ALMA MATER STUDIORUM - UNIVERSITY OF BOLOGNA

Department of Mathematics
Degree Programme of Mathematics

CLASSIFICATION OF QUADRATIC FORMS OVER $\mathbb{Q}$

Bachelor Thesis

Presented by:
Elena Bogliolo

Supervisor:
Chiar.ma Prof.ssa
Nicoletta Cantarini

Graduation Session I
Academic year 2020-2021

Contents

Introduction

Quadratic forms appear in many different areas of mathematics. The classification of relevant objects can be reduced to the classification of quadratic forms. This is the case, for example, of the Killing form in Lie theory and of the intersection form in low dimensional topology. Similarly, quadratic forms are used to classify conics and quadrics.

When facing the problem of classifying quadratic forms, it is natural to ask whether two given quadratic forms Q and Q' over a field $\mathbb{K}$ are equivalent or not, i.e., whether one can be obtained from the other through a linear transformation or not. If $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$ it is easy to answer this question. However, as we move away from these fields, the answer becomes extremely harder.

This thesis is devoted to the classification of quadratic forms over $\mathbb{Q}_p$ and $\mathbb{Q}$ through invariants. An invariant is an object associated with the quadratic form which does not change if the form is replaced with an equivalent one. Invariants are usually used to distinguish two quadratic forms which are not equivalent (see Examples 5 and 6). When $\mathbb{K} = \mathbb{Q}_p$ or $\mathbb{K} = \mathbb{Q}$ it is possible to obtain a complete set of invariants. More precisely, two quadratic forms Q and Q' are equivalent over $\mathbb{Q}_p$ if and only if they have same rank, discriminant and Hasse-Minkowski invariant (Theorem 3.2.1). The classification of quadratic forms over $\mathbb{Q}$ is then obtained using the Hasse-Minkowski theorem.

These results naturally lead to the study of quadratic forms with integer coefficients which intervenes in various questions related to modular forms, differential topology and finite groups.

The thesis is organized as follows: Chapter 1 is dedicated to the construction of the p-adic fields, which are presented as completions of the rational field with respect to the p-adic absolute values. Here the Legendre and the Hilbert symbols are introduced. Chapter 2 contains preliminary results on quadratic forms. Finally, Chapter 3 is the heart of the thesis: here the classification of quadratic forms over $\mathbb{Q}_p$ and $\mathbb{Q}$ is achieved. Several examples are given in order to clarify definitions and concepts.

The main reference for this thesis is Serre's book Cours d'Arithmétique, a masterpiece of mathematical literature.

Chapter 1

Construction of the p-adic field

There are two most common ways of defining p-adic numbers, one analytic and one algebraic. The analytic definition tells us that p-adic numbers are the completion of $\mathbb{Q}$ with respect to the p-adic metrics. The algebraic definition puts p-adic numbers as sequences. We will start off with the first definition and then introduce the algebraic one (for integers) to prove some of the properties of these sets.

1.1 Absolute values on $\mathbb{Q}$

In this section we will reach a complete classification of absolute values in $\mathbb{Q}$ up to equivalence. This is not strictly necessary for the objective of this thesis but allows a better understanding of the purpose and role of the objects that we will use. ([Gou97, Chapter III])

Definition 1.1.1. *An* ***absolute value on a field*** $\mathbb{K}$ *is a function* $|.| : \mathbb{K} \longrightarrow \mathbb{R}$ *that satisfies the following conditions:*

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

ii) $|xy|$=$|x||y|$*;*

iii) $|x+y| \leq |x| + |y|$.

We say that an absolute value is ***non-archimedean*** *if it satisfies the condition*

iv) $|x+y| \leq max\{|x|, |y|\}$.

Conversely an absolute value that does not satisfy (iv) is said to be ***archimedean****.*

Remark 1.1.2. Let $|.|$ be a non-archimedean absolute value over a field $\mathbb{K}$. Then $|n| \leq 1$ for all integers n and if $x, y \in \mathbb{K}$ and $|x| \neq |y|$, we have $|x+y| = max\{|x|, |y|\}$.

Proof. Since $x \neq y$ we can assume that $|x| > |y|$ so that $|x+y| \leq max\{|x|, |y|\} = |x|$ but $x = (x+y) - y$ so $|x| \leq max\{|x+y|, |y|\} \Longrightarrow |x| \leq |x+y| \Longrightarrow |x+y| = |x| =$

$max\{|x|, |y|\}$.

□

Using this result we can prove the following properties for non-archimedean absolute values:

Theorem 1.1.3. *Let $\mathbb{K}$ be a field with a non-archimedean absolute value $|.|$, and $\bar{B}(a,r) = \{x \in \mathbb{K} : |x - a| \leq r\}$. Then*

i) all triangles are isosceles;

ii) if $b \in \bar{B}(a,r)$ then $\bar{B}(a,r) = \bar{B}(b,r)$;

iii) every ball $\bar{B}(a,r)$ is both open and closed;

iv) any two balls are either disjoint or contained in one another.

Proof. $\boxed{i)}$ Let a, b, c be the vertices of a non degenerate triangle. Then we can assume that $|a| > |b| > |c|$ so the length of the sides is $|a - c| = max\{|a|, |c|\} = |a|, |a - b| = max\{|a|, |b|\} = |a|, |b - c| = max\{|b|, |c|\} = |b|$.

$\boxed{ii)}$ Let b be a point in the open ball $B = B(a,r) = \{x \in \mathbb{K} : |x - a| < r\}$. If x is any other point in B then $|x - b| \leq max\{|x - a|, |b - a|\} < r$ hence $B(a,r)$ is contained in $B(b,r)$. By switching the role of b and a we have the opposite inclusion. The identity for closed balls is obtained in the same way using $\leq$.

$\boxed{iii)}$ Let x be a point in the boundary of $B(a,r)$ and y in $B(a,r)$ such that $|x - y| < r$ then $|x - a| = max\{|x - y|, |y - a|\} < r$. We need to show that such y exists and for this purpose we consider a ball $B(x,s)$ with $s < r$. This ball has non empty intersection with $B(a,r)$ since x is on the boundary. We have shown that any boundary point of $B(a,r)$ belongs to $B(a,r)$ so $B(a,r)$ is closed and $B(a,r) = \bar{B}(a,r)$.

$\boxed{iv)}$ Let $B(a,r)$ and $B(b,r')$ be two balls with non empty intersection. Then, using *ii)*, any element y in the intersection is center to both the balls. The one with the smallest radius is then contained in the other.

□

The following definitions lead to a fundamental example of a non-archimedean absolute value: the p-adic absolute values. We will later prove that these are the only non-archimedean absolute values on $\mathbb{Q}$ (up to equivalence).

Definition 1.1.4. *Let $p \in \mathbb{N}$ be a fixed prime number. The p**-adic valuation** on $\mathbb{Z}$ is the function*

$$v_p : \mathbb{Z} - \{0\} \longrightarrow \mathbb{R} \tag{1.1}$$

with $v_p(n)$ the unique integer such that

$$n = p^{v_p(n)} n' \text{ with } p \nmid n' \tag{1.2}$$

and $v_p(0) = \infty$.
We extend this definition to $\mathbb{Q}$ by defining for $x = a/b \in \mathbb{Q}^*$

$$v_p(x) = v_p(a) - v_p(b). \tag{1.3}$$

This is well defined and does not depend on a and b but only on x.

Definition 1.1.5. *For $x \in \mathbb{Q}$ we define the* p***-adic absolute value*** *of x by*

$$|x|_p = p^{-v_p(x)} \textit{ if } x \neq 0 \textit{ and } |0|_p = 0. \tag{1.4}$$

Then $|.|_p$ is a non-archimedean absolute value.

Definition 1.1.6. *An absolute value induces a metric and hence a topology over $\mathbb{K}$, with a basis given by the set of open balls $B(a, r)$ for all $a \in \mathbb{K}$ and r in $\mathbb{R}$.*
Two absolute values on a field $\mathbb{K}$ are said to be ***equivalent*** *if they define the same topology over $\mathbb{K}$, that is, if every open set with respect to one is also open with respect to the other.*

Theorem 1.1.7. *Let $|.|_1, |.|_2$ be two absolute values. The following statements are equivalent:*

i) $|.|_1, |.|_2$ are equivalent
ii) for any x in $\mathbb{K}$, $|x|_1 < 1 \iff |x|_2 < 1$
iii) $\exists a \in \mathbb{R}^+$ such that $\forall x \in \mathbb{K}$ we have $|x|_1 = |x|_2^a$

Proof. $\boxed{i) \Rightarrow ii)}$ Let us assume that $\mathbb{K}$ contains an element x such that $|x|_1 < 1$ and $|x|_2 \geq 1$ then the sequence $(x^n)_{n\in\mathbb{N}}$ converges with respect to the first absolute value but not with respect to the second.
$\boxed{ii) \Rightarrow iii)}$ Let $x_0 \in \mathbb{K}, |x_0|_1 < 1$. Then by *ii)* $|x_0|_2 < 1$ hence there exists a real positive number α such that $|x_0|_1 = |x_0|_2^\alpha$. Now given any other $x \in \mathbb{K}$, if $|x|_1 = |x_0|_1$ the identity follows trivially because otherwise we would have $|x_0/x|_1 = |x/x_0|_1 = 1$ and either $|x_0/x|_2 < 1$ or $|x/x_0|_2 < 1$ contradicting *ii)*. Similarly if $|x|_1 = 1$ we must have $|x|_2 = 1$, otherwise we would have either $|x|_2 < 1$ or $|1/x|_2 < 1$, which is not possible for *ii)*. Moreover the equality for x implies the same equality for every power of x.
For this reason we can assume that $|x|_i \neq 1$ and $|x|_i \neq |x_0|_i$ for $i = 1, 2$. We can also assume $|x|_1 < 1$ otherwise we replace it with $1/x(= x^{-1})$. It is hence only left to prove that if $x \in \mathbb{K}, |x|_1 < 1$ such that $|x|_1 = |x|_2^b$ then $a = b$.

Let n, m be two positive integers, then we have, $|x|_1^n < |x_0|_1^m \iff |\frac{x^n}{x_0^m}|_1 < 1 \iff |\frac{x^n}{x_0^m}|_2 < 1 \iff |x|_2^n < |x_0|_2^m$. Taking logs of the first and last equations we get $nlog|x|_1 < mlog|x_0|_1 \iff nlog|x|_2 < mlog|x_0|_2$ or, equivalently,

$$\frac{n}{m} < \frac{log|x_0|_1}{log|x|_1} \iff \frac{n}{m} < \frac{log|x_0|_2}{log|x|_2} \tag{1.5}$$

This means that the set of fractions smaller than the first quotient and the second quotient is the same. Since there are fractions as close as we like to any real number the two fractions on the right are the same number, which means that

$$a = \frac{log|x_0|_1}{log|x_0|_2} = \frac{log|x|_1}{log|x|_2} = b. \tag{1.6}$$

$\boxed{iii) \Rightarrow i)}$ Assuming $iii)$ we get that any open ball with respect to $|.|_1$ is an open ball with respect to $|.|_2$ indeed $|x-b|_1 < r \iff |x-b|_2^a < r \iff |x-a|_2 < r^{1/a}$ which proves $i)$.

□

Definition 1.1.8. *We call* ***trivial absolute value*** *the following absolute value over* $\mathbb{Q}$*:*
$|x| = 0$ *if x=0*
$|x| = 1$ *otherwise.*
This is an archimedean absolute value.

Remark 1.1.9. The trivial absolute value is equivalent only to itself.

Remark 1.1.10. A non-archimedean absolute value cannot be equivalent to an archimedean absolute value.

Proof. We will show that if an absolute value is non-archimedean than any other equivalent absolute value is non-archimedean. Let $|x|_1^a = |x|_2$. Then if $|x+y|_1 \leq max\{|x|_1, |y|_1\}$, since a is positive, $|x+y|_2 = |x+y|_1^a \leq (max\{|x|_1, |y|_1\})^a = max\{|x|_1^a, |y|_1^a\} = max\{|x|_2, |y|_2\}$

□

Remark 1.1.11. If p and q are two different primes, the p-adic and the q-adic absolute values are not equivalent.

Proof. We have: $p = p^1 \implies v_p(p) = 1 \implies |p|_p = 1/p < 1$.
On the other hand $p = q^0 \cdot p \implies v_q(p) = 0 \implies |p|_q = 1$.

□

Theorem 1.1.12. ***(Ostrowski)***
Every non-trivial absolute value is equivalent to one of the asolute values $|.|_p$, where p is either a prime number or ∞.

Proof. We will only prove the non-archimedean part. For the archimedean part see [Gou97, Chapter III].
Let n_0 be the smallest integer such that $|n_0| < 1$. Then the following hold:
1) n_0 must be a prime.
Indeed if $n_0 = ab$ with a and b both smaller than n_0, we would have $|a| = |b| = 1$ and $|ab| = |n_0| < 1$.
Let $p = n_0$. We want to show that $|.|$ is equivalent to the the p-adic absolute value.
2) If an integer n is not divisible by p then $|n| = 1$.
Using the division algorithm we have $n = qp+r$, with $0 < r < p$. By the minimality of p we have $|r| = 1$ and $|qp| < 1$. This proves that $|n| = max\{|qp|, |r|\} = 1$.
3) $|.|$ is equivalent to the p-adic absolute value.
Given an integer n we can write it as $n = p^v n'$ with $p \nmid n'$. Then

$$|n| = |p^v||n'| = |p^v| = c^{-v} \tag{1.7}$$

where $c = |p|^{-1} > 0$. This proves the claim.

□

1.2 Completion of $\mathbb{Q}$ with respect to $|.|_p$

Given the possible absolute values over $\mathbb{Q}$ we construct a completion for each of them by analogy with what can be done in the case of $\mathbb{R}$.

Definition 1.2.1. *A field $\mathbb{K}$ is called* ***complete*** *if every Cauchy sequence of elements of $\mathbb{K}$ has a limit.*
A subset S of $\mathbb{K}$ is called dense if every open ball around every element of $\mathbb{K}$ has an element in S.

Definition 1.2.2. *The smallest field containing $\mathbb{K}$ and complete with respect to a certain absolute value $|.|$ is called* ***completion*** *of $\mathbb{K}$ with respect to $|.|$.*

Remark 1.2.3. Given that
-$|.|_\infty$ extends to $\mathbb{R}$
-$\mathbb{R}$ is complete with respect to this absolute value

-$\mathbb{Q}$ is dense in $\mathbb{R}$
it follows that $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to $|.|_\infty$.

Remark 1.2.4. Every Cauchy sequence with respect to the trivial absolute value is eventually constant, thus every field is complete with respect to this absolute value.

We now find a completion with respect to the other non-trivial absolute values over $\mathbb{Q}$.

Proposition 1.2.5. *A sequence (x_n) in $\mathbb{Q}$ is a Cauchy sequence with respect to a non-archimedean absolute value if and only if*

$$\lim_{n\to\infty} |x_{n+1} - x_n| = 0. \tag{1.8}$$

Proof. Using the definition of convergence and the following inequality we have the result.
Let $m = n + r > n$ then $|x_m - x_n| = |x_m - x_{m-1} + x_{m-1} - x_{m-2} + ... + x_{n+1} - x_n| \leq max\{|x_m - x_{m-1}|, |x_{m-1} - x_{m-2}|, ..., |x_{n+1} - x_n|\}$.
□

Remark 1.2.6. The field $\mathbb{Q}$ is not complete with respect to any of its nontrivial absolute values.([Gou97, Chapter III])

The idea behind constructing a completion of $\mathbb{Q}$ is to abstractly include limitless Cauchy sequences in the field, thinking of them as their missing limits.

