Sorbonne Université

The Hasse-Minkowski Theorem
M1 research project

Author: Breki Pálsson *Advisor:* Antoine Ducros

30. May 2022

Contents

Chapter 1

Presentation

The theory of quadratic forms has a long history. The first instances of the study of quadratic forms dates back to ancient Babylonia between 1900 and 1600BC. We have evidence in the form of tablets that suggests that the Babylonians knew that there are infinitely many solutions $(a, b, c) \in \mathbb{Z}^3$ of the equation

$$x_1^2 + x_2^2 - x_3^2 = 0$$

and how to produce them. These results are most likely one of the first results in the study of quadratic forms.

1.1 Motivation

A natural question that arises when studying Number theory and in particular Diophantine equations is the **representation problem**. That is, given some function $f : R \to F$ what are the possible values of F that f can take with inputs from R. We say that f **represents** α **over** R if there exist $\lambda \in R$ such that $f(\lambda) = \alpha$ denoted $\alpha \to_R f$. Sometimes we put a restriction on the input without explicitly mentioning it. Following this convention if $0 \in R$ we say that f represents α if $f(\lambda) = \alpha$ and $\lambda \neq 0$. In this text we will use this convention.

A special case of the representation problem is whether a polynomial P with coefficients in $\mathbb{Q}$ represents 0 over $\mathbb{Z}$. This question is generally difficult since there are infinitely many possible inputs that are discrete and we can not use elementary

analytical methods to help us in this case. However, if P represents 0 over $\mathbb{Z}$ then it also does for $\mathbb{Z}/m\mathbb{Z}$ where $m \in \mathbb{Z}$. That is

$$P(\lambda) = 0 \Rightarrow P(\lambda) \equiv 0 \pmod{m}, \quad \forall m \in \mathbb{Z}.$$

The problem whether a polynomial represents an integer over the ring $\mathbb{Z}/m\mathbb{Z}$ is trivial since there are finitely many cases to try and one could for example try them all.

We can systematically check whether a polynomial represents 0 over the ring $\mathbb{Z}/m\mathbb{Z}$, where $m = p_1^{n_k}..p_k^{n_k}$ is some integer, by using the Chinese reminder theorem, i.e.

$$0 \xrightarrow[\mathbb{Z}/p_j^{n_j}\mathbb{Z}]{} P \quad \forall j \in \{1,..,k\} \Rightarrow 0 \xrightarrow[\mathbb{Z}/m\mathbb{Z}]{} P$$

Thus if we can determine whether a polynomial represents 0 modulo all powers of prime numbers we can determine whether the polynomial represents 0 modulo any integer. The study of these questions motivates us to define the p-adic numbers.

Although it is necessary for a polynomial to represent 0 modulo all integers it is certainly not sufficient as we will see in 4.1. However, for some special cases of polynomials, for example quadratic forms, there is an equivalence.

1.2 Examples

One of the most classical problems in the theory of quadratic forms it that of the equation of *Pell-Fermat*. Although the name is not attributed to him it was known by *Brahmagupta* (598-668) more than a millennia before that.

Example 1. *Given a solution $(x_0, y_0) \in \mathbb{Z}^2$ to the equation $X^2 - nY^2 = 1$ there exists an algorithm to generate infinitely many solutions.*

The solutions are generated by an algorithm that demonstrates the multiplicative structure of the set of solutions to the above equation. Note that if $a, b, c, d, n \in \mathbb{Z}$

then:

$$(b^2 - na^2)(d^2 - nc^2) = (bd + nac)^2 - n(bc + ad)^2$$
$$(b^2 - na^2)(d^2 - nc^2) = (bd - nac)^2 - n(bc - ad)^2$$

and if

$$b^2 - na^2 = 1 \text{ and } d^2 - nc^2 = 1$$

then

$$(bd + nac)^2 - n(bc + ad)^2 = 1 \text{ and } (bd - nac)^2 - n(bc - ad)^2 = 1$$

This means that given two solutions (b, a) and (d, c) to the equation $X^2 - nY^2 = 1$ we can generate the solutions $(bd + nac, bc + ad)$ and $(bd - nac, bc - ad)$. If we pick $(b, a) = (d, c) = (x_0, y_0)$ we get the desired result.

Another classical result of quadratic forms is that of *Fermat* (1601-1665), that is which numbers are the sums of two squares. Fermat stated it in a private communication, along with hints on his method of proof, and a formal proof was then published by Euler in 1754.

Example 2. *Given an integer* $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ *then*

$$n \underset{\mathbb{Z}}{\rightarrow} X^2 + Y^2$$

if and only if $\alpha_i \equiv 0 \ (mod\ 2)$ *for all* p_i *such that* $p_i \equiv 3 \ (mod\ 4)$

G. H. Hardy writes that this *two square theorem* of Fermat "is ranked, very justly, as one of the finest in arithmetic". An elegant proof of this theorem can be found in [1] in chapter 4.

Next result is that of Lagrange (1736-1813):

Example 3.

$$n \underset{\mathbb{Z}}{\rightarrow} X_1^2 + X_2^2 + X_3^2 + X_4^2, \quad \forall n \in \mathbb{N}^*.$$

Last example is that of Legendre (1752-1833):

Example 4. *Let $n \in \mathbb{N}^*$ we can write $n = 4^a m$ such that $m \neq 0 \ mod \ 4$*

$$n \underset{\mathbb{Z}}{\rightarrow} X^2 + Y^2 + Z^2 \iff m \neq 7 \ mod \ 8.$$

One can now see a glimpse at the importance in history of quadratic forms.

Chapter 2

Preliminaries

In this chapter we will introduce concepts from number theory that will help us work with quadratic forms. We will introduce properties of finite fields, the Legendre symbol, p-adic integers, numbers and their equations, and lastly the Hilbert symbol.

2.1 Legendre Symbol

The question of whether an element of $\mathbb{F}_p$ is a square number, where p is a prime, originates to Euler. The intuition probably came from the question of whether a prime number p divides $a^n + 1$. A similar question was answered by Fermat in the case $a^n - 1$, in fact if n is a multiple of $p - 1$ we have from Fermat's little theorem that

$$a^n = a^{(p-1)m} = (a^{p-1})^m \equiv 1 \pmod{p}, \forall a \in \mathbb{F}_p^*.$$

Definition 1. *Let $p \neq 2$ be a prime number, and let $a \in \mathbb{F}_p^*$. The **Legendre symbol** of a with respect to p is defined as follows;*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } y^2 - ax^2 = 0 \text{ has a nontrivial solution in } (\mathbb{F}_p)^2, \\ -1 & \text{otherwise.} \end{cases}$$

In practice, how do we compute the Legendre symbol? Or equivalently, how can we determine whether an element of $\mathbb{F}_p^*$ is a square number? Since the number of elements in $\mathbb{F}_p^*$ is $p-1$ we have that $a^{p-1} = 1$ for all elements $a \in \mathbb{F}_p^*$. The polynomial

$x^{p-1} - 1 \in \mathbb{Z}_p[x]$ has as roots all elements of $\mathbb{F}_p^*$. Note that

$$x^{p-1} - 1 = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1).$$

And if $y^2 - ax^2 = 0$ has a nontrivial solution then we can write $a = b^2 \pmod{p}$. Furthermore $a^{\frac{p-1}{2}} = b^{p-1} = 1$ hence all elements $a \in \mathbb{F}_p^*$ such that $y^2 - ax^2 = 0$ has a nontrivial solution is a solution to the polynomial $x^{\frac{p-1}{2}} - 1$. The kernel of the map $z \to z^2$ from F_p^* is equal to $\{-1, 1\}$ and therefore there are $\frac{p-1}{2}$ squares in F_p^* and $\frac{p-1}{2}$ nonsquares in $\mathbb{F}_p^*$. Since the degree of the polynomial $x^{\frac{p-1}{2}} - 1$ is $\frac{p-1}{2}$ the other $\frac{p-1}{2}$ elements must be solutions to the polynomial $x^{\frac{p-1}{2}} + 1$ and thus the result

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}, a \in \mathbb{F}_p^*. \tag{2.1}$$

Definition 2. *If n is an odd integer let $\varepsilon(n)$ and $\omega(n)$ be defined as*

$$\varepsilon(n) \equiv \frac{n-1}{2} \ (mod\ 2) = \begin{cases} 0 & \text{if } n \equiv 1 \ (mod\ 4) \\ 1 & \text{if } n \equiv -1 \ (mod\ 4) \end{cases}, \omega(n) \equiv \frac{n^2-1}{8} \ (mod\ 2) = \begin{cases} 0 & \text{if } n \equiv \pm 1 \ (mod\ 8) \\ 1 & \text{if } n \equiv \pm 5 \ (mod\ 8) \end{cases}$$

Theorem 2.1.1. *The following formulas hold:*

$$\left(\frac{1}{p}\right) = 1, \quad \left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}, \quad \left(\frac{2}{p}\right) = (-1)^{\omega(p)}$$

The first two equations are a consequence of the identity 2.1. The last equality is not as obvious.

Let α denote a primitive 8-th root of unity in an algebraic extension of $\mathbb{F}_p$ that includes α, the element $y = \alpha + \alpha^{-1}$ verifies

$$y^2 = \alpha^2 + 2 + \alpha^{-2}\alpha^{-2}(\alpha^4 + 1) + 2 = 0 + 2 = 2$$

so we have that

$$y^p = (\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p}.$$

Using the fact that $\alpha^5 + \alpha^{-5} = \alpha^4(\alpha + \alpha^{-1}) = -y$ we can deduce that,

$$y^p = \alpha^p + \alpha^{-p} = \begin{cases} \alpha + \alpha^{-1} & \text{if } p \equiv \pm 1 \pmod 8 \\ -(\alpha + \alpha^{-1}) & \text{if } p \equiv \pm 5 \pmod 8 \end{cases}$$

$$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} = y^{p-1} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 5 \pmod 8. \end{cases}$$

This gives us a method to calculate the Legendre symbols of the numbers $1, -1, 2$. Surprisingly by using only these three equations along with the result in the next section we can determine the Legendre symbol of all the natural numbers with respect to p for any prime.

2.2 Quadratic Law Of Reciprocity

The study of the representation of p by the form $x^2 \pm qy^2$ and its relation to the representation of q by the form $x^2 \pm py^2$ naturally led to the **quadratic law of reciprocity** first conjectured by Euler and later Lagrange and then proved by Gauß in 1796.

Theorem 2.2.1 (quadratic law of reciprocity)**.** *Let p and q be two distinct primes different from 2. We have that:*

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

This result is of great importance and has been proved in numerous ways by many famous mathematicians. Gauß proved it in at least 8 different ways and most of the known proofs use the so called **Lemma of Gauß**. This link **here** shows a list of 246 different proofs of the quadratic law of reciprocity as of 2022.

Example 5.

$$\left(\frac{62}{17}\right) = \left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1)(-1)\left(\frac{11}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

This means that we cannot write $17 = x^2 - 62y^2$, $x, y \in \mathbb{Z}^2$ *or equivalently* 62 *is not a square* (*mod* 17).

2.3 p-adic numbers

In this section we will define and look at properties of the p-adic numbers, first with an algebraic approach and then with an analytic approach.

2.3.1 Algebraic approach

Consider the equations

$$x^2 \equiv 3 \pmod{11^n} \tag{2.2}$$

For $n = 1$ we have that $x_0 \equiv \pm 5 \pmod{11}$ are the only solutions.
For $n = 2$ we know that a solution has to be of the form $x_1 = x_0 + 11t_1$ where x_0 is a solution of the previous equation. Let's consider the case where $x_0 = 5$ then we have

$$\begin{aligned} (5 + 11t_1)^2 &\equiv 3 \pmod{11^2} \\ 25 + 11 \times 10t_1 + 11^2 t_1^2 &\equiv 3 \pmod{11^2} \\ 2 + 10t_1 &\equiv 0 \pmod{11} \\ t_1 &\equiv 2 \pmod{11} \end{aligned}$$

So we get that $t_1 \equiv 2 \pmod{11}$ so $x_1 = 5 + 11 \times 2$
For $n = 3$ we let $x_2 = x_1 + 11^2 t_2$ and then we solve for t_2 in the equation

$$(5 + 11 \times 2 + 11^2 t_2)^2 \equiv 3 \pmod{11^3}$$

and we get $t_2 \equiv 6 \pmod{11}$ so $x_2 = 5 + 11 \times 2 + 11^2 \times 6$
This procedure can be continued to produce a number sequence $\{x_0, x_1, ...\}$ that

satisfies the following properties

$$\begin{aligned} x_1 &\equiv 5 \pmod{11} \\ x_n &\equiv x_{n-1} \pmod{11^{n-1}} \\ x_n^2 &\equiv 3 \pmod{11^n} \end{aligned}$$

Note that in the example above we could just as easily have chosen $x_0 \equiv -5 \equiv 6 \pmod{11}$ to obtain another unique series. This gives us an idea of a structure that has information about the solutions to equations modulo powers of a prime number. This structure has a natural projection property that can be seen with the following example modulo powers of 5. Let's define $x := \{x_0, x_1, ...\}$ where

$$\begin{aligned} x_0 &= 1 \pmod 5 \\ x_1 &= 1 + 5 \times 2 \pmod{5^2} \\ x_2 &= 1 + 5 \times 2 + 5^2 \times 3 \pmod{5^3} \\ &\vdots \end{aligned}$$

In more formal words we can let $\mathbb{Z}/p^n\mathbb{Z}$ be the ring of classes of integers (mod p^n). An element x of $\mathbb{Z}/p^n\mathbb{Z}$ naturally defines an element in $\mathbb{Z}/p^{n-1}\mathbb{Z}$ by taking the class of x modulo p^{n-1}. Thus we obtain a morphism

$$\varphi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$$

which is surjective and whose kernel is $p^{n-1}\mathbb{Z}/p^n\mathbb{Z}$.

