LOCAL-GLOBAL METHODS IN ALGEBRAIC NUMBER THEORY

ZACHARY KIRSCHE

ABSTRACT. This paper seeks to develop the key ideas behind some local-global methods in algebraic number theory. To this end, we first develop the theory of local fields associated to an algebraic number field. We then describe the Hilbert reciprocity law and show how it can be used to develop a proof of the classical Hasse-Minkowski theorem about quadratic forms over algebraic number fields. We also discuss the ramification theory of places and develop the theory of quaternion algebras to show how local-global methods can also be applied in this case.

CONTENTS

1. LOCAL FIELDS

In this section, we will develop the theory of local fields. We will first introduce local fields in the special case of algebraic number fields. This special case will be the main focus of the remainder of the paper, though at the end of this section we will include some remarks about more general global fields and connections to algebraic geometry.

1.1. **Absolute values and completions.**

Definition 1.1. Let K be a field. An *absolute value* or *multiplicative valuation* on K is a function $|\cdot| : K \to \mathbb{R}$ such that the following properties hold:

(1) For any $x \in K^\times$, $|x| > 0$. Additionally, $|0| = 0$.
(2) For all $x, y \in K$, $|xy| = |x| \cdot |y|$.
(3) *(Triangle Inequality)* For all $x, y \in K$, $|x + y| \leq |x| + |y|$.

If we further require that $|x + y| \leq \max\{|x|, |y|\}$, we then say that $|\cdot|$ is a *non-archimedean* absolute value. This inequality is referred to as the *ultrametric inequality*.

We will give a few examples of absolute values:

Example 1.2. The standard Euclidean norm on $\mathbb{Q}$ gives an absolute value. We will denote this absolute value by $|\cdot|_\infty$, for reasons which will become clear soon.

Example 1.3. Let $p \in \mathbb{Z}$ be a prime. For $x \in \mathbb{Q}$ we define $\nu_p(x) = \operatorname{ord}_p(x)$, where we define $\operatorname{ord}_p(x)$ for integers x to be the largest integer n such that $p^n \mid x$ and extend it to $\mathbb{Q}$ by $\operatorname{ord}_p\left(\frac{x}{y}\right) = \operatorname{ord}_p(x) - \operatorname{ord}_p(y)$ for integers x and y. This is almost an absolute value, but it is a homomorphism from the additive group of $\mathbb{Q}$ to the multiplicative group of $\mathbb{Z}$. To flip this into an absolute value, we define $|x|_p = p^{-\nu_p(x)}$. This is called the *p-adic absolute value* on $\mathbb{Q}$ and is an example of a non-archimedean absolute value.

Example 1.4. Let $K/\mathbb{Q}$ be an algebraic number field and let $\sigma : K \to \mathbb{C}$ be a complex embedding. We then define, for $x \in K$, $|x| = |\sigma x|_{\mathbb{C}}$, where $|\cdot|_{\mathbb{C}}$ is the standard Euclidean norm on $\mathbb{C}$.

Remark 1.5. The terminology "non-archimedean" derives from the fact that the Archimedean Property fails to hold with respect to the given absolute value. We recall that the Archimedean Property of $\mathbb{R}$ states that, for $\alpha, \beta \in \mathbb{R}$, there is a positive integer $n \in \mathbb{N}$ such that $|n\alpha| > |\beta|$. However, if the absolute value $|\cdot|$ is non-archimedean, we may repeatedly apply the ultrametric inequality to see that $|n\alpha| \leq |\alpha|$ for any positive integer n, so the Archimedean Property fails to hold.

The main importance of studying these absolute values lies in studying the *completions* of various fields with respect to these absolute values. We briefly sketch the construction of the completion here:

Construction 1.6. Let $(K, |\cdot|)$ be a field with an associated absolute value. We define the completion $\hat{K}$ as follows: the objects consist of equivalence classes of Cauchy sequences $\{a_n\}$ in K, where two such sequences $\{a_n\}$ and $\{b_n\}$ are equivalent if $\lim_{n\to\infty} |a_n - b_n| = 0$. We can then define an absolute value on $\hat{K}$ by $|\{a_n\} - \{b_n\}| = \lim_{n\to\infty} |a_n - b_n|$. It is important to note that $\hat{K}$ is a field and $|\cdot|$ is an absolute value on this field as defined above.