Proposition 1.2.7. *Let $|.|_p$ be a non-archimedean absolute value on $\mathbb{Q}$. We denote by $\mathcal{C}$ (or $\mathcal{C}_p(\mathbb{Q})$), the set of all Cauchy sequences of elements of $\mathbb{Q}$*
Defining + as $(x_n) + (y_n) = (x_n + y_n)$ and $\cdot$ as $(x_n) \cdot (y_n) = (x_n \cdot y_n)$ makes $\mathcal{C}$ a commutative ring with unity.
The ideal $\mathcal{N} \subset \mathcal{C}$ of the sequences that tend to zero:

$$\mathcal{N} = \{(x_n) : x_n \longrightarrow 0\} \tag{1.9}$$

is a maximal ideal of $\mathcal{C}$.

Proof. We want to show that given a sequence (x_n) that does not tend to zero, the ideal I generated by $\mathcal{N}$ and (x_n) is $\mathcal{C}$. Hence it is sufficient to prove that 1 is in I.

Since (x_n) does not tend to zero and is a Cauchy sequence there must eventually exist an integer N and a positive number c such that $|x_n| \geq c > 0 \; \forall \; n > N$.
We define a new sequence $y_n := 0$ if $n \leq N; y_n := 1/x_n$ otherwise. Since when $n > N$

$$|y_{n+1} - y_n| = |\frac{1}{x_{n+1}} - \frac{1}{x_n}| = \frac{|x_{n+1} - x_n|}{|x_n x_{n+1}|} \leq \frac{|x_{n+1} - x_n|}{c^2} \longrightarrow 0 \tag{1.10}$$

from 1.2.5 this proves that y_n is a Cauchy sequence. Moreover

$$x_n y_n = \begin{cases} 0 & \text{if } n < N \\ 1 & \text{if } n > N \end{cases} \tag{1.11}$$

If we subtract this product from the constant sequence (1) we get a sequence that is eventually 0 so in particular it is a sequence in $\mathcal{N}$.
In other words

$$(1) - (x_n)(y_n) \in \mathcal{N} \tag{1.12}$$

i.e. (1) can be written as the sum of a multiple of (x_n) and an element of $\mathcal{N}$, hence it belongs to I.

□

We want to identify sequences that differ by elements of $\mathcal{N}$ on the ground that they ought to have the same limit. This is done by taking the quotient of the ring $\mathcal{C}$ by the ideal $\mathcal{N}$. Since $\mathcal{N}$ is a maximal ideal the quotient will be a field.

Definition 1.2.8. *We define the* ***field of*** p***-adic numbers*** *to be the quotient of the ring* $\mathcal{C}$ *by its maximal ring* $\mathcal{N}$*:*

$$\mathbb{Q}_p = \mathcal{C}/\mathcal{N} \tag{1.13}$$

Since two different constant sequences never differ by an element of $\mathcal{N}$, We can have an inclusion

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p \tag{1.14}$$

by sending $q \in \mathbb{Q}$ to the equivalence class of the constant sequence (q).
We are now left with proving that $\mathbb{Q}_p$ has the properties of a completion of $\mathbb{Q}$ (i.e. that we can extend the p-adic absolute value to $\mathbb{Q}_p$, that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ and that $\mathbb{Q}_p$ is indeed complete with respect to $|.|_p$).

Proposition 1.2.9. *Let $(x_n) \in \mathcal{C} \setminus \mathcal{N}$ then the sequence of absolute values $|x_n|_p$ is eventually stationary.*

Proof. Since (x_n) does not tend to zero we can find c and N_1 such that

$$n > N_1 \Rightarrow |x_n| \geq c > 0$$

Since (a_n) is Cauchy there also exists a number N_2 such that

$$m, n > N_2 \Rightarrow |x_n - x_m| < c \tag{1.15}$$

Since both conditions are true at once we find that if $N = max\{N_1, N_2\}$

$$n, m > N \Rightarrow |x_n - x_m| < max\{|x_n|, |x_m|\} \tag{1.16}$$

which gives $|x_n| = |x_m|$ because since $|.|$ is non-archimedean all triangles are isosceles. □

From Proposition 1.2.9 it follows that the extension $|\lambda|_p = \lim_{n\to\infty} |x_n|_p$ (with $\lambda \in \mathbb{Q}_p$ and (x_n) a sequence in the equivalence class λ) of the p-adic absolute value to the p-adic field, is well defined.

Theorem 1.2.10. *The image of $\mathbb{Q}$ under the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ is a dense subset of $\mathbb{Q}_p$.*

Proof. We need to show that any open ball around an element $\lambda \in \mathbb{Q}_p$ contains an element of $\mathbb{Q}$ (i.e. the image of $\mathbb{Q}$ given by the constant sequences). Given a fixed radius ε we will show that there is a constant sequence in $B(\lambda, \varepsilon)$.
Let (x_n) be a Cauchy sequence representing λ and $0 < \varepsilon' < \varepsilon$. By the Cauchy property there exists a number N such that $|x_n - x_m| < \varepsilon' \quad \forall\, n, m > N$. Let $y = x_n$ and consider the constant sequence (y). Now the sequence $\lambda - (y)$ is represented by $(x_n - y)$ and for the definition above $|(x_n - y)| = \lim_{n\to\infty} |x_n - y|$.
But for any $n \geq N$ we have $|x_n - y| = |x_n - x_N| < \varepsilon'$, hence

$$\lim_{n\to\infty} |x_n - y| \leq \varepsilon' < \varepsilon \tag{1.17}$$

This proves that $(y) \in B(\lambda, \varepsilon)$. □

Theorem 1.2.11. *$\mathbb{Q}_p$ is complete with respect to the p-adic absolute value $|.|_p$.*

Proof. Let (λ_n) be a Cauchy sequence of elements of $\mathbb{Q}_p$. Since the image of $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ we can find a sequence of rational numbers $(y_n)_{n\in\mathbb{N}}$, $(y_n \in \mathbb{Q})$ such that

$$\lim_{n\to\infty} |\lambda_n - (y_{(n)})| = 0 \tag{1.18}$$

where by $(y_{(n)})$ we denote the constant sequence $(y_n, ...y_n, ...)$. This is true because for every $\varepsilon_n = 1/n$ there exists a constant sequence $(y_{(n)})$ in $B(\lambda_n, 1/n)$. Hence $|\lambda_n - (y_{(n)})| < \varepsilon_n = 1/n \xrightarrow{n\to\infty} 0$.
Moreover $(y_n)_{n\in\mathbb{N}}$ is also a Cauchy sequence of elements in $\mathbb{Q}$, indeed we have:

$$\begin{aligned} |y_n - y_{(m)}| &= |(y_{(n)}) - (y_{(m)})| \leq |(y_{(n)}) - \lambda_n| + |\lambda_n - \lambda_m| + |\lambda_m - (y_{(m)})| \\ &\leq 1/n + \varepsilon + 1/m \end{aligned} \tag{1.19}$$

Let λ be the class of this sequence in $\mathbb{Q}_p$, then

$$\lim_{n\to\infty} \lambda_n = \lambda \tag{1.20}$$

Indeed for all k, $\exists N > 0$ such that $|\lambda_n - \lambda| = \lim_{i\to\infty} |(\lambda_n)_i - y_i| \leq \lim_{i\to\infty}(|(\lambda_n)_i - y_n| + |y_n - y_i|) \leq 1/k$ for all $n \geq N$ (using (1.17)).

□

Remark 1.2.12. The sets $\{x \in \mathbb{R}_+ : x = |\lambda|_p \text{ for some } \lambda \in \mathbb{Q}\}$ and $\{x \in \mathbb{R}_+ : x = |\lambda|_p \text{ for some } \lambda \in \mathbb{Q}_p\}$ are both equal to $\{p^n : n \in \mathbb{Z}\} \cup \{0\}$

1.3 The ring of p-adic integers

The following results will be needed for the characterization of quadratic forms over the p-adic fields. In particular here we prove the results leading to the characterization of squares in the p-adic fields.([Gou97, Chapter III])

Definition 1.3.1. *The ring of* ***p-adic integers*** *is defined as:*

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\} \tag{1.21}$$

We call p-adic units the invertible elements of $\mathbb{Z}_p$. This set will be denoted by $\mathbb{Z}_p^*$. From the definition we see that

$$\mathbb{Z}_p^* = \{x \in \mathbb{Q}_p : |x|_p = 1\}. \tag{1.22}$$

The following result gives an intuitive representation of p-adic integers that will be widely used later on. ([Kob84, Chapter I, Section 4]):

Lemma 1.3.2. *If $x \in \mathbb{Q}$ and $|x|_p \leq 1$, then for any i there exists an integer $\alpha \in \mathbb{Z}$ such that $|\alpha - x|_p \leq p^{-i}$. The integer α can be chosen in the set $\{0, 1, 2, 3, ...p^i - 1\}$*

Proof. Let $x = a/b$ be written in lowest terms. Since $|x|_p \leq 1$, it follows that p does not divide b, and hence b and p^i are relatively prime. So we can find integers m and n such that: $mb + np^i = 1$. Let $\alpha := am$. The idea is that mb differs from 1 by a p-adically small amount, so that m is a good approximation to $1/b$, and so am is a good approximation to $x = a/b$. More precisely, we have:

$$\begin{aligned} |\alpha - x|_p &= |am - (a/b)|_p = |a/b|_p |mb - 1|_p \leq |mb - 1|_p \qquad (1.23) \\ &= |np^i|_p = |n|_p/p^i \leq 1/p^i \end{aligned}$$

Finally, we can add a multiple of p^i to the integer α to get an integer between 0 and p^i for which the inequality $|\alpha - x|_p \leq 1/p^i$ still holds. □

Theorem 1.3.3. *Any p-adic integer a has exactly one representative Cauchy sequence of the form $\{a_i\}$ for which:*
i) $0 \leq a_i < p^i$ for i = 1,2,3,...
ii) $a_i \equiv a_{i+1}$ (mod p^i) for i = 1,2,3,...

Proof. We first prove uniqueness:
If $\{a'_i\}$ is a different sequence satisfying i) and ii), and if $a_{i_0} \neq a'_{i_o}$, then $a_{i_0} \not\equiv a'_{i_o}$, (mod p^{i_0}), because both are between 0 and p^{i_0}. But then, for all $i \geq i_0$ we would have $a_i \equiv a_{i_o} \not\equiv a'_{i_o} \equiv a'_i$ (mod p^{i_0}), i.e. $a_i \not\equiv a'_i$ (mod p^{i_0}). Thus

$$|a_i - a'_i|_p > 1/p^{i_0} \qquad (1.24)$$

This proves the uniqueness.
Now given a sequence $\{b_i\}$ we want to find an equivalent sequence $\{a_i\}$ satisfying i) and ii).
For every $j = 1, 2, 3, ...$ let N(j) be a natural number such that $|b_i - b_{i'}|_p \leq p^{-j}$ whenever $i, i' \geq N(j)$ (we are using the fact that $\{b_i\}$ is a Cauchy sequence). Notice that $|b_i|_p \leq 1$ if $i \geq N(1)$, because for all $i' \geq$ N(1)

$$|b_i|_p \leq max\{|b_{i'}|_p, |b_{i'} - b_i|_p\} \leq max\{|b_{i'}|_p, 1/p\} \qquad (1.25)$$

and $|b_{i'}|_p \xrightarrow{i' \to \infty} |a|_p \leq 1$.
We now use Lemma 1.3.2 to find a sequence of integers a_j with $0 \leq a_j < p^j$ such

that

$$|a_j - b_{N(j)}|_p \leq 1/p^i. \tag{1.26}$$

We claim that $\{a_j\}$ is the required sequence. We need to show that $a_{j+1} \equiv a_i \pmod{p^i}$ and that $\{b_j\} \sim \{a_j\}$.
Given any j, for $i \geq N(j)$, the first assertion follows because

$$\begin{aligned} |a_{j+1} - a_j|_p &= |a_{i+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p \\ &\leq max\{|a_{i+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |a_j - b_{N(j)}|_p\} \\ &\leq max\{1/p^{j+1}, 1/p^j, 1/p^j\} = 1/p^j \end{aligned} \tag{1.27}$$

The second follows from the following relations:

$$\begin{aligned} |a_i - b_i|_p &= |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \\ &\leq max\{|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_i - b_{N(j)}|_p\} \\ &\leq max\{1/p^j, 1/p^j, 1/p^j\} = 1/p^j. \end{aligned} \tag{1.28}$$

Hence $|a_i - b_i|_p \xrightarrow{i\to\infty} 0$.

□

Theorem 1.3.4. *We have $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, i.e., for every $x \in \mathbb{Q}_p$ there exists $n \geq 0$ such that $p^n x \in \mathbb{Z}_p$.*

Proof. If $x \in \mathbb{Q}_p$ we can compute its valuation $v_p(x)$. If $v_p(x) \geq 0$ then x is already an element of $\mathbb{Z}_p$. Otherwise $v_p(x)$ is negative and we have

$$v_p(p^{-v_p(x)}x) = -v_p(x) + v_p(x) = 0 \tag{1.29}$$

which means that $p^{-v_p(x)}x \in \mathbb{Z}_p$.

□

Theorem 1.3.5. *For every $n \geq 1$ the sequence*

$$0 \longrightarrow \mathbb{Z}_p \xrightarrow{g} \mathbb{Z}_p \xrightarrow{h} \mathbb{Z}/p^n\mathbb{Z} \longrightarrow 0 \tag{1.30}$$

is exact. In particular

$$\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}. \tag{1.31}$$

Proof. We define the maps in the sequence as follows:

$$g : x \mapsto p^n x \quad and \quad h : x \mapsto [x]_{p^n}. \tag{1.32}$$

Notice that the map h is well defined since it can be seen as choosing the n^{th} element in the unique sequence describing x with the properties of Theorem 1.3.3.
Now $Ker(g) = \{x : p^n x = 0\} = 0$, $Im(g) = \{y : y = p^n x$ for some x in $\mathbb{Z}_p\} = p^n\mathbb{Z}_p$, $Ker(h) = \{x : [x]_{p^n} \equiv [0]_{p^n}\} \cong p^n\mathbb{Z}$ and $Im(h) = \mathbb{Z}/p^n\mathbb{Z}$. This proves the exactness of the sequence.
We use the homomorphism theorems to conclude.

□

Theorem 1.3.6. ***(Hensel's Lemma)***
Let $F(X) = a_0 + a_1X + ... + a_nX^n$ be a polynomial with coefficients in $\mathbb{Z}_p$.
Suppose that there exists an integer $\alpha_1 \in \mathbb{Z}_p$ such that

$$\begin{cases} F(\alpha_1) \equiv 0 & (mod\ p\mathbb{Z}_p) \\ F'(\alpha_1) \not\equiv 0 & (mod\ p\mathbb{Z}_p) \end{cases} \tag{1.33}$$

where F' is the formal derivative of F.
Then there exists a unique p-adic integer $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_1$ (mod $p\mathbb{Z}_p$) and $F(\alpha)$=0.