The sequence

$$.. \to \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z} \to \ldots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$

forms what is called a projective system (see 4.1) indexed by the integers greater than 1.

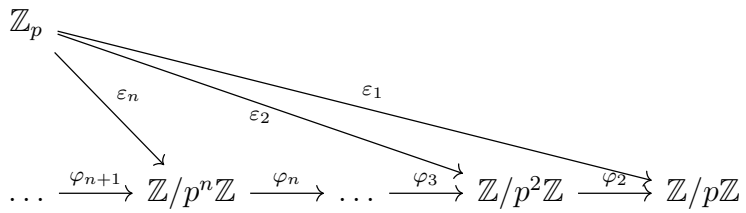
Definition 3. *The ring of* p***-adic integers*** $\mathbb{Z}_p$ *is the projective limit of the system* $(\mathbb{Z}/p^n\mathbb{Z}, \varphi_n)$ *defined above.*

In other words $\mathbb{Z}_p$ is the set of all sequences $(x_n)_{n\in\mathbb{N}}$ such that $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ and

$x_{n-1} = \varphi(x_n)$ for all $n > 1$. We note

$$\varepsilon_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$$

the function that associates to each p-adic integer its n-th component x_n.



The projective limit defines a ring structure with component-wise addition and multiplication.

We can notice that for each $z \in \mathbb{Z}$ there exists an $n \in \mathbb{N}$ such that $z < p^n$ and thus the image of z is constant in $\mathbb{Z}/p^m\mathbb{Z}, \forall m \geqslant n$ so $z \in \mathbb{Z}_p$.

Proposition 1. *An element $a \in \mathbb{Z}_p$ is invertible if and only if it is not divisible by p. In addition, a can be uniquely written in the form $a = p^n u$ where $n \in \mathbb{N}$ and u is invertible.*

We will first prove that if $a \in \mathbb{Z}/p^n\mathbb{Z}$ is not divisible by p then it is invertible. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}/p^n\mathbb{Z}$, if $a \notin p\mathbb{Z}/p^n\mathbb{Z}$, its image in $\mathbb{Z}/p\mathbb{Z}$ is not zero thus invertible. So there exist $y, z \in \mathbb{Z}/p^n\mathbb{Z}$ such that $ay = 1 - pz$ but then we have

$$\begin{aligned} ay(1 + pz + ... + p^{n-1}z^{n-1}) &= (1 - pz)(1 + pz + ... + p^{n-1}z^{n-1}) \\ &= 1 + pz + ... + p^{n-1}z^{n-1} \\ &\quad - pz - ... - p^{n-1}z^{n-1} - p^n z^n \\ &\equiv 1 \pmod{p^n}. \end{aligned}$$

This means that if $a \in \mathbb{Z}_p$ is not divisible by p then $\varepsilon_n(x)$ is invertible with inverse $y(1 + pz + .. + p^{n-1}z^{n-1})$ thus

$$\left(\sum_{i=0}^{n-1} y(pz)^i \right)_{n \in \mathbb{N}}$$

is the inverse of x in $\mathbb{Z}_p$.

Now let $x \in \mathbb{Z}_p$ not equal to zero and p divides x then there exists a largest integer n such that $\varepsilon_n(x)$ is zero then $x = p^n u$ with u not divisible by p, hence u is invertible. On the other hand p is not invertible because $p = (0, p, p, ...) \in \mathbb{Z}_p$ and 0 is not invertible in $\mathbb{Z}/p\mathbb{Z}$ thus x is not invertible.

Suppose that $a \in \mathbb{Z}_p$ and that $a = p^n u = p^m v$ such that u, v are invertible and $n \geqslant m$. Then $p^{n-m} u v^{-1} = 1$ and since 1 is invertible $n - m = 0$ an therefore $u = v$ proving uniqueness.

Definition 4. *The group of invertible elements of $\mathbb{Z}_p$ is denoted by $\mathbb{U}_p$.*

Note that $\mathbb{Z}_p$ is an integral domain and thus the field of fractions of $\mathbb{Z}_p$ is a field. We have the following definition.

Definition 5. *The field of p-**adic numbers**, denoted by $\mathbb{Q}_p$, is the field of fractions of the integral domain $\mathbb{Z}_p$.*

The ring $\mathbb{Z}_p$ is a subring of the product $\prod A_n$. Furthermore if we give A_n the discrete topology and $\prod A_n$ the product topology, the ring $\mathbb{Z}_p$ inherits a topology which turns it into a compact space, since it is closed in a product of compact spaces.

2.3.2 Analytic approach

Another approach to defining the p-adic numbers is that by completion of $\mathbb{Q}$ by the **p-adic norm** described below. As we will prove later in this text these definitions are equivalent.

Let p be a prime number and let us consider an element $\alpha \in \mathbb{Q}^*$. We can write $\alpha = p^n \frac{a}{b}$ where $a, b, n \in \mathbb{Z}$, $\gcd(a, b) = 1$ and $p \nmid a$, $p \nmid b$ in a unique way. We can define a norm $|\cdot|_p$ on $\mathbb{Q}$ with the following properties. Set $|0|_p = 0$ and $|\alpha|_p = \frac{1}{p^n}$ the integer n in this expression is called the **p-adic order** of the element α. Usually written as $v_p(\alpha)$ (we put $v_p(0) = \infty$). It is easily checked that $|\cdot|_p$ defines a norm and in addition it verifies the strong triangle inequality, i.e. $|\alpha + \beta|_p \leqslant \max\{|\alpha|_p, |\beta|_p\}$.

One can visualize the distance between the p-adic integers in the picture 2.1. Each number lies in multiple circles and the distance between numbers is related to the smallest circle containing both the numbers.

In the picture we only visualize a finite amount of numbers. We can see in the third picture that the smallest circle containing 107 and 104 is the orange one

signaling that the distance between the numbers is large in some sense, on the other hand the smallest circle containing both 107 and 7 is the green one signaling that the distance between them is less than the distance between 107 and 104 contrary to the Euclidean distance between integers.

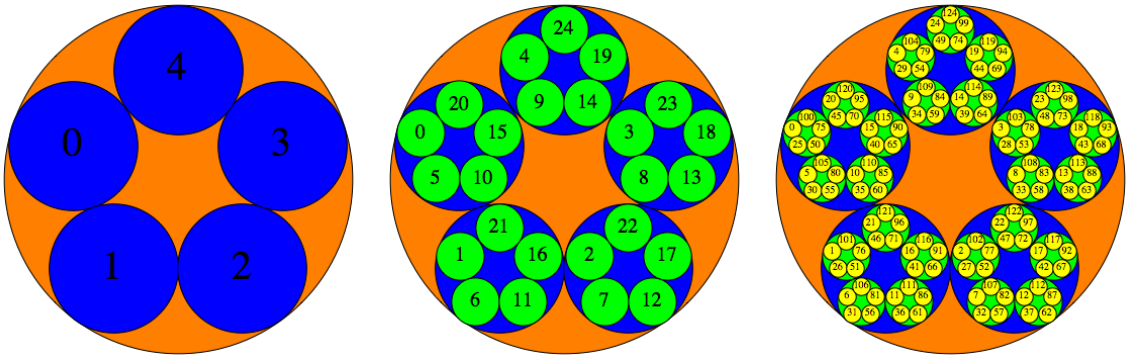


Figure 2.1: Visual representation of the distance between 5-adic integers

Definition 6. *A sequence* $\{z_m\} = z_0, z_1, \ldots$ *of p-adic numbers is said to be* ***convergent*** *to a p-adic number* z*, noted* $\lim_{n\to\infty} z_n = z$*, if*

$$\lim_{n\to\infty} v_p(z_n - z) = \infty$$

Definition 7. *If the sequence* $s_n = \sum_{i=0}^{n} \alpha_i$ *of partial sums of the* ***p-adic series***

$$\sum_{i=0}^{\infty} \alpha_i$$

with p-adic terms converges to the p-adic number α*, then we say the series* ***converges*** *and that its sum is equal to* α*.*

Proposition 2. *Let* $(\alpha_n)_{n\in\mathbb{N}}$ *be a sequence in* $\mathbb{Q}_p$*. Then* $(\alpha_n)_{n\in\mathbb{N}}$ *is a Cauchy sequence if and only if for every* $\varepsilon > 0$*, there exist some* $N \in \mathbb{N}$ *such that for all* $n \geqslant N, |\alpha_{n+1} - \alpha_n|_p < \varepsilon$

Proof. First, assume that $(\alpha_n)_{n\in\mathbb{N}}$ is a Cauchy sequence then there exist some $N \in \mathbb{N}$ such that for all $m \geqslant n \geqslant N, |\alpha_m - \alpha_n|_p < \varepsilon$ in particular $|\alpha_{n+1} - \alpha_n|_p < \varepsilon$.

Next, we assume that for every $\epsilon > 0$, there is some $N \in \mathbb{N}$ such that for all $n \geqslant N, |\alpha_{n+1} - \alpha_n|_p < \varepsilon$. Now let $m \geqslant n \geqslant N$ If $n = m$ then $|\alpha_m - \alpha_n|_p = 0$, and if

$n+k=m>n$ then

$$|\alpha_m-\alpha_n|_p=|(\alpha_{n+k}-\alpha_{n+k-1})+...+(\alpha_{n+1}-\alpha_n)|_p\leqslant\max_{n\leqslant i<n+k}|(\alpha_{i+1}-\alpha_i)|_p<\varepsilon$$

Therefore, $(\alpha_n)_{n\in\mathbb{N}}$ is a Cauchy sequence □

Proposition 3. *Let $\sum_{i=0}^{\infty}\alpha_i$ be a series of p-adic numbers, the series is convergent if and only if $\lim_{n\to\infty}\alpha_i=0$.*

Proof. Let $s_n:=\sum_{i=0}^{n}\alpha_i$. The series converges if and only if $(s_n)_{n\in\mathbb{N}}$ converges and since $\mathbb{Q}_p$ is complete it converges if and only if it is a Cauchy sequence that is if and only if for all $\varepsilon>0$ there exist an $N>0$ such that for all $n>N, |s_{n+1}-s_n|_p=|\alpha_{n+1}|_p<\varepsilon$. □

Definition 8. *We say that the series $\sum_{n=1}^{\infty}\alpha_n$ is **unconditional convergence** if all reorderings of the series converge to the same value. That is if for all permutations $\sigma:\mathbb{N}\to\mathbb{N}$ we have*

$$\sum_{n=0}^{\infty}\alpha_n=\sum_{n=0}^{\infty}\alpha_{\sigma(n)}.$$

Corollary 1. *A p-adic series is convergent if and only if it is unconditionally convergent.*

Proof. Let $(\alpha_n)_{n\in\mathbb{N}}$ be a sequence in $\mathbb{Q}_p$ and $(\alpha'_n)_{n\in\mathbb{N}}$ be a rearrangement of the sequence $(\alpha_n)_{n\in\mathbb{N}}$.