This construction is most commonly used to construct the real numbers from $\mathbb{Q}$ by completing with respect to the Euclidean norm. However, as we have been looking at all the possible absolute values on $\mathbb{Q}$, we are also interested in looking at all possible completions of $\mathbb{Q}$. To this end, we define here another class of completions of $\mathbb{Q}$:

Definition 1.7. Let $p \in \mathbb{Z}$ be a prime. Define the field of *p-adic numbers* $\mathbb{Q}_p$ to be the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

We will further develop some properties of the p-adic numbers in later sections. For now, we will focus on the problem of classifying all possible completions of an algebraic number field.

1.2. **Classifying absolute values.** We note that an absolute value on K trivially gives rise to a metric on K by $d(x, y) = |x - y|$. This allows us to study the field K as a topological space with the induced metric topology. We define an equivalence relation on absolute values by $|\cdot|_1 \sim |\cdot|_2$ if and only if they induce the same topology on K. It is immediately apparent that two absolute values induce the same completion if and only if they are equivalent.

With these definitions, one question that immediately comes up is one of classifying absolute values on a field K up to equivalence. This problem is identical to the problem of identifying all possible completions of K. This problem was first studied in the case of the field $\mathbb{Q}$, resulting in the following theorem due to Alexander Ostrowski:

Theorem 1.8. (Ostrowski) *Let $|\cdot|$ be an absolute value on $\mathbb{Q}$. Then $|\cdot|$ is equivalent to one of the following:*

1. *The standard Euclidean absolute value $|\cdot|_\infty$.*
2. *The p-adic absolute value $|\cdot|_p$ for some prime p.*

In particular, this implies that the only possible completions of $\mathbb{Q}$ are the real numbers $\mathbb{R}$ and the p-adic numbers $\mathbb{Q}_p$ for each prime p. The proof of this theorem is somewhat technical and unenlightening, so for a full proof see [6].

We next consider the case of general algebraic number fields. We recall that, unlike in the case of the rational integers, we do not generally have unique factorization into prime elements in rings of integers $\mathcal{O}_K$ for number fields, but rather we get unique factorization of ideals into prime ideals. Thus, a result similar to Ostrowski's theorem will hold, but with prime ideals instead of prime elements.

Theorem 1.9. *Let $K/\mathbb{Q}$ be an algebraic number field and $\mathcal{O}_K$ its ring of integers. Then there is exactly one equivalence class of absolute values on K corresponding to each of the following:*

1. *Each prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$, given by $|x|_\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|^{-\operatorname{ord}_\mathfrak{p}(x)}$. (We recall that $\operatorname{ord}_\mathfrak{p}(x)$ is defined for elements $x \in \mathcal{O}_K$ as the largest integer n such that $x \in \mathfrak{p}^n$, and we define it for the entire number field as before by noting that K is the field of fractions of $\mathcal{O}_K$.)*
2. *Each real embedding $\sigma : K \to \mathbb{R}$, given by $|x| = |\sigma x|_\mathbb{R}$.*
3. *Each conjugate pair of complex embeddings $\sigma : K \to \mathbb{C}$, given by $|x| = |\sigma x|_\mathbb{C}$.*

We will discuss how to arrive at this result from Ostrowski's theorem near the end of the paper. Motivated by this result, we can give the following definitions:

Definition 1.10. Let $K/\mathbb{Q}$ be a number field. An equivalence class of absolute values on K is called a *place* or a *prime* of K. If this equivalence class corresponds to a prime ideal, it is called a *finite place*. If instead it corresponds to a real or complex embedding of K, it is instead called an *infinite place*. The *local fields* of K are precisely the completions of K with respect to each place.

Notation 1.11. Given a field K, we will denote its set of places by V. Given a place $v \in V$, we will denote the completion of K with respect to v by K_v.

In what sense these fields are "local" and why they are important will be the main focus of the remainder of this paper.

Remark 1.12. It is possible to define local fields axiomatically; they are characterized primarily as fields which are complete and locally compact with respect to some absolute value. For the purpose of this paper, however, the above definition is more than sufficient.

