^2$ is $-2y$. We see that $v_2(-2) = 1$, so we can apply Hensel's Lemma to conclude that x is a square. So, the unit u is a square if and only if $u \equiv 1 \pmod{8}$. □

2.5 Hilbert symbol

In this section we will define and discuss the Hilbert symbol. The Hilbert symbol measures whether or not solutions to some polynomial exist. The symbol will be useful later to define an invariant of quadratic modules. We will denote k for either the field $\mathbb{R}$ or the p-adic field $\mathbb{Q}_p$.

Definition 2.5.1. Let $a, b \in k^\times$. We put:

$$(a,b) = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a solution not equal to 0 in } k^3. \\ -1 & \text{otherwise.} \end{cases}$$

The number $(a,b) = \pm 1$ is called the *Hilbert symbol* of a and b relative to k.

We will define the group of norms and then show an interesting correlation with the Hilbert symbol. By [1, p. 583], the following is well-defined.

Definition 2.5.2. Let E/k be any finite extension and let $\alpha \in E$. Define the *norm* to be:

$$N_{E/k} : E \to k \text{ by } N_{E/k}(\alpha) = \prod_\sigma \sigma(\alpha),$$

where the product is taken over all the embeddings of E into an algebraic closure of k. If the context is clear we will write $N(\alpha)$ for $N_{E/k}(\alpha)$.

Lemma 2.5.3. *Let E/k be any finite extension and let L be a Galois extension of k containing E, then:*

1. *The norm is a multiplicative map, i.e. $N(\alpha\beta) = N(\alpha)N(\beta)$. Moreover, $N(E)$ is a group, called the group of norms of elements of E.*
2. *Let $E = k(\sqrt{D})$ be a quadratic extension of k, then:*

$$N(a + b\sqrt{D}) = \alpha^2 - Db^2.$$

Proof. Note that for embeddings σ, we have $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$. Taking the product over all embeddings σ gives $N(\alpha\beta) = N(\alpha)N(\beta)$. The image of a group homomorphism is a subgroup. This proves 1. The assumption that $k(\sqrt{D})$ is a quadratic extension of k implies that $x^2 - D$ is irreducible over k. Its roots are $\pm\sqrt{D}$, so:

$$N(a + b\sqrt{D}) = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2.$$

This proves 2. □

Because of this lemma the following proposition makes sense.

Proposition 2.5.4. *If $a, b \in k^\times$ and $k_b = k(\sqrt{b})$, then we have $(a,b) = 1$ if and only if a belongs to the group $N(k_b^\times)$ of norms of elements of $k_b^\times$.*

Proof. If b is the square of an element c, the equation $z^2 - ax^2 - by^2 = 0$ has solution $(0, 1, c)$ and $(a, b) = 1$. In this case the proposition follows from the fact that $k_b = k$ and $N(k_b^\times) = k^\times$. If b is not a square, then k_b is quadratic over k and every element in k_b can be written as $z + \sqrt{b}y$ with $y, z \in k$. If $a \in N(k_b^\times)$, then there exists $y, z \in k$ such that $a = z^2 - by^2$. Now, $z^2 - ax^2 - by^2$ has zero $(1, y, z)$ and $(a, b) = 1$. Conversely, suppose $(a, b) = 1$. We have $x \neq 0$, otherwise $z^2 - by^2 = 0$ implies b is a square, which is a contradiction. Using this we write:

$$a = \frac{z^2}{x^2} - b\frac{y^2}{x^2},$$

so a is the norm of $\frac{z}{x} + \sqrt{b}\frac{y}{x}$. This means that $a \in N(k_b^\times)$. □

Proposition 2.5.5. *The Hilbert symbol satisfied the formulas:*

1. $(a, b) = (b, a)$ *and* $(a, c^2) = 1$,
2. $(a, -a) = 1$ *and* $(a, 1 - a) = 1$,
3. $(a, b) = 1 \implies (aa', b) = (a', b)$
4. $(a, b) = (a, -ab) = (a, (1 - a)b)$

Proof. It is obvious that $z^2 - ax^2 - by^2 = 0$ has a solution if and only if $z^2 - bx^2 - ay^2 = 0$ has a solution. Furthermore, $z^2 - ax^2 - c^2y^2 = 0$ has solution $(0, 1, c)$. This proves 1. The quadratic form $z^2 - ax^2 + ay^2 = 0$ has solution $(1, 1, 0)$ and $z^2 - ax^2 - (1 - a)y^2 = 0$ has solution $(1, 1, 1)$. This proves 2. Suppose $(a, b) = 1$. If b is a square, then 1 implies that $(aa', b) = (a', b)$. We suppose that b is not a square, so $a \in N(k_b^\times)$ by Proposition 2.5.4. Since $N(k_b^\times)$ is a group, we have that $aa' \in N(k_b^\times)$ if and only if $a' \in N(k_b^\times)$, or $(aa', b) = (a, b)$. This proves 3. If $(a, b) = 1$, then $(b, a) = 1$ and $(-ab, a) = (-a, a) = 1$. Also, $((1 - a)b, a) = (1 - a, a) = 1$. If $(a, -ab) = 1$, then $(-ab, a) = 1$ and $(-a, a) = (b^{-1}, a) = 1$. This implies that $(b, a) = (b^2, a) = 1$ and we showed that now $(a, (1 - a)b) = 1$. If $(a, (1 - a)b) = 1$, then $((1 - a)b, a) = 1$ and $((1 - a), a) = (b-1, a) = 1$. This implies that $(b, a) = (b^2, a) = 1$ and we showed that now $(a, -ab) = 1$. We conclude that if either one of (a, b), $(a, -ab)$ and $(a, (1-a)b)$ equals one, then they all equal one. This proves 4. □