Let $\varepsilon>0$ and $N\in\mathbb{N}$ such that for any $n>N, |\alpha_n|_p<\varepsilon$, then

$$\left|\sum_{n=1}^{\infty}\alpha_n-\sum_{n=1}^{N}\alpha_n\right|_p<\varepsilon$$

Such an N exist by the proposition above. Let $S=\sum_{n=1}^{N}\alpha_n$, $S'=\sum_{n=1}^{N}\alpha'_n$. Now let S_1 be the sum of all the terms in S and for which $|\alpha_n|_p\geqslant\varepsilon$ and S'_1 be the sum of all the terms in S' for which $|\alpha'_n|_p\geqslant\varepsilon$ By the construction of S, S', S_1 and S'_1 we can see that $S_1=S'_1$

By applying the strong triangle inequality we get that $|S-S_1|_p<\varepsilon$ and $|S'-S'_1|_p<\varepsilon$ and therefore $|S-S'|_p<\varepsilon$. Hence we have

$$\left|\sum_{n=1}^{\infty}\alpha_n - \sum_{n=1}^{N}\alpha'_n\right|_p = \left|\sum_{n=1}^{\infty}\alpha_n - \sum_{n=1}^{N}\alpha_n + \sum_{n=1}^{N}\alpha_n - \sum_{n=1}^{N}\alpha'_n\right|_p < \varepsilon.$$

By taking the limit as ε goes to zero we get the desired result. □

This is not true for series in $\mathbb{R}$ in general. For instance the **alternating harmonic series**

$$\ln(2) = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \frac{1}{5} - \frac{1}{6} + \dots$$
$$\frac{3}{2}\ln(2) = 1 + \frac{1}{3} - \frac{1}{2} + \frac{1}{5} + \frac{1}{7} - \frac{1}{4} + \dots$$

Proposition 4. *The completion of $\mathbb{Z}$ with respect to the norm $|\cdot|_p$, is equal to the definition 3 of $\mathbb{Z}_p$.*

Proof. We have shown that $\mathbb{Z} \subset \mathbb{Z}_p$. We need to prove that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and that $\mathbb{Z}_p$ is complete. Let $x \in \mathbb{Z}_p$. Define the sequence $y_n \in \mathbb{Z}$ as the smallest natural number such that $y_n \equiv \varepsilon_n(x)$ in $\mathbb{Z}/p^n\mathbb{Z}$. This sequence is a Cauchy sequence since for $N < i < j$ we have that

$$y_i \equiv \varepsilon_i(x) = \varepsilon_j(x) = y_j$$

in $\mathbb{Z}/p^j\mathbb{Z}$ but this means that $|y_i - y_j|_p < 1/p^j$ so $\lim_{N\to\infty}|y_j - y_i|_p = \infty$. Thus we have that $(y_n)_{n\in\mathbb{N}}$ converges to x. We know that $\mathbb{Z}_p$ is compact since it is a product of compact spaces, hence it is complete. Thus we have shown that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. □

Proposition 5. *The completion of $\mathbb{Q}$ with respect to the norm $|\cdot|_p$, is equal to definition 5 of $\mathbb{Q}_p$ and defines a topology that is locally compact and contains $\mathbb{Z}_p$ as an open subring.*

The proof is similar to that of 2.3.2 and will be left to the reader.

Theorem 2.3.1. *(Ostrowski) Every nontrivial absolute value of the field of rational numbers is of the form*

$$|\cdot|^{\alpha}, \quad 0 < \alpha \leqslant 1, \qquad \text{or} \qquad \rho^{v(\cdot)}, \quad 0 < \rho < 1$$

with $|\cdot|$ being the absolute value.

Proof. The proof is rather technical and will be omitted in this text. The reader can find the proof in Borevich [8] pp. 37-39. □

This tells us that the completion of $\mathbb{Q}$ with respect to any nontrivial norm is topologically equivalent to $\mathbb{R}$ or to $\mathbb{Q}_p$. The proof of this theorem can be found in [8]

We have defined the field $\mathbb{Q}_p$ of p-adic numbers to be the field of fractions of the inverse limit of the finite rings $\mathbb{Z}/p^n\mathbb{Z}$, and shown it to be equal to the completion of $\mathbb{Q}$ with respect to the p-adic norm. However both of these notions are rather abstract entities. If we want to work with the p-adic numbers in a more convenient and concrete manner, to perform for instance calculations, we can equivalently represent the p-adic numbers as power series.

We can write the p-adic integer x uniquely as the sequence

$$\{a_0, a_0 + pa_1, a_0 + a_1p + a_2p^2, ...\}$$

with $0 \leqslant a_n \leqslant p-1, \forall n \in \mathbb{N}$ by using the following algorithm. Let a_0 be the smallest natural number such that $a_0 \equiv \varepsilon_1(x)$ and a_n be the smallest natural number such that $a_n = \varepsilon_{n+1}(x - \varepsilon_n(x))$. We will call this representation the **canonical sequence** of x. Then x will be equal to the series:

$$\sum_{i=0}^{\infty} a_i p^i = a_0 + a_1p + a_2p^2 + ...,$$

because $a_i \in \mathbb{Z} \subset \mathbb{Z}_p$ for all i in $\mathbb{N}$ so we can regard the integers a_i as p-adic integers.

The representation of p-adic integers as the power series above is reminiscent of the expansion of real numbers as infinite decimals.

Proposition 6. *Let $\alpha \in \mathbb{Q}_p^*$. Then α has a unique representation of the form*

$$\alpha = \sum_{i=k}^{\infty} a_i p^i$$

*With $a_k \neq 0$ so $k = ord_p\alpha$, and $a_i \in \{0, 1, .., p-1\}$ for all $k < i$. We will call this sequence the **canonical sequence** of α.*

Proof. Let $\alpha \in \mathbb{Q}_p$ We can write $\alpha = \frac{p^i u}{p^j v}$ where u, v are invertible in $\mathbb{Z}_p$ so $u/v = u' \in \mathbb{Z}_p$ and $k = i - j \in \mathbb{Z}$. We can therefore write $\alpha = p^k u'$. Since $u' \in \mathbb{Z}_p$ its canonical series

$$a_0 + a_1 p + a_2 p^2 + ...$$

is well-defined with $0 < a_0 \leqslant p-1$ and $0 \leqslant a_i \leqslant p-1$. We can now write α of the form

$$\alpha = p^k \sum_{i=0}^{\infty} a_i p^i = \sum_{i=k}^{\infty} a_{i-k} p^i$$

by setting $a_i = a_{i+k}$ to obtain the desired representation.

Now suppose $\alpha = \sum_{i=k}^{\infty} a_i p^i = \sum_{i=t}^{\infty} b_i p^i$ with $a_k \neq 0, b_t \neq 0$ and $a_i \in \{0, 1, ..., p-1\}$ for all i. Thus we have

$$\alpha = \lim_{m\to\infty} \sum_{i=k}^{m} a_i p^i = \lim_{m\to\infty} \sum_{i=t}^{m} b_i p^i$$

We know that the norm $|.|_p$ is continuous and therefore

$$k = \lim_{m\to\infty} k = \lim_{m\to\infty} |\sum_{i=k}^{m} a_i p^i|_p = |\sum_{i=t}^{m} b_i p^i|_p = \lim_{m\to\infty} t = t$$

In addition we have

$$\sum_{i=k}^{\infty} (a_i - b_i) p^i = \lim_{m\to\infty} \sum_{i=k}^{m} (a_i - b_i) p^i = 0$$

Suppose that $a_s \neq b_s$ and that s is minimal. Then we have that $|a_s - b_s|_p = 1$ and then we would have

$$\left| \sum_{i=k}^{\infty} (a_i - b_i) p^i \right|_p = |p^s|_p \neq 0$$

a contradiction □

Let's determine the canonical series of the 3-adic number $\alpha = -\frac{13}{8}$. First we notice that $\left|\frac{13}{8}\right|_3 = 1$. Thus $\alpha = \sum_0^{\infty} a_i 3^i$, $a_i \in \{0, 1, 2\}$. If $\alpha \to \frac{-13}{8}$ we need

$|-\frac{13}{8}-a_0|_3<1$. Since $|8|_3=1$ we have

$$\left|-\frac{13}{8}-a_0\right|_3=|-13-8a_0|_3$$

and therefore $8a_0\equiv -13 \pmod 3$ and $c_0=1$. Proceeding in this fashion we have that $-\frac{21}{8}=\sum_{i=1}^{\infty}c_i3^i$, i.e. $-\frac{7}{8}=\sum_{i=0}^{\infty}c_{i+1}3^i$, and thus we need $\left|-\frac{7}{8}-a_1\right|_3<1$ so we have $8c_1=-7 \pmod 3$ i.e. $c_1=1$ and using the same method we get that $c_2=2$ and thus we have

$$\frac{-13}{8}=1+1\cdot 3+2\cdot 3^2+\sum_{i=3}^{\infty}c_i3^i$$

which simplifies to

$$\frac{-7}{8}=\sum_{i=0}^{\infty}c_{i+3}3^i.$$

We have already seen this equation, thus we have the recurrence relation $c_{i+2}=c_i$ for $i>0$. And we can write:

$$\frac{-13}{8}=1+\sum_{i=1}^{\infty}c_i3^i,\quad c_i=\begin{cases}1 & \text{if } i \text{ is even}\\ 2 & \text{if } i \text{ is odd}\end{cases}.$$

2.4 p-adic equations

Lemma 1. *Let ... $\to D_n \to D_{n-1} \to$ ... $\to D_1$ be a projective system, and let $D=\lim_{\leftarrow} D_n$ be its projective limit. If the D_n are finite and non empty then D is nonempty.*

Proof. See Serre ([7]) □

This lemma is useful for us because it gives us an equivalence of solutions in the p-adic integers (or p-adic numbers) to solutions in the rings $\mathbb{Z}/p\mathbb{Z}$.

If $f\in\mathbb{Z}_p[X_1,X_2,...,X_m]$ and n is an integer we will from now on use the notation f_n for the polynomial with coefficients in $\mathbb{Z}/p^n\mathbb{Z}$ deduced from f by reduction of its coefficients modulo p^n.

Proposition 7. *Let $f^{(i)}\in\mathbb{Z}_p[X_1,X_2,...,X_m]$ be polynomials with p-adic integer coefficients. The $f^{(i)}$ all have a common zero if and only if for all $n>1$, the*

polynomials $f_n^{(i)}$ have a common zero in $(A_n)^m$

Proof. Let D be the set of common zeros of the polynomials $f^{(i)}$ and D_i be the set of common zeros of the polynomials $f_n^{(i)}$ for $n > 1$. The D_n is finite for all $n > 1$ and we have that $D = \varprojlim D_n$. By the proposition above we know that D is nonempty if and only if all the D_n are nonempty which proves the proposition. □

We say that a point $x = (x_0, ..., x_m) \in (\mathbb{Z}_p)^m$ is **primitive** if $x_i \in \mathbb{U}_p$ for some $0 \geqslant i \geqslant m$ or equivalently that not all x_i are divisible by p. We define primitive elements of A_n in an analogous fashion.

Proposition 8. *Let $f^{(i)} \in \mathbb{Z}_p[X_1, ..., X_m]$ be a family of polynomials with p-adic integers coefficients. The following are equivalent:*

1. *The $f^{(i)}$ have a nontrivial common zero in $(\mathbb{Q}_p)^m$*
2. *The $f^{(i)}$ have a common primitive zero in $(\mathbb{Z}_p)^m$*
3. *For all $n > 1$, the $f_n^{(i)}$ have a common primitive zero in $(A_n)^m$*

Proof. $1 \implies 2$: If $x = (x_1, ..., x_m)$ is a nontrivial common zero of the $f^{(i)}$ in $\mathbb{Q}_p$ we put

$$y = p^{-h}x, \quad h := \inf v_p(x_1), ..., v_p(x_m)$$

Now y is a primitive element of $(\mathbb{Z}_p)^m$ and it is a common zero for all $f^{(i)}$.
$2 \implies 1$: Primitive zero is nontrivial and $\mathbb{Z}_p \subset \mathbb{Q}_p$.
The equivalence of the last two statements follow from 7 □

2.4.1 Lifting solutions

Let's assume f is a polynomial of n variables in $\mathbb{Z}_p$. A natural question to ask is whether there exist solutions to the equation $f(x) = 0$ for $x \in \mathbb{Z}_p^*$. This is not always obvious. Since $\mathbb{Z}$ is the only touchstone of $\mathbb{Z}_p$ that we have for the moment we will have to find a method to find the solutions.

Looking back at 2.3.1, that is the equation $x^2 \equiv 3 \pmod{11^n}$, gives us the intuition that we can **lift solutions** from the finite fields $\mathbb{Z}/p\mathbb{Z}$ to the field $\mathbb{Z}_p$ by means of an iterative method that is similar to the Newton–Raphson method used to

find roots to functions in $\mathbb{R}$. First we will define a **formal derivative** of a polynomial $f(x) = \sum_{i=1}^{n} a_i x^i$ as the polynomial $\sum_{i=1}^{n} i a_i x^{i-1}$ denoted $f'(x)$ thus circumventing the need for limits. In addition, if f is a polynomial of several variables we define the **formal partial derivative** denoted $\frac{\partial f}{\partial X_i}$ in the same natural way.

