university of groningen / faculty of science and engineering / mathematics and applied mathematics

The Hasse-Minkowski Theorem

Bachelor's Project Mathematics

July 2022

Student: T.M. Bredek

First supervisor: PhD. O. Lorscheid

Second assessor: PhD. P. Kilicer

Abstract

In this thesis, the Hasse-Minkowski theorem is proven for the rational numbers. We define the p-adic numbers, and then explore properties of the p-adic numbers. The Hilbert symbol is defined, and multiple properties of it are proven. Quadratic forms are introduced and we develop theories on quadratic forms that are needed to prove the Hasse-Minkowski theorem.

Contents

1 Introduction

The field of algebraic number theory is vast, and has many different topics that are researched to some degree. One of the central topics in algebraic number theory is the p-adic numbers. Most mathematicians are familiar with the relationship between the real numbers and the rational numbers. The real numbers are the completion of the rational numbers with respect to the Archimedean absolute value. This completion is done with the standard euclidean absolute value. What would happen if we choose another absolute value? Do other absolute values even exist? In this thesis we discuss the different absolute values that can be put on the rational numbers and that they are dependent on the prime numbers. Completing the rational numbers with these different absolute values yields the p-adic numbers.
Another topic that one encounters in different fields of mathematics are quadratic forms. These are polynomials with only terms of degree 2. Quadratic forms have coefficients in different fields, like the rational numbers or the p-adic numbers.
In this thesis we explore quadratic forms that have coefficients in the rational numbers and how these forms behave in the completions of $\mathbb{Q}$. In this thesis we first give some general properties of the p-adic numbers. This first section defines the p-adic numbers and the p-adic integers and then discusses the topology on the p-adic numbers, polynomials over the p-adic numbers, the units of the p-adic integers and the squares of the p-adic numbers. In the next section, the Hilbert symbol is defined and methods of computing the Hilbert symbol are given. The fourth section covers all the necessary preliminaries on quadratic forms that are needed to prove the Hasse-Minkowski theorem. Selmer's counterexample is also discussed. Students that are familiar with algebraic structures should be able to follow the arguments given in this thesis.
The main theorem proven in this thesis is the Hasse-Minkowski theorem.

Theorem (Hasse-Minkowski)**.** *A quadratic form has a nontrivial solution in the rational numbers if and only if it has a nontrivial solution in all completions of the rational numbers.*

This theorem is a first introduction to the so called local-global principles. One calls the solution in the rational numbers the global solution. With this global solution, we can find a local solution in the p-adic numbers and the real numbers. However, the Hasse-Minkowski theorem implies that if there is a solution in every completion, then we can glue these solutions together to find a global solution. It is not obvious how one would translate this notion of gluing together solutions to rigorous mathematics. It is also not always possible to find a global solution, even though there are local solutions in every completion. A famous counterexample to this is the cubic form $3x^3+4y^3+5z^3$, called Selmer's equation. This cubic form has a nontrivial solution in all of the p-adic integers, and in the real numbers, but there is no solution in the rational numbers. In [3] other counterexamples are given of different forms where we would like to apply the local-global principle, but where this is not possible. One generalization that does work is the generalization of quadratic forms to number fields. A number field is a finite extension of the rational numbers. Instead of prime numbers, number fields contain prime ideals. These prime ideals are then used to create an analogue of the p-adic valuation in number fields. Some arguments in this thesis can be generalized to these number fields without much effort, but other proofs unfortunately fall apart when generalizing to number fields. Local-global principles can also be applied on structures that are not fields, like rings or algebraic groups, but these structures require different definitions

and approaches to prove their respective local-global principles.

2 The p-adic numbers

2.1 The sets $\mathbb{Z}_p$ and $\mathbb{Q}_p$

This first section discusses the definition of the p-adic numbers. To first get some intuition, we consider different ways to express the natural numbers. Every natural number can be written as a sum of powers of a specific number. Take for example 33. On one hand this can be written as $1^*2^0 + 1^*2^5$, while on the other hand we could also write it as $2^*3^1 + 1^*3^3$ and most naturally as $3^*10^0 + 3^*10^1$. For any positive integer, we can find a p-adic expansion by using division with remainder, where we always want the coefficient of a specific power of p to be less than p itself. Otherwise an expansion like $16 = 9^*7^0 + 1^*7^1$ is possible, which is undesired. Unfortunately, this means it is not possible to give such an expansion for negative integers. To make representations for these numbers, we allow infinite series:

Definition 2.1. The p-adic integers can be defined as infinite series of the form:

$$\sum_{n=0}^{\infty} a_n p^n = a_0 + a_1 p + a_2 p^2 \dots$$

where, $a_i \in \{0, 1, \dots, p-1\}$. Here p is a prime number. The set of p-adic integers is denoted by $\mathbb{Z}_p$.

Note that in this case we are not worried about convergence of these sums. Otherwise we get that almost all of these sums would diverge[1]. We can also add negative powers of p in the series to obtain a Laurent series.

Definition 2.2. The p-adic numbers can be seen as Laurent series of the form:

$$\sum_{n=-m}^{\infty} a_n p^n = a_{-m} p^{-m} + \dots + a_{-1} p^{-1} + a_0 + a_1 p + a_2 p^2 \dots$$

where, $a_i \in \{0, 1, \dots, p-1\}$. The p-adic numbers are denoted by $\mathbb{Q}_p$.

This way we also get fractions. The p-adic numbers and p-adic integers are not always intuitive to work with. Let's think for example about $-1 \in \mathbb{Z}_p$.

Example 2.3. Since all of the a_i have positive value, what is a representation of -1? It turns out that:

$$-1 = (p-1) + p(p-1)p^2(p-1) + \dots$$

How would this ever make sense? We can get an intuition from the harmonic series. If we would not worry about convergence, we could say that:

$$\frac{1}{1-p} = 1 + p + p^2 + p^3 + \dots$$

By then multiplying both sides by $-(1-p)$ we get our representation for -1 in $\mathbb{Z}_p$.

[1] For convergence we would need that the series contains only finitely many nonzero terms.

How do we define addition and multiplication? Addition works by adding every term in the sum per power of p, but how would we define multiplication when there are an infinite amount of terms? We therefore want to reinterpret these series as a sequences. Every individual entry in a sequence is a partial sum. A sequence (s_n) would consist of the entries:

$$s_n = \sum_{n=0}^{n-1} a_n p^n = a_0 + a_1 p + a_2 p^2 + \cdots + a_{n-1} p^{n-1}$$

Note that an entry in a sequence can be any value between 0 and p^n [5, Prop 2.1.2], so each entry can be thought of as a residue class of $\mathbb{Z}/p^n\mathbb{Z}$. With this we have a sequence of partial sums in $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$. In our case we also have that by applying the canonical projection $P : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$, then $P(s_n) = s_{n-1}$ for all $n \in \mathbb{N}$. Consider the subset of $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ that have the property of $P(a_n) = a_{n-1}$ for all $n \in \mathbb{N}$. This subset is called the projective limit. There is a bijection between this set and $\mathbb{Z}_p$. By associating to the infinite series of an element in $\mathbb{Z}_p$ a sequence of partial sums (s_n) as defined above. Then every element can be identically sent to an element in the projective limit. There is a big advantage to using this projective limit. The product $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ is a ring. Therefore we inherit a form of addition and multiplication from this ring, and give this to our infinite series. Addition and multiplication are defined componentwise in the sequence. This is easier to define than the multiplication of two infinite series. Since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, it would be nice if $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$. This is true and can be seen from the fact that every element in $b \in \mathbb{Q}_p$ can be rewritten as $p^{-m}a$, where $a \in \mathbb{Z}_p$, by shifting all of the terms by m spaces.

2.2 The p-adic absolute value

With the definition of the p-adic integers and the p-adic numbers in mind, we explore some properties of these sets. The first thing we do is give them a topology. To do this, we define the p-adic absolute value. Afterwards we can use our knowledge on metric spaces to define an induced topology.

Definition 2.4. Let $a \in \mathbb{Z}$ and p be a prime number. Factor out p out of a as many times as possible such that $a = p^m b$, with $gcd(b, p) = 1$. Then we define $|a|_p = p^{-m}$. If $a = 0$, we say that $|a|_p = 0$.

As one can see, the map $|.|$ is now a map from $\mathbb{Z}$ to $\mathbb{R}_{\geq 0}$.

Theorem 2.5. The map $|.|$ defined in definition 2.4 is a norm.

Proof. By definition $a = 0 \Rightarrow |a|_p = 0$. If we have $|a|_p = 0$, then we can not have $a \neq 0$, since then $p^{-m} = 0$, which would give a contradiction. Note that if $a, b \in \mathbb{Z}$, we have $|ab|_p = p^{-(n+m)}$, where n and m are the numbers such that $a = p^n c$ and $b = p^m d$, with $gcd(c, p) = 1 = gcd(d, p)$. We compute that $p^{-(n+m)} = p^{-n}p^{-m} = |a|_p|b|_p$. Finally, observe that $|a + b|_p \leq max\{|a|_p, |b|_p\}$ since we factor p out as many times as p appears in the factorization of a or b. Clearly, $max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p$. This shows that the map $|.|_p : \mathbb{Z} \to \mathbb{R}_{\geq 0}$ is a norm. □

From this norm we obtain a metric, by setting $d(a,b) = |a-b|_p$. It can be checked that this choice satisfies all of the axioms of a metric. There are other metrics on $\mathbb{Q}$. We could for example take the 'standard' Archimedean metric. In the literature, this is denoted by $|.|_\infty$. There are valid reasons as to why we use the symbol ∞ for this absolute value. There is also the trivial norm defined from the map $|.|_0 : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ defined as sending $0 \in \mathbb{Z}_p$ to $|0| = 0 \in \mathbb{R}_{\geq 0}$ and any other $x \in \mathbb{Q}$ to $|x| = 1$. Besides positive powers of the aforementioned norms, it can be proven that these are all the norms one can place on $\mathbb{Q}$. This is Ostrowski's theorem. The positive powers are clearly equivalent to their respective norms when raised to the power of 1. The fact that these are the only norms is not immediately obvious. A proof can be found in [5, Ch.2 Prop 3.7].
With this metric, we can finally create the topology using our metric. It turns out that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to these metrics. This gives us another way of defining the p-adic integers. If we were to look at the unit disc around $0 \in \mathbb{Q}_p$, we would find that these are all the Laurent series where all the negative terms are zero. These are precisely the p-adic integers. $\mathbb{Z}_p$ is also the closure of $\mathbb{Z}$ in $\mathbb{Q}_p$.

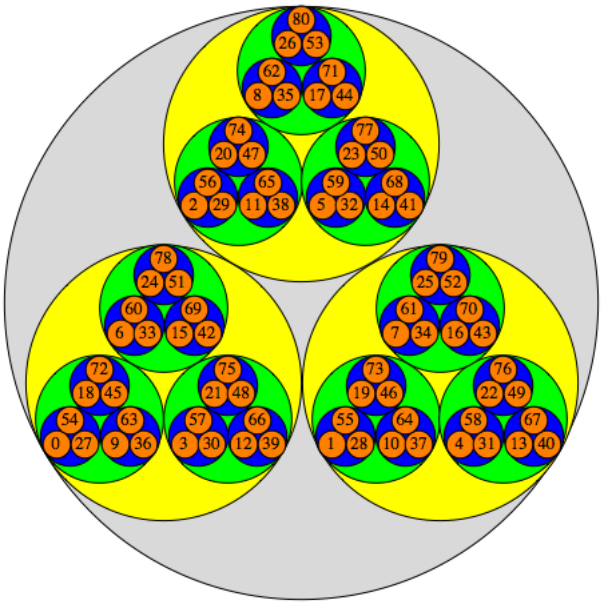

Figure 1: [4]

Figure 1 gives a visual interpretation of the 3-adic numbers. The number 0 is far away from 1, because their difference is 1, and we can not factor out 3 out of 1. On the other hand 28 is very close to 1. Their difference is 27 and we can factor out 3 three times. This gives a small distance between 28 and 1. By adding an infinite amount of layers to this picture, we obtain the p-adic numbers. The 3-adic numbers fill up the space around the circles, similarly to how the real numbers fill up the space between the rational numbers on the real line.

To get a further feel on the topology of the p-adic numbers, we can look at the Approximation Theorem. Let us return to the definition of $|.|_p$. It is useful to define a second function.

Definition 2.6. For an integer $a \in \mathbb{Z}$, the p-adic valuation of a is the integer m such that $a = bp^m$ with $gcd(b, p) = 1$. The p-adic valuation of a is denoted by $v_p(a)$.