Proof. We will show that the root α exists by constructing a Cauchy sequence of integers converging to it.
We will construct a sequence of integers $\alpha_1, \alpha_2, ..., \alpha_n, ...$ such that for all $n > 0$ we have
i) $F(\alpha_n) \equiv 0 \pmod{p^n}$
ii) $F(\alpha_n) \equiv \alpha_{n+1} \pmod{p^n}$
Such a sequence will be Cauchy since $(\alpha_n - \alpha_{n+1}) = p^n m$ with $m \in \mathbb{Z}$, hence $|\alpha_n - \alpha_{n+1}| \leq p^{-n}$.
Moreover its limit will satisfy $F(\alpha) = 0$ and $\alpha \equiv \alpha_1$ (mod p) by construction. Conversely we will show that a root α will determine such a sequence α_n. Thus once we have $\alpha_n$the theorem is proved. From the hypothesis of the theorem we know that α_1 exists. To find α_2 we use condition *ii)* which requires that $\alpha_2 = \alpha_1 + b_1p$ for some $b_1 \in \mathbb{Z}_p$. Now plugging this expression into $F(X)$ we get:

$$\begin{aligned} F(\alpha_2) &= F(\alpha_1 + b_1p) = \overbrace{F(\alpha_1) + F'(\alpha_1)b_1p + \text{ terms in } p^n}^{Taylorexpansion} \quad n \geq 2 \\ &\equiv F(\alpha_1) + F'(\alpha_1)b_1p \pmod{p^2} \end{aligned} \tag{1.34}$$

We are left with proving that we can find α_2 such that

$$F(\alpha_1) + F'(\alpha_1)b_1p \equiv 0 \pmod{p^2}$$

We know that $F(\alpha_1) = px$ for some x. The equation then becomes

$$px + F'(\alpha_1)b_1p \equiv 0 \pmod{p^2} \tag{1.35}$$

We are looking for an element b_1 that solves this equation. We notice that $F'(\alpha_1)$ is not divisible by p and hence is invertible in $\mathbb{Z}_p$.
We can take

$$b_1 \equiv -x(F'(\alpha_1))^{-1} \pmod{\text{p}} \tag{1.36}$$

(b_1 is in fact in $\mathbb{Z}$ and we can choose the unique element that verifies $0 \leq b_1 \leq p-1$). The same calculation works to get $a_n + 1$ from a_n. Hence we can obtain a sequence uniquely determined at each step.

□

Example 1. Let $F(X) = X^3 - X - 2$. We have $F(0) \equiv 0 \pmod 2$ and $F(1) \equiv 0 \pmod 2$, while $F'(0) \equiv 1 \pmod 2$ and $F'(1) \equiv 0 \pmod 2$. Therefore Hensel's Lemma implies that there is a unique $\alpha \in \mathbb{Z}_2$ such that $F(\alpha) = 0$ and $\alpha \equiv 0 \pmod 2$.
Although 1 is a root of $F(X) \pmod 2$, it does not lift to a root in $\mathbb{Z}_2$ since it does not even lift to a root (mod 4): $F(1) \equiv 2 \pmod 4$ and $F(3) \equiv 2 \pmod 4$, so if $\beta \in \mathbb{Z}_2$ and $\beta \equiv 1 \pmod 2$, then $\beta \equiv 1$ or $3 \pmod 4$ and therefore $F(\beta) \equiv 2 \not\equiv 0 \pmod 4$.

From Hensel's Lemma we can finally prove the following results.

Theorem 1.3.7. *Let $p \neq 2$ be a prime, and $b \in \mathbb{Z}_p^*$ a p-adic unit. If there exits α_1 such that $\alpha_1^2 \equiv b$ (mod $p\mathbb{Z}_p$), then b is the square of an element of $\mathbb{Z}_p^*$.*

Proof. We apply Hensel's Lemma to the polynomial $F(X) = X^2 - b$. Indeed from the statement of the theorem $F(\alpha_1) \equiv 0 \pmod p$ and since $p \neq 2$ and $b \in \mathbb{Z}_p^*$ (so in particular $p \nmid b$) we have that $2\alpha_1 \not\equiv 0 \pmod p$. By Hensel's Lemma there exists a root of $F(X)$, i.e. b is the square of an element of $\mathbb{Z}_p^*$.

□

This property can be extended to all elements of $\mathbb{Q}_p$ by noticing that any $x \in \mathbb{Q}_p$ can be written as $x = p^{v_p(x)}x'$ with $x' \in \mathbb{Z}_p^*$ (indeed by definition of $v_p(x)$, $p \nmid x'$ so $|x'|_p = 1$).

Theorem 1.3.8. *Let p be a prime. An element $x \in \mathbb{Q}_p$ is a square in $\mathbb{Q}_p$ if and only if $x = p^{2n}y^2$ for some $n \in \mathbb{Z}$ and $y \in \mathbb{Z}_p^*$.*

If $p \neq 2$ then the quotient $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$ has order 4, and the set $\{1, p, c, cp\}$, with $c \in \mathbb{Z}_p^*$ an element whose reduction modulo p is not a quadratic residue, is a complete set of representatives.

Proof. The first statement follows from the fact that the powers of p and the p-adic units do not "mix". For the second statement we recall the fact that $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ (Theorem 1.3.5), hence $(\mathbb{Z}_p/p\mathbb{Z}_p)^*$ is cyclic and every non-residue y, verifies $[y]_R = [n]_R$ where n is an arbitrary non-residue and R is the set of residues.

□

Remark 1.3.9. In particular if $x \in \mathbb{Z}$ then $x = p^a p_2^{a_2} ... p_n^{a_n}$. By Theorem 1.3.8, x is a square in $\mathbb{Q}_p$ if and only if a is even, indeed if $\{p, p_2, ..., p_n\}$ are n different primes then $p_2^{a_2} ... p_n^{a_n} \in \mathbb{Z}_p^*$.

Example 2. Since $2 = 3^2$ is a square in $\mathbb{Z}/7\mathbb{Z}$, Theorem 1.3.7 shows that 2 is a square in $\mathbb{Z}_7$. Moreover, by Theorem 1.3.8, for every $n \in \mathbb{Z}$, $7^{2n} \cdot 2$ is a square in $\mathbb{Q}_7$. On the other hand, since 2 is not a quadratic residue modulo 5, then 2 is not a square in $\mathbb{Q}_5$.

Theorem 1.3.10. *The subgroup $(\mathbb{Q}_p^*)^2$ is open in $\mathbb{Q}_p^*$.*

Proof. Let $x \in \mathbb{Q}_p^*$ be a square, from Theorem 1.3.8 $x = p^{2n}y^2$ with $n \in \mathbb{Z}$ and $y \in \mathbb{Z}_p^*$. Let $z \in \mathbb{Q}_p$ be such that $|z - x| < p^{-2n}$, since $|z| = |z - x + x| = max\{|z - x|, |x|\}$ we have $|z|_p = |x|_p = p^{-2n}$ and hence $z = p^{2n}w$ for some $w \in \mathbb{Z}_p^*$. Then we have

$$|z - x| = p^{-2n}|w - y^2| < 2^{-2n} \tag{1.37}$$

from which $|w - y^2| < 1$. This means that $w - y^2 \equiv 0 \pmod{p}$. Using 1.3.7 we have that w is also a square of an element in $\mathbb{Z}_p^*$.

□

Remark 1.3.11. Theorem 1.3.10 does not require $p \neq 2$, indeed it uses only the first statement of Theorem 1.3.8.

Since in Theorem 1.3.7 we use that $p \nmid 2\alpha_1$, we need to treat separately the case in which $p = 2$. For this reason we state a stronger version of Hensel's Lemma followed by the classification of 2-adic squares. ([Cas86, Chapter IV, Section 3])

Theorem 1.3.12. ***(General Hensel's Lemma)***
Let $\mathbb{K}$ be a field complete with respect to a non archimedean absolute $|.|$ value, and A the ring of elements with absolute value lower than or equal to 1 (in particular we

are interested in $\mathbb{Q}_p$ and $\mathbb{Z}_p$).
Let f(x) be a polynomial in $A[x]$, and let $a_0 \in A$ satisfy

$$|f(a_0)| < |f'(a_0)|^2. \tag{1.38}$$

Then there exists an element $a \in A$ such that f(a)=0.

Proof. The proof works in a similar way to the one we have seen.
Again we are aiming to find a Cauchy sequence converging to our solution. We do so by choosing $a_1 = a_0 + b_0$ with b_0 the element satisfying $f(a_0) + b_0 f'(a_0) = 0$. b_0 exists because $\mathbb{K}$ is a field and it is in A because $f(a_0)$ and $f'(a_0)$ are in A and using (1.38).
We iterate this procedure to reach the result.

□

Theorem 1.3.13. *Let $b \in \mathbb{Z}_2^*$. Then b is a square if and only if $b \equiv 1 \pmod{8}$. The quotient group $\mathbb{Q}_2^*/(\mathbb{Q}_2^*)^2$ has order 8 and a complete set of representatives is* $\{1, -1, 5, -5, 2, -2, 10, -10\}$.

Proof. $\boxed{\Rightarrow}$ If b is a square then $b = a^2$ for some unit a. Since a is a unit, $2 \nmid a$ hence if we use the representation $b_0 + b_1 p + ... + b_n p^n ...$ of p-adic integers that we can find from Theorem 1.3.3 taking $b_i = (a_i - a_{i-1})/p^{i-1}$ and $b_0 = a_0$ we can rewrite the statement in the following form:
given $a = 1 + 2a_1 ... 2^n a_n ...$, $b = a^2 = 1 + 0 + 0 + 2^3 b_3 + ... + 2^n b_n ....$ This is true because $b_1 = a_0 a_1 + a_1 a_0 = 2a_1$ and $b_2 = a_1 a_0 + a_1^2 + a_2 a_0 + a_0 a_2 = 2a_2 + a_1 + a_1^2 = 2(a_2 + a_1)$ since $a_i \in \{0, 1\}$ for all i.
$\boxed{\Leftarrow}$ If $b \equiv 1 \pmod{8}$, b is a unit so $|b|_2$=1. Consider the polynomial $f(x) = x^2 - b$. Then $f(1) = 1 - b$ and $f'(x) = 2x \Rightarrow |f'(1)|_2^2 = |2|_2^2 = (1/2)^2$. if $|f(1)|_2 \leq max\{1, |b|_2\} \geq 1/4$ we can apply General Hensel's Lemma, from which we have the proof. This happens whenever $8 \mid (1 - b)$ hence whenever $b \equiv 1 \pmod{8}$.
For the second statement we recall the fact that for all x in $\mathbb{Q}_2$, $x = 2^i u$ for some i in $\mathbb{Z}$ and u in $\mathbb{Z}_2^*$. Then x is a square if and only if i is even and u is a square. There are four equivalence classes of units up to addition of a square. Indeed any unit can be congruent to 1,-5,5,-1 (mod 8). In addition we can choose an even or odd power for 2, hence 2 is also a generator.

□

1.4 Hilbert symbol

In this section $\mathbb{K}$ will designate either the field $\mathbb{R}$ or $\mathbb{Q}_p$.
We call V the set of all prime numbers and infinity.

The purpose behind introducing the Hilbert symbol will be clear in Chapter 3 when we talk about invariants for quadratic forms over the p-adic fields.
In order to prove some essential properties of the Hilbert symbol we will first introduce the Legendre symbol and the reciprocity law. ([Ser95, Chapter 1, Section 3.3])

Definition 1.4.1. *For any prime number p and an integer a coprime to p, we define the* ***Legendre symbol*** $\left(\frac{a}{p}\right)$ *in the following way*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \textit{if } a \textit{ is a square in } \mathbb{Z}/p\mathbb{Z} \\ -1 & \textit{otherwise} \end{cases} \tag{1.39}$$

Remark 1.4.2. The product $a \cdot b$, with $a, b \in (\mathbb{Z}/p\mathbb{Z})^*$, is a quadratic residue if and only if a and b are both squares or both non squares. This is due to the fact that $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group. Hence we have the following property:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \tag{1.40}$$

Example 3. Let us consider the group $(\mathbb{Z}/7\mathbb{Z})^*$. This is cyclic generated by 3 (it is easy to see that 3 has indeed order 6). It follows from Example 2 that the Legendre symbol $\left(\frac{2}{7}\right) = 1$, indeed $2 \equiv_7 3^2$. Besides, any other integer $z \in \mathbb{Z}$ is congruent to 3^α modulo 7, for some $\alpha = \{1, .., 6\}$. Hence $z \cdot 2 = 3^\alpha \cdot 3^2 = 3^{\alpha+2}$ is a square if and only if $\alpha + 2 \equiv 0$ modulo 2, i.e. if and only if α is even.

Theorem 1.4.3. ***(Quadratic Reciprocity Law)***
Let p be an odd prime number. If q is an odd prime number other than p, we have

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right). \tag{1.41}$$

Proof. We will omit this proof that can be found in [Ser95, Chapter 1, Section 3.3]. □

Definition 1.4.4. *For $a, b \in \mathbb{K}^*$ we define:*

$$\begin{cases} (a, b) = 1 & \textit{if } z^2 - ax^2 - by^2 = 0 \textit{ has a non zero solution in } \mathbb{K}^3 \\ (a, b) = -1 & \textit{otherwise.} \end{cases} \tag{1.42}$$

The number $(a, b) = \pm 1$ is called the ***Hilbert symbol*** *of a and b and defines a map*

$$(.\,,.) : \mathbb{K}^*/\mathbb{K}^{*2} \times \mathbb{K}^*/\mathbb{K}^{*2} \longrightarrow \{-1, 1\}. \tag{1.43}$$

Definition 1.4.5. *Let $E/\mathbb{K}$ be a field extension in which E is finite-dimensional. If u is in E, then the multiplication $\Gamma_u : E \to E$, given by $\Gamma_u : y \mapsto uy$, is a $\mathbb{K}$-linear map. If $\{e_1, ..., e_n\}$ is a basis of E, then Γ_u is represented by a matrix $A = [a_{i.j}]$ with entries in $\mathbb{K}$. We define the* ***field norm*** *of u to be: $N(u) = det(\Gamma_u)$.*
This definition does not depend on the choice of the basis.([Rot02, Chapter XI, Section 2])

Example 4. If E=$\mathbb{K}(\sqrt{d})$ is a quadratic field, then a basis for E/$\mathbb{K}$ is $B = \{1, \sqrt{d}\}$. If $u = a + b\sqrt{d}$, then the matrix of Γ_u, with respect to B, is: $\begin{bmatrix} a & bd \\ b & a \end{bmatrix}$ hence $N(u) = a^2 - db^2$.

Theorem 1.4.6. *Let a,b $\in \mathbb{K}^*$ and $\mathbb{K}_b = \mathbb{K}(\sqrt{b})$ the field obtained by extending $\mathbb{K}$ with a square root of b.*
In order to have $(a, b) = 1$ it is necessary and sufficient that a belongs to the group of the (field) norms of the elements in $\mathbb{K}_b^*$. We will indicate this group by $N\mathbb{K}_b^*$.

Proof. If b is a square of an element c in $\mathbb{K}^*$, the equation $Z^2 - aX^2 - bY^2$ has $(c, 0, 1)$ as a solution hence $(a, b) = 1$. The theorem follows because $\mathbb{K}_b = \mathbb{K}$ and $N\mathbb{K}_b^* = \mathbb{K}^*$.
If b is not a square then $\mathbb{K}_b$ is a quadratic field over $\mathbb{K}$. If $a \in N\mathbb{K}_b^*$ then there exist z, y such that $a = z^2 - by^2$ so that the quadratic form $Z^2 - aX^2 - bY^2$ has a non zero root $(z, 1, y)$, hence $(a, b) = 1$.
Conversely if $(a, b) = 1$, the polynomial $Z^2 - aX^2 - bY^2$ has a zero $(z, x, y) \neq (0, 0, 0)$; since b is not a square $x \neq 0$. We conclude that a is the norm of the element $\frac{z}{x} + \beta\frac{y}{x}$. □

Theorem 1.4.7. ***(Properties of the Hilbert symbol)***
The following properties hold:
i) $(a, b) = (b, a)$ and $(a, c^2) = 1$;
ii) $(a, -a) = 1$ and $(a, 1 - a) = 1$;
iii) $(a, b) = 1 \Rightarrow (aa', b) = (a', b)$;
iv) $(a, b) = (a, -ab) = (a, (1 - a)b)$.