In the rest of this section, we will try to prove bilinearity of the Hilbert symbol, i.e. $(aa', b) = (a, b)(a', b)$.

Theorem 2.5.6. *If $k = \mathbb{R}$, we have $(a, b) = 1$ if $a > 0$ or $b > 0$, and $(a, b) = -1$ if $a, b < 0$.*

Proof. If $a > 0$, then $z^2 - ax^2 - by^2 = 0$ has solution $(1, 0, \sqrt{a})$. If $b > 0$, then $(0, 1, \sqrt{b})$ is a solution. If $a, b < 0$ then $ax^2 + by^2 \leqslant 0$ and $z^2 = ax^2 + by^2$ only has the trivial solution. □

Lemma 2.5.7. *Let $v \in \mathbb{Z}_p^\times$. If the equation $z^2 - px^2 - vy^2 = 0$ has a nontrivial solution in $\mathbb{Q}_p$, it has a solution (x, y, z) such that $z, y \in \mathbb{Z}_p^\times$ and $x \in \mathbb{Z}_p$.*

Proof. Suppose (x_0, y_0, z_0) is the nontrivial zero, define:

$$h = \inf\{v_p(x_0), v_p(y_0), v_p(z_0)\}.$$

Define $(x, y, z) = (p^{-h}x_0, p^{-h}y_0, p^{-h}z_0)$, it is clear that $x, y, z \in \mathbb{Z}_p$ and at least on of them in $\mathbb{Z}_p^\times$. We will prove that $y, z \in \mathbb{Z}_p^\times$. If it did not then either $y \equiv 0 \pmod{p}$ or $z \equiv 0 \pmod{p}$. We have $z^2 - vy^2 = px^2$, so $z^2 - vy^2 \equiv 0 \pmod{p}$ and we know that $v \not\equiv 0 \pmod{p}$. From this we conclude that both y and z are congruent to zero mod p, so $y, z \notin \mathbb{Z}_p^\times$. We have $px^2 \equiv 0 \pmod{p^2}$ since y and z are squared: $z^2 - vy^2 = px^2$. This in turn implies that $x \equiv 0 \pmod{p}$ or $x \notin \mathbb{Z}_p^\times$, which is a contradiction since we assumed that at least one of x, y and z are in $\mathbb{Z}_p^\times$. □

Definition 2.5.8. If $p \neq 2$ and $x \in (\mathbb{Z}/p\mathbb{Z})^\times$. The *Legendre symbol* of x, denoted $\left(\frac{x}{p}\right)$, is defined as:

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a square,} \\ -1 & \text{else.} \end{cases}$$

By Euler's criterion, which had been discovered earlier and was known to Legendre, we can also define $\left(\frac{x}{p}\right)$ as $x^{(p-1)/2} \pmod{p}$. We will also use this equivalence. It is also easy to see that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ using this definition.

Theorem 2.5.9. *If $k = \mathbb{Q}_p$ with $p > 2$ and if we write $a = p^\alpha u$ and $b = p^\beta v$, where u and v belong to $\mathbb{Z}_p^\times$, we have:*

$$(a, b) = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{\bar{u}}{p}\right)^\beta \left(\frac{\bar{v}}{p}\right)^\alpha.$$

Here, $\bar{u}$ and $\bar{v}$ are the images of u and v of reduction mod p and $\epsilon(p)$ denotes $(p-1)/2$ mod 2.

Proof. We can reduce α and β modulo 2 by Proposition 2.5.5, so due to symmetry of the Hilbert symbol we have three cases.

1. If $\alpha, \beta \equiv 0 \pmod 2$, then we should check that $(u, v) = 1$. We choose $z = 1$, we will prove there exists a solution to $ux^2 + vy^2 = 1$. By Theorem 2.4.3, it suffices to find a solution of $ux^2+vy^2-1 \equiv 0 \pmod p$, where $u, v \in (\mathbb{Z}/p\mathbb{Z})^\times$. We define $S = \{1 - ux^2 : x \in \mathbb{Z}/p\mathbb{Z}\}$ and we define $T = \{vy^2 : y \in \mathbb{Z}/pZ\}$. Since there are $(p+1)/2$ squares in $\mathbb{Z}/p\mathbb{Z}$, we have $|S| + |T| = p+1$, so $|S \cap T| \neq 0$, which means that there exists a solution to $ux^2 + vy^2 - 1 \equiv 0 \pmod p$.