This function is often more useful than the absolute value itself, since we get the same information as we get from the norm, except the p-adic valuation gives an integer instead of a power of p, which can be more convenient to work with. The p-adic valuation directly tells us how many times a prime p appears in the prime factorization of a number.

Theorem 2.7 (Approximation theorem)**.** Take a finite subset V' of $V = \{\infty, 2, 3, 5, \dots\}$. The image of $\mathbb{Q}$ in $\prod_{v \in V'} \mathbb{Q}_v$ is dense in this product.

Proof. By the properties of the product topology, we can freely add elements of V as we like. So suppose that $V' = \{\infty, p_1, p_2, \dots, p_n\}$. Take a point in the product $\prod_{v \in V'} \mathbb{Q}_v$. We need to show that for all points of the form $(x_\infty, x_1, x_2, \dots, x_n)$, there is a point arbitrarily close to this point that is of the from $(q, q, q, \dots, q)$, where there are $n + 1$ entries of $q \in \mathbb{Q}$. We multiply by some integer, so that all of the x_i are in their respective p-adic integers. We need a specific q such that $|q - x_\infty|_\infty < \varepsilon$ and for all other entries $v_{p_i}(q - x_{p_i}) \geq N$ for all $N \in \mathbb{N}$. This last condition is equivalent to $|q - x_p|_p < \varepsilon$. There is an integer z such that $v_{p_i}(q - x_{p_i}) \geq N$, obtained by multiplying enough powers of the p_i. Call this number w. Choose another integer q that is coprime to all the p_i. From our knowledge of topology, we know that the numbers of the form y/q^m with y and m integers are dense in $\mathbb{R}$. Take a number $u = y/q^m$ such that $|w - x_\infty + up_1^N \dots p_n^N| \leq \varepsilon$. Then the number $w + up_1^N \dots p_n^N$ is the number in $\mathbb{Q}$ that has the desired property. □

Another concept we define is the notion of primitiveness.

Definition 2.8. A point $(x_1, x_2, \dots, x_n) \in \mathbb{Z}_p^m$ is primitive if there is at least one x_i that is invertible, or equivalently that there is an element with $v_p(x_i) = 0$.

This definition is used for one theorem that is used in the proof of the Hasse-Minkowski theorem.

Theorem 2.9. Let f_i be homogeneous polynomials of degree 2 in m variables with p-adic integers coefficients. Then the f_i have a nontrivial common zero in $\mathbb{Q}_p^m$ if and only if the f_i have a common primitive zero in $\mathbb{Z}_p^m$.

Proof. A common primitive zero in $\mathbb{Z}_p^m$ is also a nontrivial zero in $\mathbb{Q}_p^m$. Conversely, assume that there is a nontrivial common zero in $\mathbb{Q}_p^m$. This zero is a vector $x = (x_1, \dots, x_n)$. We construct a common primitive zero by setting $h = \min_{i \in \{1,2,\dots,m\}}\{v_p(x_i)\}$. The p-adic integer $p^{-h}x$ has the desired properties. □

Theorem 2.9 works in general for all homogeneous polynomials, but this is not necessary for this thesis.
Another essential tool for studying polynomials over $\mathbb{Z}_p$ is Hensel's lemma.

Theorem 2.10 (Hensel's Lemma)**.** Let $f(X)$ be a polynomial with p-adic integer coefficients. If there is an $a \in \mathbb{Z}_p$ such that $f(a) \equiv 0 \mod p$ and $f'(a) \not\equiv 0 \mod p$, then we can lift this to a solution in $\mathbb{Z}_p$.

Proof. We first prove that for all $N \geq 1$, there is an $a_n \in \mathbb{Z}_p$ such that $f(a_n) \equiv 0 \mod p^n$ and $a_n \equiv a \mod p$ with induction. The base case follows from the assumptions of Hensel's lemma. We want to construct a_{n+1} from a_n. By assumption a_n has $f(a_n) \equiv 0 \mod p^n$. Take $a_{n+1} = a_n + p^n t_n$ for some $t_n \in \mathbb{Z}_p$ that we will have to find. It can be checked with the binomial formula that the following polynomial equation is true: $f(x+y) = f(x) + f'(x)y + g(x,y)y^2$ for some $g(x,y)$. Apply this on $x = a_n$ and $y = p^n t_n$. This gives $f(a_n + p^n t_n) = f(a_n) + f'(a_n)p^n t_n + zp^2 n t_n^2$ for some $z \in \mathbb{Z}_p$. The last term vanishes when looking at this equation $\mod p^{n+1}$. The second term is already multiplied by p^n, so both $f'(a_n)$ and t_n are only relevant $\mod p$. With this we reduce this to $f'(a)p^n t_n \mod p^{n+1}$. From this we obtain the relation $f(a_n + p^n t_n) \equiv 0 \mod p$ if and only if $f'(a_n)t_n \equiv -f(a_n)/p^n \mod p$. By the inductive assumption, the last ratio is in $\mathbb{Z}_p$. Because $f'(a_n) \neq 0$ there is always a t_n that satisfies this equation. Pick this t_n. This t_n gives the desired result. We now have a sequence of a_n all satisfying the conditions $f(a_n) \equiv 0 \mod p^n$ and $a_n \equiv a \mod p$. It can also be shown that these a_n satisfy $a_{n+1} \equiv a_n \mod p^n$. This shows that the a_n are a cauchy sequence. The limits of these sequences are also in $\mathbb{Z}_p$. Call this limit α. The p-adic integer α has $\alpha \equiv a_n \mod p^n$. For $n = 1$, this gives $\alpha \equiv a \mod p$. Then

$$\alpha \equiv a_n \mod p^n \implies f(\alpha) \equiv f(a_n) \mod p^n$$

This condition implies that $|f(\alpha)|_p \leq \frac{1}{p^n}$. This holds for all n, so $f(\alpha) = 0$. This proves the theorem. □

There are many different formulations and generalizations of Hensel's lemma. The strongest version of Hensel's lemma states that factozisations of a polynomial $f \equiv \bar{g}\bar{h}$ in $\mathbb{F}_p$ can be lifted to a factorization $f = gh$ in $\mathbb{Z}_p$. Neukirch gives a full statement [5, p. 129].

2.3 Units

This section discusses the units of $\mathbb{Z}_p$. Since $\mathbb{Q}_p$ is a field, all of its elements, with the exception of 0, are units. The group of units of $\mathbb{Z}_p$ is more interesting. The units of $\mathbb{Z}_p$ necessarily need that they have norm 1. This follows from the fact that $|ab|_p = |a|_p|b|_p$ and the fact that for all $a \in \mathbb{Z}_p$ we always have that $|a|_p \leq 1$. Therefore we need that $|a^{-1}|_p = 1$. This is equivalent to saying that the first term of a as a formal series is nonzero. If this term is nonzero, we can not factor p out of the series, which implies that the norm is 1. Remember that the first term of our p-adic integer $a = \sum_{i=0}^{\infty} a_i p^i$ can be represented by elements of $\mathbb{F}_p$. If a_0 is nonzero, there exists an inverse of a_0 in $\mathbb{F}_p$. With this knowledge, we find an inverse of a p-adic integer. The inverse a^{-1} of a must have the property that $a^{-1}a = 1$. Consider the product $ab = (\sum_{i=0}^{\infty} a_i p^i)(\sum_{i=0}^{\infty} b_i p^i)$. If we expand this, we find that it is equal to $a_0 b_0 p^0 + (a_1 b_0 + a_0 b_1)p^1 + (a_2 b_0 + a_1 b_1 + a_0 b_2)p^2 + \ldots$. Since we know all of the a_i, we first find b_0. We want the product to equal 1, so set b_0 equal to a_0^{-1}. The rest of the terms have to be zero. This gives an infinite system of equations where we have the equations $0 = \sum_{i=0}^{n}(a_i b_{n-i})$. We recursively find b_k using the previous b_i we computed. This gives equations $b_i = a_0^{-1}(\sum_{i=1}^{n}(a_i b_{n-i})$ that can be solved. By representing the p-adic integers as sequences, we find the inverses componentwise. We still need that $a_0 \neq 0$, otherwise the inverse would not exist. Besides the group of units, there are some more interesting subgroups of $\mathbb{Z}_p$. These are U_n, with $n \in \mathbb{N}$. The U_n are defined as the sets $1 + p^n\mathbb{Z}_p$. We are particularly interested in the group U_1. This group is the largest of all the U_n, and contains elements

of the form $1 + \sum_{i=1}^{\infty} a_i p^i$, which are essentially p-adic integers where the first term is equal to 1. It is clear that U/U_1 is isomorphic to $\mathbb{F}_p^*$, which in turn is isomorphic to $\mathbb{Z}/(p-1)\mathbb{Z}$. Furthermore, we observe that U_n/U_{n+1} is isomorphic to $\mathbb{Z}/(p)\mathbb{Z}$. Take the map

$$(1 + p^n x) \mapsto (x \bmod p).$$

This map is a homomorphism, since $(1+p^n x)(1+p^n y) = 1 + p^n x + p^n y + p^{2n} xy$. The higher order term then disappears because of the quotient with U_{n+1}. Then we combine the two middle terms, and we see that the map is a homomorphism. This can also be used to prove that U_1/U_{n-1} is of order p^{n-1}. Let us return to U_1. In general this group also has a convenient structure on its own.

Theorem 2.11. If $p \neq 2$, U_1 is as a group isomorphic to $\mathbb{Z}_p$.

This theorem requires the following lemma.

Lemma 2.12. If $p \neq 2$, then $x \in U_n - U_{n+1}$ implies that $x^p \in U_{n+1} - U_{n+2}$

Proof. Take $x \in U_n - U_{n+1}$, so $x = 1 + mp^n$, with $m \in \{1, 2, \ldots, p-1\}$. Then, expand the product $(1 + mp^n)^p$ to $1 + mp^{n+1} + \cdots + m^p p^{np}$. The extra power of p comes from the binomial theorem. All of the exponents are larger than $n+2$, except for the first two, so $x^p \equiv 1 + mp^{n+1} \mod p^{n+2}$. This is not in U_{n+2} because there is a lower power term, but in U_{n+1}. □

With this lemma we can prove Theorem 2.11.

Proof. Take an element $a \in U_1 - U_2$. Lemma 2.12 shows that, $a^p \in U_2 - U_3$. Repeatedly apply Lemma 2.12 to elements of the form a^{p^i} to conclude that they are in $U_{i+1} - U_{i+2}$. We project these elements back to U_1/U_n, and call them a_n. A computation shows that $(a_n)^{p^{n-2}} \neq 1$, but $(a_n)^{p^{n-1}} = 1$. Remember that U_1/U_n has order p^{n-1}, which means it is a cyclic group. From the computation, we see that a_n is a generator of this group. We set up an isomorphism from $\mathbb{Z}/p^{n-1}\mathbb{Z}$ to U_1/U_n defined as $b \mapsto (a_n)^b$. This gives the following commutative diagram:

$$\begin{array}{ccc} \mathbb{Z}/p^n\mathbb{Z} & \longrightarrow & U_1/U_{n+1} \\ \downarrow & & \downarrow \\ \mathbb{Z}/p^{n-1}\mathbb{Z} & \longrightarrow & U_1/U_n \end{array}$$

By applying the same logic to other U_i we get a tower of maps. Take the projective limit of both sides. On the left hand side we get a projective limit of $\mathbb{Z}/p^{n-1}\mathbb{Z}$, which is a representation of $\mathbb{Z}_p$. On the right hand side we get the projective limit of U_1/U_n. The groups U_n get smaller as n goes to ∞, so this limit is equal to U_1. Therefore, $\mathbb{Z}_p$ is isomorphic to U_1. □

In the case where $p = 2$, the result is slightly different.

Theorem 2.13. If $p = 2$, then U_2 is isomorphic to $\mathbb{Z}_2$, and U_1 is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times U_2$.

Proof. The proof that U_2 is isomorphic to $\mathbb{Z}_2$ is similar to the previous proof. Then use the fact that $U_1/U_2 = \mathbb{Z}/2\mathbb{Z}$. □

With this knowledge, we have a representation of $\mathbb{Q}_p^*$.

Theorem 2.14. If $p \neq 2$, then $\mathbb{Q}_p^*$ and $\mathbb{Z} \times U$.

Proof. Take an element $a \in \mathbb{Q}_p^*$. Write a as $p^n u$ for some $n \in \mathbb{Z}$ and $u \in U$, which implies that $\mathbb{Q}_p^*$ is isomorphic to $\mathbb{Z} \times U$. The part containing n gives the $\mathbb{Z}$ part, and the u gives the second part of the product. □

If we had a more specific structure of U, this would give us an even more detailed representation of $\mathbb{Q}_p^*$.

Theorem 2.15. The group U is isomorphic to $\mathbb{F}_p^* \times U_1$.