Proof. $\boxed{i)}$ If $Z^2 - aX^2 - bY^2$ has a non zero solution (h, i, j) then (h, j, i) is a solution of $Z^2 - bX^2 - aY^2$. Given $Z^2 - aX^2 - c^2Y^2$, $(h, 0, h/c)$ is a solution for every h in the field.
$\boxed{ii)}$ Similarly given $Z^2 - aX^2 + aY^2$, $(0, j, j)$ is solution for every j in the field. The second equality is proved by observing that for $Z^2 - aX^2 - (1 - a)Y^2$, (h, h, h) is a solution for every h in the field.

$\boxed{iii)}$ If $Z^2 - aX^2 - bY^2$ has a non zero solution then, by Theorem 1.4.6, a is an element of the group $N\mathbb{K}_b^*$, we then have

$$a' \in N\mathbb{K}_b^* \Longleftrightarrow aa' \in N\mathbb{K}_b^* \tag{1.44}$$

$\boxed{iv)}$ is a consequence of $ii), iii)$. Indeed, from $ii)$ $(a, -a) = 1$, $\overbrace{\Longrightarrow}^{\text{from } iii)}$ $(a, -ab) = (a, b)$. One can use the same argument for the second equality.

□

Theorem 1.4.8. ***(Hilbert Symbol in terms of Legendre Symbol)***
In $\mathbb{Q}_p$ for a given prime p, if we write $a = p^\alpha u$ and $b = p^\beta v$, where u and v are p-adic units and α, β are integers, then

$$(a,b)_p = \begin{cases} (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha & \text{if } p \neq 2 \\ (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)} & \text{if } p = 2 \end{cases} \tag{1.45}$$

where $\varepsilon(u) = \frac{u-1}{2}$ and $\omega(u) = \frac{u^2-1}{8}$.
Note that by definition of the Hilbert symbol, $(a, b)_\infty = 1$ if $a > 0$ or $b > 0$; $(a, b)_\infty = -1$ if $a < 0$ and $b < 0$.

Proof. We will omit the proof of this result because it would require to state many other results that are not useful to our purpose. The complete proof can be found in [Ser95, Chapter III, Section 1.2].

□

Remark 1.4.9. By bilinearity of the Hilbert symbol we mean the following properties:

$$(a^2, b) = (a, b)^2 \quad \text{and} \quad (aa', b) = (a, b)(a', b) \tag{1.46}$$

.

Theorem 1.4.10. *Hilbert symbol is bilinear and non-degenerate over the $\mathbb{F}_2$-vector space $\mathbb{K}^*/\mathbb{K}^{*2}$.*

Proof. Let $a = p^\alpha u$, $a' = p^{\alpha'} u'$, $b = p^\beta v$, with α, α' and β in $\mathbb{Z}$ and u, u' and v are p-adic units. Due to Theorem 1.4.8 we have two cases:
$\boxed{a)\ p \neq 2}$.

$$\begin{aligned} (aa', b) &= (-1)^{(\alpha+\alpha')\beta\varepsilon(p)} \left(\frac{uu'}{p}\right)^\beta \left(\frac{v}{p}\right)^{(\alpha+\alpha')} \\ &= (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha (-1)^{\alpha'\beta\varepsilon(p)} \left(\frac{u'}{p}\right)^\beta \left(\frac{v}{p}\right)^{\alpha'} \\ &= (a, b)(a', b) \end{aligned} \tag{1.47}$$

In order to prove that the Hilbert symbol is non-degenerate it is sufficient to find, for all $a \in \mathbb{K}^*/\mathbb{K}^{*2} \setminus \{1\}$, an element b such that $(a, b) = -1$. From Theorem 1.3.8 a can be p, c or cp, with c not a square modulo p. In each of these cases we can choose $b = c, p$ and c respectively. For example, from (1.45), $(c, p) = (-1)^{\alpha\beta\varepsilon(p)}\left(\frac{u}{p}\right)^{\beta}\left(\frac{v}{p}\right)^{\alpha}$ with $\alpha = 0$, $\beta = 1$, $u = c$ and $v = 1$; moreover, since c is not a square modulo p, $\left(\frac{c}{p}\right) = -1$.

$\boxed{\text{b) } p = 2}$ Notice that, $\frac{uu'-1}{2}\left(=\frac{u(u'-1)+u-1}{2}\right)$ and $\frac{u-1}{2}+\frac{u'-1}{2}$ have the same parity (remember that u and u' are odd for hypothesis). For this reason they are interchangeable in the exponent of (-1).

Similarly for $\frac{(uu')^2-1}{8}\left(=\frac{u^2(u'^2-1)+u^2-1}{8}\right)$ and $\frac{u^2-1}{8}+\frac{u'^2-1}{8}$. Hence we can write

$$\begin{aligned}(aa', b) &= (-1)^{\varepsilon(uu')\varepsilon(v)+(\alpha+\alpha')\omega(v)+\beta\omega(uu')} \qquad (1.48)\\ &= (-1)^{(\varepsilon(u)+\varepsilon(u'))\varepsilon(v)+(\alpha+\alpha')\omega(v)+\beta(\omega(u)+\omega(u'))}\\ &= (a, b)(a', b).\end{aligned}$$

In order to prove that the Hilbert symbol is non-degenerate we recall that, from Theorem 1.3.13, a complete set of representatives for $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ is $\{1, -1, 5, -5, 2, -2, 10, -10\}$. Using this and (1.45) for every element a in this set different from 1 we can find an element b such that $(a, b) = -1$. □

Theorem 1.4.11. ***(Hilbert))***
If $a, b \in \mathbb{Q}^*$ we have that $(a, b)_v = 1$ for almost every v in V, and

$$\prod_{v \in V}(a, b)_v = 1. \qquad (1.49)$$

Proof. Since Hilbert Symbol is bilinear it is sufficient to show the result for a and b primes or equal to -1. In each case Theorem 1.4.8 allows us to compute (a, b).

$\boxed{1}$ $a = -1$, $b = -1$. We have

$$(-1, -1)_\infty = (-1, -1)_2 = -1 \quad \text{and} \quad (-1, -1)_p = 1 \; p \neq 2, \infty$$

$\boxed{2}$ $a = -1$, $b = l$ with l a prime number.
If $l = 2$ we have

$$(-1, 2)_v = 1 \quad \text{for all } v \in V;$$

if $l \neq 2$ we find

$$\begin{aligned}(-1, l)_v &= 1 \quad \text{if } v \neq 2, l\\ \text{and} \quad (-1, l)_2 &= (-1, l)_l = (-1)^{\varepsilon(l)}.\end{aligned}$$

$\boxed{3}$ $a = l, b = l'$ for some primes l and l'.
If $l = l'$

$$(l, l)_v = (-1, l)_v$$

so we go back to case 2.
If $l \neq l'$ and $l' = 2$ we have

$$\begin{gathered}(l, 2)_v = 1 \quad \text{for } v \neq 2, l \\ \text{and} \quad (l, 2)_2 = (-1)^{\omega(l)}, \quad (l, 2)_l = \left(\tfrac{2}{l}\right) = (-1)^{\omega(l)}.\end{gathered}$$

If $2 \neq l \neq l' \neq 2$ we have

$$\begin{gathered}(l, l')_v = 1 \quad \text{for } v \neq 2, l, l' \\ \text{and} \quad (l, l')_2 = (-1)^{\varepsilon(l)\varepsilon(l')}, \quad (l, 2)_l = \left(\tfrac{l'}{l}\right), \quad (l, l')_{l'} = \left(\tfrac{l'}{l}\right)\end{gathered}$$

By Theorem 1.4.3 we have

$$\left(\frac{l}{l'}\right)\left(\frac{l'}{l}\right) = (-1)^{\varepsilon(l)\varepsilon(l')}$$

The product is again 1. □

Lemma 1.4.12. ***(Chinese remainder theorem)***
Let $a_1, ..., a_n$ and $m_1, ..., m_n$ be integers such that m_i is coprime with m_j for all i, j. There exists an integer a such that $a \equiv a_i$ (mod m_i) for all i.

Proof. Let m be the product of the m_i. The Bezout theorem shows that the canonical homomorphism

$$\mathbb{Z}/m\mathbb{Z} \to \prod_{i=1}^{i=n} \mathbb{Z}/m_i\mathbb{Z} \tag{1.50}$$

is an isomorphism. □

Lemma 1.4.13. ***(Approximation theorem)***
Let S be a finite part of V. The image of $\mathbb{Q}$ in $\prod_{v \in S} \mathbb{Q}_v$ is dense in the product, where the topology is the product topology.

Proof. Even if it means enlarging we can suppose that

$$S = \{\infty, p_1, ..., p_n\} \tag{1.51}$$

where the p_i are distinct primes. We want to prove that $\mathbb{Q}$ is dense in $\mathbb{R} \times \mathbb{Q}_{p_1} \times ... \times \mathbb{Q}_{p_n}$. Let $(x_\infty, x_1, ..., x_n)$ be a point in this product; we want to show that it is adherent to $\mathbb{Q}$. Up to homothety of integer ratio, we can suppose $x_i \in \mathbb{Z}_{p_i}$ for all

$1 \leq i \leq n$. We need to prove that for all $\varepsilon > 0$, and all integers $N \geq 0$, there exists $x \in \mathbb{Q}$ such that:

$$|x - x_\infty| < \varepsilon \quad \textit{and} \quad v_{p_i}(x - x_i) \geq N \quad \textit{for } i = 1, ..., n. \tag{1.52}$$

Using Lemma 1.4.12 with $m_i = p_i^N$, there exists $x_0 \in \mathbb{Z}$ such that $x_0 \equiv x_i \pmod{p_i^N}$ for all i and hence $v_{p_i}(x_0 - x_i) \geq N$ for all i. We then choose a prime q different form p_i for all i. The rational numbers a/q^m with $a \in \mathbb{Z}$ and $m \geq 0$ are dense in $\mathbb{R}$. We can now choose an element $u = a/q^m$ such that:

$$|x_0 - x_\infty + up_1^N ... p_n^N| \leq \varepsilon \tag{1.53}$$

The number $x = x_0 + up_1^N ... p_n^N$ proves the lemma. □

Lemma 1.4.14. ***(Dirichlet theorem)***
If $a, m \geq 1$ are two coprime integers, there exist infinitely many primes p such that $p \equiv a$ (mod m).

Proof. We will omit the proof and it can be found in [Ser95, Chapter VI, Section 4]. □

Theorem 1.4.15. *Let $(a_i)_{i \in I}$ be a finite family of elements in $\mathbb{Q}^*$, and $(\varepsilon_{i,v})_{i \in I, v \in V}$ a family of numbers equal to ± 1. There exists an element $x \in \mathbb{Q}^*$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all i in I and v in V, if and only if, are verified the following:*
i) Almost all $\varepsilon_{i,v}$ are equal to 1.
ii) For all $i \in I$, $\prod_{v \in V} \varepsilon_{i,v} = 1$.
iii) For all $v \in V$, there exists $x_v \in \mathbb{Q}_v^*$ such that $(a_i, x_v)_v = \varepsilon_{i,v}$

Proof. The necessity of *i*) and *ii*) results from Theorem 1.4.11, that of *iii*) is trivial (we can choose $x_v = x$).
Let $(e_{i,v})$ be a family of numbers equal to ± 1 that satisfy conditions *i*), *ii*) and *iii*). Up to multiplication by a square of an integer, we can suppose that all the a_i are integers. Let S be the subset of V consisting of $\infty, 2$, and of all the prime factors of the integers a_i. Let T be the set of $v \in V$ such that exists $i \in I$ for which $\varepsilon_{i,v} = -1$. These two sets are finite.
We distinguish two cases:
$\boxed{a) \quad S \cap T = \emptyset}$. We set

$$a = \prod_{l \in T \setminus \{\infty\}} l \quad \textit{and} \quad m = 8 \prod_{l \in S \setminus \{2, \infty\}} l \tag{1.54}$$

Since $S \cap T = \emptyset$ a and m are coprime. From Lemma 1.4.14 there exists a prime number $p \equiv a$ (mod m) such that $p \notin S \cup T$. We want to show that the number

$x = ap$ satisfies the request, i.e $(a_i, x)_v = \varepsilon_{i,v}$ for all i, v.
If $v \in S$ we have $\varepsilon_{i,v} = 1$ since $S \cap T = \emptyset$, hence we need to verify that $(a_i, x)_v = 1$. If $v = \infty$ it is trivial since $x > 0$. If v is a prime, $x \equiv a^2 \pmod{m}$, from which (using Lemma 1.4.12) $x \equiv a^2 \pmod{8}$ and $x \equiv a^2 \pmod{v}$ if $v \neq 2$. Since x and a are two v-adic units x is a square in $\mathbb{Q}_v^*$ (Theorem 1.3.7), hence we have $(a_i, x)_v = 1$.
If $v \notin S$ then $a - i$ is a v-adic unit . If $v \neq 2$ from Theorem 1.4.8 we have

$$(a_i, b)_v = \big(\frac{a_i}{v}\big)^{v_v(b)} \quad for\ all\ b \in \mathbb{Q}_v^*. \tag{1.55}$$

If $l \notin T \cup \{p\}$, x is a v-adic unit where $v_v(x) = 0$, hence 1.55 shows that $(a_i, x)_v = 1$. Since $v \notin T$ we also have $\varepsilon_{v,i} = 1$.
If $v \in T$, we have $v_v(x) = 1$; from condition $iii)$ there exist $x_v \in \mathbb{Q}_v^*$ such that $(a_i, x_v)_v = \varepsilon_{i,v}$ for all $i \in I$. One of the $\varepsilon_{i,v} = -1$ $(v \in T)$ hence from 1.55 we must have $v_v(x_v) \equiv 1 \pmod{2}$. From this we have:

$$(a_i, x)_v = \big(\frac{a_i}{v}\big) = (a_i, x_v)_v = \varepsilon_{i,v} \quad for\ all\ i \in I. \tag{1.56}$$

The only case left is v=p. From Theorem 1.4.11 we have

$$\prod_{l \neq p} (a_i, x)_l = 1 \cdot (a_i, x)_p^{-1} = (a_i, x)_p. \tag{1.57}$$

This leads to

$$(a_i, x)_p = \prod_{l \neq p} (a_i, x)_l = \prod_{l \neq p} \varepsilon_{i,l} \underbrace{=}_{from\ ii)} \varepsilon_{i,p} \tag{1.58}$$

$\boxed{b)\quad S \cap T \neq \emptyset}$ From Theorem 1.3.10 we have that $(\mathbb{Q}_v^*)^2$ forms an open subgroup of $\mathbb{Q}_v^*$. From Lemma 1.4.13 there exists $x' \in \mathbb{Q}^*$, such that x'/x_v is a square in $\mathbb{Q}_v^*$ for all v is S.[1] This x verifies $[x] = [x_v]$ in $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$). In particular we have

$$(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v} \quad for\ all\ v \in S. \tag{1.59}$$

We set $\mu_{i,v} = \varepsilon_{i,v}(a_i, x')_v \in \{-1, 1\}$; this family verifies $i), ii)$ and $iii)$, and $\mu_{i,v} = 1$ for all $v \in S$. Defining T' as the set of v for which there exists an $i \in I$ that gives $\mu_{i,v} = -1$, we have that $S \cap T' = \emptyset$. From case $a)$ we have that there exists an element $y \in \mathbb{Q}^*$ such that $(a_i, y)_v = \mu_{i,v}$ for all $i \in I$ and all $v \in V$. If we set $x = yx'$, x satisfies the request. □

[1] To make explicit the way in which we use Lemma 1.4.13 we recall the fact that $\prod_{v \in S} \mathbb{Q}_v^{*2}$ is open in in $\prod_{v \in S} \mathbb{Q}_v$, hence $\prod_{v \in S} x_v \mathbb{Q}_v^{*2}$ is also open in the same product; since $\mathbb{Q}$ is dense in $\prod_{v \in S} \mathbb{Q}_v$ there exists an element $x \in \mathbb{Q}$ such that $x \in \prod_{v \in S} x_v \mathbb{Q}_v^{*2}$.