2. If $\alpha \equiv 1$, $\beta \equiv 0 \mod 2$, then we should check that $(pu, v) = \left(\frac{\bar{v}}{p}\right)$. We just proved that $(u, v) = 1$, so we have $(pu, v) = (p, v)$ by Proposition 2.5.5. We need to check that $(p, v) = \left(\frac{\bar{v}}{p}\right)$. If v is square, then we have that $(p, v) = \left(\frac{\bar{v}}{p}\right) = 1$. If v is not square, then $\left(\frac{\bar{v}}{p}\right) = -1$ by Theorem 2.4.9. If $(p, v) = 1$, then the previous lemma implies that $z^2 - px^2 - vy^2 = 0$ has a solution such that $z, y \in \mathbb{Z}_p^\times$, which implies that v is a square modulo p. This is a contradiction so we conclude that $(p, v) = -1$.

3. If $\alpha, \beta = 1$, then we should check if $(pu, pv) = (-1)^{(p-1)/2}\left(\frac{\bar{u}}{p}\right)\left(\frac{\bar{v}}{p}\right)$. By Proposition 2.5.5 we have $(pu, pv) = (pu, -p^2uv)$. Since $(pu, p^2) = 1$ we also get $(pu, -p^2uv) = (pu, -uv)$. Using what we proved in 2 we see that:
$$(pu, pv) = (pu, -uv) = \left(\frac{\overline{-uv}}{p}\right).$$
We have seen that the Legendre symbol is multiplicative and using the formula for the symbol we also see that $\left(\frac{\bar{-1}}{p}\right) = (-1)^{(p-1)/2}$, so we are done. □

This Theorem allows us to prove that the Hilbert symbol is bilinear. Before we do that, we first prove a similar formula for $p = 2$. We define two functions for this. It is clear that they are well defined.

Definition 2.5.10. We define $\epsilon : \mathbb{Z}_2^\times \to \mathbb{Z}/2\mathbb{Z}$ by:
$$\epsilon(u) = \frac{u-1}{2} \pmod 2,$$
and $\omega : \mathbb{Z}_2^\times \to \mathbb{Z}/2\mathbb{Z}$ by:
$$\omega(u) = \frac{u^2-1}{8} \pmod 2.$$

Lemma 2.5.11. *If $u, v \in \mathbb{Z}_2^\times$, then:*
$$\epsilon(uv) = \epsilon(u) + \epsilon(v) \text{ and } \omega(uv) = \omega(u) + \omega(v).$$

Proof. We want to show that $(u-1)/2 + (v-1)/2 \equiv (uv-1)/2 \pmod 2$. This is equivalent to showing that $u-1+v-1 = uv-1 \pmod 4$. It is easy to see that this is true since $u \equiv 1$ or $3 \pmod 4$ and $v \equiv 1$ or $3 \pmod 4$. For the second equation, it is easy to verify that:

$$\omega(u) = \begin{cases} 0 & \text{if } u \equiv \pm 1 \pmod 8 \\ 1 & \text{if } u \equiv \pm 3 \pmod 8 \end{cases} = \frac{u^2-1}{8} \pmod 2.$$

The lemma then follows by verifying every combination. □

Theorem 2.5.12. *If $k = \mathbb{Q}_2$ and if we write $a = p^\alpha u$ and $b = p^\beta v$, where u and v belong to $\mathbb{Z}_2^\times$, we have:*

$$(a,b) = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)}.$$

Proof. We can reduce α and β modulo 2 by Proposition 2.5.5, so due to symmetry of the Hilbert symbol we have three cases.

1. If $\alpha, \beta \equiv 0 \pmod 2$, then we should check that $(u,v) = 1$ when u or v is congruent to $1 \pmod 4$ and $(u,v) = -1$ otherwise. If $u \equiv 1 \pmod 4$, then we see that $u \equiv 1 \pmod 8$ or $u \equiv 5 \pmod 8$. In the first case, u is a square by Theorem 2.4.10 and in the second case $u + 4v \equiv 1 \pmod 8$, since v is congruent to $1, 3, 5$ or $7 \pmod 8$. Again, by Theorem 2.4.10, there exists $w \in \mathbb{Z}_p^\times$ such that $w^2 = u + 4v$. The form $z^2 - ux^2 - vy^2$ has thus $(1, 2, w)$ as zero and $(u,v) = 1$. When $v \equiv 1 \pmod 4$, the same argument holds. Suppose now that neither u nor v is congruent to $1 \pmod 4$. If this is the case, then $u \equiv v \equiv -1 \pmod 4$. If (x, y, z) is a solution of $z^2 - ux^2 - vy^2 = 0$, then we can force that at least one of x, y and z to be in $\mathbb{Z}_p^\times$ by multiplying the solution with $p^{-\inf\{v_p(x), v_p(y), v_p(z)\}}$. Now, since the squares in $\mathbb{Z}/4\mathbb{Z}$ are 0 and 1, we know that $z^2 + x^2 + y^2 \equiv 0 \pmod 4$ implies that x, y, z are congruent to $0 \pmod 2$, which contradicts that at least on of them is in $\mathbb{Z}_p^\times$. We conclude that $(u,v) = -1$.