To prove this theorem we need the next lemma involving exact sequences.

Lemma 2.16. Consider the exact sequence of commutative groups

$$0 \to A \to B \to C \to 0,$$

where the cardinality of A and C are finite and $gcd(\#A, \#C) = 1$. Consider the set $B' = \{b \in B | (\#C)b = 0\}$. The group B is isomorphic to the direct sum of A and B'. The group B' is also isomorphic to C.

Proof. Let $\#A = a$ and $\#C = c$. Because $gcd(a, c) = 1$, by Bézout's identity, there are integers r, s such that $ar + bs = 1$. If $x \in A \cap B'$, then $ax = 0$ because the order of A is a, and $bx = 0$ by the definition of B'. So, on one hand $(ar + bs)x = 0$. But on the other hand $(ar + bs)x = x$. This must mean $A \cap B' = 0$. All elements in B can be seen as $arx + bsx$. By definition, $bB' = 0$, which implies that $bE \subset A$ by exactness so, $bsx \in A$. From $abE = 0$, we conclude that $arx \in B'$. This means $A \oplus B' = B$, and the projection from B to C takes the subgroup B' to C isomorphically. □

This lemma mostly proves Theorem 2.15. Apply the lemma on the sequence

$$1 \to U_1/U_n \to U/U_n \to \mathbb{F}_p^* \to 1.$$

We know that the order of U_1/U_n is p^{n-1}, and the order of $\mathbb{F}_p^*$ is $p - 1$. These orders have greatest common divisor 1. The group U/U_n contains a subgroup isomorphic to $\mathbb{F}_p^*$. The projection U/U_n to U/U_{n-1} takes this subgroup to the subgroup of U/U_{n-1} that is also isomorphic to $\mathbb{F}_p^*$. Taking a projective limit, there is also a subgroup of U that is isomorphic to $\mathbb{F}_p^*$. We already know that U/U_1 is isomorphic to $\mathbb{F}_p^*$. From this, we conclude that $U \cong U_1 \times \mathbb{F}_p^*$. With this new representation of U, we find that $\mathbb{Q}_p^* \cong \mathbb{Z} \times U_1 \times \mathbb{F}_p^*$.

2.4 Squares of $\mathbb{Q}_p$

This section discusses the group $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. In Chapter 4 the group $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ will appear multiple times throughout this thesis. We want to know what these groups look like for different primes p. To do this, we prove the next theorem.

Theorem 2.17. Assume that $p \neq 2$. Take an element $x \in \mathbb{Q}_p^*$ written as $x = p^n u$, where $u \in U$. The element x is a square if and only if n is even and the image of u into $U/U_1 \cong \mathbb{F}_p^*$ is a square. This would mean the image of u has Legendre symbol 1.

Proof. We know that U is isomorphic to $\mathbb{F}_p^* \times U_1$. Therefore, write u as (a, u_1). By Theorem 2.14 and Theorem 2.15, $\mathbb{Q}_p^* \cong \mathbb{Z} \times U_1 \times \mathbb{F}_p^*$ we need that both a and u_1 are squares, and n must be even. The group U_1 under multiplications is isomorphic to $\mathbb{Z}_p$ under addition $p \neq 2$. Because 2 is invertible, all of the elements there are squares. This leaves the requirement that n is even, and that the element a is a square. This proves the theorem. □

Theorem 2.18. If $p \neq 2$, the group $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Proof. This follows from Theorem 2.17. The group $\mathbb{Q}_2^* \cong 2\mathbb{Z} \times \mathbb{F}_P^{*2} \times U_1$. Dividing this out gives the desired result. □

A similar result can be given for the case where $p = 2$. Proves of these statements are found in chapter 2 of [7]. For this thesis, the following theorems are relevant.

Theorem 2.19. An element $p^n u \in \mathbb{Q}_2^*$ is a square if and only if n is even and $u \equiv 1 \mod 8$.

Theorem 2.20. If $p = 2$, the group $\mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

3 The Hilbert symbol

In this section, we discuss a useful tool that we use to define the invariant ε on quadratic forms. The next section discusses this in more detail.

3.1 Definition of the Hilbert symbol

Let us give the definition of the Hilbert symbol.

Definition 3.1. For two nonzero p-adic numbers a and b, we let:

$(a, b) = 1$ if $z^2 - ax^2 - by^2 = 0$ has a nontrivial solution with $(x, y, z) \in \mathbb{Q}_p$ (or $\mathbb{R}$)
$(a, b) = -1$ else

This number (a, b) is called the Hilbert symbol of a and b.

The Hilbert symbol does not change when we multiply a or b with squares. Suppose that we would multiply a with a square c^2 and b with another square d^2. Then we take these squares into x^2 and y^2 respectively, and relabel $(cx)^2$ to v^2 and $(dy)^2$ to w^2 to find the same Hilbert symbol of a and b. We first proof the following theorem about the Hilbert symbol:

Theorem 3.2. Assume that $a, b \in \mathbb{Q}_p^*$. Then $(a, b) = 1$ if and only if a belongs to the group of the norms of elements of $\mathbb{Q}_p(\sqrt{b})^*$.

Proof. Now assume that a belongs to the group of the norms of elements in $\mathbb{Q}_p(\sqrt{b})^*$. We can assume that b is not a square. Otherwise, the field extension would be trivial. We denote by β a square root of b. Every element in our field can be written as $c + \beta d$. Here the norm is defined by $c^2 - bd^2$. We can use our assumption that a can be written as the norm of an element in our extension. So $a = c^2 - bd^2$ for some c and d in $\mathbb{Q}_p$. Now we see that $c^2 - a - bd^2 = 0$, so the triple $(c, 1, d)$ is a nontrivial solution. Now assume that $(a, b) = 1$. So there is a nontrivial triple (z, x, y) such that $z^2 - ax^2 - by^2 = 0$. Observe that $x \neq 0$ since otherwise b would be a square, and the statement is true since then $\mathbb{Q}_p(\sqrt{b}) = \mathbb{Q}_p$. This means we can divide by x. We see that a must be equal to $\left(\frac{z}{x}\right)^2 - \left(\frac{\beta y}{x}\right)^2$, where β is a square root of b. This is the norm of the element $\left(\frac{z}{x}\right) + \left(\frac{\beta y}{x}\right)$. □

The Hilbert symbol satisfies the following properties.

Theorem 3.3. Let $a, b, c, d \in \mathbb{Q}_p^*$. We have that:

$i)$ $(a, b) = (b, a)$
$ii)$ $(a, c^2) = 1$
$iii)$ $(a, -a) = 1$ and if $a \neq 1$ then $(a, 1 - a) = 1$
$iv)$ $(a, b) = 1 \implies (ad, b) = (d, b)$
$v)$ $(a, b) = (a, -ab)$ and if $a \neq 1$ then $(a, b) = (a, (1 - a)b)$

The condition that $a \neq 1$ when $1 - a$ appears is necessary because the Hilbert symbol is undefined when either a or b is zero.

Proof. $(a,b) = (b,a)$ follows directly from the definition of the Hilbert symbol. Next $(a,c^2) = 1$, since we could then choose the triple $(c,0,1)$ to get a nontrivial zero. For the symbol $(a,-a)$ the triple $(0,1,1)$ is a nontrivial solution and for $(a,1-a)$ the triple $(1,1,1)$ is a nontrivial solution. To prove the implication we can use Theorem 3.2. Since $(a,b) = 1$, the element a can be written as the norm of an element in $\mathbb{Q}_p(\sqrt{b})^*$. Note that the norm has the property that $N(xy) = N(x)N(y)$. This must mean that d can be written as a norm if and only if ad can be written as a norm. This proves the implication. The last equality combines *i*), *iii*) and *iv*), with $d = b$ applied on the symbol $(a,-a)$. By the previous parts $(a,-a) = (-a,a) = 1$, so by part *iv*), we have that $(b,a) = (-ab,a)$. The same can be done on the symbol $(a,1-a)$. □

It turns out that the Hilbert symbol is bilinear in the sense that $(ab,c) = (a,c)(b,c)$, which we prove in the next section.

3.2 Computing the Hilbert symbol

In this section we give explicit formulas for the computation of the Hilbert symbol in different fields. We first look at $\mathbb{Q}_\infty = \mathbb{R}$.

Theorem 3.4. In $\mathbb{R}$, the Hilbert symbol $(a,b) = -1$ if and only if both $a < 0$ and $b < 0$.

Proof. If $(a,b) = -1$, then there is no solution to $z^2 - ax^2 - by^2 = 0$. This only happens if both a and b are less than 0. Conversely, first assume that $a < 0$ and $b < 0$. The equation does not have a nontrivial zero because we are adding nonnegative terms. Without loss of generality, assume $a > 0$ and $b < 0$. Set $x = \frac{\sqrt{z^2 - by^2}}{a}$ to get a nontrivial solution, and since $b < 0$, the square root is always real. Finally, if both $a > 0$ and $b > 0$, there is also a nontrivial solution. □

We can move on to the remaining cases of the p-adic numbers. Consider the fields $\mathbb{Q}_p$, where $p \neq 2$. For this, we define the map ε:

$$\varepsilon(z) = \frac{z-1}{2} \bmod 2 = \begin{cases} 0, \text{ if } z \equiv 1 \bmod 4 \\ 1, \text{ if } z \equiv -1 \bmod 4 \end{cases}$$

We can use this map to find an expression for (a,b) when a and b are in $\mathbb{Q}_p$ and $p \neq 2$.

Theorem 3.5. For any $a, b \in \mathbb{Q}_p$ with $p \neq 2$, first write a as $p^c u$ and b as $p^d v$, with $u, v \in U$. Then we have:

$$(a,b) = (-1)^{cd\varepsilon(p)} \left(\frac{u}{p}\right)^d \left(\frac{v}{p}\right)^c$$

where $(\frac{a}{b})$ denotes the Legendre symbol.

To prove that this is the case, we need the following lemma.

Lemma 3.6. Let $v \in U$. If the equation $z^2 - px^2 - vy^2 = 0$ has a nontrivial solution in $\mathbb{Q}_p$, then there is a solution with $z, y \in U$ and $x \in \mathbb{Z}_p$.

Proof. From Theorem 2.9 we obtain a primitive solution. This solution has the properties that we want. Assume that the obtained solution does not have the desired properties. Then, either $y \equiv 0 \mod p$ or $z \equiv 0 \mod p$. Because $z^2 - vy^2 \equiv 0 \mod p$, and because $v \in U$, we would actually need that both z and y are not congruent to 0 mod p. But this would imply that $px^2 \equiv 0 \mod p^2$. This then implies that $x \equiv 0 \mod p$. This means that this is not a primitive point, since x, y and z are all divisible by p. □

We start proving Theorem 3.5.

Proof. We first notice that we have 4 cases. We can take both c and d mod 2, since multiplying by -1 two times does not change the outcome. We can also make use of the symmetry of the Hilbert symbol to skip the case where $c = 0$ and $d = 1$. This is the same as the case where $c = 1$ and $d = 0$. So let us first consider the case where $c = d = 0$. In this case we need to look at the symbol (u, v). This would have to be equal to 1. If we look at the equation $z^2 - ux^2 - vy^2 \mod p$, we know that this has a nontrivial solution by Corollary 2 on page 6 in [7]. By a stronger version of Hensel's lemma in [7] we get a nontrivial solution in our field, hence $(u, v) = 1$ as desired.
We can go to the case where $c = 1$, and $d = 0$. We need to show that $(pu, v) = \left(\frac{v}{p}\right)$. Observe that $(pu, v) = (p, v)$ by applying part $iv)$ of Theorem 3.3 to the symbol (u, v). This can be done since $(u, v) = 1$ as seen in the previous case. So we need to prove that $(p, v) = \left(\frac{v}{p}\right)$. If v is a square, by the definitions of both symbols, both are equal to 1. If v is not a square, we have that $\left(\frac{v}{p}\right) = -1$. By Lemma 3.6, if a nontrivial solution exists, there would also be a solution with $z, y \in U$ and $x \in \mathbb{Z}_p$, which can not be the case, since this contradicts the fact that $\left(\frac{v}{p}\right) = -1$. Finally, we assume that both $c = d = 1$. The symbol (pu, pv) can be rewritten using part $v)$ of Theorem 3.3 to $(pu, pv) = (pu, -p^2uv) = (pu, -uv)$. The last equality follows from the fact that we can take squares out of the symbol. We use the previous case to find that this is equal to $\left(\frac{-uv}{p}\right)$. Using our knowledge of the Legendre symbol, this is equal to $\left(\frac{-1}{p}\right)\left(\frac{u}{p}\right)\left(\frac{v}{p}\right)$. We know that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Substituting this in our equation, we see that this is precisely the desired result. □

With the explicit formula we prove the following theorem.