Chapter 2

Quadratic forms

This chapter contains general definitions and results that will be useful to reach the classification of quadratic forms over $\mathbb{Q}_p$ and $\mathbb{Q}$.

2.1 Definitions

Definition 2.1.1. *Given a module V over a commutative ring A, we call* ***quadratic form*** *a map $Q : V \longrightarrow A$ that satisfies the following properties:*

1. *$Q(ax) = a^2Q(x)$ for $a \in A$ and $x \in V$;*

2. *the map $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$ is a bilinear form.*

The pair (Q, V) is called a quadratic module.

Since we are interested in the case in which V is a finite dimensional vector space over a field $\mathbb{K}$ we will always assume that $\mathbb{K}$ is a field of characteristic $\neq 2$.

Remark 2.1.2. The product:

$$x \cdot y = 1/2[Q(x + y) - Q(x) - Q(y)] \tag{2.1}$$

defines a symmetric bilinear form associated with Q. (Here we see why the characteristic of the field is asked to be $\neq 2$.) This definition establishes a one-to-one correspondence between quadratic forms and bilinear symmetric forms. Indeed if $Q(x)$ is quadratic, (2.1) defines a symmetric bilinear form. On the other hand, if $\cdot$ defines a symmetric bilinear product then, $Q(x) = x \cdot x$ uniquely defines a quadratic form.

Definition 2.1.3. *Given two quadratic modules (Q, V) and (Q', V') we call **morphism** of (Q, V) in (Q', V') every linear map $f : V \longrightarrow V'$ such that $Q' \circ f = Q$*

Definition 2.1.4. *Let (V, Q) be a quadratic module over a field $\mathbb{K}$. Two elements x,y of V are called **orthogonal** if $x \cdot y$=0. We denote by $H^{\perp}$ the set of orthogonal elements to a subset H of V. $V^{\perp}$ is called the **radical** of V. Its codimension in V is called the rank of Q. If $V^{\perp}$=0 then we say that Q is non-degenerate.*

Definition 2.1.5. *Given a basis $\{e_i\}$ of V, the matrix $M = (a_{ij})$ where $a_{ij} = e_i \cdot e_j$ is symmetric. Moreover for $x = \sum x_i e_i$, $Q(x) = \sum a_{ij} x_i x_j$.*
This gives a way of representing Q as a homogeneous second degree polynomial $f = \sum_{i,j} a_{i,j} X_i X_j$. The polynomial f depends on the choice of the basis.

Remark 2.1.6. Through a change of bases X, the matrix A' of Q with respect to the new basis is $A' = X^T AX$. In particular using Binet theorem we find that

$$det(A') = det(A)det(X)^2. \tag{2.2}$$

This shows that the "determinant of Q" is defined up to multiplication by an element of $\mathbb{K}^{*2}$.

Definition 2.1.7. *We call the determinant of Q up to multiplication by elements of $\mathbb{K}^{*2}$, the **discriminant** of Q and we denote it by $d(Q)$.*
From the definition of $d(Q)$ and by Remark 2.1.6 we immediately have that $d(Q)$ is invariant under change of basis in V.

Remark 2.1.8. If Q is non-degenerate then $d(Q) \in \mathbb{K}^*/\mathbb{K}^{*2}$ otherwise $d(Q) = 0$. Since in $\mathbb{C}$ all elements are squares $\mathbb{C}^*/\mathbb{C}^{*2} = \{[1]\}$. Using the same argument, when $\mathbb{K} = \mathbb{R}$, since all positive numbers are squares, the quotient has two equivalence classes [1] and [-1].

Example 5. Let us consider the quadratic forms $f = X^2 + 2Y^2$ and $g = X^2 + Y^2$. By Definition 2.1.5, the symmetric matrices associated to f and g are

$$M_f = \begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix} \quad and \quad M_g = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2.3}$$

respectively. The determinants of these matrices are $det(M_f) = 2$ and $det(M_g) = 1$. By Remark 2.1.6 and Definition 2.1.7, if $det(M_f)$ is not congruent to $det(M_g)$ modulo

$\mathbb{K}^{2*}$ (i.e. if $d(f) \neq f(g)$ in $\mathbb{K}$), the quadratic modules $(\mathbb{K}^2, f)$ and $(\mathbb{K}^2, g)$ are not isomorphic. In particular, by Example 2, $(\mathbb{Q}_5^2, f)$ and $(\mathbb{Q}_5^2, g)$ are not isomorphic.

Definition 2.1.9. *A basis $(e_1, ..., e_n)$ of a quadratic module (V, Q) is called an* ***orthogonal basis*** *if its elements are two by two orthogonal.*
In this case V=Span$\{e_1\}\hat{\oplus}...\hat{\oplus}$Span$\{e_n\}$, where $\hat{\oplus}$ denotes the direct orthogonal sum, and hence the matrix associated Q with respect to this basis is diagonal:

$$\begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \\ 0 & 0 & \cdots & a_n \end{bmatrix}. \tag{2.4}$$

If x=$x_1e_1 + ... + x_ne_n$, then Q(x)=$a_1x_1^2 + ... + a_nx_n^2$ and the polynomial f associated with Q with respect to this basis is $f = a_1X_1^2 + ... + a_nX_n^2$.

Theorem 2.1.10. *All quadratic modules (V, Q) have an orthogonal basis.*

Proof. We prove this by recurrence on $dim(V) = n$, the case $n = 1$ is trivial.
If $Q(x) = 0$ for all x in Q, then all bases are orthogonal.
If there exists in V an element e_1 such that $Q(e_1) \neq 0$ then the orthogonal H of *Span*$\{e_1\}$ is an hyperplane of V and since the restriction of Q to *Span*$\{e_1\}$is non-degenerate, we have $V = Span\{e_1\}\hat{\oplus}H$. By the recursive hypothesis, H has an orthogonal basis $(e_2, ..., e_n)$ and so $(e_1, .., e_n)$ proves the theorem. □

Definition 2.1.11. *An element x of a quadratic module (V,Q) is called* ***isotropic*** *if $x \neq 0$ and $Q(x) = 0$.*

Lemma 2.1.12. *Let (V, Q), be a quadratic non-degenerate module over $\mathbb{K}$ and* **e** *= $\{e_1...e_n\}$ and* ***e'*** *= $\{e'_1...e'_n\}$ two orthogonal bases of V. Then there exists $x \in \mathbb{K}$ such that $e_x = e'_1 + xe'_2$ is not isotropic and the plan $P =$ Span$\{e_1, e_x\}$ is non-degenerate.*

Proof. We have $e_x \cdot e_x = e'_1 \cdot e'_1 + x^2(e'_2 \cdot e'_2)$, hence we must choose $x^2 \neq -(e'_1 \cdot e'_1)/(e'_2 \cdot e'_2)$. Moreover in order to have $Q_{|P}$ non degenerate it is necessary and sufficient to have

$$(e_1 \cdot e_1)(e_x \cdot e_x) - (e_1 \cdot e_x)^2 \neq 0 \tag{2.5}$$

If we write this product explicitly and use hypothesis *iii*) the first member becomes $-2x(e_1 \cdot e'_1)(e_1 \cdot e'_2)$. From *iii*) also follows that $(e_1 \cdot e'_1) \neq 0$ and $(e_1 \cdot e'_2) \neq 0$ hence e_x verifies the conditions of the lemma if and only if $x \neq 0$ and $x^2 \neq -(e'_1 \cdot e'_1)/(e'_2 \cdot e'_2)$. We have at most three unacceptable values for x. Since $\mathbb{K}$ has at least four elements the lemma holds. If $\mathbb{K} = \mathbb{F}_3$ all non null squares are equal to 1, we can choose $x = 1$. □

Theorem 2.1.13. *Let (V, Q) be a quadratic non-degenerate module over $\mathbb{K}$ with $dimV = n \geq 3$. If $\boldsymbol{e}$=$\{e_1...e_n\}$ and $\boldsymbol{e}' = \{e'_1...e'_n\}$ are two orthogonal bases of V, then there exists a finite sequence $\boldsymbol{e}^{(0)}, \boldsymbol{e}^{(1)}, ..., \boldsymbol{e}^{(m)}$ of orthogonal bases of V such that $\boldsymbol{e}^{(0)} = \boldsymbol{e}$, $\boldsymbol{e}^{(m)} = \boldsymbol{e}'$, and $\boldsymbol{e}^{(i)}$ has one element in common with $\boldsymbol{e}^{(i+1)}$ for all $0 \leq i < m$ (this property is called contiguity).*

Proof. We distinguish three cases:
i)

$$(e_1 \cdot e_1)(e'_1 \cdot e'_1) - (e_1 \cdot e'_1)^2 \neq 0. \tag{2.6}$$

In particular e_1 and e'_1 are not proportional. Hence $P = Span\{e_1, e'_1\}$ is a plane. For this reason we can find two vectors $\varepsilon_2 \perp e_1$ and $\varepsilon'_2 \perp e'_1$ such that

$$P = Span\{e_1, \varepsilon_2\} \text{ and } P = Span\{e'_1, \varepsilon'_2\}. \tag{2.7}$$

Moreover from (2.6) we have that $Q_{|P}$ is non-degenerate, hence we can decompose V as the direct sum of P and its orthogonal H. Let $\{e''_3, ..., e''_n\}$ be an orthogonal basis of $H = P^{\perp}$. Then the following sequence satisfies the request:

$$\mathbf{e} \rightarrow \{e_1, \varepsilon_2, e''_3, ..., e''_n\} \rightarrow \{e'_1, \varepsilon'_2, e''_3, ..., e''_n\} \rightarrow \mathbf{e}' \tag{2.8}$$

ii)

$$(e_1 \cdot e_1)(e'_2 \cdot e'_2) - (e_1 \cdot e'_2)^2 \neq 0. \tag{2.9}$$

We proceed as in case *i)* by replacing e'_1 with e'_2.
iii)

$$(e_1 \cdot e_1)(e'_i \cdot e'_i) - (e_1 \cdot e'_i)^2 = 0 \quad \text{ for } i = 1, 2. \tag{2.10}$$

Using Lemma 2.1.12 we have an e_x for which we can find e''_2 such that (e_x, e''_2) is an orthogonal basis of $Span\{e'_1, e'_2\}$. If we consider

$$\mathbf{e}'' = \{e_x, e''_2, e'_3, ..., e'_n\} \tag{2.11}$$

$\mathbf{e}'$ and $\mathbf{e}''$ are contiguous and using *i)*, since $Span\{e_x, e_1\}$ is non-degenerate, we can link $\mathbf{e}$ and $\mathbf{e}''$ with a chain of contiguous bases. □

Definition 2.1.14. *We call* ***hyperbolic plane*** *every quadratic module that has a bases consisting of two elements $\{x, y\}$ such that x, y are isotropic and $x \cdot y \neq 0$. We can suppose $x \cdot y = 1$ hence the matrix of the quadratic form with respect to*

$\{x, y\}$ is $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ and its discriminant is -1.

Theorem 2.1.15. *Let $x \neq 0$ be an isotropic element of a quadratic non-degenerate module (V, Q). Then there exists a subspace U of V that contains x and is hyperbolic.*

Proof. Since V is non-degenerate, there exists an element $z \in V$ such that $x \cdot z = 1$. The element $y = 2z - (z \cdot z)x$ is isotropic and $x \cdot y = 2$. The subspace $U = Span\{x, y\}$ satisfies the request. □

Lemma 2.1.16. *Let (V, Q) and (V', Q') be two isomorphic non-degenerate quadratic modules. If U is degenerate subspace of V, and s is an injective morphism from U to V', then we can extend s to an injective morphism $s_1 : U_1 \to V'$ where U is an hyperplane of U_1.*

Proof. Let x be a non-zero element of the radical of the form restricted to U, and $l : U \to \mathbb{K}$ a linear map where $l(x) = 1$. Since V is non-degenerate there exists $y \in V$ such that $l(u) = u \cdot y$ for all $u \in U$. Moreover we can suppose $y \cdot y = 0$ by possibly replacing y with $y - (\frac{1}{2}y \cdot y)x$. The subspace $U_1 = U \oplus Span\{y\}$ contains U as an hyperplane. With the same construction for $U' = s(U)$, with $x' = s(x)$ and $l' = l \circ s^{-1}$, we have $U_1' = U' \oplus Span\{y'\}$. Let $s_1 : U_1 \to U_1'$ be the linear map such that $s_{1|U} = s_{|U}$ and that maps $y \mapsto y'$. Then s_1 satisfies the request. □

Theorem 2.1.17. ***(Witt Theorem)***
If (V, Q) and (V', Q') are isomorphic and non-degenerate, every injective morphism

$$s : U \to V' \tag{2.12}$$

of a subspace U of V to V', can be extended to an isomorphism betwwen V and V'.

Proof. Since V and V' are isomorphic we can suppose $V = V'$. Using Lemma 2.1.16, we can suppose U non-degenerate. We argue by induction on $dim\, U$.
If $dim\, U = 1$, U is generated by a non-isotropic element x; if $y = s(x)$, we have $y \cdot y = x \cdot x$. We can choose $\varepsilon = \pm 1$ such that $x + \varepsilon y$ is not isotropic (if this is not possible we would have $2x \cdot x + 2x \cdot y = 0 = 2x \cdot x - 2x \cdot y$ from which $x \cdot x = 0$). We choose such an ε and let H be the hyperplane orthogonal to $z = x + \varepsilon y$. we have $V = Span\{z\}\hat{\oplus}H$. Let σ be the reflection with respect to H. Since $x - \varepsilon y \in H$, we have

$$\sigma(x - \varepsilon y) = x - \varepsilon y \quad \textit{and} \quad \sigma(x + \varepsilon y) = -x - \varepsilon y \tag{2.13}$$

hence $\sigma(x) = -\varepsilon y$; therfore, the automorphism $-\varepsilon\sigma$ extends s.
If $dim\ U > 1$, we decompose $U = U_1 \hat{\oplus} U_2$ with $U_1, U_2 \neq 0$. By the recursive

hypothesis, the restriction s_1 of s to U_1 can be extended to an automorphism $\sigma_1 : V \to V$ with $\sigma_{1|U_1} = s_{|U_1}$. Up to replacing s with $\sigma_1^{-1} \circ s$, we can suppose that s is the identity over U_1. The morphism s hence sends U_2 to the orthogonal V_1 of U_1; by the recursive hypothesis, the restriction of s to U_2 can be extended to an automorphism σ_2 of V_1. The automorphism σ of V such that $\sigma_{|U_1} = Id_{U_1}$ and $\sigma_{|V_1} = \sigma_2$ proves the theorem. □

Corollary 2.1.18. *Two isomorphic subspaces of a non-degenerate quadratic module have isomorphic orthogonals.*

Proof. We extend the isomorphism over the two subspaces to an automorphism and consider the restriction of this map to the orthogonals. □

Definition 2.1.19. *Let*

$$f(X) = \sum_{i=1}^{n} a_{ii} X_i^2 + 2 \sum_{i<j} a_{ij} X_i X_j \tag{2.14}$$

be a quadratic form in n variables over $\mathbb{K}$. We set $a_{i,j} = a_{j,i}$ if $i > j$, so that the matrix $A = a_{i,j}$ is symmetric. The couple $(\mathbb{K}^n, f)$ is a quadratic module, called the quadratic module associated to f.