2. If $\alpha = 1, \beta = 0$, then we should check if $(2u, v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(v)}$. We will first show that $(2, v) = (-1)^{\omega(v)}$. By the definition of $\omega(v)$, this is equivalent to saying $(2,v) = 1$ if and only if $v \equiv \pm 1 \pmod 8$. By Lemma 2.5.7 if $(2,v) = 1$, there exists $x, y, z \in \mathbb{Z}_2$ such that the form $z^2 - 2x^2 - vy^2 = 0$ and $y, z \equiv 1 \pmod 2$. The only squares in $\mathbb{Z}/8\mathbb{Z}$ are $0, 1$ and 4. So, $y^2 \equiv z^2 \equiv 1 \pmod 8$ and $1 - 2x^2 - v \equiv 0 \pmod 8$, which implies that $v \equiv \pm 1 \pmod 8$. Conversely, if $v \equiv 1 \pmod 8$, then v is a square by Theorem 2.4.10 and thus $(2,v) = 1$. In the case that $v \equiv -1$

(mod 8), then the equation $z^2 - 2x^2 - vy^2 \equiv 0 \pmod 8$ has solution $(1,1,1)$. By Proposition 2.4.3, this solution lifts to a true solution, so we have $(2,v) = 1$. In case 1 we showed that $(u,v) = (-1)^{\epsilon(u)\epsilon(v)}$, so we will now show that $(2u,v) = (2,v)(u,v)$ to conclude the proof. If $(2,v) = 1$ or $(u,v) = 1$, then $(2u,v) = (u,v)$ or $(2u,v) = (2,v)$ by Proposition 2.5.5, so $(2u,v) = (2,v)(u,v)$. It remains to show the equality when $(2,v) = (u,v) = -1$. We showed that $(2,v) = 1$ if and only if $v \equiv \pm 1 \pmod 8$, which means that $(2,v) = 1$ implies that $v \equiv 3$ or $5 \pmod 8$. In case 1 we showed that $(u,v) = -1$ implies that $u, v \equiv 3 \pmod 4$, so $u, v \equiv 3$ or $-1 \pmod 8$. This means that $v \equiv 3 \pmod 8$ and $u \equiv 3$ or $-1 \pmod 8$. By Proposition 2.5.5 we have $(u,v) = (c^2u, d^2v)$, so we are allowed to multiply u, v by squares. Note that by Theorem 2.4.10 $v/3 = w^2$ for some $w \in \mathbb{Z}_p^\times$ and $v/w^2 = 3$, so we can assume that $v = 3$. Using this logic, we can suppose that $v = 3$ and $u = -1$ or $v = -5$ and $u = 3$. The equations:

$$z^2 + 2x^2 - 3y^2 = 0 \text{ and } z^2 - 6x^2 + 5y^2 = 0,$$

have $(1,1,1)$ as solution, so $(2u,v) = 1$.

3. If $\alpha, \beta = 1$, then we should check if $(2u,2v) = (-1)^{\epsilon(u)\epsilon(v)+\omega(u)+\omega(v)}$. By Proposition 2.5.5 we have that $(2u,2v) = (2u,-4uv) = (2u,-uv)$. We have already proven in case 2 that:

$$(2u,2v) = (2u,-uv) = (-1)^{\epsilon(u)\epsilon(-uv)+\omega(u)+\omega(-uv)}.$$

Note that $\epsilon(-1) = 1, \omega(-1) = 0$ and $\epsilon(u)(1+\epsilon(u)) = 0$, we conclude using Lemma 2.5.11 that the above exponent is equivalent to:

$$\epsilon(u)\epsilon(v) + \omega(u) + \omega(v). \qquad \square$$

Using these formulas for the Hilbert symbol, we can prove the main theorem of this section.

Theorem 2.5.13. *The Hilbert symbol is bilinear, i.e.* $(aa'.b) = (a,b)(a',b)$.