Theorem 3.7. The Hilbert symbol is bilinear in the sense that $(ac, b) = (a, b)(c, b)$.

Proof. This is a direct computation. Let $a = p^d u$ and $b = p^e v$ and $c = p^f w$. Then:

$$(ac, b) = (-1)^{(d+f)e\varepsilon(p)} \left(\frac{uw}{p}\right)^e \left(\frac{v}{p}\right)^{(d+f)} = (-1)^{de\varepsilon(p)}(-1)^{fe\varepsilon(p)} \left(\frac{uw}{p}\right)^e \left(\frac{v}{p}\right)^{(d+f)}$$

and:

$$(a, b)(c, b) = (-1)^{de\varepsilon(p)} \left(\frac{u}{p}\right)^e \left(\frac{v}{p}\right)^d (-1)^{fe\varepsilon(p)} \left(\frac{w}{p}\right)^e \left(\frac{v}{p}\right)^f$$

□

Unfortunately, the formula given in Theorem 3.5 does not work for the specific field $\mathbb{Q}_2$. To obtain an explicit formula for this field, we introduce the map ω:

$$\omega(z) = \frac{z^2-1}{8} \bmod 2 = \begin{cases} 0, \text{ if } z \equiv \pm 1 \bmod 8 \\ 1, \text{ if } z \equiv \pm 5 \bmod 8 \end{cases}$$

Using this map, we define an explicit formula in that case that $p = 2$.

Theorem 3.8. For any $a, b \in \mathbb{Q}_2$ first write them as $2^c u$ and $2^d v$ respectively, with $u, v \in U$. Then we have:

$$(a, b) = (-1)^{\varepsilon(u)+\varepsilon(v)+c\omega(v)+d\omega(u)}$$

Proof. By the same reasoning as in the proof of Theorem 3.5 we consider c and d as either 0 or 1. Assume that $c = d = 0$. In this case, the formula tells us that $(u, v) = 1$ if either $u \equiv 1 \mod 4$ or $v \equiv 1 \mod 4$. Otherwise it is -1. Assume that $u \equiv 1 \mod 4$. This implies that $u \equiv 1 \mod 8$ or $u \equiv 5 \mod 8$. If $u \equiv 1 \mod 8$, it is a square by Theorem 2.19, so the Hilbert symbol is equal to 1. In the other case, we take another element $u + 4v \equiv 1 \mod 8$. There is an element w such that $w^2 = u + 4v$. Then $(w, 1, 2)$ is a nontrivial solution to $z^2 - ux^2 - vy^2$. Hence the symbol is equal to 1.
Assume that both u and v are $-1 \mod 4$. If there is a primitive solution to $z^2 - ux^2 - vy^2$, then $z^2 + x^2 + y^2 \equiv 0 \mod 4$. However only 0 and 1 are squares in $\mathbb{Z}/4\mathbb{Z}$. Therefore x and y and z are all $0 \mod 4$. If they are $0 \mod 4$, they are $0 \mod 2$. This contradicts the primitiveness of the solution, hence we must have that $(u, v) = -1$.
In the second case assume that $c = 1$ and $d = 0$. We need to show that $(2u, v) = (-1)^{\varepsilon(u)\varepsilon(v)+\omega(v)}$. Note that $(2, v) = 1$ if and only if $v \equiv \pm 1 \mod 8$. If we have that $(2, v) = 1$, then by Lemma 3.6 there is a solution in $\mathbb{Z}_2$ to $z^2 - 2x^2 - vy^2$ that is primitive. This would mean that $y \not\equiv 0 \mod 2$ and $z \not\equiv 0 \mod 2$. By the structure of $\mathbb{Z}/8\mathbb{Z}$ we can conclude that $y^2 \equiv z^2 \equiv 1 \mod 8$ and reducing the polynomial $\mod 8$ we find that $1 - 2x^2 - v \equiv 0 \mod 8$. The squares of $\mathbb{Z}/8\mathbb{Z}$ are $0, 1$ and 4. We can conclude that $v \equiv \pm 1 \mod 8$. Either v is a square or $(1, 1, 1)$ is a solution which we lift to $\mathbb{Z}_p$ using Hensel's lemma to a full solution. In either case we can conclude that $(2, v) = 1$. Our next objective is showing that $(2u, v) = (u, v)(2, v)$. By part $iv)$ of Theorem 3.3, this is true if at least one of the symbols is equal to 1. If both are -1, then this is equivalent to $v \equiv 3 \mod 8$ and $u \equiv 3 \mod 8$ or $u \equiv 7 \mod 8$. By multiplying with squares we can reduce this to $u = -1$ and $v = 3$ or $u = 3$ and $v = -5$. Then the equations $z^2 + 2x^2 - 3y^2 = 0$ and $z^2 - 6x^2 + 5y^2 = 0$ both have $(1, 1, 1)$ as a solution, hence the symbol $(2u, v) = 1 = (2, v)(u, v)$. This proves this case.
In the last case, assume that $c = d = 1$, where we want to check that

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

By part $v)$ of Theorem 3.3 the symbol is equal to $(2u, -4uv) = (2u, -uv)$. The equality follows because 4 is a square. The second part is now a unit, so by the previous case, we have $(2u, 2v) = (-1)^{\varepsilon(u)\varepsilon(-uv)+\omega(-uv)}$. Both ε and ω are homomorphisms. We can split the exponent into $\varepsilon(u)(\varepsilon(-1) + \varepsilon(u) + \varepsilon(v) + \omega(-1) + \omega(u) + \omega(v)$. A computation shows that $\varepsilon(-1) = 1$ and $\omega(-1) = 0$. Furthermore, $\varepsilon(u)(1 + \varepsilon(u)) = 0$, hence the exponent is equal to $\varepsilon(u)\varepsilon(v) + \omega(u) + \omega(v)$, which is the desired result. □

3.3 Properties of the Hilbert symbol

With the current results we prove some more advanced properties of the Hilbert symbol. These results often involve all of the different Hilbert symbols in different fields of a pair of numbers.

Definition 3.9. Let V be the set of prime numbers, alongside ∞. For some $a, b \in \mathbb{Q}^*$, denote $(a,b)_v$ the Hilbert symbol of the image of a and b in $\mathbb{Q}_v$.

The set V is often called the set of places. In this thesis, we are only interested in the fields $\mathbb{Q}_p$ where p is a prime number, but this notion can be generalised to all number fields, which are finite extensions K of the field $\mathbb{Q}$. We first prove Hilbert's Reciprocity Law.

Theorem 3.10 (Hilbert's Reciprocity Law)**.** For two $a, b \in \mathbb{Q}^*$, we have that $(a,b)_v = 1$ for almost all $v \in V$ and:

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

The proof of this theorem makes heavy use of the formulas given in Theorems 3.5 and 3.8.

Proof. First notice that we can use the bilinearity proven in Theorem 3.7 to split the symbol at a specific place into products of symbols of the prime factors of the numbers a and b and possibly -1. Therefore, we only need to prove the theorem for the case where a and b are prime numbers or -1. Assume that $a = b = -1$. From the explicit formulas given in Section 3.2 it can be seen that $(-1,-1)_2 = (-1,-1)_\infty = -1$ and $(-1,-1) = 1$ for all other cases. This means that for almost all the places the symbol is 1, and the product is also equal to 1, since there are exactly two factors equal to -1. By symmetry, we can handle the cases where $a = -1$ and $b = p$, and $a = p$ and $b = -1$ at the same time. We further subdivide the problem in the case where $p = 2$ and $p \neq 2$. If $p = 2$, then by our formulas, $(-1,2)_v = 1$ for all $v \in V$, and the product is also equal 1. If $p \neq 2$, then we see that $(-1,p)_v = 1$ if $v \neq p$ and $v \neq 2$, proving that for almost all v, $(-1,p)_v = 1$. Furthermore, $(-1,p)_2 = (-1,p)_p = (-1)^{\varepsilon(p)}$. Once again, we have exactly two factors of -1, so the product must equal 1. Assume that both a and b are prime numbers. If they are the same, then we use part v) of Theorem 3.3 to see that $(p,p)_v = (p, -p^*(-1))_v = (p,-1)_v$. We have reduced this to the previous case. This means we are left with a and b being two distinct primes. Once again, we consider the case where either a or b is equal to 2 separately. By Theorem 3.5, we have that $(2,p)_v = 1$ for $v \neq 2$ and $v \neq p$, which proves that for almost all v, $(2,p)_v = 1$. Then $(2,p)_2 = (-1)^{\omega(p)}$ and $(2,p)_p = \left(\frac{2}{p}\right) = (-1)^{\omega(p)}$ by our knowledge on the Legendre symbol. Finally, we consider the case where both primes are not equal to 2. Then, $(a,b)_2 = (-1)^{\varepsilon(a)\varepsilon(b)}$ and $(a,b)_a = \left(\frac{b}{a}\right)$ and $(a,b)_b = \left(\frac{a}{b}\right)$. We use our knowledge of the Legendre symbol to see that $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\varepsilon(a)\varepsilon(b)}$. This cancels with the expression of $(a,b)_2$, so we once again conclude that the product of these three factors is equal to 1. For the other symbols $(a,b)_v$ where v is not 2, a or b, we have that $(a,b)_v = 1$ by Theorem 3.5, so we conclude that almost all symbols are equal to 1. □

Hilbert's product formula is equivalent to the quadratic reciprocity law in $\mathbb{Q}$. In the proof we used the fact that $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\varepsilon(a)\varepsilon(b)}$, which is the quadratic reciprocity law we are

familiar with [8, p. 23]. It can be proven that Hilbert's Reciprocity law also implies the quadratic reciprocity. A proof is given in [2]. The proof uses the explicit formula's for the Hilbert symbol and shows that they give equivalent conditions for the quadratic reciprocity law. The main reason that Hilbert's reciprocity law is interesting is that it generalises to more than $\mathbb{Q}$, while the quadratic reciprocity might not.
There are more properties of the Hilbert symbol that need to be discussed. The next theorem tells us when there are rational numbers that have a certain Hilbert symbol.

Theorem 3.11. let $A = (a_i)_{i\in I}$ be a finite subset of $\mathbb{Q}^*$. Let $(\varepsilon_{i,v})$ be a set of numbers equal to 1 or -1. There is an $x \in \mathbb{Q}^*$ such that $(a_i, x)_v = \varepsilon_{i,v}$ for all i and v if and only if we have that

$$\begin{aligned}&\text{almost all } \varepsilon_{i,v} = 1,\\ &\text{for all } i \in I \text{ we have } \prod_{v\in V} \varepsilon_{i,v} = 1,\\ &\text{for all } v \text{ there is a } x_v \in \mathbb{Q}_v^* \text{ such that } (a_i, x_v)_v = \varepsilon_{i,v} \text{ for all } i.\end{aligned}$$

Proof. If there is such an x, then from Theorem 3.10 the first two conditions are met, and the third condition is met by taking $x_v = x$ for all $v \in V$. For the other direction, first multiply the a_i with a square to make them integers. let S be a finite subset of V containing $2, \infty$ and the prime factors of the a_i. Let T be the set of all places where there is an i with $\varepsilon_{i,v} = -1$. The set T is finite by Theorem 3.10. Assume that $S \cap T = \emptyset$. Then take $a = \prod_{i\in T|i\neq\infty} i$ and $m = 8\prod_{j\in S|j\neq 2,\infty} j$. These two are coprime, because the intersection of S and T is empty. By Dirichlet's theorem on arithmetic progressions, there is a prime number such that $p \equiv a \mod m$ that also is not in both S and T. Set $x = ap$. For all $v \in S$ the symbol $\varepsilon_{i,v} = 1$ because the intersection of S and T is empty. The symbol $(a_i, x)_v$ is equal to 1 if $v = \infty$, because $x > 0$. In the other case, v is a prime number q. Then $x \equiv a^2 \mod m$, which means $x \equiv a^2 \mod 8$ if $q = 2$ and $x \equiv a^2 \mod q$ otherwise. Both x and a are q-adic units, so x is a square, so $(a_i, x)_v = 1$. Now $v = q \notin S$, the a_i are q-adic units. Because $2 \in S$ we can also assume that $q \neq 2$, so by Theorem 3.5, the following equation is true for all $v \in Q_q^*$:

$$(a_i, b)_q = \left(\frac{a_i}{q}\right)^{v_q(b)}.$$

If then $q \notin T \cup \{p\}$, the x is a q-adic unit, so $v_q(x) = 0$. By the equation, we find that $(a_i, x)_q = 1$. Because $q \notin T$, it is clear that $\varepsilon_{i,q} = 1$. If $q \in T$, then $v_q(x) = 1$. With the third condition we can find $x_q \in \mathbb{Q}_q^*$ such that $(a_i, x_q) = \varepsilon_{i,q}$ for all i. One of these is equal to -1, so $v_q(x_q) \equiv 1 \mod 2$. By the explicit formulas $(a_i, x)_q = \left(\frac{a_i}{q}\right) = (a_i, x_q)_q = \varepsilon_{i,q}$. In the final case the prime q is equal to p. We already know all the other symbols, so we can use them to find this symbol.

$$(a_i, x)_p = \prod_{v\neq p}(a_i, x)_v = \prod_{v\neq p} \varepsilon_{i,v} = \varepsilon_{i,p}$$

which is the desired result. To prove the general case where $S \cap T \neq \emptyset$, the Approximation Theorem (Theorem 2.7) is used. By Theorem 2.7, there is a $x' \in \mathbb{Q}^*$ such that x'/x_v are

squares in $\mathbb{Q}_v^*$. This follows from the openness of the squares [7]. Then $(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v}$. Take $b_{i,v} = \varepsilon_{i,v}(a_i, x')_v$. It can be verified that these $b_{i,v}$ satisfy the conditions, and that $b_{i,v} = 1$ if $v \in S$. Then we can use the proven version where $S \cap T = \emptyset$ to show that there is a $v \in \mathbb{Q}^*$ with $(a_i, y)_v = b_{i,v}$ for all i and v. Set $x = yx'$, and we can verify that this x gives the desired result. This proves the theorem.