Definition 2.1.20. *Two quadratic forms f and f' are said to be equivalent if the associated quadratic modules are isomorphic. In this case we write $f \sim f'$. If A and A' are the matrices associated to f and f', then there exists an invertible matrix X such that $A' = X^T \cdot A \cdot X$.*

Definition 2.1.21. *A quadratic form in two variables is called* ***hyperbolic*** *if*

$$f \sim X_1 X_2 \sim X_1^2 - X_2^2. \tag{2.15}$$

Definition 2.1.22. *We say that a quadratic form f* ***represents*** *the element $a \in \mathbb{K}$ if there exists $x \in \mathbb{K}^n$, $x \neq 0$, such that $f(x) = a$.*

Given two quadratic forms f in n variables and g in m variables, we denote by $f \dot{+} g$ the quadratic form in $n + m$ variables defined by

$$f(X_1, ..., X_n) + g(X_{n+1}, ..., X_{n+m}). \tag{2.16}$$

Similarly we denote by $f \dot{-} g$ the subtraction of f and g.

Theorem 2.1.23. *Let f be a quadratic form in n variables that represents 0 and is not degenerate. Then $f \sim f_2 \dot{+} g$, where f_2 is hyperbolic and g is a quadratic form in $n - 2$ variables. Moreover, f represents all elements of $\mathbb{K}$.*

Proof. The result follows from Theorem 2.1.15. Indeed f represents 0 if and only if the quadratic module associated has a non zero isotropic element x. Hence there exists an hyperbolic subspace that contains x. The restriction of f to this subspace gives f_2. Moreover an hyperbolic form represents all elements of $\mathbb{K}$. In fact since its matrix is of the form $\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ up to a change of basis, for all $a \in \mathbb{K}$ $\left[\frac{a}{2}, 1\right]\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\begin{bmatrix}\frac{a}{2}\\ 1\end{bmatrix} =$ a □

Corollary 2.1.24. *Let $g = g(X_1, ..., X_{n-1})$ a quadratic non-degenerate form and $a \in \mathbb{K}^*$. The following properties are equivalent:*

i) g represents a;

ii) $g = h\dot{+}aZ^2$ where h is a form in n-2 variables;

iii) The form $f = g\dot{-}aZ^2$ represents 0.

Proof. $\boxed{i) \Rightarrow ii)}$ If g represents a there exists an element $x \neq 0$ such that $x \cdot x = a$. If $H = Span(x)^{\perp}$, $h = g_{|H}$ gives $ii)$.

$\boxed{ii) \Rightarrow i)}$ It is trivial with $x = (0, ..., 0, 1)$.

$\boxed{i) \Rightarrow iii)}$ It is trivial with vector $(x_1, ..., x_{n-1}, 1)$ where $g((x_1, ..., x_{n-1})) = a$.

$\boxed{iii) \Rightarrow i)}$ If f has a non trivial zero $(x_1, ..., x_{n-1}, z)$ then, if $z = 0$, $g((x_1, ..., x_{n-1})) = 0$. In this case from Theorem 2.1.23 we have that g represents all elements of $\mathbb{K}$. If $z \neq 0$, $g(\frac{1}{z}(x_1, ..., x_{n-1})) = a$. □

Corollary 2.1.25. *Let g and h be two non-degenerate quadratic forms of rank ≥ 1, and $f = g\dot{-}h$. The following properties are equivalent:*

i) f represents 0;

ii) there exists $a \in \mathbb{K}^*$ represented by g and h;

iii) there exists $a \in \mathbb{K}^*$ such that $g\dot{-}aZ^2$ and $h\dot{-}aZ^2$ represent 0.

Proof. $\boxed{i) \Rightarrow ii)}$ A non trivial zero of f can be written in the form (x, y), with $g(x) = h(y)$. If $g(x) = h(y) = a \neq 0$ $ii)$ is verified. If $a = 0$, at least one between g and h represents 0. Hence it represents all elements of $\mathbb{K}$ and in particular the elements represented by the other quadratic form.

$\boxed{ii) \Rightarrow i)}$ It is trivial.

$\boxed{ii) \Leftrightarrow iii)}$ Follows from Corollary 2.1.24.

□

Theorem 2.1.26. *Let $f = g\dot{+}h$ and $f' = g'\dot{+}h'$ be two non-degenerate quadratic forms. If $f \sim f'$ and $g \sim g'$ then $h \sim h'$.*

Proof. By Corollary 2.1.18, given two isomorphic modules and two isomorphic subspaces of these modules their orthogonals are still isomorphic. □

2.2 Quadratic forms over $\mathbb{C}$ and $\mathbb{R}$

I recall the main results giving a complete classification of quadratic forms over $\mathbb{C}$ and $\mathbb{R}$.

Remark 2.2.1. By Theorem 2.1.10 we can always find an orthogonal basis for a quadratic form. In particular, given a non-degenerate quadratic form f and an orthogonal basis $\mathbf{e} = \{e_1, ..., e_n\}$, if $a_i = e_i \cdot e_i$ is a square in the field $\mathbb{K}$ on which we are working, then the vector $\hat{e}_i = \frac{1}{\sqrt{a_i}} e_i$ is still orthogonal to all e_j, $j \neq i$ and $\hat{e}_i \cdot \hat{e}_i = 1$.

Theorem 2.2.2. *Two quadratic forms over $\mathbb{C}$ are equivalent if and only if they have the same rank.*

Proof. Since in $\mathbb{C}$ all elements are squares, by Remark 2.2.1, every non-degenerate quadratic form f in $\mathbb{C}$, is equivalent to $X_1^2 + X_2^2 + ... + X_n^2$ where n is the rank of f. □

Remark 2.2.3. Since in $\mathbb{R}$ all positive elements are squares, by Remark 2.2.1, every non-degenerate quadratic form f in $\mathbb{R}$, is equivalent to

$$X_1^2 + X_2^2 + ... + X_r^2 - Y_1^2 - Y_2^2 ... - Y_s^2 \tag{2.17}$$

where $r + s = n$ and n is the rank of f.

Definition 2.2.4. *Given a quadratic module (V, Q) with $V = \mathbb{R}$ or $\mathbb{C}$, a basis* $\boldsymbol{e} = \{e_1, ..., e_n\}$ *is called* ***orthonormal*** *when $Q(e_i) = \pm 1$ for all $i = 1, ..., n$ (i.e. $e_i \cdot e_i = \pm 1$).*

Theorem 2.2.5. ***(Sylvester)***
Let f be a quadratic form of rank n on $\mathbb{R}$. Then f is equivalent to the form

$$X_1^2 + ... + X_r^2 - Y_1^2 - ... - Y_s^2 \tag{2.18}$$

with $r + s = n$. The pair (r, s) is called the ***signature*** *of the quadratic form and is an invariant of the form.*

Proof. Proving the statement is equivalent to proving that, given two orthogonal bases $\mathbf{e} = \{e_1, ..., e_n\}$ and $\mathbf{e}' = \{e'_1, ..., e'_n\}$ of a non-degenerate quadratic module

(V, Q) with V vector space of dimension n over $\mathbb{R}$, it occurs that

$$\#\{e_i \in \mathbf{e},\ s.t.\ Q(e_i) > 0\} = \#\{e'_i \in \mathbf{e}',\ s.t.\ Q(e'_i) > 0\}$$

and

$$\#\{e_i \in \mathbf{e},\ s.t.\ Q(e_i) < 0\} = \#\{e'_i \in \mathbf{e}',\ s.t.\ Q(e'_i) < 0\}.$$

Let $V_{\mathbf{e},+} := Span\{e_i \in \mathbf{e},\ s.t.\ Q(e_i) > 0\}$, $V_{\mathbf{e}',+} := Span\{e'_i \in \mathbf{e}',\ s.t.\ Q(e'_i) > 0\}$, $V_{\mathbf{e},-} := Span\{e_i \in \mathbf{e},\ s.t.\ Q(e_i) < 0\}$ and $V_{\mathbf{e}',-} := Span\{e'_i \in \mathbf{e}',\ s.t.\ Q(e'_i) < 0\}$, since $\mathbf{e}$ and $\mathbf{e}'$ are two bases we have $V = V_{\mathbf{e},+} \oplus V_{\mathbf{e},-}$ and $V = V_{\mathbf{e}',+} \oplus V_{\mathbf{e}',-}$. Hence it is sufficient to show that $dimV_{\mathbf{e},+} = dimV_{\mathbf{e}',+}$.

Let us assume that $dimV_{\mathbf{e},+} > dimV_{\mathbf{e}',+}$ and hence $dimV_{\mathbf{e},-} < dimV_{\mathbf{e}',-}$. Using the Grassmann formula we find that

$$V_{\mathbf{e},+} \cap V_{\mathbf{e}',-} \neq \{0\}. \tag{2.19}$$

This gives an absurd since if there is a vector v such that $v \in V_{\mathbf{e},+} \cap V_{\mathbf{e}',-}$, then $v = \sum_{e_i \in V_{\mathbf{e},+}} x_i e_i$ and $v = \sum_{e'_j \in V_{\mathbf{e}',-}} y_j e'_j$. Hence

$$Q(v) = \textstyle\sum_{e_i \in V_{\mathbf{e},+}} x_i^2 (e_i \cdot e_i) > 0$$

and

$$Q(v) = \textstyle\sum_{e'_j \in V_{\mathbf{e}',-}} y_j^2 (e'_j \cdot e'_j) < 0.$$

This proves that $dimV_{\mathbf{e},+} = dimV_{\mathbf{e}',+}$. □

Corollary 2.2.6. *Two quadratic forms f and g over $\mathbb{R}$ are equivalent if and only if they have the same rank and signature.*

Chapter 3

Quadratic forms over $\mathbb{Q}$

For the content of this chapter we mainly refer to [Ser95, Chapter 4].

3.1 Quadratic forms over $\mathbb{Q}_p$

We consider non degenerate quadratic modules over $\mathbb{Q}_p$, with $\mathbb{Q}_p$ designing the p-adic field for some prime p. We will denote by (x, y) the Hilbert symbol for x and y in $\mathbb{Q}_p$.
Since we assume the quadratic form Q non degenerate, $d(Q)$ is an element in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.

In Chapter 2 we observed that given a quadratic form Q, its discriminant does not depend on the choice of the basis. Moreover, given an orthogonal basis $\mathbf{e} = \{e_1, ..., e_n\}$ and defining $a_i = e_i \cdot e_i$, we have

$$d(Q) = a_1 ... a_n \text{ (in } \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}). \tag{3.1}$$

This is an invariant of the quadratic form Q.

Definition 3.1.1. *Given a_i and $\mathbf{e}$ as above and denoting by (a_i, a_j) the Hilbert symbol of a_i and a_j, we define*

$$\varepsilon(\boldsymbol{e}) = \prod_{i<j} (a_i, a_j) \tag{3.2}$$

where the empty product is meant to be equal to 1.

From the definition of the Hilbert symbol it follows that $\varepsilon(\mathbf{e}) \in \{-1, 1\}$. Moreover ε is an invariant of the quadratic form Q. This is proved in the following theorem.

Theorem 3.1.2. *The number $\varepsilon(\boldsymbol{e})$ does not depend on the choice of* $\mathbf{e}$.

Proof. We argue by induction on the dimension of the vector space.
If n=1 $\varepsilon(\mathbf{e})$=1. If n=2 $\varepsilon(\mathbf{e})$=1 if and only if the quadratic form $Z^2 - a_1X^2 - a_2Y^2$ represents 0. By Corollary 2.1.24, this is equivalent to asking that $a_1X^2 + a_2Y^2$ represents 1. This condition does not depend on the choice of $\mathbf{e}$. For $n > 2$ we recall that by Theorem 2.1.13 it is sufficient to prove $\varepsilon(\mathbf{e}) = \varepsilon(\mathbf{e}')$ for $\mathbf{e}$, $\mathbf{e}'$ contiguous bases. We will also use the properties of the Hilbert symbol proved in Theorem 1.4.7 and Theorem 1.4.10.
Since the Hilbert symbol is symmetric we can assume $e_1 = e'_1$ and consequently $a_1 = a'_1$.
We can write

$$\varepsilon(\mathbf{e}) = (a_1, a_2...a_n) \prod_{2\leq i<j} (a_i, a_j) = (a_1, d(Q)a_1) \prod_{2\leq i<j} (a_i, a_j) \tag{3.3}$$

Similarly, since (.,.) is invariant under multiplication by elements in $\mathbb{Q}_p^{*2}$

$$\varepsilon(\mathbf{e}') = (a_1, d(Q)a_1) \prod_{2\leq i<j} (a'_i, a'_j) \tag{3.4}$$

We can now use the recursive hypothesis on $Span\{e_1\}^{\perp}$.

□

We can now write $\varepsilon(Q)$ instead of $\varepsilon(\mathbf{e})$ without ambiguity. We will call $\varepsilon(Q)$ the Hasse-Minkowski invariant.

Example 6. The quadratic forms $f = 2X^2 + 3Y^2$ and $g = 6X^2 + Y^2$ have the same discriminant $d = 6$. We want to see whether they have the same Hasse-Minkowski invariant in $\mathbb{Q}_2$. We have $\varepsilon_2(f) = (2,3)_2$ and, since $2 = 2^1 \cdot 1$ and $3 = 2^0 \cdot 3$, using the same notation as in Theorem 1.4.8, we have $\alpha = 1$, $\beta = 0$, $u = 1$ and $v = 3$ hence $\varepsilon(u) = 0 = \omega(u)$ and $\varepsilon(v) = 1 = \omega(v)$. By Theorem 1.4.8 we find out that $(2,3)_2 = (-1)^{0+1+0} = -1$.
Now, $\varepsilon_2(g) = (6,1)_2$ and arguing as above we obtain $\alpha = 1$, $\beta = 0$, $u = 3$ and $v = 1$ from which $\varepsilon(u) = 1 = \omega(u)$ and $\varepsilon(v) = 0 = \omega(v)$. Hence, by Theorem 1.4.8, $(6,1) = (-1)^{0+0+0} = 1$.
Since $\varepsilon_2(f) = -1 \neq 1 = \varepsilon_2(g)$ f and g are not equivalent in $\mathbb{Q}_2$.

Theorem 3.1.3. *The following statements hold:*

a) The number of elements of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is 2^r with $r = 2$ for $p \neq 2$ and $r = 3$ for $p = 2$.

b) If $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ and $\varepsilon = \pm 1$, let H_a^ε be the set of elements x such that (x,a)= ε. If $a = 1$, H_a^1 has 2^r elements and $H_a^{-1} = \emptyset$. If $a \neq 1$, H_a^ε has 2^{r-1} elements.

c) Let $a, a' \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ and $\varepsilon, \varepsilon' = \pm 1$. We suppose that $H_a^\varepsilon, H_{a'}^{\varepsilon'}$ are non empty. Then $H_a^\varepsilon \cap H_{a'}^{\varepsilon'} = \emptyset$ if and only if $a = a'$ and $\varepsilon = -\varepsilon'$.