Proof. We first prove the theorem for $\mathbb{Q}_p$. Suppose $aa' = p^\alpha u$, $a = p^{\alpha_1}u_1$, $a' = p^{\alpha_2}u_2$, with $u = u_1u_2$ and $\alpha = \alpha_1 + \alpha_2$. Also suppose $b = p^\beta v$. The theorem then follows from the two proven formulas for the Hilbert symbol, using the fact that the Legendre symbol is multiplicative, $\epsilon(uv) = \epsilon(u) + \epsilon(v)$ and $\omega(uv) = \omega(u) + \omega(v)$. The case $k = \mathbb{R}$ follows directly from Theorem 2.5.6. $\square$

Remember that given a nondegenerate quadratic module (k^n, f), with $n \in \mathbb{N}_{>0}$, we have that the discriminant $d(f) \in k^\times/(k^\times)^2$ is invariant under change of basis. We also proved in Proposition 1.4.2 that f has an orthogonal basis $e = (e_1, \ldots, e_n)$. If we put $a_i = e_i \cdot e_i$, then $f \sim a_1x_1^2 + \ldots + a_nx_n^2$ and we conclude that $d(f) = a_1 \ldots a_n$. We will now define another invariant of (k^n, f).

Definition 2.5.14. Suppose (k^n, f) is a quadratic module and $e = (e_1, ..., e_n)$ is an orthogonal basis, also define $a_i = e_i \cdot e_i$. We define:

$$\epsilon(e) = \prod_{i<j}(a_i, a_j) = \pm 1.$$

We will show that $\epsilon(e)$ is an invariant of (k^n, f).

Corollary 2.5.15. *The number $\epsilon(e)$ does not depend on the choice of the orthogonal basis e.*

Proof. If $n = 2$, one has $\epsilon(e) = 1$ if and only if the form $z^2 - a_1x_1^2 - a_2x_2^2$ has a zero. By Corollary 1.5.6 this means that $\epsilon(e) = 1$ if and only if $a_1x_1^2 + a_2x_2^2$ represents 1, which is equivalent to saying that there exists $v \in k^2$ such that $f(v) = 1$, but this does not depend on e. For $n \geqslant 3$, we use induction on n. Suppose $e' = (e'_1, \ldots, e'_n)$ is another orthogonal basis. By Proposition 1.4.5, it suffices to prove that $\epsilon(e) = \epsilon(e')$ when e and e' are contiguous. Note that $\epsilon(e')$ does not change, when we permute the e'_i, so we can assume that $e_1 = e'_1$. If we put $a'_i = e_i \cdot e_i$, then $a_1 = a'_1$. Since the Hilbert symbol is bilinear and the fact that $(a_1, a_1^2) = 1$, we have:

$$\epsilon(e) = (a_1, a_2 \ldots a_n) \prod_{2 \leqslant i<j} (a_i, a_j) = (a_1, d(f)a_1) \prod_{2 \leqslant i<j} (a_i, a_j).$$

Note that $d(f)$ is invariant as element in $k^\times/(k^\times)^2$. So, similarly,

$$\epsilon(e) = (a_1, d(f)a_1) \prod_{2 \leqslant i<j} (a'_i, a'_j).$$

We can apply the inductive hypothesis to the orthogonal complement of e_1 to show that:

$$\prod_{2 \leqslant i<j} (a_i, a_j) = \prod_{2 \leqslant i<j} (a'_i, a'_j),$$

which implies that $\epsilon(e) = \epsilon(e')$, so we are done. □

We will write $\epsilon(f)$ instead of $\epsilon(e)$ from now on.

2.6 Local–global principle

All quadratic forms considered in this section have coefficients in $\mathbb{Q}$ and are nondegenerate. We will denote by Ω the union of the set of prime numbers and the symbol ∞, and we put $\mathbb{Q}_\infty = \mathbb{R}$. Let $f \sim a_1x_1^2 + \ldots + a_nx^2$ be a quadratic form. Let $v \in \Omega$, the injection $\mathbb{Q} \to \mathbb{Q}_v$ allows us to view f as a quadratic form in $\mathbb{Q}_v$. We will denote this by f_v. The invariants of f_v will be denoted by $d_v(f)$ and $\epsilon_v(f)$. It is clear that $d_v(f)$ is the image of $d(f)$ by $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \to \mathbb{Q}_v^\times/(\mathbb{Q}_v^\times)^2$ and that:

$$\epsilon_v(f) = \prod_{i<j}(a_i, a_j)_v.$$

Lemma 2.6.1. *If $a, b \in \mathbb{Q}^\times$, then $(a, b)_v = 1$ for all but finitely many elements of Ω and:*

$$\prod_{v\in\Omega}(a, b)_v = 1.$$

Proof. We can multiply a and b by squares, so we are allowed to assume that $a = \pm p_1 \ldots p_k$ and $b = \pm p_1' \ldots p_l'$ are prime factorizations of a and b. We get:

$$\begin{aligned}\prod_{v\in\Omega}(a, b)_v &= \prod_{v\in\Omega}(a, \pm 1)_v(a, p_1')_v \ldots (a, p_l')_v \\ &= \prod_{v\in\Omega}(\pm 1, \pm 1)_v(p_1, \pm 1)_v \ldots (p_k. \pm 1)_v \ldots (\pm 1, p_l')_v(p_1, p_l')_v \ldots (p_k, p_l')_v.\end{aligned}$$

We see that we only need to prove the theorem when a or b are equal to -1 or to a prime number. We will use Theorems 2.5.6 2.5.9 and 2.5.12. Using symmetry of the Hilbert symbol, we look at three cases.