□

Finally, we prove this theorem related to p-adic units.

Theorem 3.12. Let $a, b \in \mathbb{Z}_p^*$. Then we have that $(a, b)_p = 1$.

Proof. Consider the equation $z^2 - \bar{a}^2 - \bar{b}y^2 \mod p$. Here $\bar{a} = a \mod p$. We define the set $T = \{ct^2 | t \in \mathbb{F}_p\}$. Its size is $1 + \frac{p-1}{2}$. The first term comes from $c = 0$, and the rest from the other squares in $\mathbb{F}_p^*$. Then set $z = 1$. The set of all elements of the form $1 - by^2$ also contains $1 + \frac{p-1}{2}$ elements using the same logic. Because of the size of these sets and the pigeonhole principle, they share at least one element. This yields a solution of the equation $1^2 - \bar{a}x^2 - \bar{b}y^2$ in $\mathbb{F}_p$. Then by Hensel's lemma, we can lift these solutions to a solution in $\mathbb{Z}_p$, which shows that the Hilbert symbol is 1. We have to be careful with lifting this solution since we can not simply lift two variables at the same time. The first lift can be without any problems, but after that we have to make sure that the derivative is still nonzero. □

4 Quadratic forms

In this section, we discuss all the preliminaries on quadratic forms that are necessary to understand the proof of the Hasse-Minkowski theorem.

4.1 Basics of quadratic forms

We start by giving the definition of a quadratic form.

Definition 4.1. Let k be a field, and V a vector space over k. Let $Q : V \to k$ be a function such that:

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

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

Definition 4.1 can be generalised to commutative rings, and modules over such rings, but since we are only interested in the fields $\mathbb{Q}_p$ and $\mathbb{R}$, this is not necessary. Quadratic modules have a natural choice for a scalar product. This scalar product is defined as long as we are working over fields with a characteristic that is not equal to 2. This is no problem for us, since $\mathbb{Q}_p$ and $\mathbb{R}$ have characteristic 0.

Definition 4.2. The scalar product is a symmetric bilinear form defined as:

$$(x, y) \mapsto x.y = \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$$

Note that $x.x = \frac{1}{2}(Q(2x) - Q(x) - Q(x)) = \frac{1}{2}(4Q(x) - Q(x) - Q(x)) = \frac{1}{2}(2Q(x)) = Q(x)$. Every quadratic form gives rise to a symmetric bilinear form with this relation. To get an easier way to handle these forms, we define the matrix of a quadratic form.

Definition 4.3. Pick a basis of V with $dim(V) = n$. The matrix A of Q is defined element-wise, with $a_{ij} = e_i.e_j$, where the e_i are the basis vectors of V. Then for a vector $x = \sum_{i=1}^{\infty} x_i e_i$, we have $Q(x) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j$.

Let us check whether this does indeed satisfy the definition of a quadratic form. If we would multiply our vector x by a scalar a, then every element of the vector is multiplied by a. Putting ax in $Q(x) = \sum_{1 \leq i,j \leq n} a_{ij} x_i x_j$, observe that every term has a factor of a^2, since we always multiply 2 entries of the vector in every individual term of the sum. This means we can factor out a^2, and the first part of Definition 4.1 is satisfied. Consider the map $(x, y) \mapsto Q(x + y) - Q(x) - Q(y)$. We need to check that $(bx, y) = b(x, y)$. So:

$$Q(bx + y) - Q(bx) - Q(y) = \sum_{1 \leq i,j \leq n} a_{ij}(bx_i + y_i)(bx_j + y_j) - \sum_{1 \leq i,j \leq n} a_{ij} bx_i bx_j - \sum_{1 \leq i,j \leq n} a_{ij} y_i y_j$$

Expand the terms in the first sum to $b^2x_ix_j + bx_iy_j + bx_jy_i + y_iy_j = b^2x_ix_j + b(x_iy_j + x_jy_i) + y_iy_j$. Notice that we can split the first sum into three separate sums, where two of them are equal to the sums of $Q(bx)$ and $Q(y)$. This leaves just the sum $\sum_{1 \leq i,j \leq n} a_{ij} b(x_iy_j + x_jy_i)$. By taking

out the b of the sum, we obtain $b(x,y) = b(\sum_{1\leq i,j\leq n} a_{ij}(x_iy_j + x_jy_i)$. By the symmetry of (x,y), we can conclude that $(x,cy) = c(x,y)$. This means our new way of defining Q satisfies the criteria to be a quadratic form. What would happen if we were to change the basis of the vector space V with an invertible matrix X? This gives a new matrix B, with $B = XAX^T$. Applying the determinant on both sides gives the equality $det(B) = det(A)det(X)^2$. We can conclude that $det(A)$ is determined up to multiplication with a nonzero square. This constant is called the discriminant of Q, denoted by $disc(Q)$.
By defining the scalar product, we have also defined orthogonality. Two vectors are orthogonal if their scalar product is equal to 0. For a subspace W, define the orthogonal complement W^o as the set of vectors that are orthogonal to all elements in W. There might be a special set of vectors that are orthogonal to all other vectors. That would be the set V^o, which we call the radical of V. A quadratic form is called nondegenerate if $V^o = 0$. This is equivalent with $disc(Q) \neq 0$. If that is the case, then the matrix has full rank. With our notion of orthogonality we define orthogonal sums.

Definition 4.4. Let V be a vector space. The space V is the orthogonal direct sum of a set of pairwise orthogonal subspaces U_i if $V = \oplus_{1\leq i\leq m} U_i$.

By restricting Q to the subspaces U_i, we get a set of m quadratic forms (U_i, Q_i). In this case, we have that $Q(x) = \sum_{i=1}^{m} Q_i(x_i)$. With the power of orthogonality, we use this to make orthogonal bases.

Definition 4.5. A basis $(e_i)_{i\in I}$ of V is orthogonal if all of the basis vectors are pairwise orthogonal. This implies that $V = \oplus_{i\in I} ke_i$, where k is the base field.

If the basis is orthogonal, the quadratic module has a diagonal matrix, which means that every quadratic form can be written as $\sum_{i=1}^{n} a_i x_i^2$. Since having an orthogonal basis means that there are significantly less terms in the quadratic form to deal with, orthogonal bases are in general easier to work with than any ordinary basis.

Theorem 4.6. Every quadratic module has an orthogonal basis.

Proof. This basis can be constructed by applying the Gram-Schmidt procedure on the columns of the matrix of the quadratic module. □

Definition 4.7. If $Q(x) = 0$, then x is isotropic. A subspace of V that has the property that all of its elements are isotropic is also called isotropic.

By the way quadratic forms are constructed, 0 is always an isotropic element. Furthermore, if x is an isotropic element, then the span of x is an isotropic subspace. To see this, notice that an element in $span(x)$ looks like ax. We can take a out of the quadratic form: $Q(ax) = a^2Q(x) = 0$. The definition of a hyperbolic plane is closely related to this concept.

Definition 4.8. If a quadratic module has two isotropic basis vectors x and y, and $x.y \neq 0$, then this quadratic module is called a hyperbolic plane.

An hyperbolic plane is always nondegenerate, which can be seen from the fact that $x.y \neq 0$. We can prove the following theorem on the existence of hyperplanes.

Theorem 4.9. Let (V, Q) be a nondegenerate quadratic module. If x is isotropic, then there exists a subspace of V that is a hyperbolic plane containing x.

Proof. V is nondegenerate. So we can find an element z such that $x.z = 1$. If $x.z \neq 1$, we normalize the scalar product by multiplying z with $\frac{1}{x.z}$. We claim that $2z-(z.z)x = 2z-Q(z)x$ is isotropic. We show this by adding 0 in a smart way.

$$Q(2z - (z.z)x) = Q(2z - Q(z)x) + Q(2z) - Q(2z) + Q(Q(z)x) - Q(Q(z)x)$$

Then notice that we can group three terms together to get:

$$Q(2z) + Q(Q(z)x) + 2(2z. - Q(z)x).$$

The second term is equal to 0 because x is isotropic. By bilinearity, the scalar product reduces to $-2Q(z)(z.x) = -2Q(z)$. Finally, we can change the first term to $4Q(z)$. Then we find that $4Q(z) + 2(-2Q(z)) = 0$, so the element $2z - (z.z)x$ is isotropic. Furthermore,

$$x.(2z - (z.z)x) = (x.2z) - Q(z)(x.x) = 2(x.z) - Q(z)Q(x) = 2.$$

The space $xk + (2z - (z.z)x)k$ is a hyperbolic plane. Both of the basis vectors are isotropic, and their scalar product is nonzero. □

Theorem 4.9 enables us to prove the next theorem.

Theorem 4.10. If (V, Q) is nondegenerate and there exists an isotropic $x \neq 0$, then $Q(V) = k$.

Proof. By Theorem 4.9, we can assume that there is a hyperplane containing x. For any $a \in k$, we can choose the element $x + \frac{a}{2}y$. Then by adding $0 = -Q(x) = -\frac{a^2}{4}Q(y) = -Q(\frac{a}{2}y)$, we find:

$$Q(x + \frac{a}{2}y) = Q(x + \frac{a}{2}y) - Q(x) - Q(\frac{a}{2}y) = 2(x.\frac{a}{2}y) = a$$

So, for every $a \in k$, there is an element $z \in V$ such that $Q(z) = a$. □

With Theorem 4.6, we return to the discriminant of Q. Since every quadratic module has an orthogonal basis, by picking this basis the matrix of Q is a diagonal matrix. This makes computing the discriminant easy. It is just the product of the elements on the diagonal. Remember that this is unique up to multiplication by a square. If a module is nondegenerate, the discriminant is nonzero. In this case we view the the discriminant as an element of k^*/k^{2*}.

4.2 Equivalence of quadratic forms

In our proof of the Hasse-Minkowski we want to reduce the amount of quadratic forms that we need to consider. This is why in this section we discuss equivalence of quadratic forms. For now, the fields k are the p-adic numbers. The real numbers are easier to handle, but they do require different techniques from the p-adic numbers. Assume that we have a homogeneous quadratic polynomial f of n variables. The amount of terms of the polynomial f is called the rank. The polynomial $f(x_1, x_2, \ldots, x_n)$ looks like $\sum_{i=1}^{n} a_{ii}x_i^2 + 2\sum_{1\leq i<j\leq n} a_{ij}x_ix_j$. Then (k^n, f) is a quadratic module, with an associated matrix $A = (a_{ij})$. The first part of this section is similar to Subsection 4.1.

Definition 4.11. Two quadratic forms f and g are equivalent if the corresponding modules are isomorphic. This is equivalent to saying there exists an invertible matrix B such that $g(x) = f(Bx)$. If f and g are equivalent, we say $f \sim g$.

Another easier way to see that two forms are equivalent is by showing that there exists an nonsingular matrix B such that $G = BFB^T$, where G and F are the matrices of g and f respectively. We want to combine different forms to create new forms. To do this, we use the orthogonal sum.

Definition 4.12. If $f(x_1, x_2, \ldots, x_n)$ and $g(y_1, y_2, \ldots, y_m)$ are two quadratic forms over the spaces V and W respectively, then $f \dot{+} g$ is the quadratic form $f(x_1, x_2, \ldots, x_n) + g(y_1, y_2, \ldots, y_m)$ in $n + m$ variables over the space $V \times W$. If it is clear that we are talking about this type of sum we write the normal $+$.