Proof. $\boxed{\text{a)}}$ Is proved in Chapter 1, Theorem 1.3.8 and Theorem 1.3.13.
$\boxed{\text{b)}}$ If $a = 1$ $(x, 1) = 1$ for all x. If $a \neq 1$ by Theorem 1.4.10 the map $b \mapsto (a, b)$ is linear ($\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is a $\mathbb{F}_2$-vector space) and maps $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ to $\{-1, 1\}$. Its kernel is H_a^1 which must then be an hyperplane of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ and hence has 2^{r-1} elements. Its complement is H_a^{-1} and has $2^r - 2^{r-1} = 2^{r-1}(2-1)$ elements.
$\boxed{\text{c)}}$ From *b)* H_a^ε has either $0, 2^{r-1}$ or 2^r elements. If H_a^ε and $H_{a'}^{\varepsilon'}$ are non empty and disjoint the only possibility is that they are complementary and have 2^{r-1} elements each. In statement *b)* we saw that H_a^1 is an hyperplane and H_a^{-1} its complementary. Since H_a^1 and $H_{a'}^1$ are both subspaces their intersection is not empty. Hence ε and ε' are not both equal to 1. Moreover if they were both equal to -1 we would have $H_{a'}^{-1} = (H_a^{-1})^C = H_a^1$ which can not happen since the null vector is in H_a^1 and not in $H_{a'}^{-1}$. For this reason it must be $\varepsilon = -\varepsilon'$. We can assume $\varepsilon = -1$. Since $(H_{a'}^{\varepsilon'})^C = H_a^\varepsilon = (H_a^{-\varepsilon})^C$ it must be $H_{a'}^{\varepsilon'} = H_a^{-\varepsilon}$. This means that $H_a^1 = H_{a'}^1$; In other words

$$(x, a) = (x, a') \qquad \textit{for all } x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}. \tag{3.5}$$

By Theorem 1.4.10 the Hilbert symbol is non-degenerate hence (3.5) implies $a = a'$. □

Theorem 3.1.4. *Let f be a quadratic form of rank n, and d and ε its two invariants defined above. Then f represents 0 if and only if:*
i) n=2 and d=-1 (in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$);
ii) n=3 and (-1,-d)=ε;
iii) n=4 and $d \neq 1$ or if d=1 $\varepsilon = (-1, -1)$;
iv) n$\geq$5.

It is useful to state the following consequences of Theorem 3.1.4.

Corollary 3.1.5. *Let $x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. x is represented by f if and only if:*
i) n=1 and d=x;
ii) n=2 and (x,-d)=ε;
iii) n=3 and $d \neq -x$ or if d=-x $\varepsilon = (-1, -d)$;
iv) n$\geq$4.

Proof. of Theorem 3.1.4.
We write f in the form $f \sim a_1X_1^2 + ... + a_nX_n^2$
$\boxed{i)}$ The form represents 0 if and only if $-a_1/a_2$ is a square. But $-a_1/a_2 = -a_1a_2 = -d$ in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, so $-d = 1$ in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$.
$\boxed{ii)}$ f represents 0 if and only if $-a_3f \sim -a_3a_1X_1^2 - a_3a_2X_2^2 - X_3^2$ represents 0. By definition of the Hilbert symbol, this condition is equivalent to $(-a_3a_1, -a_3a_2) = 1$. Using the bilinearity of the symbol we can write

$$(-1,-1)(-1,a_3)(-1,a_2)(a_3,-1)(a_3,a_3)(a_3,a_2)(a_1,-1)(a_1,a_3)(a_1,a_2) = 1 \tag{3.6}$$

Since $(a_3,-1)$ appears twice we can delete it, moreover since $(a,b) = (a,-ab)$ $(a_3,a_3) = (-1,a_3)$

$$\underbrace{(-1,-1)\overbrace{(-1,a_2)(-1,a_3)(-1,a_1)}^{(-1,d)}}_{(-1,-d)}\overbrace{(a_1,a_2)(a_1,a_3)(a_2,a_3)}^{\varepsilon} = 1 \tag{3.7}$$

From which $(-1,-d) = \varepsilon$.
$\boxed{iii)}$ By Corollary 2.1.25 f represents 0 if and only if there exists $x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ represented both by

$$a_1X_1^2 + a_2X_2^2 \quad \text{and} \; - a_3X_3^2 - a_4X_4^2 \tag{3.8}$$

By Corollary 3.1.5 *ii)*, x has the previous property if and only if $(x, -a_1a_2) = (a_1, a_2)$ and $(x, -a_3a_4) = (-a_3, -a_4)$.
If we call A the class of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ defined by the first condition and B the one defined by the second, in order to have that f does not represent 0 we need to find that the intersection of A and B is empty. From Theorem 3.1.3, point *c)*, the two sets of solutions to the previous equalities are disjoint if and only if

$$a_1a_2 = a_3a_4 \text{ and } (a_1,a_2) = -(-a_3,-a_4) \tag{3.9}$$

The first condition is equivalent to $d = 1$ in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. If this is realized we have

$$\varepsilon = (a_1,a_2)(a_3,a_4)\underbrace{(a_1,a_3)(a_1,a_4)(a_2,a_3)(a_2,a_4)}_{=(a_3a_4,a_3a_4)} \tag{3.10}$$

$$\varepsilon = (a_1,a_2)(a_3,a_4)\underbrace{(-1,a_3a_4)}_{(x,x)=(-1,x)} \tag{3.11}$$

$$\varepsilon = (a_1, a_2)(a_3, -a_4)\underbrace{(-1, a_3)(-1, a_3)}_{=1}\underbrace{(-1, a_4)}_{=(-1,-1)(-1,-a_4)} \tag{3.12}$$

using condition two we can write

$$\varepsilon = -\underbrace{(a_1, a_2)(a_1, a_2)}_{=1}(-1, -1) \tag{3.13}$$

from which the thesis follows.

$\boxed{iv)}$ It is sufficient to prove the thesis for n=5. Indeed if every quadratic form of rank 5 represents 0 then given f of rank $n > 5$ we can write $f = g \dotplus h$ with $rank(g) = 5$ and $rank(h) = n - 5$. Hence if $g((x_1, ..., x_5)) = 0$ then $f((x_1, ..., x_5, 0, ..., 0)) = 0$.

Using Corollary 3.1.5 and Theorem 3.1.3, a form of rank ≥2 represents at least 2^{r-1} elements of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$, hence f represents at least an element a in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ different from d.

We can write $f \sim aX^2 + g$ with g quadratic form of rank 4. The discriminant of g is d/a hence it is different from 1. Using $iii)$ we have the result. □

3.2 Classification of quadratic forms over $\mathbb{Q}_p$

Theorem 3.2.1. ***(Equivalence)***

Given a prime p, two quadratic forms over $\mathbb{Q}_p$, are equivalent if and only if they have the same rank, discriminant and invariant ε.

Proof. We have already seen that equivalent forms have the same invariants $d(Q)$ and ε and the same rank.

The other way round can be proved by recurrence on the rank n of the forms.

By Corollary 3.1.5, if two quadratic forms have the same invariants then they represent the same elements of $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. Hence, given two quadratic forms, f and g, of rank n, we can find an element a represented by both the forms. This allows us to write

$$f \sim aZ^2 + f' \text{ and } g \sim aZ^2 + g' \tag{3.14}$$

where f' and g' are two forms of rank $n - 1$ and we have that

$$\begin{gathered} d(f') = d(f)a = d(g)a = d(g') \\ \text{and} \\ \varepsilon(f') = \varepsilon(f)(a, d(f')) = \varepsilon(g)(a, d(g')) = \varepsilon(g'). \end{gathered} \tag{3.15}$$

We can then apply the recursive hypothesis.

□

Example 7. In Example 5 we proved that the quadratic forms $f = X^2 + 2Y^2$ and $g = X^2 + Y^2$ are not equivalent over $\mathbb{Q}_5$. We now want to prove that they are equivalent over $\mathbb{Q}_7$. By Theorem 3.2.1 it is sufficient to show that these two forms have the same rank, discriminant and Hasse-Minkowski invariant. The rank is 2 for both forms. In Example 2 we saw that 2 is a square in $\mathbb{Q}_7$ and for this reason $1 \equiv 2$ modulo $\mathbb{Q}_7^{2*}$, hence $d(f) = d(g)$ in $\mathbb{Q}_7$. We are left with proving that $\varepsilon_7(f) = \varepsilon_7(g)$. This is true using Theorem 1.4.8 observing that in both cases $\alpha = 0 = \beta$.

Theorem 3.2.2. ***(Existence)***
Given $n \geq 1, d \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ and $\varepsilon = \pm 1$, a quadratic form f of rank n such that $d(f) = d$ and $\varepsilon(f) = \varepsilon$ exists if and only if we have:

$$\begin{aligned} n = 1, \varepsilon = 1; \quad &or \quad n = 2, d \neq -1; \\ or \quad n = 2, \varepsilon = 1; \quad &or \quad n \geq 3. \end{aligned} \tag{3.16}$$

Proof. Case $n = 1$ is trivial since ε is the empty product.
For $n = 2$, $f \sim aX^2 + bY^2$, and if $d = -1$, $\varepsilon(f) = (a, b) = (a, -ab) = (a, 1) = 1$, hence we can not have $d(f) = -1$ and $\varepsilon(f) = -1$ for the same form.
The other way around, if $d = -1$ and $\varepsilon = 1$ we choose $f = X^2 - Y^2$. If $d \neq -1$ by Theorem 3.1.3 there exists a in $\mathbb{Q}_p^*$ such that $(a, -d) = \varepsilon$. The form $f = aX^2 + adY^2$ satisfies the requests.
If $n = 3$ and we choose $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ different from $-d$, from what we have just seen there exists a quadratic form g of rank 2 such that $d(g) = ad$ and $\varepsilon(g) = \varepsilon(a, -d)$ $(ad \neq -1)$; the form $aZ^2 + g$ fits.
The case $n \geq 4$ follows from $n = 3$ by adding $X_4^2 + ... + X_n^2$ to a quadratic form g of rank 3 verifying the requests.

□

Theorem 3.2.3. ***(Number of classes)***
The number of classes of quadratic forms over $\mathbb{Q}_p$ with $p \neq 2$ (respectively p=2) is:
i) equal to 4 (respectively 8) if n=1;
ii) equal to 7 (respectively 15) if n=2;
iii) equal to 8 (respectively 16) if $n \geq 3$.

Proof. By Theorem 1.3.8 (respectively Theorem 1.3.13) d can assume 4 values (respectively 8) while ε can always assume two values (-1 and 1).

□

3.2.1 Classification of quadratic forms over $\mathbb{R}$

In Chapter 2.2 we saw that two quadratic forms f and g of rank n over $\mathbb{R}$ are equivalent if and only if they have the same signature.
Here we show that knowing $d_\infty(f)$ and $\varepsilon_\infty(f)$ is insufficient to classify quadratic forms over $\mathbb{R}$. In particular they only give information on the signature modulo 4.

Theorem 3.2.4. *Given two non-degenerate quadratic forms f and g over $\mathbb{R}$, the following statements are equivalent:*

i) If (r, s) and (r', s') are the signatures of f and g, respectively, then $s \equiv s'$ modulo 4;

ii) $d_\infty(f) = d_\infty(g)$ and $\varepsilon_\infty(f) = \varepsilon_\infty(g)$.

Proof. $\boxed{i) \Rightarrow ii)}$ It is easy to verify that if $s \equiv s'$ modulo 4, in particular $s \equiv s'$ modulo 2, hence $d(f) \equiv d(g)$ modulo $\mathbb{R}^{2*}$. Moreover $(a, b)_\infty = -1$ if and only if $a < 0$ and $b < 0$, hence $\varepsilon_\infty = (-1)^{s(s-1)/2}$, with $s(s-1)/2$ being the number of Hilbert symbols in ε_∞ in which both elements are less than 0. If $s' = s + 4k$ with $k \in \mathbb{Z}$ then

$$(-1)^{s'(s'-1)/2} = (-1)^{s(s-1)/2+2k(s-1)+2ks+8k^2} = (-1)^{s(s-1)/2}. \tag{3.17}$$

$\boxed{ii) \Rightarrow i)}$ Conversely if $d_\infty(f) = d_\infty(g)$ then

$$s \equiv s' \quad (mod\, 2). \tag{3.18}$$

Moreover if $\varepsilon_\infty(f) = \varepsilon_\infty(g)$ then the number of Hilbert symbols equal to -1 has the same parity for f and g. This happens only if $s \equiv s'$ modulo 4. Indeed by 3.18 $s = s' + 2k$ with $k \in \mathbb{Z}$, but $(-1)^{s(s-1)/2} = \varepsilon_\infty(f) = \varepsilon_\infty(g) = (-1)^{s'(s'-1)/2}$ and

$$\begin{array}{rcl} (-1)^{(s'+2k)(s'+2k-1)/2} & = & (-1)^{s'(s'-1)/2} \\ & \Leftrightarrow & \\ (s'+2k)(s'+2k-1)/2 & \equiv & s'(s'-1)/2 \quad (mod\, 2). \end{array}$$

This happens if and only if $k(s' + s' - 1) + 2k^2 \equiv_2 0$ and hence if and only if $k \equiv_2 0$. □

Theorem 3.2.4 shows that we can not use the results seen in Chapter 3.1 for $\mathbb{R}$. The crucial reason relies in the fact that in the proof of Theorem 3.1.4 and Corollary 3.1.5, we used Theorem 3.1.3.

3.3 Hasse-Minkowski

From now on all the quadratic forms are supposed to be over $\mathbb{Q}$ and non degenerate. We call V the set of all prime numbers and infinity.

Remark 3.3.1. Let $f \sim a_1X_1^2 + ...a_nX_n^2$ be a quadratic form of rank n. For every $v \in V$ the injection $\mathbb{Q} \hookrightarrow \mathbb{Q}_v$ allows to consider f as a quadratic form over $\mathbb{Q}_v$ (we will denote this by f_v). Due to Section 3.2, in order to give a complete classification of the forms f_v we need the two invariants $\mathrm{d}(f_v)$ and $\varepsilon(f_v)$.
In particular $\mathrm{d}(f_v)$ is the image of $d(f)$ through the map $\mathbb{Q}^*/\mathbb{Q}^{*2} \to \mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ and

$$\varepsilon(f_v) = \prod_{i<j}(a_i, a_j)_v \tag{3.19}$$

where by $(a_i, a_j)_v$ we mean the Hilbert symbol of a_i, a_j on the field $\mathbb{Q}_v$.

We associate the following invariants to the form f:

i) The discriminant $d(f) \in \mathbb{Q}^*/\mathbb{Q}^{*2}$.

ii) For all $v \in V$ the Hasse-Minkowski invariants of f_v.

iii) The signature (r,s) of the real quadratic form f_∞.

The invariants $\mathrm{d}(f_v)$, $\varepsilon(f_v)$ and (r, s) are called local invariants of f.

Theorem 3.3.2. ***(Hasse-Minkowski)***
Let f be a quadratic form over $\mathbb{Q}$. Then f represents 0 if and only if for all $v \in V$, the quadratic form f_v represents 0.
(In other words f has a "global" zero if and only if it always has a "local" zero).