1. If $a, b = -1$, then $(-1, -1)_\infty = (-1, -1)_2 = 1$ and $(-1, -1)_v = 1$ if $v \neq 2, \infty$. The product is equal to one.

2. If $a = -1$, $b = l$ with l prime. If $l = 2$, then l is a unit if $v \neq 2$, so since -1 is a unit we get $(-1, 2)_v = 1$. If $v = 2$, then it is also easy to see that $(-1, 2)_v = 1$ using the formula for the Hilbert symbol. If $l \neq 2$, then $(-1, l)_v = 1$ if $v \neq 2, l$ since l is a unit in this case. We also have $(-1, l)_2 = (-1)^{\epsilon(l)}$ and $(-1, l)_l = \left(\frac{-1}{l}\right) = (-1)^{\epsilon(l)}$. The product is equal to one.

3. If $a = l$, $b = l'$ with l and l' primes, then we can suppose that $l \neq l'$. If $l = l'$, then by Proposition 2.5.5 we have $(l, l) = (l, -l^2) = (l, -1)$, which is a case we have discussed. If $l \neq l'$ and $l' = 2$, then $(l, 2)_v = 1$ for $v \neq 2, l$. We also have $(v, 2)_2 = (-1)^{\omega(l)}$ and $(l, 2)_l = \left(\frac{2}{l}\right) = (-1)^{\omega(l)}$.

The product is equal to one. If $l \neq l'$ and they are different then 2, then $(l,l')_v = 1$ for $v \neq 2, l, l'$. We also have $(l,l')_2 = (-1)^{\epsilon(l)\epsilon(l')}$, $(l,l')_l = \left(\frac{l'}{l}\right)$ and $(l,l')_{l'} = \left(\frac{l}{l'}\right)$. By quadratic reciprocity [5, p. 7] we have:

$$\left(\tfrac{l}{l'}\right)\left(\tfrac{l'}{l}\right) = (-1)^{\epsilon(l)\epsilon(l')},$$

so the product is equal to one. □

Lemma 2.6.2. *Let S be a finite subset of Ω. The image of $\mathbb{Q}$ in $\prod_{v\in S}\mathbb{Q}_v$ is dense in this product.*

Proof. Since we use the product topology we are allowed to enlarge S. Suppose that $S = \{\infty, p_1, \ldots, p_n\}$, where p_i are distinct primes. Assume that $\epsilon, N > 0$. We need to prove that for a point:

$$(x_\infty, x_1, \ldots, x_n) \in \mathbb{R} \times \mathbb{Q}_{p_1} \times \ldots \times \mathbb{Q}_{p_n},$$

there exists $x \in \mathbb{Q}$ such that $|x - x_\infty|_\infty < \epsilon$ and $v_{p_i}(x - x_i) \geqslant N$ for all i. If we can find $x \in \mathbb{Q}$ such that this holds for the point $(ax_\infty, ax_1, \ldots, ax_n)$, then the point x/a has the desired properties. We conclude that we are allowed to assume that $x_i \in \mathbb{Z}_{p_i}$ for all i. By the Chinese remainder theorem using relatively prime integers $p_1^N, \ldots, p_n^N$, there exists $x_0 \in \mathbb{Z}$ such that we have $v_{p_i}(x_0 - x_i) \geqslant N$ for all i. Now choose $q \geqslant 2$, which is relatively prime to all p_i. The rational numbers of the form a/q^m for $a \in \mathbb{Z}$ and $m \geqslant 0$ are dense in $\mathbb{R}$, because $1/q^m$ can get infinitely small. We can thus find number $u = a/q^m$ such that:

$$|x_0 - x_\infty + up_1^N \ldots p_n^N| \leqslant \epsilon.$$

The number $x = x_0 + up_1^N \ldots p_n^N$ suffices, since:

$$v(x - x_i) \geqslant \min\{v_{p_i}(x_0 - x_i), v_{p_i}\left(up_1^N \ldots p_n^N\right)\} \geqslant N. \qquad \square$$

The following theorem is proven in [5, p.24]

Theorem 2.6.3. *Let $(a_i)_{i\in I}$ be a finite family of elements in $\mathbb{Q}^\times$ and let $(\epsilon_{i,v})_{i\in I, v\in\Omega}$ be a family of numbers equal to ± 1. In order that there exists $x \in \mathbb{Q}^\times$ such that $(a_i, x)_v = \epsilon_{i,v}$ for all $i \in I$ and all $v \in \Omega$, it is necessary and sufficient that the following conditions be satisfied:*

1. *Almost all the $\epsilon_{i,v}$ are equal to 1.*
2. *For all $i \in I$ we have $\prod_{v\in\Omega} \epsilon_{i,v} = 1$.*
3. *For all $v \in \Omega$ there exists $x_v \in \mathbb{Q}_v^\times$ such that $(a_i, x_v)_v = \epsilon_{i,v}$ for all $i \in I$.*

Theorem 2.6.4 (Hasse's local-global principle)**.** *A nondegenerate quadratic form f represents 0 if and only if for all $v \in \Omega$, the form f_v represents 0.*

Proof. If f represent 0, then it is clear that f_v represents 0 for all $v \in \Omega$. Conversely suppose that f_v represents 0 for all $v \in \Omega$. By Proposition 1.5.8 we can write $f \sim a_1x_1^2 + \ldots + a_nx_n^2$. We look at four cases.