This definition is very similar to how we defined orthogonal sums in Subsection 4.1. There is also the operation $\dot{-}$ defined as $f \dot{-} g = f \dot{+} (-g)$. In a similar way to how we defined hyperbolic planes in Definition 4.8, we also want to define it for our new forms.

Definition 4.13. A quadratic form $f(x_1, x_2)$ in two variables is hyperbolic if $f \sim x_1x_2 \sim x_1^2 - x_2^2$.

This might not be intuitive at first, but this is equivalent to saying that the quadratic module (k^2, f) is a hyperbolic plane. If the form is similar to x_1x_2, then if either x_1 or x_2 is zero, the form yields zero. Thus both basis vectors are isotropic. The inner product is also nonzero. The matrix of x_1x_2 can also be turned into the matrix of $x_1^2 - x_2^2$, so they are equivalent. We also want to translate the notion of isotropic elements. This is done by saying that f represents an element a if there exists a nonzero vector x such that $f(x) = a$. So, f represents 0 if there is a nonzero x such that $f(x) = 0$. In this case, x is an isotropic element of the quadratic module (k^n, f). There is a translation of Theorems 4.9 and 4.10 to this alternate way of defining quadratic forms.

Theorem 4.14. If f is nondegenerate and represents 0, then $f \sim f_2 \dot{+} g$, with f_2 hyperbolic. We also have that every element of k is represented by f.

Using this theorem we can prove the following fact.

Theorem 4.15. If g is a nondegenerate quadratic form in $n - 1$ variables and $a \in k^*$, then the following are equivalent:

i) g represents a.

ii) $g \sim h \dot{+} ax^2$ where h is in $n - 2$ variables.

iii) $g \dot{-} ax^2$ represents 0.

Proof. First assume that g represents a. This means there exists an x such that $x.x = Q(x) = a$. The orthogonal complement U of xk has the property that $V = U \oplus xk$. This must mean that $g \sim h \dot{+} ax^2$, since their modules are isomorphic. Here h is the quadratic form of U. Also, because g represents a, the form $g \dot{-} ax^2$ represents 0. Choose the element y such that $g(y) = a$, and $x = 1$. It is clear that $g(y) \dot{-} ax^2 = 0$, so $g \dot{-} ax^2$ represents 0. Assume that $g \sim h \dot{+} ax^2$. We choose the 0 element in the space of h and set $x = 1$. Then $h \dot{+} ax^2 = a$, and since $g \sim h \dot{+} ax^2$, the quadratic form g also represents a. Finally, assume that $g \dot{-} ax^2$ represents 0. The nontrivial zero is $(x_1, \ldots, x_{n-1}, z)$. If $z = 0$, it is clear that g represents 0 and then also a. If this is not the case, then $g(x_1/z, \ldots, x_{n-1}/z) = a$. □

A similar theorem is also required for the proof of a later theorem.

Theorem 4.16. If both g and h are quadratic forms of rank greater than or equal to 1, then these are equivalent:

i) $f = g \dot{-} h$ represents 0.
ii) There is an $a \in k^*$ such that both g and h represent a.
iii) There is a $b \in k^*$ such that both $g - bz^2$ and $h - bz^2$ represent 0.

Proof. The equivalence follows from Theorem 4.15, specifically the equivalence of part *i)* and part *iii)* of that theorem. If $g(x) = h(y) = a$, then the element $z = (x, y)$ can be put in f to find $f(z) = g(x) - h(y) = a - a = 0$, thus *ii)* $\implies$ *i)*. The only implication that is left to prove is *i)* $\implies$ *ii)*. Since f represents 0, there is an element (x, y) such that $g(x) = h(y)$. If $g(x) = a = h(y)$, then we are done. If $g(x) = h(y) = 0$, then g represents zero. Because the forms are nondegenerate, we can apply a translation of Theorem 4.10 to see that g represents all elements of k, so also some nonzero value of $h(y)$. This proves the theorem. □

4.3 The discriminant and the invariant ε

The final tools that are needed to prove the Hasse-Minkowski are two invariants. The first is the discriminant, discussed in Subsection 4.1. The other is the invariant ε. This invariant relies heavily on the Hilbert symbol, introduced in Section 3. First take an orthogonal basis $(e_1, e_2, \ldots, e_n) = \mathbf{e}$ of V. By Theorem 4.6, we know that this can be done for any V. In this case, the matrix A associated to the quadratic form is diagonal, and the elements on the diagonal are $a_i = e_i.e_i$.

Definition 4.17. We define $\varepsilon(\mathbf{e}) = \prod_{i<j}(a_i, a_j) = \pm 1$.

One might wonder if the choice of basis gives a different Hilbert symbol. This is not the case.

Theorem 4.18. $\varepsilon(\mathbf{e})$ is independent of the choice of (orthogonal) basis.

To prove Theorem 4.18, we use contiguous bases.

Definition 4.19. If two bases share at least one element, then they are contiguous.

We want to prove the following theorem on contiguous bases.

Theorem 4.20. If (V, Q) is a nondegenerate quadratic module of dimension greater than 3 with two orthogonal bases $\mathbf{e} = (e_1, e_2, \ldots, e_n)$ and $\mathbf{e}' = (e'_1, e'_2, \ldots, e'_n)$, then there is a sequence of orthogonal bases $\mathbf{e}^0, \mathbf{e}^1, \ldots, \mathbf{e}^m$ with $\mathbf{e} = \mathbf{e}^0$, $\mathbf{e}' = \mathbf{e}^m$ and for all i, $\mathbf{e}^i$ is contiguous with $\mathbf{e}^{i+1}$.

To prove this theorem, we need the next lemma.

Lemma 4.21. There is an $a \in k$ such that $e_a = e'_1 + ae'_2$ is not isotropic, and together with e_1, it forms a nondegenerate plane.

Proof. Firstly, $e_a.e_a = (e_1'.e_1') + a^2(e_2' + e_2') + (e_1'.ae_2') + (ae_2'.e_1')$. The last two terms are zero, since the bases are orthogonal. We want $Q(e_a) = e_a.e_a \neq 0$, so choose an a such that $a^2 \neq -\frac{(e_1'.e_1')}{(e_2'+e_2')}$. The plane generated by e_1 and e_a should be nondegenerate. This is equivalent with the condition that the discriminant of the matrix is nonzero, so the following equation must hold: $(e_1.e_1)(e_a.e_a) - (e_1.e_a)^2 \neq 0$. If we assume that $(e_1.e_1)(e_1'.e_1') - (e_1.e_1') = 0$ and $(e_1.e_1)(e_2'.e_2') - (e_1.e_2') = 0$, then we can rewrite 0 to $-2a(e_1.e_1')(e_1.e_2')$. By nondegeneracy, $e_1.e_1$ and $e_1.e_2$ are both nonzero. By some computations we can show that e_a satisfies the conditions, if we would pick an a such that $a \neq 0$ and $a^2 \neq -\frac{(e_1'.e_1')}{(e_2'+e_2')}$, alongside the condition that $(e_1.e_1)(e_1'.e_1') - (e_1.e_1') = 0$ and $(e_1.e_1)(e_2'.e_2') - (e_1.e_2') = 0$. The conditions take away three values of a, but since our field is infinite, this is no problem. □

This allows us to prove Theorem 4.20.

Proof. First assume that $(e_1.e_1)(e_1'.e_1') - (e_1.e_1')^2 \neq 0$. This means the discriminant of the matrix of this quadratic module is nonzero, and thus nondegenerate. That is, the space $P = ke_1 + ke_1'$ is nondegenerate. We could also pick some other basis vectors that are orthogonal to e_1 and e_1' to make a better basis for the space. This gives $P = e_1k + e_ok$ and $P = e_1'k + e_o'k$. We can take the orthogonal complement of P. Take some orthogonal basis of P^o, and call it $\mathbf{f}$. Then the basis $(e_1, e_o, \mathbf{f})$ is contiguos with $\mathbf{e}$ and $(e_1', e_o, \mathbf{f})$. This last basis is contiguous with $\mathbf{e}'$. This proves the statement. Similarly, if $(e_1.e_1)(e_2'.e_2') - (e_1.e_2')^2 \neq 0$, the same proof can be used. In the last case, both $(e_1.e_1)(e_1'.e_1') - (e_1.e_1') = 0$ and $(e_1.e_1)(e_1'.e_1') - (e_1.e_2')^2 = 0$. Using Lemma 4.21, there exists $e_a = e_1' + ae_2'$. It is not isotropic, so there is another vector e_2'' to make a hyperbolic plane with it. The basis $(e_a, e_2'', e_3', \ldots e_n')$ is an orthogonal basis of V. It is contiguous with $\mathbf{e}'$. Using the same proof of the first case, this basis is contiguous with $\mathbf{e}$. Combine the chains of basis changes to get that $\mathbf{e}$ and $\mathbf{e}'$ are contiguous. □

We can finally prove Theorem 4.18.

Proof. The proof is split in three cases, dependent on the dimension of V. If $dim(V) = 1$, $\varepsilon(e_1)$ is always 1, since there is nothing to multiply. If $n = 2$, by definition, $\varepsilon(\mathbf{e}) = 1$ if $z^2 - ax^2 - by^2$ represents 0. By Theorem 4.15, this is equivalent to $ax^2 + by^2$ representing 1. So, then there must exist a $v \in V$ with $Q(v) = 1$, which in turn is independent on the choice of basis. The rest of the cases are proven using induction on n, the dimension of V. The base case where $n = 2$ is already proven. We use Theorem 4.20 to show that we only need to show that equality holds if the bases are contiguous. Then we can repeat the same argument a finite amount of times on the chain of contiguous bases. The Hilbert symbol is symmetric. We can therefore shuffle the basis vectors such that $e_1 = e_1'$. Let $a_i' = e_1'.e_1' = e_1.e_1 = a_1$. Then, $\varepsilon(\mathbf{e}) = (a_1, a_2a_3 \ldots a_n) \prod_{2 \leq i < j} (a_i, a_j)$. We can put an extra square in the Hilbert symbol without changing its value. In this case, put a_1^2 in the second element of the first Hilbert symbol. The second part can then be rewritten to $d(Q)a_1$. The same can be done for $\varepsilon(\mathbf{e}') = (a_1, a_1d(Q)) \prod_{2 \leq i < j} (a_i', a_j')$. The inductive hypothesis can be applied on the orthogonal complement of e_1, which has one dimension less. In this space, the products $\prod_{2 \leq i < j} (a_i, a_j)$ and $\prod_{2 \leq i < j} (a_i', a_j')$ are equal. Hence, the products $(a_1, a_1d(Q)) \prod_{2 \leq i < j} (a_i, a_j)$ and $(a_1, a_1d(Q)) \prod_{2 \leq i < j} (a_i', a_j')$ are also equal. This proves the theorem. □

Since the invariant ε is independent of basis, we write $\varepsilon(Q)$ instead of $\varepsilon(\mathbf{e})$. With all of these invariants, we prove the next theorem.

Theorem 4.22. The quadratic form f represents 0 if and only if:

$$\begin{aligned} &i)\ n = 2 \text{ and } d = -1 \text{ or,} \\ &ii)\ n = 3 \text{ and } (-1, -d) = \varepsilon \text{ or,} \\ &iii)\ n = 4 \text{ and } d \neq 1 \text{ or } d = 1 \text{ and } \varepsilon = (-1, -1) \text{ or,} \\ &iv)\ n \geq 5. \end{aligned}$$

Here $d = d(f)$ and $\varepsilon = \varepsilon(f)$.

Proof. The proof is done in four different cases, depending on the rank of the form f. Let $n = 2$. In this case $f \sim ax^2 + by^2$. This form can only represent zero if $\frac{-a}{b}$ is a square. In the group k^*/k^{*2}, we have that $\frac{-a}{b} = -ab = -d$. If then $d \neq -1$, the expression $\frac{-a}{b}$ would not be a square. So we must have $d = -1$. This completes the proof for $n = 2$.
Let $n = 3$. Then f represents 0 if and only if $ax^2 + by^2 + cz^2$ represents 0. We can normalize this function to $\frac{a}{c}x^2 + \frac{b}{c}y^2 + z^2 - -\frac{a}{c}x^2 - -\frac{b}{c}y^2 + z^2$. By the definition of the Hilbert symbol, this form represents 0 if and only if $\left(-\frac{a}{c}, -\frac{b}{c}\right) = 1$. First multiply by squares to reduce this to $(-ac, -bc)$. By Theorem 3.7 that states that the Hilbert symbol is bilinear,

$$\begin{aligned} &(-ac, -bc) \\ &= (-1, -bc)(ac, -bc) \\ &= (-1, -bc)(a, -bc)(c, -bc) \\ &= (-1, -1)(-1, b)(-1, c)(a, -bc)(c, -bc) \\ &= (-1, -1)(-1, b)(-1, c)(-1, a)(a, b)(a, c)(c, -bc) \\ &= (-1, -1)(-1, b)(-1, c)(-1, a)(a, b)(a, c)(-1, c)(b, c)(c, c). \end{aligned}$$

There are two factors of $(-1, c)$ in the product, and they cancel each other out. By part v) of Theorem 3.3, $(c, c) = (-1, c)$. By the bilinearity, we combine the factors $(-1, a)(-1, b)(-1, c)$ into $(-1, abc)$. Also, the factors (a, b), (a, c) and (b, c) give the invariant ε and $abc = d$. This reduces our formula to $(-1, -1)(-1, d)\varepsilon$. Using bilinearity again, we can combine the final two symbols to obtain the condition $(-1, -d)\varepsilon = 1$. Since $\varepsilon \in \{-1, 1\}$, multiplying both sides by ε gives the condition $(-1, -d) = \varepsilon$, which is the desired result.