Proof. The necessity is trivial since if no element of $\mathbb{Q}_v^n$ maps onto 0 through f, in particular no element of $\mathbb{Q}^n$ does.
To see that the condition is sufficient we write f in the form

$$f = a_1X_1^2 + ... + a_nX_n^2 \quad \text{with} \quad a_i \in \mathbb{Q}^*. \tag{3.20}$$

By replacing f with $a_1^{-1}f$ we can suppose $a_1 = 1$.
We now consider the cases n=2,3,4 and ≥ 5 separately.
$\boxed{\text{Case } n = 2}$

$f = X_1^2 - aX_2^2$, since f_∞ represents 0 in $\mathbb{Q}_\infty = \mathbb{R}$ then $a > 0$.
If we write a in the form

$$a = \prod_p p^{v_p(a)}, \tag{3.21}$$

since f_p represents 0, a is a square in $\mathbb{Q}_p$, therefore $v_p(a)$ is even (Theorem 1.3.8 and Theorem 1.3.13). Since this holds for every p, a is a square in $\mathbb{Q}$ and f represents 0.

$\boxed{\text{Case } n = 3}$

$f = X_1^2 - aX_2^2 - bX_3^2$, up to multiplication by two squares we can assume a and b as two square-free integers (i.e. $v_p(a)$, $v_p(b)$ are equal to 0 or 1 for all primes p). We can suppose $|a| \leq |b|$. By recurrence on the integer $m = |a| + |b|$ we can argue as follows:
If $m = 2$ then $f = X_1^2 \pm X_2^2 \pm X_3^2$. The case $f = X_1^2 + X_2^2 + X_3^2$ is ruled out since f_∞ does not represent 0. In the other cases the zero is trivial (i.e. $(1, 1, 0)$ or $(1, 0, 1)$).
If $m > 2$, i.e. $|b| \geq 2$, $b = \pm p_1 ... p_k$ with p_i different primes for $i = 1, ..., k$. We want to show that a is a square modulo p_i for all primes in b. If $a \equiv 0\ (mod\ p_i)$ this is trivial, else a is a p-adic unit. By hypothesis there exists $(x, y, z) \in (\mathbb{Q}_p)^3$ such that

$$z^2 - ax^2 - by^2 = 0. \tag{3.22}$$

We can suppose (x, y, z) to be primitive (i.e., that not all x, y and z are divisible by p_i, since $\frac{1}{p^h}(x, y, z)$ with $p^h|x, y$ and z, is still a zero). We then have

$$z^2 - ax^2 \equiv 0\ (mod\, p_i). \tag{3.23}$$

If it was $x \equiv 0\ (mod\ p_i)$ we would as well have $z \equiv 0\ (mod\ p_i)$. But in this case by^2 would be divisible by p_i^2. This cannot happen since $v_{p_i}(b) = 1$ and (x, y, z) is primitive. So we have $x \not\equiv 0\ (mod\ p_i)$ and from (3.22) it follows that a is a square modulo p_i. Since $\mathbb{Z}/b\mathbb{Z} = \prod \mathbb{Z}/p_i\mathbb{Z}$, a is also a square modulo b. There exist two integers t and b' such that

$$t^2 = a + bb' \tag{3.24}$$

and we can choose t such that $|t| \leq |b|/2$. Since $bb' = t^2 - a$ we can think of bb' as a field norm for the extension $\mathbb{K}(\sqrt{a})/\mathbb{K}$ where $\mathbb{K}$ is either $\mathbb{Q}$ or $\mathbb{Q}_v$. We conclude that f represents 0 in $\mathbb{K}$ if and only if $f' = X_1^2 - aX_2^2 - b'X_3^2$ does. This is due to the fact that $Z^2 - \alpha X^2 - \beta Y^2$ has a non zero root when $\alpha = z^2 - \beta y^2$, and on the other hand if $Z^2 - \alpha X^2 - \beta Y^2$ has a non zero root (z, x, y) then a is the norm of the element $\frac{z}{x} + \beta \frac{y}{x}$ (see the proof of Theorem 1.4.6). In particular f' represents 0 in every $\mathbb{Q}_v$. But we also have

$$|b'| = |\frac{t^2 - a}{b}| \leq \frac{|b|}{4} + 1 < |b| \qquad (\text{ since } |b| \geq 2) \tag{3.25}$$

We write b' as $b''u$ with b'' and u integers and b'' square-free. Of course $|b''| < |b|$ hence we can apply the recursive hypothesis to the form $f'' = X_1^2 - aX_2^2 - b''X_3^2$.

$\boxed{\text{Case } n = 4}$

$f = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$. By Corollary 2.1.25 f_v represents 0 if and only if there exists an element $x_v \in \mathbb{Q}_v^*$ that is represented both by $aX_1^2 + bX_2^2$ and $cX_3^2 + dX_4^4$. Using Corollary 3.1.5 this happens when $(x_v, -d) = \varepsilon$, i.e.

$$(x_v, -ab)_v = (a, b)_v \quad \text{and} \quad (x_v, -cd)_v = (c, d)_v. \tag{3.26}$$

Since by Theorem 1.4.11 $\prod_{v \in V}(a, b)_v = \prod_{v \in V}(c, d)_v = 1$ and, for almost all v, $(a, b)_v = 1$; then we can apply Theorem 1.4.15 (with $\{a_i \ for \ i \in I\} = \{-ab, -cd\}$ and $\{\varepsilon_{i,v} \ for \ i \in I \ an \ v \in V\} = \{(a, b)_v \ for \ v \in V\} \cup \{(c, d)_v \ for \ v \in V\}$) from which we have that there exists an element $x \in \mathbb{Q}^*$ such that

$$(x, -ab)_v = (a, b)_v \quad and \quad (x, -cd)_v = (c, d)_v \quad for \ all \ v \in V. \tag{3.27}$$

The form $aX_1^2 + bX_2^2 - xZ^2$ represents 0 in every $\mathbb{Q}_v$ hence it represents 0 in $\mathbb{Q}$. We conclude that x is represented in $\mathbb{Q}$ by both $aX_1^2 + bX_2^2$ and $cX_3^2 + dX_4^2$, using the same argument. This proves that f represents 0.

$\boxed{\text{Case } n \geq 5}$

We argue by recurrence on n. We write f in the form

$$f = h \dot{-} g, \tag{3.28}$$

with $h = a_1X_1^2 + a_2X_2^2$ and $g = -(a_3X_3^2 + ... + a_nX_n^2)$. Let S be the part of V consisting of $\infty, 2$ and those primes p for which $v_p(a_i) \neq 0$ for an $i \geq 3$; this is a finite set. Let $v \in S$, since f_v represents 0 there exists an element $a_v \in \mathbb{Q}_v^*$ represented by both h and g, i.e. there exists $(x_1^v, ..., x_n^v)$ such that

$$h(x_1^v, x_2^v) = a_v = g(x_3^v, ..., x_n^v). \tag{3.29}$$

By Theorem 1.3.10 the squares in $\mathbb{Q}_v^*$ form an open subgroup. Using Lemma 1.4.13 there exist $x_1, x_2 \in \mathbb{Q}$ such that $a = h(x_1, x_2)$ and we have $a/a_v \in (\mathbb{Q}_v^*)^2$ for all $v \in S$. (In order to explain this passage we argue as explained in the footnote [1] of Theorem 1.4.15, with both x_1 and x_2, and we obtain that the image through h has the required property). We now consider the form

$$f_1 = aZ^2 \dot{-} g. \tag{3.30}$$

If $v \in S$ then g represents a_v in $\mathbb{Q}_v$ and hence it also represents a since a/a_v is a square; we conclude that f_1 represents 0, in $\mathbb{Q}_v$.
If $v \notin S$ the coefficients $-a_3, ..., -a_n$ are v-adic units, the same is true for $d_v(g)$ and since $p \neq 2$, we have $\varepsilon_v(g) = 1$. Since $rank(g) \geq 3$, Theorem 3.1.4 shows that g represents 0 hence f_1 represents 0 (we are using Theorem 1.4.8 from which we have that the Hilbert symbol of two units is 1). In all the cases f_1 represents 0 in $\mathbb{Q}_v$, since the rank of f_1 is $n-1$, the recurrence hypothesis shows that f_1 represents 0 in $\mathbb{Q}$, i.e. g represents a in $\mathbb{Q}$ as well as h represents a. Hence f represents 0 in $\mathbb{Q}$. □

Corollary 3.3.3. *Let $a \in \mathbb{Q}^*$. f represents a in $\mathbb{Q}$ if and only if it represents a in every $\mathbb{Q}_p$.*

Proof. It results using Theorem 3.3.2 on $aZ^2 \dot{-} f$. □

Corollary 3.3.4. *A quadratic form f of rank ≥ 5 represents 0 if and only if it is indefinite, i.e. if it represents 0 in $\mathbb{R}$.*

Proof. It is trivial since from Theorem 3.1.4 f represents 0 in every $\mathbb{Q}_p$. □

Corollary 3.3.5. *Let f be a quadratic form of rank $n = 3$. If f represents in every $\mathbb{Q}_v$ except at most one, then f represents 0. The same statements holds if f has rank $n = 4$ and $d(f) = 1$.*

Proof. If $n = 3$ then by Theorem 3.1.4 f represents 0 if and only if

$$(-1, -d(f))_v = \varepsilon_v(f). \tag{3.31}$$

The two families $\varepsilon_v(f)$ and $(-1, -d(f))_v$ satisfy the product formula in Theorem 1.4.11. Hence if (3.31) is verified for all v apart from one it is verified for all v.
If $n = 4$ and $d = 1$, we reason in the same way replacing 3.31 with

$$(-1, -1)_v = \varepsilon_v(f). \tag{3.32}$$

□

3.4 Classification of quadratic forms over $\mathbb{Q}$

Theorem 3.4.1. *Let f, f' be two quadratic forms over $\mathbb{Q}$. f and f' are equivalent if and only if they are equivalent over every $\mathbb{Q}_v$.*

Proof. The necessity is trivial, to prove the sufficiency we reason by recurrence over the rank n of f and f'. If $n = 0$ there is nothing to prove. If not there exists an element $a \in \mathbb{Q}^*$ such that a is represented by f and f' (Corollary 3.3.3). We have then from Theorem 2.1.26 $g \sim g'$ over all $\mathbb{Q}_p$. The hypothesis of recurrence shows that $g \sim g'$ over $\mathbb{Q}$ and hence $f \sim f'$ over $\mathbb{Q}$. □

Corollary 3.4.2. *Let (r, s) and (r', s') be the signatures of f and f'. f and f' are equivalent if and only if we have:*

$$d(f) = d(f'), \quad (r, s) = (r', s') \quad and \quad \varepsilon_p(f) = \varepsilon_p(f') \quad for\ every\ prime\ p. \tag{3.33}$$

Proof. This is equivalent to saying that f and f' are equivalent over every $\mathbb{Q}_v$. □

Example 8. We want to see whether or not the quadratic forms $f = X^2+2Y^2+2Z^2$ and $g = X^2 + Y^2 + Z^2$ are equivalent over $\mathbb{Q}$.
The discriminats are $d(f) = 4$ and $d(g) = 1$, hence $d(f) \equiv d(g)$ modulo $\mathbb{Q}^{2*}$. Moreover the signatures (r, s) and (r', s') are both equal to $(3, 0)$.
Finally

$$\begin{aligned} &\varepsilon_p(f) = (1, 2)_p(1, 2)_p(2, 2)_p = (1, 2)_p^2(2, 2)_p = (2, 2)_p \\ while \quad & \\ &\varepsilon_p(g) = (1, 1)_p(1, 1)_p(1, 1)_p = (1, 1)_p^2(1, 1)_p = (1, 1)_p. \end{aligned}$$

By Theorem 1.4.8 we have that, when $p \neq 2$ then $(2, 2)_p = 1$ and when $p = 2$ we have $(2, 2)_2 = 1$. On the other hand $(1, 1)_p = 1$ for all primes p, again using Theorem 1.4.8.
By Corollary 3.4.2 we have proved that the quadratic forms f and g are indeed equivalent over $\mathbb{Q}$.

Remark 3.4.3. The parameters d, ε_v and (r, s) are not arbitrary. Indeed they verify the following relations:

i) $\varepsilon_v = 1$ for almost all $v \in V$ and $\prod_{v\in V} \varepsilon_v = 1$;
ii) $\varepsilon = 1$ if $n = 1$, or if $n = 2$ and $d_v := [d] = [-1]$ in $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$;
iii) $r, s \geq 0$ and $r + s = n$;
iv) $d_\infty = (-1)^s$;
v) $\varepsilon_\infty = (-1)^{s(s-1)/2}$.

Conversely

Theorem 3.4.4. *Let $d, (\varepsilon_v)_{v\in V}$ and (r, s) satisfying $i) - v)$ of Remark 3.4.3. Then there exists a quadratic form of rank n having $d, (\varepsilon_v)_{v\in V}$ and (r, s) as its invariants.*

Proof. Case $n = 1$ is trivial
If $n = 2$ since the Hilbert symbol is non-degenerate and condition *ii*) is verified by hypothesis, there exists $x_v \in \mathbb{Q}_v^*$ such that $(x_v, -d)_v = \varepsilon_v$. From this and condition *i*), using Theorem 1.4.15 we have that there exists $x \in \mathbb{Q}^*$ such that $(x, -d)_v = \varepsilon_v$ for all $v \in V$. The form $xX^2 + xdY^2$ proves the theorem in this case.
If $n = 3$, let S be the set of $v \in V$ such that $(-d, -1)_v = -\varepsilon_v$; This is a finite set since $(-d, -1)_v = 1$ for almost all $v \in V$ and $\varepsilon_v = 1$ for almost all $v \in V$ (Theorem 1.4.11). If $v \in S$ we choose an element $c_v \in \mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ different from $-d_v$. Using the Approximation Theorem (1.4.13) there exists an element $x \in \mathbb{Q}^*$ such that $[x] = [x_v]$ in $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ for all $v \in S$. (It works as explained in footnote [1] to the Theorem 1.4.15). From what we have just proven, there exists a form g of rank 2 such that $d(g) = cd$, $\varepsilon_v(g) = (c, -d)_v\varepsilon_v$ for all $v \in V$. Then the form $f = cZ^2\dot{+}g$ proves this case.
If $n \geq 4$, we reason by recurrence over n. Let us suppose $r =\geq 1$, thanks to the hypothesis of recurrence there exists a quadratic form g of rank $n-1$ with invariants $d, (\varepsilon_v)_{v\in V}$ and $(r-1, s)$. The form $X^2\dot{+}g$ satisfies the request. Finally if $r = 0$, we build a form h of rank $n-1$, with invariants $-d, \varepsilon_v(-1, -d)_v$ and $(0, n-1)$. The form $f = -X^2\dot{+}h$ proves the theorem. □

Bibliography

[Kob84] Neal Koblitz. *p-adic Numbers, p-adic analysis, and Zeta-Functions*. Graduate Texts in Mathematics. Springer, 1984.

[Cas86] J.W.S. Cassels. *Local Fields*. London Mathematical Society Student Texts. 3. Cambridge University Press, 1986.

[Ser95] Jean-Pierre Serre. *Cours d'Arithmétique*. Le Mathématicien. Presses Universitaires de France, 1995.

[Gou97] Fernando Q. Gouvea. *p-adic Numbers, An Introduction*. Universitext. Springer, 1997.

[Rot02] Joseph J. Rotman. *Advanced Modern Algebra*. Vol. 114. Graduate Studies in Mathematics. American Mathematical Society, 2002.