Lemma 2. *Let $f \in \mathbb{Z}_p[X]$ and let f' be its derivative. Let $x \in \mathbb{Z}_p, n, k \in \mathbb{Z}$ such that*

$$0 \leqslant 2k < n, \quad f(x) = 0 \ (mod\ p^n), \quad v_p(f'(x)) = k.$$

Then there exist $y \in \mathbb{Z}_p$ such that

$$f(y) \equiv 0 \ (mod\ p^{n+1}), \quad v_p(f'(y)) = k, \quad y \equiv x \ (mod\ p^{n-k}).$$

Proof. We write y of the form $x + p^{n+k}z, z \in \mathbb{Z}_p$. By Taylor's formula we have

$$f(y) = f(x) + p^{n-k} z f'(x) + p^{2n-2k} a, a \in \mathbb{Z}_p.$$

Since $f(x) = 0 \pmod{p^n}$ and $f'(x) = 0 \pmod{p^k}$ we can write $f(x) = p^n u$, $f'(x) = p^k v$ with $u \in \mathbb{Z}_p$ and $v \in \mathbb{U}_p$. This allows us to choose z such that

$$b = zv = 0 \pmod{p}.$$

From this we get

$$f(y) = f(x) + p^n(b + zv) + p^{2n-2k} a \equiv 0 \pmod{p^{n+1}}$$

since $2n - 2k > n$. Finally by applying Taylor's formula again to f' we can see that $f'(y) \equiv p^k v \pmod{p^{n-k}}$, and since $n - k > k$, we see that $v_p(f'(y)) = k$. □

Theorem 2.4.1. *Let $f \in \mathbb{Z}_p[X_1, ..., X_m], x = (x_i) \in (\mathbb{Z}_p)^m$, $n, k \in \mathbb{Z}$ and $j \in \mathbb{Z}$ such that $0 \leqslant j \leqslant m$. Suppose that $0 < 2k < n$ and that*

$$f(x) = 0 \ (mod\ p^n) \quad \text{and} \quad v_p\left(\frac{\partial f}{\partial X_j}(x)\right) = k.$$

Then there exists a zero y of f in $(\mathbb{Z}_p)^m$ which is congruent to x modulo p^{n-k}.

Proof. Suppose that $m = 1$. By using the above lemma to $x^{(0)} = x$, we obtain

$x^{(1)} \in \mathbb{Z}_p$ congruent to $x^{(0)} \equiv \pmod{p^{n-k}}$) and such that

$$f(x^{(1)}) \equiv 0 \pmod{p^{n+1}} \quad \text{and} \quad v_p(f'(x^{(1)})) = k$$

we can continue to apply the lemma to $x^{(1)}$, by replacing n by $n+1$ and so on. By induction we have a sequence $x^{(0)}, x^{(1)}, ..., x^{(q)}, ...$ such that

$$x^{(q+1)} = x^{(q)} \pmod{p^{n+q-k}}, \quad f(x^{(q)}) = 0 \pmod{p^{n+q}}.$$

This sequence is a Cauchy sequence and since $\mathbb{Z}_p$ is a complete metric space we have that $(x^{(n)})_{n\in\mathbb{N}}$ converges to a limit y, we have that $f(y) = 0$ by the continuity of f and that $f = x \pmod{p^{n-k}}$ hence we have proved the theorem for $m = 1$.

For $m > 1$ we can reduce it to the case of $m = 1$ by first fixing all the variables except for x_0, i.e. let $\bar{f} \in \mathbb{Z}_p[X_1]$ be the polynomial in one variable obtained by replacing $x_i, 0 < i$ by x_i thus there exists a $y_0 \in \mathbb{Z}_p$ such that

$$y_0 \equiv x_0 \pmod{p^{n-k}}, \quad \bar{f}(y_0) = 0.$$

We can do this for all $0 < i$ to get $y = (y_i)_{0\leqslant i\leqslant m}$ that satisfies the desired condition. □

Given an x and y as stated in the theorem above we say that x **lifts to a solution** y of f .

Definition 9. *If f is a polynomial over a field k, a zero of f is called **simple** if at least one of the partial derivatives $\frac{\partial f}{\partial X_j}$ is nonzero at x.*

Corollary 2. *(Hensel's Lemma) Every simple zero of the reduction modulo p of a polynomial $f \in \mathbb{Z}_p[X_1, ..., X_m]$ lifts to a zero of f in $\mathbb{Z}_p$.*

Corollary 3. *Let p be a prime, $a \in \mathbb{Z}_p^*$, $Q(X) = \sum_{i=1}^{n} a_i X_i X_j$ be a homogeneous polynomial of degree 2 with coefficients in $\mathbb{Z}_p$ such that $\det(a_{ij})$ is invertible and $a_{ij} \in \mathbb{Z}_p$. If $p = 2$ then every solution x of $f(x) \equiv a \pmod 8$ lifts to a solution in $\mathbb{Z}_p$ and if $p \neq 2$ then every solution of the equation $f(x) = a \pmod p$ lifts to a solution in $\mathbb{Z}_p$.*

2.4.2 Squares in $\mathbb{Q}_p$

In seeking to understand quadratic forms over a global field F and its subrings, an important approach over the years has been to first consider quadratic forms over the completions of F with respect to F's discrete spots, and then try to tie together whatever we have learned in the local settings to obtain conclusions over F. In our case $\mathbb{Q}$ is our global field and $\mathbb{Q}_p$ and $\mathbb{R}$ will be our local fields. We have already seen knowing the squares of numbers in the field $\mathbb{Z}/p\mathbb{Z}$ gives us a lot to work with so a natural progression is to study the squares of the p-adic numbers. With some clever observations we can deduce that the square class of an element $a \in \mathbb{Q}_p$ is determined by a's canonical representation in a smaller ring.

Let's extend the definition of the Lagrange symbol to that of all units of $\mathbb{Q}_p$, for $p \neq 2$ by defining

$$\left(\frac{u}{p}\right) := \left(\frac{\varepsilon_1(u)}{p}\right).$$

Recall that $\varepsilon_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ is the natural projection from the p-adic integers to the integers modulo p^n. We will see how this is a natural extension with the following theorem,

Theorem 2.4.2. *Let $\alpha = p^n u \in \mathbb{Q}_p^*$, with $n \in \mathbb{Z}$, p a prime and $u \in \mathbb{U}_p$. Then:*

1. *if $p \neq 2$: then $\alpha \in (\mathbb{Q}_p^*)^2 \iff n \equiv 0 \ (mod\ 2)$ and $\left(\frac{u}{p}\right) = 1$*
2. *if $p = 2$: then $\alpha \in (\mathbb{Q}_2^*)^2 \iff v \equiv 0 \ (mod\ 2)$ and $\varepsilon_3(u) = 1$.*

Proof. Assume that p is an odd prime number and let $u \in \mathbb{U}_p$. Then by Hensel's lemma we know that if u has a solution to the equation $u \equiv x^2 \pmod{p}$ then the equation $x^2 = u \in \mathbb{Z}_p[X]$ also has a solution. In addition if $u \in \mathbb{U}_p$ is a square in $\mathbb{Z}_p$ then $u = x^2$ with $x \in \mathbb{U}_p$ and then $\varepsilon_1(x)\varepsilon_1(x) = \varepsilon_1(u)$ thus $\varepsilon_1(u)$ is a square modulo p. So u is a square in $\mathbb{U}_p$ if and only if its projection mod p is a square.

Now if $p = 2$ and $\varepsilon_3(u) = 1$ then the equation $x^2 = u \pmod{8}$ has a solution and by Hensel's lemma the equation $x^2 = u \in \mathbb{Z}_p[X]$ also has a solution. On the other hand if u is a square in $\mathbb{U}_p$ then by the same argument as above $\varepsilon_3(u)$ is a square in $\mathbb{Z}/8\mathbb{Z}$. By looking at all the possible squares of $\mathbb{Z}/8\mathbb{Z}$ we can see that $\varepsilon_3(u) = 1$.

And we know that if $\alpha \in \mathbb{Q}_p^*$ we can write α uniquely (1) as $\alpha = p^n a$ where $n \in \mathbb{Z}$

and $a \in \mathbb{U}_p$.

$$\alpha \in (\mathbb{Q}_p^*)^2 \iff \exists s \in \mathbb{Z}, v \in \mathbb{U}_p, p^n a = (p^s v)^2 \iff \exists s \in \mathbb{Z}, v \in \mathbb{U}_p n = 2s, a = v^2,$$

giving us the desired result. □

Assume that p is an odd prime, and note that the Legendre symbol is equal to one for $u \in \mathbb{U}_p$ if and only if u is a square in $\mathbb{U}_p$ and is multiplicative and therefore our extension of the Legendre symbol is consistent with previous results.

2.5 Hilbert Symbol

In this paragraph we will be working with the fields $K = \mathbb{Q}_p$ or $K = \mathbb{R}$ so for convenience sake K will denote one of these fields.

Definition 10. *Hilbert symbol Let $a, b \in K^*$ we define the Hilbert symbol of a and b as (a, b) and*

$$(a,b) = \begin{cases} 1 & \text{if } z^2 - ax^2 - by^2 = 0 \text{ has a nontrivial solution in } K^3, \\ -1 & \text{otherwise.} \end{cases}$$

We will also denote, to be precise, $(a, b) = (a, b)_\infty$ if $K = \mathbb{R}$ and $(a, b) = (a, b)_p$ if $K = \mathbb{Q}_p$.

The Hilbert symbol is somehow analogous to the Legendre symbol and is connected to it by an equation as we will discuss later in this text.

An equivalent manner to define the Hilbert symbol is that $(a, b) = 1$ if a or b are square numbers or if a is equal to the norm of an element of the quadratic extension $K[\sqrt{b}]$ and $(a, b) = -1$ otherwise.

2.5.1 Properties of the Hilbert symbol

Proposition 9. *The Hilbert symbol satisfies the formulas:*

$$(a,b) = (b,a) \text{ and } (a,c^2) = 1,$$
$$(a,-a) = 1 \text{ and } (a,1-a) = 1,$$
$$(a,b) = 1 \Rightarrow (aa',b) = (a',b),$$
$$(a,b) = (a,-ab) = (a,(1-a)b).$$

Proof. The symmetry of the Hilbert symbol is obvious. Note that $(c,0,1)$ is a nontrivial zero of $z^2 - ax^2 - c^2y^2$ giving us $(a,c^2) = 1$.

Also $(0,1,1)$ and $(1,1,1)$ are nontrivial solutions to $z^2 - ax^2 + ay^2$ and $z^2 - ax^2 - (1-a)y^2$ respectively giving us $(a,-a) = (a,1-a) = 1$.

To prove the third line in the proposition we can first note that if a or b are square then by the first the third line is true by line 1.

Now suppose that a and b are not square. We will prove that $(a,b) = 1 \iff a \in NK_b^*$, the subgroup of norms of elements of the quadratic extension $K[\sqrt{b}]$.

We first proof ($\Leftarrow$). Suppose that $a \in NK_b^*$ then we can write $a = z_0^2 - by_0^2$ and thus $z^2 - ax^2 - by^2$ has a nontrivial solution i.e. $(a,b) = 1$.

And then ($\Rightarrow$). Now suppose that $(a,b) = 1$ then there exist $(x_0,y_0,z_0) \in (K)^3$ with $x_0 \neq 0$ because otherwise b would be a square. Back to the proof of

$$(a,b) = 1 \Rightarrow (aa',b) = (a',b)$$

$$(a',b) = 1 \iff a' \in NK_b^* \iff aa' \in NK_b^* \iff (aa',b) = 1$$

Lastly

$$(a,b) = (a,-a)(a,b) = (a,-ab), \quad (a,b) = (a,1-a)(a,b) = (a,(1-a)b)$$

□

From this we can deduce that the Hilbert symbol is (multiplicatively) bilinear:

$$(ab, c) = (a, c)(b, c)$$
$$(a, bc) = (a, b)(a, c)$$

symmetric:

$$(a, b) = (b, a)$$

nondegenerate with respect to $(K^*)^2$:

$$(a, b) = 1 \quad \forall b \iff a \in (K^*)^2$$

on the vector space $K^*/(K^*)^2$.