To prove the final two cases we need two lemmas. The first is a consequence of the second case that we have already proven.

Lemma 4.23. If $a \in k^*/k^{*2}$, then a rank two form f represents zero if and only if $(a, -d) = \varepsilon$.

Proof. This is proven by constructing a form of rank 3 that represents 0. Consider the form $g = f \dot{-} az^2$. This form represents 0 if and only if f represents a. The invariants of this form are $d(g) = -ad(f)$ and $\varepsilon(g) = (-a, d)\varepsilon$. By applying the already proven part $ii)$ of Theorem 4.22 on the form g, we get the condition $(-1, -(-ad)) = (-a, d)\varepsilon$. By part $v)$ of Theorem 3.3, $(-a, d) = (-a, ad)$. Taking this to the other side, and using bilinearity, gives the condition $(a, ad) = (a, -d) = \varepsilon$. □

The second lemma is a lot more complicated.

Lemma 4.24. Recall that in Theorem 2.18 and Theorem 2.20 we gave explicit representations of k^*/k^{*2}. Here the size of the groups was 2^r elements with $r = 2$ if $p \neq 2$ and $r = 3$ if $p = 2$. Let $a \in k^*/k^{*2}$ and $\varepsilon = \pm 1$. The set $H_a^\varepsilon = \{x \in k^*/k^{*2} | (x, a) = \varepsilon\}$ has 2^{r-1} elements if $a \neq 1$. If $a = 1$, then H_1^1 has size 2^r, and $H_1^{-1} = \emptyset$. Furthermore, if we have $a, b \in k^*/k^{*2}$ and $\varepsilon\ \varepsilon'$, and assume that both H_a^ε and $H_b^{\varepsilon'}$ are nonempty. Then, $H_a^\varepsilon \cap H_b^{\varepsilon'} =$ if and only if $a = b$ and $\varepsilon = \varepsilon'$.

Proof. If $a = 1$, this is a square, which means the Hilbert symbol is always 1. If $a \neq 1$, then since the Hilbert symbol is nondegenerate, we define a surjective homomorphism $b \mapsto (a, b)$. This implies that its kernel must have 2^{r-1} elements, and its kernel is H_a^1. Its complement H_a^{-1} in turn must have 2^{r-1} elements. If $a = b$ and $\varepsilon = -\varepsilon'$, then by definition $H_a^\varepsilon \cap H_b^{\varepsilon'} = \emptyset$. To prove the final part of this lemma, assume that $H_a^\varepsilon \cap H_b^{\varepsilon'} = \emptyset$, and both are nonempty. They must have 2^{r-1} elements. From this we can conclude that $H_a^1 = H_b^1$, which in turn is equivalent to $(x, a) = (x, b)$ for all x. By the nondegeneracy of the Hilbert symbol, we need $a = b$ and $\varepsilon = -\varepsilon'$. This proves the lemma. □

With both lemmas, we can continue the proof of Theorem 4.22.

Proof. Let $n = 4$. By Theorem 4.16, this is only possible if there are two forms that represent the same element. These two forms are equivalent to $ax^2 + by^2$ and $-a'z^2 - b'w^2$. Using Lemma 4.23, we know that such an element c is represented by these forms if and only if $(c, -ab) = (a, b)$ and $(c, -a'b') = (-a', -b')$. Denote the set of all elements c that satisfy the first equation with A. The set of all elements that satisfy the second equation is denoted by B. Both of these sets are nonempty. For example, $a \in A$ and $-a' \in B$. The quadratic form f does not represent zero if and only if $A \cap B =$. By Lemma 4.24, this is in turn equivalent to $ab = a'b'$ and $(a, b) = -(-a', -b')$. Because $ab = a'b'$, the discriminant is a square, so $d = 1$. If this is the case, then $\varepsilon = (a, b)(a, a')(a, b')(b, a')(b, b')(a', b')$. By bilinearity and part v) of Theorem 3.3, the invariant ε gets reduced to

$$
\begin{aligned}
&(a, b)(a', b')(a, a'b')(b, a'b') = \\
&(a, b)(a', b')(a, a'b')(b, a'b') = \\
&(a, b)(a', b')(ab, a'b') = \\
&(a, b)(a', b')(a'b', a'b') = \\
&(a, b)(a', b')(-1, a'b') = \\
&(a, b)(a', b')(-1, a')(-1, b') = \\
&(a, b)(-1, a')(-a', b') = \\
&(a, b)(-1, -1)(-a', -1)(-a', b') = \\
&(a, b)(-a', -b')(-1, -1).
\end{aligned}
$$

Using the condition $(a, b) = -(-a', -b')$, this finally reduces to $\varepsilon = -(-1, -1)$, which proves this case.
Let $n = 5$. By Lemmas 4.23 and 4.24, a form of rank 2 represents at least 2^{r-1} elements. This is also true for forms of higher ranks, by taking some entries of an input vector to be 0. Thus, f represents at least one other element besides d. Call this element a. Then, f is equivalent to a quadratic form $g \dot{+} az^2$. The form g is one rank lower than f. Its discriminant

is equal to $d/a \neq 1$. Because we have proven the previous case, g represents 0. Then by the way f is written (take $x = 0$), it also represents 0. The same procedure can be done for forms of higher ranks, which proves the theorem. □

Knowing when a form represents 0 is enough to find when it represents any a. This leads to the following corollary.

Theorem 4.25. If $a \in k^*/k^{*2}$, then a quadratic form f represents a if and only if:

$$\begin{aligned} &i)\ n = 1 \text{ and } d = a \\ &ii)\ n = 2 \text{ and } (a, -d) = \varepsilon \\ &iii)\ n = 3 \text{ and } d \neq a \text{ or } d = -a \text{ and } \varepsilon = (-1, -d) \\ &iv)\ n \geq 4 \end{aligned}$$

Here $d = d(f)$ and $\varepsilon = \varepsilon(f)$.

The proof of the second case of this theorem is given in Lemma 4.23. The proof of the other cases is analogous. Theorem 4.25 is of course quite powerful. It gives us specific conditions to show if any element a can be represented by a quadratic form. However, since $a \in k^*/k^{*2}$, we still do not know requirements for any element in the field. We also know that any form of rank greater than 5 in a field $\mathbb{Q}_p$ represents 0. The next theorem is useful for reducing the number of quadratic forms that need to be considered in a proof concerning all quadratic forms.

Theorem 4.26. For two quadratic forms to be equivalent, it is necessary and sufficient that they have the same rank, discriminant and invariant ε.

Proof. That two equivalent forms have the same invariants follows from the definitions of those invariants. The converse statement is proven by induction on the rank of the quadratic form. If $n = 0$, there is nothing to proof. By Theorem 4.25, two quadratic forms f and g with the same invariants represent the same elements in k^*/k^{*2}. Both can be written in the form $f' \dot{+} ax^2$ and $g' \dot{+} ax^2$, for some element a that they both represent. The forms f' and g' have one rank less. By the induction hypothesis, these are equivalent if they have the same invariants. Computations show that this is the case:

$$\begin{aligned} &d(f') = ad(f) = ad(g) = d(g') \\ &\varepsilon(f') = \varepsilon(f)(a, d(f')) = \varepsilon(g)(a, d(g') = \varepsilon(g'). \end{aligned}$$

All the invariants are the same, hence the forms f' and g' are equivalent. By induction, f and g are equivalent. □

Computing whether two forms are equivalent is now easy. We need to compute the invariants, instead of doing some complicated matrix computations.
Our work on quadratic forms over $\mathbb{Q}_p$ does not fully translate to quadratic forms over $\mathbb{R}$. In $\mathbb{R}$ every quadratic form is equivalent to $\sum_{i=1}^{r} x_i^2 - \sum_{j=1}^{s} y_j^2$. If either $s = 0$ or $r = 0$, then this form does not represent zero, since the form only sums positive or negative terms, hence never getting to 0 except when we set all variables to 0. If both r and s are nonzero, the quadratic form represents every element in $\mathbb{R}$. The invariants d and ε are also defined differently in $\mathbb{R}$.

Definition 4.27. The invariants ε and d are defined as follows:

$$\varepsilon(f) = (-1)^{s(s-1)/2}$$
and
$$d(f) = (-1)^s.$$

It can be proven that parts of Theorem 4.22 also hold for the real case. The first three requirements also work in the real case. The last condition definitely does not hold, since a real quadratic form with more than 4 variables can easily not represent a number. A counterexample would be the quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2$, which does not represent any nonnegative number. The next theorem covers a case where Theorem 4.22 does generalise to $\mathbb{R}$.

Theorem 4.28. A real quadratic form with 3 variables satisfying $(-1, -d) = \varepsilon$ represents 0.

Proof. We know that there are only four of these forms up to equivalence. A computation shows that $(-1, 1)_\infty = 1$ and $(-1, -1)_\infty = -1$.

$$\text{If } f = x^2 + y^2 + z^2,\ d(f) = 1,\ \varepsilon(f) = 1,$$
$$\text{if } f = x^2 + y^2 - z^2,\ d(f) = -1,\ \varepsilon(f) = 1,$$
$$\text{if } f = x^2 - y^2 - z^2,\ d(f) = 1,\ \varepsilon(f) = -1,$$
$$\text{if } f = -x^2 - y^2 - z^2,\ d(f) = -1,\ \varepsilon(f) = -1.$$

Indeed, the first and fourth forms do not represent zero, and they have that $(-1, -d) \neq \varepsilon$. The second and third do represent zero and they have that $(-1, -d) = \varepsilon$. □

5 Local-Global Principles

5.1 The Hasse-Minkowski theorem

With all of the groundwork laid down, we can begin to prove the Hasse-Minkowski theorem. The proof is taken from [7]. So far we have covered invariants and quadratic forms. If f is a quadratic form over $\mathbb{Q}$, then $f \sim a_1x_1^2 + a_2x_2^2 + \cdots + a_1x_n^2$. Let V be the set of all places, so $V = \{\infty, 2, 3, 5 \dots\}$. The invariants are defined as $d(f) = \prod_{i=1}^{n} a_i$ and with the injection $\mathbb{Q} \longrightarrow \mathbb{Q}_v$, f can be seen as a quadratic form over $\mathbb{Q}_v$, denoted by f_v. In these extended fields we define $d_v(f)$ and $\varepsilon_v(f)$. The invariants $d_v(f)$ are the image of $d(f)$ in $\mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$. The other invariant is defined as $\varepsilon_v(f) = \prod_{i<j}(a_i, a_j)_v$.

Theorem 5.1. A quadratic form f represents 0 in $\mathbb{Q}$ if and only it represents 0 in $\mathbb{Q}_v$ for all $v \in V$.

If a form represents 0 in $\mathbb{Q}$, then by the injection of $\mathbb{Q}$ into $\mathbb{Q}_v$, it also represents 0 in all of those fields. The other direction will have to be proven in multiple different cases, depending on the rank n of the quadratic form.

5.1.1 The case $n = 1$

Proof. The theorem only applies if the form f represents 0 in $\mathbb{R}$. In $\mathbb{R}$ the form can be seen as $f(x) = ax^2$, which never represents 0. The theorem is then vacuously true. □

In all other cases, f can be written as $\sum_{i=1}^{n} a_i x_i^2$. By dividing with a_1, we can also assume that $a_1 = 1$. From now on, also assume that the quadratic form f represents 0 in all of the fields $\mathbb{Q}_v$.