1.3. **Global fields.** In this section, we will briefly discuss how we might generalize the theory of local fields to fields which are not algebraic number fields. As it turns out, the theory of local fields applies equally well to the case of function fields of certain algebraic curves. Though the remainder of this paper will focus exclusively on the case of algebraic number fields, it is nevertheless important to explore the more general theory of global fields. To this end, we give a definition:

Definition 1.13. A *global field* is either one of the following:

(1) An algebraic number field $K/\mathbb{Q}$.
(2) The function field of an algebraic curve over a finite field.

Note that function fields of algebraic curves over finite fields are precisely finite extensions of $\mathbb{F}_q(x)$ for some q. In order to illustrate the connection between the different types of global fields, we first give a lemma:

Lemma 1.14. *Let $|\cdot|$ be an absolute value on some field K and let T be the image of the natural map $\mathbb{Z} \to K$. Then $|\cdot|$ is non-archimedean if and only if the set of values $S = \{|m| : m \in T\}$ is bounded.*

Proof. If $|\cdot|$ is non-archimedean, then, for $m > 0$ we have $|m| = |1+1+\ldots+1| \leq |1|$. Similarly, $|-m| = |m|$, so the set S is clearly bounded by $|1| = 1$. For the converse, suppose that S is bounded. For any $x, y \in K$ and $0 \leq r \leq n$, we have $|x|^r|y|^{n-r} \leq \max\{|x|^n, |y|^n\} = (\max\{|x|, |y|\})^n$. We also have that there is some N such that $\binom{n}{r} \leq N$. We then have:

$$\begin{aligned} |x+y|^n &= \left|\sum_{r=0}^{n} \binom{n}{r} x^r y^{n-r}\right| \\ &\leq (n+1)N \max\{|x|, |y|\}^n \end{aligned}$$

Taking the n-th root and sending $n \to \infty$ yields the ultrametric inequality, so $|\cdot|$ is non-archimedean, as claimed.

□

We then obtain a useful corollary:

Corollary 1.15. *Let K be a field with $\mathrm{ch}(K) \neq 0$. Then any absolute value on K is non-archimedean.*

Thus, we may use an almost identical method to prove the following theorem about the completions of global fields:

Theorem 1.16. *Let K be the function field of an algebraic curve C over a finite field $\mathbb{F}_q$, let $\mathcal{O}_P$ be the local ring at a point $P \in C$ and let $\mathfrak{m}_P$ be its maximal ideal. Then the absolute values on K are in one-to-one correspondence with the points $P \in C$, with the correspondence given by $|f|_P = |\mathcal{O}_P/\mathfrak{m}_P|^{-\operatorname{ord}_P(f)}$.*

Thus, we obtain exactly one absolute value for each point on the curve. Furthermore, what we have actually done in both this case and in the case of algebraic number fields is construct exactly one local field for each non-trivial *discrete valuation ring* contained in the field K. For a more thorough discussion of this case and its connections to algebraic geometry and the theory of schemes, see [3] I.13-14.

2. The p-adic numbers

2.1. **The Chevalley-Warning theorem.** While not a statement directly about the p-adic numbers, the Chevalley-Warning theorem in conjunction with another result called Hensel's lemma is one of the most useful tools for solving polynomial equations over the p-adics.

Theorem 2.1. (Chevalley-Warning) *Let $q = p^m$ for some prime p and let $\{f_\alpha\}$ be a finite collection of polynomials in $\mathbb{F}_q[x_1, \ldots, x_n]$ such that $\sum_\alpha \deg(f_\alpha) < n$. Let $Z \subseteq \mathbb{F}_q^n$ be the set of common zeroes of the f_α. Then $|Z| \equiv 0 \pmod p$, where $|Z|$ denotes the cardinality of Z.*

To prove this, we will use the following lemma:

Lemma 2.2. *Let $u > 0$ be an integer. Then:*

$$\sum_{x \in \mathbb{F}_q} x^u = \begin{cases} -1 & u \equiv 0 \pmod{q-1} \\ 0 & \text{otherwise} \end{cases}$$

Proof. First, we note that, if $u \equiv 0 \pmod{q-1}$, we have by Fermat's Little Theorem that $x^u = 1$ for $x \neq 0$. Thus, we have that $\sum x^u = -1$. For $x \not\equiv 0 \pmod{q-1}$, we recall that the group $\mathbb{F}_q^\times$ is cyclic. This means that there is an element $y \in \mathbb{F}_q^\times$ such that $y^u \neq 1$. Such an element must have the property that $\sum x^u = \sum (xy)^u = y^u \sum x^u$. This implies that the sum must be 0, as claimed. □