Lemma 3. *Let $v \in U_p$ be a p-adic unit. If the equation $z^2 - px^2 - vy^2 = 0$ has a nontrivial solution in $\mathbb{Q}_p$, it has a solution (z, x, y) such that $z, y \in \mathbb{U}_p$ and $x \in \mathbb{Z}_p$.*

Proof. We have by 8 that the given equation has a primitive solution (z, x, y) in $\mathbb{Z}_p$. We will show that the solution satisfies the stated property. Suppose that $z \notin \mathbb{U}_p$ or $y \notin \mathbb{U}_p$ or in other words $p|y$ or $p|z$. Since

$$z^2 - vy^2 \equiv 0 \pmod{p}$$

and $v \in \mathbb{U}_p$, this means that p divides both y and z and therefore $px^2 = 0 \pmod{p^2}$ that is $p|x$. This contradicts the fact that (z, x, y) is a primitive solution. □

Theorem 2.5.1. *We have:*

$$(a, b)_\infty = \begin{cases} 1 & \text{if } a > 0 \text{ or } b > 0, \\ -1 & \text{otherwise.} \end{cases}$$
$$(a, b)_2 = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)}$$
$$(a, b)_p = (-1)^{\alpha\beta\varepsilon(p)} \left(\frac{\bar{u}}{p}\right)^\beta \left(\frac{\bar{v}}{p}\right)^\alpha$$

where $a = p^\alpha u$ and $b = p^\beta v$ and $u, v \in \mathbb{U}$ and $\bar{u} := \varepsilon_1(u), \bar{v} := \varepsilon_1(v)$.

Proof. The case for $(a, b)_\infty$ is trivial. Suppose that $p \neq 2$. First we observe that the

exponents α and β depend only on their representative class modulo 2. Thus we only have to consider three cases.

Case where $\alpha = 0, \beta = 0$: The equation

$$z^2 - ux^2 - vy^2 = 0$$

has a nontrivial solution by 0.3. And since the discriminant of this quadratic form is in $\mathbb{U}_p$ it lifts to a p-adic solution. Hence $(u, v) = 1$.

Case where $\alpha = 1, \beta = 0$: Since $(u, v) = 1$ by the argument above we have that $(pu, v) = (p, v)$ by the biliniarity of the Hilbert symbol. Thus we must prove that

$$(v, p) = \left(\frac{\bar{v}}{p}\right).$$

Since $v \in \mathbb{U}$ the Legendre symbol $\left(\frac{\bar{v}}{p}\right) = \pm 1$ if it is equal to 1 then it is a square. Otherwise it is equal to -1 and then the above lemma shows that $z^2 - px^2 - vy^2 = 0$ does not have a nontrivial solution so $(p, v) = -1$.

Case where $\alpha = 1$, $\beta = 1$: We must prove that

$$(pu, pv) = (-1)^{\varepsilon(p)} \left(\frac{\bar{u}}{p}\right) \left(\frac{\bar{v}}{p}\right).$$

We have that

$$(pu, pv) = (pu, -p^2uv) = (pu, -uv)$$

and by the case above we have that

$$(pu, pv) = (pu, -uv) = \left(\frac{-\bar{u}\bar{v}}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{\bar{u}\bar{v}}{p}\right) = (-1)^{\varepsilon(p)} \left(\frac{\bar{u}}{p}\right) \left(\frac{\bar{v}}{p}\right).$$

The proof for $p = 2$ is similar to that of the proof above and will be omitted the curious reader can see [7]. □

For convenience sake we will denote $\mathbb{Q}_\infty = \mathbb{R}$ and $\mathcal{V} = \{p, p \text{ is prime}\} \cup \{\infty\}$.

Theorem 2.5.2. *(Hilbert's law of reciprocity) If $a, b \in \mathbb{Q}^*$, we have $(a, b)_v = 1$ for*

all $v \in \mathcal{V}/A$ where A is a finite set and

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

Proof. Let $a = (-1)^{n_0}p_1^{n_1}p_2^{n_2}...p_k^{n_k}$, $b = (-1)^{m_1}p_1^{m_1}p_2^{m_2}...p_l^{m_l}$ be the factorisation of a and b with the p_i prime numbers and $m_i, n_j \in \mathbb{Z}$ for convenience we will let $p_0 := -1$. This factorisation is unique. Since the Hilbert symbol is bilinear we have that

$$\prod_{v\in\mathcal{V}}(a,b)_v = \prod_{p_i|a}\prod_{p_j|b}(\prod_{v\in\mathcal{V}}(p_i,p_j)_v)^{n_i m_j}.$$

It suffices to prove the result for -1, and prime numbers.

Case where $a = -1$, $b = -1$: We have that $(-1,-1)_\infty = -1$ and

$$(-1,-1)_2 = (-1)^{\varepsilon(-1)\varepsilon(-1)} = -1 \text{ and }, \quad (-1,-1)_p = (-1)^0\left(\frac{-1}{p}\right)^0\left(\frac{-1}{p}\right)^0 = 1 \text{ if } p \neq 2.$$

Case where $a = -1, b = \ell, \ell$ *is prime:* One has $(-1,2)_\infty = 1$. If $\ell = 2$ one has

$$(-1,2)_p = (-1)^0\left(\frac{-1}{p}\right)^0\left(\frac{2}{p}\right)^0 = 1$$

for all primes p. If $\ell \neq 2$

$$(-1,\ell)_p = (-1)^0\left(\frac{-1}{p}\right)^0\left(\frac{-1}{p}\right)^0 = 1, \text{if } p \neq \ell, 2 \text{ and} \quad (-1,\ell)_\ell = (-1,\ell)_2 = (-1)^{\varepsilon(\ell)}.$$

The product $(-1,\ell)_l(-1,\ell)_2$ is equal to 1.

Case where $a = \ell, b = \ell', \ell$ *and* ℓ' *are prime:* Since ℓ, ℓ' are positive $(\ell,\ell')_\infty = 1$. If $\ell = \ell'$ we have that

$$(\ell,\ell)_v = (\ell,-\ell^2)_v = (\ell,-1)_v(\ell,\ell^2)_v = (\ell,-1)_v.$$

We have already considered this case above. If $\ell \neq \ell'$ we can assume $\ell < \ell'$. If $\ell = 2$

we have $(\ell, 2)_p = 1$ for all $p \neq \ell', 2$ and

$$(\ell, \ell')_2 = (-1)^{\varepsilon(\ell)\varepsilon(\ell')}, \quad (\ell, \ell')_l = \left(\frac{\ell'}{\ell}\right), \quad (\ell, \ell')_{\ell'} = \left(\frac{\ell}{\ell'}\right),$$

$$(\ell, 2)_2 = (-1)^{\omega(\ell)}, \quad (l, 2)_l = \left(\frac{2}{\ell}\right) = (-1)^{\omega(\ell)}$$

By the law of quadratic reciprocity we have that

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

Hence the product equals to 1. □

This theorem is analogous to the theorem of quadratic reciprocity and in fact uses the theorem in its proof. The finite set of v where $(a, b)_v = -1$ is a subset of the prime factors of a and b in addition to ∞. The product formula is essentially equivalent to the law of quadratic reciprocity. It is however more interesting since it extends to all algebraic number fields.

Theorem 2.5.3. *Let $(a_i)_{i\in I}$ be a finite family of elements in $\mathbb{Q}^*$ and let $(\epsilon_{i,v})_{i\in I, v\in\mathcal{V}}$ be a family of numbers equal to ± 1. There exist $x \in \mathbb{Q}^*$ such that $(a_i, x)_v = \epsilon_{i,v}$ for all $i \in I$ and $v \in \mathcal{V}$ if and only if*

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

This theorem is crucial as we will later see later on but will be stated without proof. In fact this theorem lets us pass from the local setting to the global and is thus a key element in proving the case $n = 4$ of the Hasse-Minkowski theorem. The proof relies on the famous Dirichlet theorem which uses results from complex analysis and is highly nontrivial, stated below.

Theorem 2.5.4 (Dirichlet theorem)**.** *If a and m are relatively prime integers bigger than zero, there are infinitely many prime numbers p such that $p \equiv a \pmod m$*

Chapter 3

Quadratic forms

In this chapter we will assume that F is a field of characteristic not equal to 2 and V is a F-vector space. The theory of quadratic forms can simplify polynomials over a field to simpler forms. It categorizes quadratic forms to equivalence classes, and provides invariants to each equivalence class. We will see in the proof of Hasse-Minkowski Theorem how this simplification saves us much trouble.

We will first introduce the quadratic forms in a general sense and then look at some results by restricting ourselves to certain fields.

There are few definitions of quadratic forms. The following is the most intuitive:

Definition 11. *A* ***quadratic form*** *in n variables, sometimes called an n-**ary quadratic form**, over a field F is a function $Q : F^n \to F$ of the form*

$$Q(x_1, ..., x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \in F[x_1, ..., x_n].$$

A quadratic form is a **homogeneous polynomial** (see 20) of degree 2 in n variables with coefficients in F.

Definition 12. *Let Q be a quadratic form over F the bilinear symmetric map $B : V \times V \to F$*

$$B(\boldsymbol{x}, \boldsymbol{y}) = \frac{Q(\boldsymbol{x} + \boldsymbol{y}) - Q(\boldsymbol{x}) - Q(\boldsymbol{y})}{2}$$

is called its ***associated bilinear form*** *.*

It is easily checked that the associated bilinear form is bilinear and symmetric,

that is $B(-, \mathbf{y})$ and $B(\mathbf{x}, -)$ are both linear and $B(\mathbf{x}, \mathbf{y}) = B(\mathbf{y}, \mathbf{x})$. Note that $B(\mathbf{x}, \mathbf{x}) = Q(\mathbf{x})$ and that if B is some bilinear symmetric form $B : V \times V \to F$ and $(e_i)_{1 \leqslant i \leqslant n}$ is a basis for V then we we can deduce that

$$B(\mathbf{x}, \mathbf{x}) = \sum_{i=1}^{n} a_{ij} x_i x_j, \quad a_{ij} := B(e_i, e_j).$$

This tells us that there is a bijective correspondence between symmetric bilinear forms and quadratic forms.

Now some notation. Let $Q(x_1, ..., x_n)$ and $H(x_1, ..., x_m)$ be two quadratic forms; we will denote by $Q + G$ the quadratic form

$$Q(x_1, ..., x_n) + H(x_{n+1}, ..., x_{n+m})$$

and set $f - q = f + (-q)$

3.1 Matrix representation

Let $Q(x_1, ..., x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$ be an n-ary quadratic form over F. Since F has characteristic not equal to 2 and F is commutative we can use this symmetry to write Q in a more convenient way by replacing a_{ij} and a_{ji} with $\frac{a_{ij}+a_{ji}}{2}$. This does not change the quadratic form and gives us the relation $a_{ij} = a_{ji}$.

Definition 13. *With the convention above the symmetric matrix $A = (a_{ij}) \in M_n(F)$ is called the **Gramm matrix** of Q.*

Note that A is symmetric. We can express a quadratic form Q in terms of linear algebra with it's Gramm matrix A as follows

$$Q(\mathbf{x}) = \mathbf{x}^t A \mathbf{x}, \quad \mathbf{x} = (x_1, ..., x_n)$$

An example of a quadratic form and it's Gramm matrix A.

$$Q(x, y) = 2x^2 - 8xy - 17y^2, \quad A = \begin{pmatrix} 2 & -4 \\ -4 & -17 \end{pmatrix}$$

By clever choice of basis $u = 2x + y$, $v = x + 3y$, we can write

$$Q(x, y) = 2x^2 - 8xy - 17y^2 = u^2 - 2v^2 = H(u, v)$$

Now if $H(u, v)$ represents some integer n over $\mathbb{Q}$ then we can explicitly represent the same integer in the form Q over $\mathbb{Q}$. For instance

$$1 = H(3, 2) = Q\left(\frac{7}{5}, \frac{1}{5}\right)$$

Quadratic forms Q and H that are related this way set up a bijection between the representations

$$n \underset{\mathbb{Q}}{\rightarrow} Q \quad , \quad n \underset{\mathbb{Q}}{\rightarrow} H$$

Definition 14. *Let Q and H be n-ary quadratic forms over a field F, with respective Gramm matrices A, C. We say that say that H is **represented by** Q over F, denoted $H \underset{F}{\rightarrow} Q$, if there exist a matrix $X \in M_n(F)$ such that $C = X^t A X$.*

Definition 15. *Let Q and H be as in the definition above, We say that Q and H are **equivalent** over F, denoted $Q \sim H$,if there exist $X \in GL_n(F)$ such that $C = X^t A X$.*

Out of all the possible quadratic forms this equivalence is an equivalence relation and in the study of representation two quadratic forms in the same equivalence class represent exactly the same elements. Because given two equivalent quadratic forms Q and Q' with Gramm matrices A and B we can express A by means of B and an invertible matrix X. That is $A = X^t B X$ and thus we have:

$$Q(\mathbf{x}) = \mathbf{x}^t A \mathbf{x} = \mathbf{x}^t X^t B X \mathbf{x} = (X\mathbf{x})^t B (X\mathbf{x}) = \mathbf{y}^t B \mathbf{y}^t = Q'(\mathbf{y})$$

and since $X \in GL_n(F)$ there is a bijection between $\mathbf{x}$ and $\mathbf{y}$ and thus between the representations of Q and Q'.