5.1.2 The case $n = 2$

Proof. Rewrite the form to $x_1^2 - a_2x_2^2$. The form f_∞ represents 0. This is only the case if $a_2 > 0$. This term can be written as $\prod_p p^{v_p(a_2)}$. Here v_p is the p-adic valuation defined in Definition 2.6. The forms f_p all represent 0. This must mean that a_2 is a square in $\mathbb{Q}_p$, which implies that $v_p(a_2)$ is even in all fields $\mathbb{Q}_p$. Therefore, a_2 is a product of squares, which is also a square. Hence, a_2 is a square in $\mathbb{Q}$. Take the input $(\sqrt{a_2}, 1)$. This shows that f represents 0 in $\mathbb{Q}$. □

5.1.3 The case $n = 3$

Proof. In this case, our quadratic form looks like $x_1^2 - ax_2^2 - bx_3^2$. By taking all square factors into the squares, we can assume that $v_p(a)$ and $v_p(b)$ are either 0 or 1 for all primes. Without loss of generality, assume that $|a| \leq |b|$. If this is not the case, simply flip a and b. The proof is done by induction on the integer $m = |a| + |b|$. The base case has $m = 2$. Then f can be one of four different forms: $x_1^2 \pm x_2^2 \pm x_3^2$. The form must represent 0 in $\mathbb{R}$, so we do not have to consider the case $x_1^2 + x_2^2 + x_3^2$. In all other cases, the form represents 0, either by the element $(1, 1, 0)$ or $(1, 0, 1)$. This proves the base case. For induction, assume that $m > 2$. Since $|a| \leq |b|$ and $|b| \geq 2$ the number b has a prime factorization. It is also square free, so $b = \pm p_1 p_2 \dots p_k$. Take a specific p_i. If $a \equiv 0 \bmod p$, then a is a square modulo p. If

$a \not\equiv 0 \bmod p$, then a is in U, the set of p-adic units. By assumption, f_{p_i} represents 0, so there is a triplet (x', y', z') with the property $(z')^2 - a(x')^2 - b(y')^2 = 0$. By Theorem 2.9, we can assume that this triplet is primitive. Therefore, $(z')^2 - a(x')^2 \equiv 0 \bmod p_i$. If $x' \equiv 0 \bmod p_i$, this reduces to $(z')^2 \equiv 0 \bmod p_i$, which implies that z would be divisible by p_i. Furthermore, $b(y')^2$ is then divisible by p_i^2, and because $v_{p_i}(b) = 1$, y is also divisible by p_i. This contradicts with the fact that (x', y', z') is primitive. So, we can assume that $x' \not\equiv 0 \bmod p_i$. We conclude that a is a square mod p, otherwise we can not have $(z')^2 - a(x')^2 \equiv 0 \bmod p_i$. By the structure theorem for finite abelian groups, we know that $\mathbb{Z}/b\mathbb{Z} = \prod_{j=1}^{k} \mathbb{Z}/p_j\mathbb{Z}$. Because we did not pick any particular p_i, we can assume that a is a square in all of the factors of $\mathbb{Z}/b\mathbb{Z}$, hence a square in $\mathbb{Z}/b\mathbb{Z}$ itself. There exist integers c and d such that $d^2 = a + bc$. This is the case because a and b are square free. In particular, choose d such that $|d| \leq |b|/2$. By rewriting the equation, we find that $bc = d^2 - a$. Both a and d^2 are squares. The value $d^2 - a$ is the norm of an element in $k(\sqrt{a})/k$. By the property $|bc| = |b||c|$, f represents 0 if and only if the form $g = x_1^2 - ax_2^2 - cx_3^2$ represents 0. Because f represents 0 in all $\mathbb{Q}_v$, so does g. Also note that $|c| = \left|\frac{d^2-a}{b}\right| \leq \frac{|b|}{4} + 1 < |b|$. The first inequality follows from the fact that $|d| \leq |b|/2$ and the second inequality follows from the fact that $|b| \geq 2$. Finally, write c as $c'u^2$, with c' square free. Then we can use the inductive hypothesis by noting that $|c'| < |b|$. This means that $h = x_1^2 - ax_2^2 - c'x_3^2$ represents 0 and is equivalent to g by taking the square of u out of x_3^2. So g represents 0, which was equivalent to f representing 0. This proves this case. □

5.1.4 The case $n = 4$

Proof. Without loss of generality, write $f = ax_1^2 + bx_2^2 - (cx_3^2 + dx_4^2)$. By Theorem 4.16 and the fact that f_v, represents 0, there exist elements $x_v \in \mathbb{Q}_v^*$ that are represented by both $ax_1^2 + bx_2^2$ and $cx_3^2 + dx_4^2$ (in $\mathbb{Q}_v$). By Theorem 4.25 that also works in $\mathbb{R}$ by the last results of Section 4, this is only true if both $(x_v, -ab)_v = (a, b)_v$ and $(x_v, cd)_v = (c, d)_v$. We use the product formula from Theorem 3.10, to find that $\prod_{v \in V}(a, b)_v = 1 = \prod_{v \in V}(c, d)_v$. Theorem 3.11 tells us there exists an $x \in \mathbb{Q}$ with the properties $(x, -ab)_v = (a, b)_v$ and $(x, -cd)_v = (c, d)_v$. Because of this, the form $ay^2 + bz^2 - xw^2$ represents zero in $\mathbb{Q}_v$ for all $v \in V$. We have proven the case where $n = 3$, so this implies that the form $ay^2 + bz^2 - xw^2$ represents 0 in $\mathbb{Q}$, which means that x is represented by $az^2 + by^2$. This reasoning can be applied to $cz^2 + dy^2$, to find that it also represents x in $\mathbb{Q}$. Both of the forms represent the same element, so the original form f represents 0 in $\mathbb{Q}$. This proves this case. □

5.1.5 The case $n \geq 5$

The final proof will be done by trying to reduce the rank of a quadratic form of rank 5 or greater to one of lower rank. Then the results follows from induction.

Proof. Take the form $f = h - g$ and split it into the forms $h = a_1x_1^2 + a_2x_2^2$ and $g = -(a_3x_3^2 + \cdots + a_nx_n^2)$. Take a subset S of V containing $2, \infty$ and the primes such that $v_p(a_i) \neq 0$ for some specific $i \geq 3$. By the way fractions work, this must be a finite set. For some $v \in S$ the form f_v represents 0, which by Theorem 4.16 is equivalent to having an element a_v that is represented by both h and g. The squares of $\mathbb{Q}_v^*$ are an open set. The Approximation Theorem 2.7 can be applied to find two rational numbers x', y' such that if $a = h(x', y')$, then $\frac{a}{a_v} \in \mathbb{Q}_v^{*2}$ for all $v \in S$. Also, if $v \in S$, the element a_v is represented by

g. Then by taking the square root of $\frac{a}{a_v}$ out of the form, g also represents a. Then the form $az^2 - g$ represents 0. If we do not have $v \in S$, then $-a_3, \ldots, -a_n$ are v-adic units by the definition of S. Their product is also a v-adic unit. This product is equal to the discriminant of g. Because $v \neq 2$, all of the v-adic units have Hilbert symbol equal to 1 by Theorem 3.12. By Theorem 4.22, g represents a, and so $az^2 - g$ represents a in $\mathbb{Q}_v$. This form is one rank less than f, so it represents 0 in $\mathbb{Q}$. That implies that g represents a in $\mathbb{Q}$. The other form h also represents a, and thus, f represents 0, which proves the final case. □

As discussed in Section 1, the Hasse-Minkowski theorem is an example of a local-global principle. These principles state that when there is a solution in all local fields, then there is a solution in the global field. In the case of the Hasse-Minkowski theorem, the $\mathbb{Q}_p$ and $\mathbb{R}$ are the local fields, and $\mathbb{Q}$ is the global field. The Hasse-Minkowski theorem can be generalized to finite extensions K of $\mathbb{Q}$.

5.2 Selmer's equation

On the other hand there are also situations where even though there are local solutions in all places, we can prove that there is no global solution. The first example that one might encounter is Selmer's equation.

Theorem 5.2. the cubic form $3x^3 + 4y^3 + 5z^3$ has solutions in $\mathbb{R}$ and all the $\mathbb{Q}_p$, but not in $\mathbb{Q}$.

The proof that there are local solutions will rely mostly on Hensel's lemma.

Proof. The fact that there is a nontrivial zero in $\mathbb{R}$ is clear. The point $(1, (4/3)^{1/3}, 0)$ is a solution. The proof of the existence of solutions in $\mathbb{Q}$ is split in three cases. The first case considers $p = 3$, the second case $p = 5$ and the last case covers the other primes. By applying Hensel's lemma we want to show that certain numbers are cubes in the p-adic numbers. Consider the 3-adic numbers. We need to find a solution to $3x^3 + 4y^3 + 5z^y = 0$ in $\mathbb{Q}_p$. Set $x = 0$ and $z = -1$. We have to find y such that $4y^3 - 5 = 0$, or equivalently $y^3 = \frac{5}{4}$. Considering this equation $\bmod 9$, we find $5{*}4^{-1} \equiv 5{*}7 \equiv -1 \bmod 9$. This is however not strong enough to use Hensel's lemma yet. For a solution y we want that $|f(y)|_3 \leq |f'(y)|_3^2$. So we want a y such that $|y^3 - \frac{5}{4}|_3 \leq \frac{1}{9}$. Therefore we consider the equation $\bmod 27$. We want a y such that $y^3 \equiv \frac{5}{4} \bmod 27$. In this group we take $y = 2$. By using Hensel's lemma to lift the solution to $\mathbb{Z}_p$, we conclude that $\frac{5}{4}$ is a 3-adic cube, and therefore there is a solution to Selmer's equation in $\mathbb{Q}_3$.
Assume that $p = 5$. Take $x = 1$ and $z = 0$ to reduce the equation to $3 + 4y^3 = 0$ or $y^3 = \frac{-3}{4}$. In $\mathbb{Z}/5\mathbb{Z}$ we see that $-\frac{3}{4} \equiv 2^3 \bmod 5$. By applying Hensel's lemma on $x^3 + \frac{3}{4}$ we can get a full solution in $\mathbb{Q}_5$.
With these two cases covered we can assume that both 3 and 5 are not congruent to $0 \bmod p$. If $p \equiv 1 \bmod 3$, then the subgroup of the cubes of $(\mathbb{Z}/p\mathbb{Z})^*$ has index 3. Otherwise, every element of the group is a cube. If 3 is a cube $\bmod p$, then by applying Hensel's lemma on $x^3 - 3$ we solve the equation with the solution $(x, 1, -1)$, where x has that $x^3 = \frac{1}{3}$. In the other case 3 is not a cube in $(\mathbb{Z}/p\mathbb{Z})^*$, which means there are more elements that are not cubes. Therefore, by our earlier observation, we have that $p \equiv 1 \bmod 3$. Every element in $(\mathbb{Z}/p\mathbb{Z})^*$ can be written as b^3, $3b^3$ or $9b^3$ for some b. This also applies to 5. If $5 \equiv b^3 \bmod p$,

we can just apply Hensel's lemma on $x^3 - 5$ to conclude that 5 is a cube, and therefore $(-y, y, -1)$ with $y^3 = 5$ is a solution. If $5 \equiv 3b^3 \mod p$, then $\frac{5}{3}$ is a cube and $(x, 0, -1)$ with $x^3 = \frac{5}{3}$ is the nontrivial solution. Lastly, assume that $5 \equiv 9b^3 \mod p$. Multiply both sides by 3 to get that $15 \equiv 27b^3 \equiv (3b)^3 \mod p$. By applying Hensel's lemma on $x^3 - 15$ we find that 15 is a cube. Take the point $(3t, 5, -7)$ with $t^3 = 15$. This solves Selmer's equation, and we can conclude that Selmer's equation has a solution in $\mathbb{Q}_p$ for all p. □

The proof that there are no solutions in $\mathbb{Q}$ is more involved, and uses theory that is beyond the scope of this thesis. A proof can be found in [1]. Similarly there are quartic forms that also do not have a global solution, even though they do have local solutions. The form $2z^2 = x^4 - 17y^4$ is an example of such a form [6].

References

[1] Keith Conrad, 2022. https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf.

[2] Timothy Curry. Quadratic and hilbert reciprocity, 2014.

[3] Yoshinosuke Hirakawa. Counterexamples to the local-global principle associated with swinnerton-dyer's cubic form, 2019.

[4] Heiko Knospe, 2022. http://www.nt.th-koeln.de/fachgebiete/mathe/knospe/p-adic/.

[5] Jürgen Neukirch. *Algebraic number theory*, volume Grundlehren der mathematischen Wissenschaften. Springer, 1999.

[6] Öncül Öztürün. Euler's trick and second 2-descents, 2005.

[7] Jean-Pierre Serre. *A course in arithmetic*. Springer, 1993.

[8] Geemen L.N.M. van, H.W. Lenstra, F. Oort, and J. Top. Advanced algebraic structures, 2021.