With this lemma, we can now proceed to prove the Chevalley-Warning theorem:

Proof. Let $\{f_\alpha\}$ be as in the statement of the theorem. We then define a polynomial $P(x_1, \ldots, x_n) = \prod_\alpha (1 - f_\alpha^{q-1})$. Let $x \in \mathbb{F}_q^n$. Then, if $x \in Z$, we have that $f_\alpha(x) = 0$ for all α, implying that $P(x) = 1$. If $x \notin Z$, there is an α such that $f_\alpha(x) \neq 0$. Then, by Fermat's Little Theorem, we conclude that $f_\alpha(x)^{q-1} = 1$, implying that $P(x) = 0$. Thus, we have that $P(x) = \mathbf{1}_Z(x)$, the indicator function for the set Z.

Next, we define $S(f) = \sum_{x \in \mathbb{F}_q^n} f(x)$. Then the above discussion implies that $|Z| \equiv S(P) \pmod p$. Next, by the hypothesis that $\sum_\alpha \deg(f_\alpha) < n$, we note that $\deg(P) < n(q-1)$. This means that P is an $\mathbb{F}_q$-linear combination of monomials $x_1^{e_1} \cdots x_n^{e_n}$ with $\sum e_i < n(q-1)$. In particular, we note that at least one of the e_i must be strictly less than $q-1$. Then, by fixing all other variables and summing over the variable x_i, we see by the previous lemma that the sum must be 0. Thus, we conclude that $S(P) = 0$, and thus the theorem holds. □

One important corollary to this theorem is a result that is often referred to as Chevalley's theorem:

Corollary 2.3. (Chevalley) *Let $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ with $\deg(f) < n$. Then if f has no constant term, it must have a non-trivial zero.*

Proof. This follows immediately from the Chevalley-Warning theorem applied to a single polynomial. We conclude that $|Z| \equiv 0 \pmod{p}$ for some $p \geq 2$, but we also know that $0 \in Z$. Thus, there must be at least one other element of Z, proving the corollary.

□

To end the section, we give an example of the Chevalley-Warning theorem in action. We will revisit this example several times throughout the paper, showing how the various techniques discussed allow us to make non-trivial statements about the polynomial.

Example 2.4. Define the polynomial $f(x) = 5x^2 + 7y^2 - 13z^2$ over $\mathbb{Z}$. We note that f must have a nontrivial solution modulo p for any prime p by Chevalley's theorem.

2.2. **The p-adic integers.** One important object in the study of the algebraic properties of the p-adic numbers is the ring of p-adic integers $\mathbb{Z}_p$. We give here the definition:

Definition 2.5. The ring of *p-adic integers* $\mathbb{Z}_p$ is the ring of elements $x \in \mathbb{Q}_p$ such that $|x|_p \leq 1$.

Remark 2.6. We note that the function ν_p which we defined earlier on $\mathbb{Q}$ also extends to $\mathbb{Q}_p$ and still takes on only integer values. The reason for this is that the possible values of $|\cdot|_p$ on $\mathbb{Q}$ form a discrete set, so its extension to $\mathbb{Q}_p$ must also only take on those values, allowing us to define ν_p for all elements of $\mathbb{Q}_p$. With this in mind, we can also characterize $\mathbb{Z}_p$ as those elements with $\nu_p(x) \geq 0$. In particular, the relation $|x|_p = p^{-\nu_p(x)}$ still holds.

With this in mind, we make the following observation:

Proposition 2.7. *An element $u \in \mathbb{Z}_p$ is a unit if and only if it is not divisible by p - that is, $\nu_p(u) = 0$.*

Proof. This follows almost immediately if we consider that every element $u \in \mathbb{Q}_p$ has an inverse. Thus, u is a unit in $\mathbb{Z}_p$ if and only if $|u|_p, |u^{-1}|_p \leq 1$. However, the valuation $|\cdot|_p$ is multiplicative, so both have to be precisely equal to 1, thus proving the result.