Note that

$$\det(B) = \det(X)^2 \det(A).$$

And since $X \in GL_n(R)$ we have $\det(X) \in F^*$ so the determinant of our Gramm matrix is invariant modulo squares in F^*.

Definition 16. *For a quadratic form Q we will call it's* ***discriminant*** *noted $d(Q)$ the equivalence class of the determinant of it's Gramm matrix in $F/(F^*)^2$. If $d(Q) \neq 0$ we say that Q is* ***nondegenerate****, and that it is* ***degenerate*** *otherwise.*

Theorem 3.1.1. *Let Q be a quadratic form in n variables over a field F. There exists $a_1, ..., a_n \in F$ such that*

$$Q \sim a_1 X_n^2 + ... + a_n X_n^2$$

Proof. See Serre [7] □

The theorem above can be proved in two different ways. First by recurrence on the dimension and using the fact that we can decompose our space into the span of an element, at which the quadratic form does not vanish, and its orthogonal complement. Another interesting proof is algorithmic by using the **algorithm of Gauß.** which is discussed in [3].

The Gramm matrix of the second quadratic form above is $\begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}$ and $d(Q) = a_1...a_n$

Definition 17. *The* ***rank*** *of Q defined in the theorem above is the number of indices i such that $a_i \neq 0$. It is equal to n if and only if $d(Q) \neq 0$.*

Theorem 3.1.2. *Let G be a nondegenerate quadratic form in n variables with and let $a \in F^*$. The following properties are equivalent:*

i) G represents a

ii) $G \sim H + aZ^2$ where H is a nondegenerate quadratic form in $n-1$ variables

iii) The form $F = G - aZ^2$ represents 0

Proof. The proof is quite straightforward and the curious reader can see Serre [7] for its details. □

We can still answer questions about representation for a degenerate quadratic form that is equivalent to

$$a_1 X_1^1 + .. + a_n X_n^2$$

because we can always define a quadratic form in fewer variables by disregarding the variables X_i for which $a_i = 0$ and thus using results that require the form to be nondegenerate.

3.2 quadratic forms over $\mathbb{F}_q$ and $\mathbb{C}$

In this section we will denote $q = p^n$ where p is some odd prime not equal to 2 and n is an integer and $\mathbb{F}_q$ a field with q elements.

Theorem 3.2.1. *Let $n > 1$. An n-ary quadratic form Q over $\mathbb{F}_q$ represents all elements of $\mathbb{F}_q^*$. In addition if $n > 2$ it represents all elements of $\mathbb{F}_q$.*

Proof. It suffices to proof that for all $a, b, c \in \mathbb{F}_q$ not equal to zero the equation

$$ax^2 + by^2 = c$$

has a solution. Let

$$A := \{ax^2 | x \in \mathbb{F}_q\}, \quad B := \{c - by^2 | y \in \mathbb{F}_q\}$$

One sees that both A and B have $\frac{q+1}{2}$ elements hence their intersection is nonempty. Thus we have a solution to the equation. □

Theorem 3.2.2. *Every nondegenerate quadratic form Q over $\mathbb{F}_q$ of rank $n \geqslant 1$ is equivalent to a quadratic form:*

$$X_1^2 + ... + X_{n-1}^2 + aX_n^2, \quad a \in \mathbb{F}_q^*$$

Proof. If $n = 1$ the statement is obvious. If $n \geqslant 2$, suppose that the statement is true for $n-1$, then by the theorem above Q represents 1 and by 3.1.2 Q is equivalent to a form $Z^2 + G$ where G is a form in $n-1$ variables with $d(G) \neq 0$. So by induction we have our result. □

Corollary 4. *Each quadratic form Q in over $\mathbb{F}_q$, such that $d(Q) \neq 0$, is uniquely determined by its rank and discriminant*

This results allows us to classify all quadratic forms of $\mathbb{F}_p$.

Theorem 3.2.3. *There is only one equivalence class of nondegenerate forms in n variables over* $\mathbb{C}$.

Proof. We can assume that our form can be written as

$$a_1X_1^2 + ... + a_nX_n^2$$

but since $\sqrt{a_1} \in \mathbb{C}$ we can use the change of variables $X_i \to \frac{1}{\sqrt{a_i}}X_i$ to get the desired result. □

3.3 Quadratic forms over $\mathbb{Q}_p$ and $\mathbb{R}$

Let Q be a nondegenerate n-ary quadratic form over $\mathbb{Q}_v$ where $v \in \mathcal{V}$ or we know that it is equivalent to a quadratic form

$$a_1X_1^2 + a_2X_2^2 + ... + a_nX_n^2$$

Let $e := \prod_{i<j}(a_i, a_j)_v$ we want to show that if Q is equivalent to another quadratic form

$$b_1X_1^2 + b_2X_2^2 + ... + b_nX_n^2$$

then $e = \prod_{i<j}(b_i, b_j)_v$

If $n = 1$ then $e = 1$. If $n = 2$ then one has $e = (a_1, a_2)$ so $e = 1$ if and only if the form

$$Z^2 - a_1X_1^2 - a_2X_2^2$$

represents 0 equivalently by 3.1.2 that $a_1X_1^2 + a_2X_2^2$ represents 1 but if $b_1X_1^2 + b_2X_2^2$ is also equivalent to Q then it also represents 1 and thus $(a_1, a_2) = (b_1, b_2)$.

If $n \geqslant 3$ we will give an idea of a proof of our claim by induction. The proof uses two theorems that we ask the reader to believe in, **Witt's Cancellation Theorem** and **Witt's Chain Equivalence Theorem** which can be seen in [4]. The idea of Witt's Chain Equivalence Theorem is that if B and B' are two orthogonal bases, one can construct a chain $B = B_1, B_2, ..., B_n = B'$ of orthogonal bases such that each B_i is obtained from B_{i-1} by changing at most two basis elements. In our case this means that we can assume that $a_1 = b_1$. On the other hand a consequence of

Witt's Cancellation Theorem tells us that if

$$a_1X_1^2 + ... + a_nX_n^2 \sim b_1X_1^2 + ... + b_nX_n^2 \quad \text{and} \quad a_1X_1^2 \sim b_1X_1^2$$

then

$$a_2X_2^2 + ... + a_nX_n^2 \sim b_1X_1^2 + b_2X_2^2 + ... + b_nX_n^2.$$

Note that since $d(Q) = a_1...a_n = b_1...b_n$ we have:

$$\prod_{i<j}(a_i, a_j)_v = (a_1, a_2a_3...a_n)_v \prod_{1<i<j}(a_i, a_j)_v = (a_1, a_1d(Q))_v \prod_{1<i<j}(a_i, a_j)_v$$

$$\prod_{i<j}(b_i, b_j)_v = (b_1, b_2b_3...b_n)_v \prod_{1<i<j}(b_i, b_j)_v = (b_1, b_1d(Q))_v \prod_{1<i<j}(b_i, b_j)_v$$

Now by induction on the quadratic forms

$$a_2X_2^2 + ...a_nX_n^2, \quad b_2X_2^2 + ... + b_nX_n^2$$

we have that $\prod_{1<i<j}(a_i, a_j) = \prod_{1<i<j}(b_i, b_j)$ and since $a_1 = b_1$ we have that $\prod_{i<j}(a_i, a_j)_v = \prod_{i<j}(b_i, b_j)_v$

Definition 18. *Let Q be a nondegenerate quadratic form of rank n that is equivalent to the quadratic form*

$$a_1X_1^2 + a_2X_2^2 + ... + a_nX_n^2$$

*We define the **Hasse invariant** e as*

$$e(Q) = \prod_{i<j}(a_i, a_j) \in \{1, -1\}$$

3.3.1 Representation

In this section p is a prime number.

Definition 19. *For $a \in \mathbb{Q}_p^*$ and $e \in \{1, -1\}$, we define*

$$H_a^e = \{x \in \mathbb{Q}_p^* | (a, x)_p = e\}$$

.

Lemma 4. *Suppose $H_a^e \neq \emptyset$ and $H_{a'}^{e'} \neq \emptyset$. Then*

$$H_a^e \cap H_{a'}^{e'} = \emptyset \iff a = a' \text{ and } e' = -e$$

Proof. $\Leftarrow$ is clear. We prove $\Rightarrow$.

Suppose $a \in (\mathbb{Q}_p^*)^2$ then $H_a^e = \mathbb{Q}_p^*$, but $\emptyset \neq H_{a'}^{e'}$ a contradiction with the hypothesis $H_a^e \cap H_{a'}^{e'} = \emptyset$. We can now assume that a, a' are not square numbers in $\mathbb{Q}_p^*$.

Let's view the Hilbert symbol as a map $(a, -)_p : \mathbb{Q}_p^*/\mathbb{Q}_p^*)^2 \to \{1, -1\}$ since a is not a square this is a surjective homomorphism; therefore the kernel, H_a^1, is the union of half of the square classes in $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$, as is H_a^{-1} (the other coset of the kernel), and hence $H_a^1 \cup H_a^{-1} = \mathbb{Q}_p^*$, a disjoint union; and similarly $H_{a'}^1 \cup H_{a'}^{-1} = \mathbb{Q}_p^*$. Then the hypothesis forces the equalities $H_a^{-e} = H_{a'}^{e'}$ and $H_a^e = H_{a'}^{-e'}$ giving us the desired result.

□

Theorem 3.3.1. *The n-ary quadratic form Q of rank n over $\mathbb{Q}_p$ represents 0 if and only if:*

i) $n = 2$ *and* $d(Q) = -1$

ii) $n = 3$ *and* $(-1, d(Q)) = e(Q)$

iii) $n = 4$ *and ether* $d \neq 1$ *or* $d = 1$ *and* $e(Q) = (-1, -1)$

iv) $n \geqslant 5$.

Proof.

i) The case $n = 2$:

The form $Q = a_1x_1^2 + a_2x_2^2$ represents 0 if and only if

$$a_1Q \sim x_1^2 - (-a_1a_2)x_2^2$$

represents 0 but this means that $-a_1a_2$ is a square in K and thus $d = a_1a_2 = -1$ in $K^*/(K^*)^2$

ii) The case $n = 3$:

The form $Q = a_1x_1^2 + a_2x_2^2 + a_3x_3^2$ represents 0 if and only if the form

$$-a_3Q \sim -a_3a_1x_1^2 - a_3a_2x_2^2 - x_3^2$$

Now by the definition of the Hilbert symbol we have that the form represents 0 if and only if

$$1 = (-a_3a_1, -a_3a_2) = (-1,-1)(-1,a_1)(-1,a_2)(a_3,a_3)(a_1,a_2)(a_1,a_3)(a_2,a_3)$$

but since $(a_3, a_3) = (-a_3^2, a_3) = (-1, a_3)$ we have that the form Q represents zero if and only if $1 = (-1, -d(Q))e(Q)$ that is $(-1, d(Q)) = e(Q)$.

iii) The case $n = 4$:

The form $Q = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$ represents 0 if and only there exist an element $x \in K^*/(K^*)^2$ such that the forms

$$a_1x_1^2 + a_2x_2^2 \text{ and } -a_3x_3^2 - a_4x_4^2$$

both represent x. That is by the case $n = 3$ it is equivalent to the following $(x, -a_1a_2) = -1$ and $(x, -a_3a_4) = -1$. Let A be the subset of $K^*/(K^*)^2$ that satisfies the first condition and B be the subset of $K^*/(K^*)^2$ that satisfies the second condition. Now A and B are nonempty because $a_1 \in A$ and $-a_3 \in B$. By 4 the relation $A \cap B = \emptyset$ is equivalent to

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

The first condition means that $d = 1$. If it is fulfilled one has

$$e(Q) = (a_1, a_2)(a_3, a_4)(a_3a_4, a_3a_4).$$

By using the relation $(x, x) = (-1, x)$ we get

$$e(Q) = (a_1, a_2)(a_3, a_4)(-, a_3a_4) = (a_1, a_2)(-a_3, a_4)(-1, -1)$$

And using $(a_1, a_2) = -(-a_3, -a_4)$ gives us the relation $e(Q) = -(-1, -1)$, in con-

clusion if $d \neq 1$ then the Q represents 0 over K and if $d = 1$ then it represents 0 if and only if $e(Q) \neq -(-1,-1)$ i.e. $e(Q) = (-1,-1)$

iv) The case $n \geqslant 5$: It suffice to treat the case $n = 5$. The proof of part *ii*) of the corollary below is a direct consequence of part *ii*) above and does not need the result *iv*) that we are proving. By using 4 and part *ii*) of the corollary below, we see that a quadratic form of rank 2 represents at least 2 elements of $K^*/(K^*)^2$ (because the number of elements in $K^*/(K^*)^2$ is 4 or 8), and the same is true for a quadratic form of rank $\geqslant 2$. Thus Q represents an element $a \in K^*/(K^*)^2$ distinct from d. One has

$$Q \sim aX^2 + Q'$$

where Q' is a quadratic form of degree 4 with discriminant equal to $d/a \neq 1$ thus by *iii*) in the corollary below we know that Q' represents 0 and so Q does also. □

Corollary 5. *Let $a \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. The n-ary quadratic form Q over $\mathbb{Q}_p$ of rank n represents a if and only if:*

i) $n = 1$ *and* $d(Q) = a$

ii) $n = 2$ *and* $(a, d(Q)) = e(Q)$

iii) $n = 3$ *and either* $d \neq -a$ *or* $d = -a$ *and* $e(Q) = (-1,-1)$

iv) $n \geqslant 4$.