1. If $n = 2$, then we assume that $f = x_1^2 - ax_2^2$. Since f_∞ represents 0 we have that $a > 0$. When we write $a = p_1^{d_1} \ldots p_l^{d_l}$, with p_i different primes, we see that a is a square in $\mathbb{Q}$ if all d_i are even. Since a is square in all $\mathbb{Q}_{p_i}$, we have that $v_{p_i}(a)$ is even, so d_i is even for all i.

2. If $n = 3$, then we assume that $f = x_1^2 - ax_2^2 - bx_3^2$. By Proposition 2.5.5 we can multiply a and b by squares, so we assume that a and b are square free integers. By symmetry of the Hilbert symbol we can also assume that $|a|_\infty \leqslant |b|_\infty$. We prove by induction on $m = |a|_\infty + |b|_\infty$. If $m = 2$, then $a = \pm 1$ and $b = \pm 1$, so:

$$f = x_1^2 \pm x_2^2 \pm x_3^2.$$

   If $f = x_1^2 + x_2^2 + x_3^2$, then f_∞ only has a trivial solution, so we don't look at this case. In the other cases f represents 0. If $m > 2$, then $|b|_\infty \geqslant 2$ and we will show that a is square modulo a prime p with $p \mid b$. If $a \equiv 0 \pmod{p}$, then we are done, so suppose that $a \not\equiv 0 \pmod{p}$ or in other words that a is a p-adic unit in $\mathbb{Q}_p$. By hypothesis there exists $(x, y, z) \in \mathbb{Q}_p^3$ such that $z^2 - ax^2 - by^2 = 0$. We can force that at least one of x, y and z is in $\mathbb{Z}_p^\times$ by multiplying the solution with $p^{-\inf\{v_p(x), v_p(y), v_p(z)\}}$. Since $p \mid b$, we have $z^2 \equiv ax^2 \pmod{p}$. If $x \equiv 0 \pmod{p}$, then $z \equiv 0 \pmod{p}$ and $by^2 \equiv 0 \pmod{p^2}$. We assumed that $v_p(b) = 1$, so $y \equiv 0 \pmod{p}$, which is a contradiction. We conclude that $x \not\equiv 0 \pmod{p}$, so since $z^2 \equiv ax^2 \pmod{p}$, we have that a is square modulo p. We conclude that a is a square modulo b using the Chinese remainder theorem (b is square free). There exists an integer t such that $a \equiv t^2 \pmod{b}$ and also $a \equiv (t + cb)^2 \pmod{b}$ for all $c \in \mathbb{Z}$. This means that we can choose t in such a way that $|t| \leqslant |b|/2$. There also exists an integer b' such that $bb' = t^2 - a$. This shows that bb' is a norm of the extension $k(\sqrt{a})/k$ where $k = \mathbb{Q}$ or $k = \mathbb{Q}_p$. Because $bb' \in N(k_a^\times)$ we have that $b \in N(k_a^\times)$ if and only if $b' \in N(k_a^\times)$. Using the same argument as in Proposition 2.5.4, we conclude that f represents 0 in k if and only if $f' = x_1^2 - ax_2^2 - b'x_3^2$ represents 0 in k. We have that:

$$|b'| = \left|\frac{t^2 - a}{b}\right| \leqslant \left|\frac{t^2}{b}\right| + \left|\frac{a}{b}\right| \leqslant \frac{|b|}{4} + 1 < |b|,$$

since $|t| \leqslant |b|/2$ and $|b| \geqslant 2$. We can write b' in the form $b''u^2$ with b'' a square free integer and u an integer, so $|b''| < |b|$. By the induction hypothesis $f'' = x_1^2 - ax_2^2 - b''x_3^2$ represents 0 and because $f'' \sim f'$ we know that f' represents 0 and we conclude that f represents 0.