□

This observation along with the previous remark about extending ν_p to all of $\mathbb{Q}_p$ leads to the following important corollary:

Corollary 2.8. *Any element $x \in \mathbb{Z}_p$ can be written as $x = p^n u$ for some integer $n \geq 0$ and some unit $u \in \mathbb{Z}_p$. Furthermore, any element $x \in \mathbb{Q}_p$ can be written as $x = p^n u$ for u a unit in $\mathbb{Z}_p$ and $n \in \mathbb{Z}$.*

Another consequence of this result is that the field of p-adic numbers $\mathbb{Q}_p$ is actually the field of fractions of $\mathbb{Z}_p$. In fact, it is possible to construct the p-adic numbers (and, more generally, completions of number fields with respect to finite places) by first constructing the p-adic integers and then constructing the p-adic numbers as its field of fractions. This construction is a special case of the *completion* of a ring:

Construction 2.9. Let K be an algebraic number field and let $\mathcal{O}_K$ be its ring of integers. Let $\mathfrak{p} \subset \mathcal{O}_K$ be a prime ideal. Then we define $A_n = \mathcal{O}_K/\mathfrak{p}^n$. There is a canonical sequence of maps $\varphi_n : A_n \to A_{n-1}$. These give rise to a projective system, so we define the inverse limit $A = \lim_{\leftarrow} A_n$. We then define $K_\mathfrak{p}$ to be the field of fractions of A.

In the example of $\mathbb{Q}_p$, the ring A is the ring $\mathbb{Z}_p$. Elements of A are sequences $(\ldots, a_3, a_2, a_1)$ with the property that $\varphi_n(a_n) = a_{n-1}$. We can think of this as some element a with $a_n \equiv a \pmod{\mathfrak{p}^n}$. This intuition will be extremely helpful in the next section, where we will show how to lift solutions to polynomial equations from A_{n-1} to A_n and, under certain conditions, to solutions in A.

2.3. **Hensel's lemma.** One question which will be of particular interest in this paper is that of finding zeroes of polynomials over local fields. For this, the main result we will be using is what is known as Hensel's lemma. We give here the statement in the particular case of $\mathbb{Z}_p$:

Lemma 2.10. (Hensel's Lemma) *Let $f \in \mathbb{Z}_p[x]$ be a polynomial. Suppose that there exists an element $x \in \mathbb{Z}_p$ such that $f(x) \equiv 0 \pmod{p^n}$ and $f'(x) \not\equiv 0 \pmod{p}$. Let $m \leq n$. Then there exists an element $y \in \mathbb{Z}_p$ such that $f(y) \equiv 0 \pmod{p^{m+n}}$ and $x \equiv y \pmod{p^n}$.*

Proof. By Taylor's theorem, we have that for any $z \in \mathbb{Z}_p$, $f(x + p^n z) = f(x) + p^n z f'(x) + p^{2n} b$ for some $b \in \mathbb{Z}_p$. Note that, modulo p^{m+n} we have $f(x + p^n z) \equiv f(x) + p^n z f'(x)$ because $m+n \leq 2n$. Next, noting that $f(x) = p^n k$ for some $k \in \mathbb{Z}_p$, we have that $p^{-n} f(x + p^n z) \equiv k + z f'(x) \pmod{p^m}$. Thus, we have a non-trivial linear equation, so we may always find a z such that $k + z f'(x) \equiv 0 \pmod{p^m}$. We then conclude that $f(x + p^n z) \equiv 0 \pmod{p^{m+n}}$, so this is our desired lift. □

We note that this exact result holds with identical proof in the more general case of non-archimedean completions of an algebraic number field. That is, if we have a solution modulo $\mathfrak{p}^n$ for some prime ideal $\mathfrak{p}$ and the derivative at that point does not lie in $\mathfrak{p}$, then we can lift to a solution modulo $\mathfrak{p}^{m+n}$.