Point *iv*) of 3.3.1 is rather interesting and one can ask questions if homogeneous polynomials of higher degree also have this property of always representing 0 if the form has enough variables. In fact E. Artin made the conjecture that all homogeneous polynomials of degree d over $\mathbb{Q}_p$ in at least $d^2 + 1$ variables have a nontrivial zero. The case $d = 3$ has been solved affirmatively and the general case was open for about thirty years. It was only in 1966 that G. Terjanian showed that **Artins conjecture** is false: there exist a homogeneous polynomial of degree 4 over $\mathbb{Q}_2$ in 18 variables that has no trivial zero.

Theorem 3.3.2. *Two quadratic forms over $\mathbb{Q}_p$, p prime, are equivalent if and only if they have the same rank, same discriminant and same Hasse invariant e.*

Proof. If two quadratic forms are equivalent they have the same discriminant and Hasse invariant. Now suppose that two quadratic forms Q and P have the same rank, discriminant and Hasse invariant. We will prove the claim by induction on the rank. The case $n = 0$ is trivial. The quadratic forms represent the same elements by 5 thus we can find $a \in K^*$ which is represented at the same time by Q and P this allows us to write

$$Q \sim aX^2 + Q' \text{ and } P \sim aX^2 + P'$$

Where the forms Q' and P' are of rank $n-1$ and

$$d(Q') = ad(Q) = ad(P) = d(P')$$

$$e(Q') = e(Q)(a, d(Q')) = e(P)(a, d(P')) = e(P')$$

By the induction hypothesis $Q' \sim P'$ and therefore $Q \sim P$ giving us the desired result. □

Now lets look at the real case.

Theorem 3.3.3. *(Sylvester law of inertia) Let Q be be a nondegenerate quadratic form in n variables over $\mathbb{R}$. Then Q is equivalent to $X_1^2 + ... + X_r^2 - Y_1^2 - ... - Y_s^2$ With $r + s = n$. In addition no two of these are equivalent.*

Proof. We can assume that our form can be written as

$$a_1X_1^2 + ... + a_nX_n^2$$

but since $\sqrt{|a_1|} \in \mathbb{R}$ we can use the change of variables $X_i \to \frac{1}{\sqrt{|a_i|}}X_i$ to get an equivalent quadratic form

$$\text{sign}(a_1)X_1^2 + ... + \text{sign}(a_n)X_n^2.$$

Which is equivalent to

$$X_1^2 + ... + X_r^2 - Y_1^2 - ... - Y_s^2$$

with $r = \{i \in 1, ..., n | \text{sign}(a_i) = 1\}$. For a proof that no two quadratic forms that are written like this are equivalent see Norman [6] pp. 360-361. □

With the r, s defined above we say that the pair (r, s) is the **signature** of the quadratic form over $\mathbb{R}$ we say that the quadradic form is **definite** if r or s are equal to zero and **indefinite** otherwise. The Hasse invariant for a form Q with signature (s, r) is equal to

$$e(Q) = (-1)^{s(s-1)/2}$$

since $(-1, -1) = -1$ and its discriminant is equal to

$$d(Q) = (-1)^s.$$

3.4 Quadradic forms over $\mathbb{Q}$

Let $Q \sim a_1X_1^2 + ... + a_nX_n^2$ be a quadratic form of rank n. We associate to it the following invariants

1. The discriminant $d(Q)$
2. Let $v \in \mathcal{V}$. The injection $\mathbb{Q} \to \mathbb{Q}_v$ allows one to view Q as a quadratic form, which we will denote Q_v over $\mathbb{Q}_v$. The invariants of $\mathbb{Q}_v$ will be denoted by $d_v(Q)$ and $e_v(Q)$; it is clear that $d_v(Q)$ is the image of $d(Q)$ by $\mathbb{Q}^*/(\mathbb{Q}^*)^2 \to \mathbb{Q}_v^*/(\mathbb{Q}_v^*)^2$; and we have
$$e_v(Q) = \prod_{i<j} (a_i, a_j)_v.$$
3. The **signature** (r, s) of the real quadratic form is another invariant of Q

The invariants e_v, d_v and (r, s) are sometimes called **local invariants** of Q.

As we have seen equivalence of nondegenerate quadratic forms over $\mathbb{C}, \mathbb{R}$ and $\mathbb{Q}_l$ are easy using only one or two invariants. On the other hand finding the invariant for $\mathbb{Q}$ is not as trivial. As we move further away from algebraic closed fields, equivalence of quadratic forms over a field is harder to see

Chapter 4

The Hasse-Minkowski Theorem

By now we have the necessary tools to prove an elegant result from 1924 first proved by Hermann Minkowski and later generalized to number fields by Helmut Hasse. The importance of the theorem stems from it's link between local properties solutions in $\mathbb{Q}_p$ and $\mathbb{R}$ and it's global properties, $\mathbb{Q}$ and $\mathbb{Z}$ and from the simple arithmetical question: in order to determine whether an equation of a certain type has a solution in rational numbers, is it sufficient to test whether it has solutions over complete fields of real and p-adic numbers, where we can apply analytical tools such as Newton's method and its p-adic counterpart Hensel's lemma.

Theorem. *(Hasse-Minkowski) A quadratic form Q over $\mathbb{Q}$ represents 0 if and only if for all $v \in \mathcal{V}$ the form Q_v represents 0.*

By 3.1.1 we can suppose that

$$Q(X_1, ..., X_n) = a_1X_1^2 + a_2X_2^2 + ... + a_nX_n^2, \quad a_i \in \mathbb{Q}^*$$

furthermore we know that Q represents 0 if and only if a_1Q represents 0, so we can assume that

$$Q(X_1, ..., X_n) = X_1^2 + a_2X_2^2 ... + a_nX_n^2, \quad a_i \in \mathbb{Q}^*$$

Lastly we can assume that the a_i are square free integers by using a suitable change of variables. We can write $a_i = \frac{a_i'r_i^2}{b_i't_i^2}$ with $t, r \in \mathbb{Z}, (a_i', b_i') = 1$ and a_i', b_i' square free

integers. We can then use the change of variables $X_i \to \frac{t_i}{r_i b_i'} X_i$ to obtain

$$a_i X_i^2 \to a_i' b_i' X_i^2$$

And thus

$$X_1^2 + a_2 X_2^2 + ... + a_n X_n^2 \to X_1^2 + a_2' b_2' X_2^2 + ... + a_n' b_n' X_n^2$$

Since $(a_i', b_i') = 1$ and a_i', b_i' are square free integers then $a_i' b_i'$ is a square free integer for all i

We only need to consider the cases $n > 1$ because if Q has only one variable then the result is evident because $X^2 = 0 \iff X = 0$.

Case $n = 2$

We can assume that $Q = X_1^2 - aX_2^2$, $a \in \mathbb{Q}$. Since Q represents 0 in $\mathbb{R}$, we know that $a > 0$. First we will write a in it's unique prime factorization as follows:

$$a = \prod_{p \text{ prime}} p^{v_p(a)}.$$

The fact that Q_p represents 0 tells us that a is a square in $\mathbb{Q}_p$ 3.1.2, hence $v_p(a)$ is *even*. This tells us that a is a square in $\mathbb{Q}$ also and therefore Q also represents 0.

Case $n = 3$

This particular case was first proved (in somewhat different terminology) by Legendre in 1785[2]. We can assume that $Q = X_1^2 - aX_2^2 - bX_3^2$ where a, b are square free integers. We can furthermore assume that $0 < |a| \leqslant |b|$. Let $m = |a| + |b|$. We will show that the statement is true for all m by using strong induction.

If $m = 2$: we can write

$$Q = X_1^2 \pm X_2^2 \pm X_3^2;$$

because if $Q = X_1^2 + X_2^2 + X_3^2$ then Q_∞ would not represent 0. But then we already know infinitely many solutions to the equation $Q(X_1, X_2, X_3) = 0$, i.e. some the

Pythagorean triplets.

If $m > 2$ and we assume that the statement is true for integers less that m. We know $|b| \geqslant 2$ and that b is a square free integer so we can write

$$b = \pm p_1 p_2 ... p_k$$

where p_i are distinct primes. We will prove that a is a square modulo p for all $p \in \{p_1, .., p_k\}$.

If $a \equiv 0 \pmod{p}$ then a is clearly a square. Otherwise $a \in \mathbb{U}_p$ because a is not divisible by p. By our hypothesis there exists $(x, y, z) \in (\mathbb{Q}_p)^3$ such that

$$z^2 - ax^2 - by^2 = 0$$

We can suppose that (x, y, z) is a primitive solution in $(\mathbb{Z}_p)^3$ by 8.

Notice that $z^2 - ax^2 = 0 \pmod{p}$. Suppose that $x \equiv 0 \pmod{p}$ then $z \equiv 0 \pmod{p}$ furthermore

$$by^2 = z^2 - ax^2 \equiv 0 \pmod{p^2}$$

and since b is assumed square free this can only mean that y is divisible by p, a contradiction to the fact that (x, y, z) is primitive.

Thus $x \not\equiv 0 \pmod{p}$. Looking at the equation $z^2 - ax^2 \equiv 0 \pmod{p}$ and $x \neq 0 \pmod{p}$ we can see that a is a square modulo p.

By the Chinese reminder theorem 0.1 we have the following:

$$\mathbb{Z}/b\mathbb{Z} \simeq \prod_i^k \mathbb{Z}/p_i\mathbb{Z}$$

and therefore a is a a square modulo b. That is $t^2 \equiv a \pmod{b}$, i.e. there exist $t \in \mathbb{Z}$ with $|t| < \frac{|b|}{2}$ and $b' \in \mathbb{Z}$ such that

$$t^2 = a + bb' \quad \text{i.e.} \quad t^2 - a = bb'.$$

Thus we have that bb' is a norm of the extensions $K(\sqrt{a})/K$ where $K = \mathbb{Q}$ or $K = \mathbb{Q}_v$. From this we can simplify our form to that of Q' defined below by using

the algebra of the Hilbert symbol

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

This means that Q represents 0 over $\mathbb{Q}$ if and only if the same is true for:

$$Q' = X_1^2 - aX_2^2 - b'X^2.$$

In particular we have that Q'_p represents 0 for all $v \in \mathcal{V}$. We also have that

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

The first inequality is the triangle inequality, the next inequality is derived by $|t| < \frac{|b|}{2}, |a| \leqslant |b|$ and the last inequality stems from the fact that $2 \leqslant |b|$. If we write $b' = u^2 b''$ where b'' is square free we have that

$$Q'' = X_1^2 - aX_2^2 - b''X_3^2$$

is equivalent to Q' and in addition we have by the induction hypothesis that Q'' represents 0 and therefore Q' does also and equivalently Q does as well.

Case $n = 4$

We can write $Q = aX_1^2 + bX_2^2 - (cX_3^2 + dX_4^2)$. Let $v \in \mathcal{V}$. Since Q_v represents 0, there exists $0 \neq (X_1, X_2, X_3, X_4) \in (\mathbb{Q}_p)^4$ such that $aX_1^2 + bX_2^2 = (cX_3^2 + dX_4^2)$ so there exists a $x_v \in \mathbb{Q}_p^*$ which is represented both by

$$aX_1^2 + bX_2^2 \quad \text{and} \quad cX_3^2 + dX_4^2$$

by 5, it applies equally to $v = \infty$ this is equivalent to

$$(x_v, -ab)_v = (a,b)_v \quad \text{and} \quad (x_v, -cd)_v = (c,d)_v, \quad \forall v \in \mathcal{V}$$

By Hilbert's law of reciprocity we know that $\prod_{v\in V}(a,b)_v = \prod_{v\in V}(c,d)_v$ we apply 2.5.3 to obtain the existence of $x \in \mathbb{Q}^*$ such that

$$(x,-ab)_v = (a,b)_v \quad \text{and} \quad (x,-cd)_v = (c,d)_v, \quad \forall v \in \mathcal{V}$$

again this is equivalent to the statement that

$$aX_1^2 + bX_2^2 - xZ^2 \quad \text{and} \quad cX_3^2 + dX_4^2 - xZ^2$$

represents zero in each of the $\mathbb{Q}_v$ and hence in $\mathbb{Q}$ by the argument of the case $n = 3$. But then x is represented both by $aX_1^2 + bX_2^2$ and $cX_3^2 + dX_4^2$ and thus Q represents 0 in $\mathbb{Q}$

Case $n \geqslant 5$

We provide a rather complete sketch of the proof, asking the reader to accept a few facts about quadratic forms, or to see [7] for the requisite theory. We will use induction on n. We write Q of the form $Q = P - Q'$ where

$$P = a_1X_1^2 + a_2X_2^2 \text{ and } Q' = -(a_3X_3^2 + ... + a_nX_n^2).$$

Let $S \subset \mathcal{V}$ be the subset consisting of $\infty, 2$, and the numbers p such that $v_p(a_i) \neq 0$ for one $i \geqslant 3$.This set is finite since the set of prime divisors of all the a_i is obviously finite.