3. If $n = 4$, then we assume that $f = ax_1^2 + bx_2^2 - (cx_3^2 + dx_4^2)$. By assumption, for all $v \in \Omega$ we have that f_v represents 0 and by Corollary 1.5.7 there exists $x_v \in \mathbb{Q}_v^\times$ such that the form $g = ax_1^2 + bx_2^2 - x_v y_1^2$ and $h = cx_3^2 + dx_4^2 - x_v y_2^2$ represent 0. We have that g represents 0 if and only if $x_v g$ represents 0 and:

$$x_v g \sim x_v a x_1^2 + x_v b x_2^2 - y_1^2,$$

represents 0 if:

$$(x_v a, x_v b)_v = (x_v, x_v)_v (x_v, ab)_v (a, b)_v = (x_v, -ab)_v (a, b)_v = 1.$$

This is equivalent to saying that $(x_v, -ab)_v = (a, b)_v$. We conclude that:

$$(x_v, -ab)_v = (a, b)_v \text{ and } (x_v, -cd)_v = (c, d)_v \text{ for all } v \in \Omega.$$

By Lemma 2.6.1, we can use Theorem 2.6.3, so there exists $x \in \mathbb{Q}^\times$ such that:

$$(x, -ab)_v = (a, b)_v \text{ and } (x, -cd)_v = (c, d)_v \text{ for all } v \in \Omega.$$

We conclude that f represents 0 by as similar argument as made before.

4. If $n \geqslant 5$, then we assume that $f = h - g$, where $h = a_1 x_1^2 + a_2 x_2^2$ and $g = -(a_3 x_3^2 + \ldots + a_n x_n^2)$. We prove by induction. Let S be the subset of Ω consisting of ∞, 2 and the prime numbers p such that $v_p(a_i) \neq 0$ for an $i \geqslant 3$. It is clear that S is finite. If $v \in S$, then f_v represents 0 by assumption. By Corollary 1.5.7 there exists $a_v \in \mathbb{Q}_v^\times$ which is represented by h and g. This means that there exits $x_{1,v}, \ldots, x_{n,v} \in \mathbb{Q}_v$ such that:

$$h(x_{1,v}, x_{2,v}) = a_v = g(x_{3,v}, \ldots, x_{n,v}).$$

Define $n_v = 1$ if $v \neq 2$ and $n_2 = 3$. By Lemma 2.6.2 we can choose $x_1, x_2 \in \mathbb{Q}$ such that $|x_i - x_{i,\infty}|_\infty < |x_{i,\infty}|_\infty$ and $x_i \equiv x_{i,v} \pmod{p^{v_p(a_v)+n_v}}$ for every $v \in S - \{\infty\}$. Now, for every $v \in S - \{\infty\}$, we have:

$$a = h(x_1, x_2) \equiv h(x_{1,v}, x_{2,v}) = a_v \pmod{p^{v_p(a_v)+n_v}}$$

We see that $a/a_v \equiv 1 \pmod{p^{n_v}}$. Using Theorem 2.4.10 and Theorem 2.4.9 we conclude that a/a_v is square in $\mathbb{Q}_v^\times$ if $v \in S - \{\infty\}$. Since $|x_i - x_{i,\infty}|_\infty < |x_{i,\infty}|_\infty$, we conclude that a/a_∞ is a square in $\mathbb{R}^\times$. Define $f_1 = az^2 - g$. If $v \in S$, then g represents a_v in $\mathbb{Q}_v$ and also a because a/a_v is a square in $\mathbb{Q}_v^\times$. We see that f_1 represents 0 in $\mathbb{Q}_v$. Assume $v \notin S$. Note that $f_1 = az^2 - g$ represents 0 if $g_1 = a_3x_3^2 + a_4x_4^2 + a_5x_4^2$ represents 0. Using a similar argument as in the case $n = 4$ this is the case if:

$$(-a_5a_3, -a_5a_4) = (-1, -d_v(g_1))(a_3, a_4)(a_3, a_5)(a_4, a_5) = 1,$$

which is equivalent to saying that $(-1, -d_v(g_1)) = \epsilon_v(g_1)$. We have that $-a_3, \ldots, -a_5$ are v-adic units, because $v \notin S$. We have seen in the proof of Theorem 2.5.9 that $(u, u')_v = 1$ for units u and u'. We conclude that f_1 represents 0 for all $v \in \Omega$. The rank of f_1 is $n - 1$, so by the inductive hypothesis we have that f_1 represents 0 in $\mathbb{Q}$. We conclude that g represents a in $\mathbb{Q}$ and since h represents a in $\mathbb{Q}$, we have that f represents 0. □

Corollary 2.6.5. *If $a \in \mathbb{Q}^\times$, then a nondegenerate quadratic form f represents a if and only if for all $v \in \Omega$, the form f_v represents a.*

Proof. By Corollary 1.5.6, the form $f = f(x_1, \ldots, _n)$ represents a if and only if $f - ax_{n+1}$ represents 0. The corollary follows from the local-global principle. □

References

[1] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[2] Fernando Q. Gouvêa. *p-adic numbers*. Universitext. Springer, Cham, third edition, 2020. An introduction.

[3] T. Y. Lam. *Introduction to quadratic forms over fields*, volume 67 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2005.

[4] Steven Roman. *Advanced linear algebra*, volume 135 of *Graduate Texts in Mathematics*. Springer, New York, third edition, 2008.

[5] J.-P. Serre. *A course in arithmetic*, volume No. 7 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Heidelberg, 1973.