Let $p \in S$. Since Q_p represents 0 by hypothesis, implies that there exists $a_p \in \mathbb{Q}_p^*$ which is represented in $\mathbb{Q}_p$ by both P and Q', and there exist $x_i^p \in \mathbb{Q}_p, i = 1, ..., n$ such that $P(x_1^p, x_2^p) = a_p = Q'(x_3^p, ..., x_n^p)$.

It can be shown that the squares of Q_p^* form an open set. Then by the Approximation theorem 0.2, there must exist $x_1, x_2 \in \mathbb{Q}$ such that, if $a = P(x_1, x_2)$, then $\frac{a}{a_v} \in (\mathbb{Q}_v^*)^2$ for all $v \in S$.

Now consider the form $f_1 = aZ^2 - Q'$. For each $v \in S$ we know Q' represents a_v in $\mathbb{Q}_v$, and since $\frac{a}{a_v} \in (\mathbb{Q}_v^*)^2$ we have that Q' also represents a since

$$Q'(z_3, ..., z_n) = a_v \Rightarrow Q\left(z_3\sqrt{\frac{a}{a_v}}, .., z_n\sqrt{\frac{a}{a_v}}\right) = a.$$

But that means that f_1 represents 0 in $\mathbb{Q}_v$.

Now if $v \notin S$ then by the construction of f_1, it can be shown that f_1 also represents 0 for each $p \notin S$; this is a consequence of the fact that, for $p \notin S$, the coefficients of Q' are p-adic units (by the definition of S). This implies easily that the discriminant $d(Q')$ of Q' considered over each $\mathbb{Q}_p$, $p \notin S$ is also a unit; less easily, it implies that $E(Q') = 1$, and these two facts together imply that f_1 represents 0 in $\mathbb{Q}_v$ for every $v \in \mathcal{V}$.

Since the rank of f_1 is of rank $n-1$ our induction hypothesis shows that f_1 represents 0 in $\mathbb{Q}$, in other words Q' represents a in $\mathbb{Q}$ and since we already showed that P represents a, this implies that $Q = P - Q'$ represents 0, completing the proof of the Hasse-Minkowski Theorem.

Corollary 6. *Let $a \in \mathbb{Q}^*$. A quadratic form Q represents a over $\mathbb{Q}$ if and only if it does so over $\mathbb{Q}_v$ for all $v \in \mathcal{V}$*

This follows from the theorem applied to the form $aZ^2 - Q$.

Corollary 7 (Meyer)**.** *A quadratic form of rank $\geqslant 5$ represents zero if and only if it is indefinite.*

Corollary 8. *Two quadratic forms Q and Q' over $\mathbb{Q}$ are equivalent if and only if they are equivalent over $\mathbb{Q}_v$ for all $v \in \mathcal{V}$.*

4.1 Examples and Counterexamples

Unfortunately, the Hasse-Minkowski Theorem is not necessarily true for higher-degree polynomials. For example, in 1951, Ernst Selmer showed that the homogeneous degree-3 polynomial

$$f(x, y, z) = 3x^3 + 4y^3 + 5z^3 \tag{4.1}$$

represents zero in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p but not in $\mathbb{Q}$. Determining why the Hasse-Minkowski Theorem fails for certain higher-degree polynomials is an area of active research [8].

Example 6. *Let us determine if the quadratic form*

$$5X^2 + 7Y^2 - 13Z^2$$

has a non trivial zero over $\mathbb{Q}$.

We show this using the Hasse-Minkowski theorem and Hensel's Lemma. Consider the form in the following cases:

1. Over $\mathbb{R}$: Since the signature of the quadratic form is $(2, 1)$ it has a nontrivial solution over $\mathbb{R}$

2. Over $\mathbb{Q}_p$, $p \notin \{2, 5, 7, 13\}$: Then by 0.3 there exist a nontrivial zero, that is also simple, in the reduction of the quadratic form the the ring $\mathbb{Z}/p\mathbb{Z}$ and then by Hensel's lemma it lifts to a nontrivial zero in the field $\mathbb{Q}_p$.

3. Over $\mathbb{Q}_2$: Consider the reduction of the quadratic form in $\mathbb{Z}/8\mathbb{Z}$, $g(x, y, z) = 5X^2 + 7Y^2 - 13Z^2 \in \mathbb{Z}/8\mathbb{Z}[x, y, z]$ and its zero $(x_0, y_0, z_0) = (1, 0, 1)$

   $$5 \times 1^2 + 7 \times 0^2 - 13 \times 1^2 = 5 - 13 = -8 = 0 \pmod 8$$

   in addition $\frac{\partial g}{\partial x}|_{x_0,y_0,z_0} = 10 \neq 0$ so by Hensel's lemma we can lift this solution to a solution in $\mathbb{Q}_2$.

4. Over $\mathbb{Q}_5$: Consider the reduction of the quadratic form in $\mathbb{Z}/5\mathbb{Z}$, $g(x, y, z) = 7Y^2 - 13Z^2 \in \mathbb{Z}/5\mathbb{Z}[x, y, z]$ and its zero $(x_0, y_0, z_0) = (0, 2, 1)$

   $$7 \times 2^2 - 13 \times 1^2 = 28 - 13 = 15 = 0 \pmod 5$$

   in addition $\frac{\partial g}{\partial z}|_{x_0,y_0,z_0} = 26 \neq 0$ so by Hensel's lemma we can lift this solution to a solution in $\mathbb{Q}_5$.

5. Over $\mathbb{Q}_7$: Consider the reduction of the quadratic form in $\mathbb{Z}/7\mathbb{Z}$, $g(x, y, z) = 5x^2 - 13Z^2 \in \mathbb{Z}/7\mathbb{Z}[x, y, z]$ and its zero $(x_0, y_0, z_0) = (2, 0, 1)$

   $$5 \times 2^2 - 13 \times 1^2 = 20 - 13 = 7 = 0 \pmod 7$$

in addition $\frac{\partial g}{\partial y}|_{x_0,y_0,z_0} = 26 \neq 0$ so by Hensel's lemma we can lift this solution to a solution in $\mathbb{Q}_7$.

6. Over $\mathbb{Q}_{13}$: Consider the reduction of the quadratic form in $\mathbb{Z}/13\mathbb{Z}$, $g(x, y, z) = 5X^2 + 7Y^2 \in \mathbb{Z}/13\mathbb{Z}[x, y, z]$ and its zero $(x_0, y_0, z_0) = (3, 1, 0)$

$$5 \times 3^2 + 7 \times 1^2 = 45 + 7 = 0 \pmod{13}$$

in addition $\frac{\partial g}{\partial y}|_{x_0,y_0,z_0} = 10 \neq 0$ so by Hensel's lemma we can lift this solution to a solution in $\mathbb{Q}_{13}$.

Now we have shown that the quadratic form represents zero over $\mathbb{Q}_v$ for all $v \in \mathcal{V}$ and then by the Hasse-Minkowski theorem it also does over $\mathbb{Q}$

Appendix

Definition 20. *Let F be a field. A function $f : V \to W$ between two F-vector spaces V and W is called homogeneous of degree k if*

$$f(s\boldsymbol{v}) = s^k f(\boldsymbol{v}) \quad \forall s \in F, \forall \boldsymbol{v} \in V$$

For some $k \in \mathbb{Z}$.

Definition 21. *Let $\{R_i\}_{i \in I}$ be a family of rings with morphisms $\varphi_{ij} : R_j \to R_i$ for all $i \leq j$ such that φ_{ii} is the identity on R_i and $\varphi_{ki} = \varphi_{kj} \circ \varphi_{ji}$ for all $i \leq j \leq k$. **The projective limit**, denoted $\varprojlim R_n$ is the set of all sequences (R_n) with the property $a_n \in R_n$ and $\varphi(a_j) = a_i$ for all $i \leq j$. The rings R_i along with the morphisms φ_{ij} are called a projective system.*

The inverse limit $\varprojlim R_n$ has a natural ring structure given by component-wise addition and multiplication. This system satisfies the so called

Theorem 0.1. *(Chinese remainder theorem) Let $a_1, ..., a_k$, $n_1, ..., n_k$ be integers with the k_i being pairwise relatively prime and let $N = n_1 n_2 ... n_k$. There exist an integer an integer $a \pmod N$ such that $a \equiv a_i \pmod{n_i}$ for all $1 \leq i \leq k$.*

Proof. For each i with $1 \leq i \leq n$, put $m_i = N/n_i$. Notice that since the moduli are relatively prime, and m_i is the product of all the moduli other than n_i, we have that $n_i m_i \equiv N \equiv 0 \pmod N$, and hence m_i has a multiplicative inverse modulo n_i, call it y_i. Moreover, note that m_i is a multiple of n_j for all $j \neq i$. Let

$$a = y_1 a_1 m_1 + y_2 a_2 m_2 + ... + y_k a_k m_k$$

For each $1 \leq i \leq k$, we obtain

$$x \equiv y_i a_i m_i \equiv a_i \pmod{n_i}$$

Now for the uniqueness $\pmod{N}$. Suppose that x and y both solve the congruences. Then we have that for each i that n_i is a divisor of $x - y$. Since the n_i are relatively prime, this means that N is a divisor of $x - y$ and hence $x \equiv y \pmod{N}$ □

Theorem 0.2 (Approximation theorem)**.** *Let S be a finite subset of $\mathcal{V}$. The image of $\mathbb{Q}$ in $\prod_{v \in S} \mathbb{Q}_v$ is dense in this product (for the product topology of those of $\mathbb{Q}_v$).*

Being free to enlarge S, we can suppose that $S = \{\infty, p_1, ..., p_n\}$ where the p_i are distinct prime numbers and we must proof 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 and let us show that this point is adherent to $\mathbb{Q}$. After multiplying by some integer we can suppose that $x_i \in \mathbb{Z}_{p_i}$ for all $1 \leqslant i \leqslant n$. Now one has to proof that, for all $\varepsilon > 0$ and $N > 0$, there exist $x \in \mathbb{Q}$ such that

$$|x - x_\infty| \leqslant \varepsilon, \text{ and } v_{p_i}(x - x_i) \geqslant N, \text{ for all } 1 \leqslant i \leqslant n.$$

By the Chinese remainder theorem applyed to $n_i = p_i^N$, there exist $x_0 \in \mathbb{Z}$ such that $v(x_0 - x_i) \geqslant N$ for all i. Choose a prime number q grater than all the p_i. The rational numbers of the form $a/q^m, a \in \mathbb{Z}, m \geqslant 0$, are dense in $\mathbb{R}$. Choose such a number $u = a/q^m$ with

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

The rational number $x = x_0 + up_1^N ....p_n^N$. Has the desired property.

Theorem 0.3 (Chevalley- Warning)**.** *Let $f_\alpha \in K[X_1, ..., X_n]$ be a family of polynomials, with coefficients in a finite field K with characteristic p, in n variables such that $\deg(f_\alpha) < n$, and V be the set of their common zeros then:*

$$Card(V) \equiv 0 \ (mod\ p)$$

See Serre [7].

Index

Bibliography

[1] Martin Aigner and Günter M. Ziegler. Proofs from the book, 1998.

[2] L. E. Dickson. *History of the theory of numbers.* Chelsea Publishing, 1971.

[3] Antoine Ducros. *Algèbre 1 (ens, première année).* 2021.

[4] Larry J. Gerstein. *Basic Quadradic Forms*, volume 90 of *Graduate Studies in Mathematics.* American Mathematical Society, 2008.

[5] Heiko Knospe. The p-adic integers and their topology, Aug 2019.

[6] C. W. Norman. *Undergraduate Algebra : A First Course.* Oxford University Press, first edition edition, 1986.

[7] Jean-Pierre Serre. *Cours d'arithmétique.* Presses Universitaires de France, 1970.

[8] I. R. Shafarevich Z. I. Borevich. *Number Theory.* Academic Press, New York and London, 1966.