By far the most important consequence of this fact for the purpose of this paper is the following corollary:

Corollary 2.11. *Let f be as above. Suppose that there exists an element $x \in \mathbb{Z}_p$ such that $f(x) \equiv 0 \pmod{p}$ and $f'(x) \not\equiv 0 \pmod{p}$. Then there exists an element $y \in \mathbb{Z}_p$ such that $f(y) = 0$.*

The idea behind this corollary is simple: we simply continue to apply Hensel's lemma to get a solution modulo p^n for each n. In the end, this corresponds precisely to an element of the inverse limit described above, so it is actually a zero of the p-adic polynomial. We return to the previously discussed example to illustrate the power of this result:

Example 2.12. Let $f(x, y, z) = 5x^2 + 7y^2 - 13z^2$. We claim that this has a p-adic solution for each prime p. First, suppose $p \neq 2, 5, 7, 13$. Then by Chevalley-Warning we know that there exists a non-trivial solution (x_0, y_0, z_0) modulo p. Without loss of generality suppose $x_0 \neq 0$. We then define $g(x) = 5x^2 + 7y_0^2 - 13z_0^2$. We know that this has a solution x_0 with $g(x_0) \equiv 0 \pmod{p}$. Further, we know that

$g'(x_0) = 10x_0 \not\equiv 0 \pmod{p}$. (This is simply because we know $p \nmid 10$.) Thus, by Hensel's lemma, this lifts to a solution in $\mathbb{Z}_p$, as claimed.

For the special case where $p = 2, 5, 7, 13$, we can also apply Hensel's lemma. However, we have no way of guaranteeing that the solution from Chevalley-Warning satisfies that $g'(x) \not\equiv 0 \pmod{p}$. Thus, in each of these cases we must find a solution modulo p explicitly, but the proof from there is entirely identical.

In the next section, we will show how we can lift these "local" zeroes of a polynomial into a "global" zero - that is, a rational zero of the polynomial $f(x, y, z)$.

3. The Hasse-Minkowski theorem

The Hasse-Minkowski theorem is a first example of what are referred to as *local-global principles*. This term is applied to results which allow us to discern information about a global field by looking at this information over a local field. To this end, we will first introduce the Hilbert symbol and the Hilbert reciprocity law. We will then give some preliminary information about quadratic forms in order to give a statement of the Hasse-Minkowski theorem for algebraic number fields. Finally, we will give a complete proof of this theorem.

3.1. The Hilbert symbol.

We will begin by giving a definition of the Hilbert symbol.

Definition 3.1. Let K be a field and let $a, b \in K^\times$. Define the *Hilbert symbol* (a, b) as $+1$ if there is a non-trivial triple $(x, y, z) \in K^3$ such that $z^2 - ax^2 - by^2 = 0$. Otherwise we let $(a, b) = -1$. If K is a global field and v is a place of K, we define $(a, b)_v$ as the Hilbert symbol over K_v.

We list a few basic properties of the Hilbert symbol:

Proposition 3.2. *Let $a, b, c \in K^\times$. Then:*

(1) $(a, b) = (b, a)$.
(2) $(a, c^2) = +1$.
(3) $(a, -a) = (a, 1 - a) = +1$.
(4) $(aa', b) = (a, b)(a', b)$.
(5) $(a, b) = (a, -ab) = (a, (1 - a)b)$.

The proofs of these facts follow almost immediately from the definition of the Hilbert symbol. The main result about the Hilbert symbol, which will be useful in several proofs throughout the remainder of this paper, is the Hilbert reciprocity law:

Theorem 3.3. (Hilbert reciprocity) *Let K be an algebraic number field and let V be its set of places. Let $a, b \in K$. Then $(a, b)_v = +1$ for all but finitely many places $v \in V$ and:*

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

In other words, the number of places $v \in V$ for which $(a, b)_v = -1$ is a finite, even number. The proof of this result for general algebraic number fields requires some facts from class field theory and is beyond the scope of this paper. We note that a proof for the specific case of $K = \mathbb{Q}$ exists through direct computation of the Hilbert symbols over the p-adic fields. For this proof, see [4].

3.2. **The Hasse-Minkowski theorem.** In this section, we will be dealing with quadratic forms over algebraic number fields. For the purposes of this paper, a quadratic form over K is a degree 2 homogeneous polynomial $f \in K[x_1, \ldots, x_n]$. Such a form is said to *represent* 0 if there exists a non-zero element $x \in K^n$ such that $f(x) = 0$.

Theorem 3.4. (Hasse-Minkowksi) *Let K be an algebraic number field and let f be a quadratic form over K. Then f represents 0 over K if and only if it represents 0 over K_v for all places $v \in V$.*

Proof. The necessity of this condition is obvious - if f has a nontrivial zero in K^n, it trivially has that exact same solution in K_v^n. Thus, it remains only to prove sufficiency. We first note that by a linear change of variables we may assume that $f(x) = \sum a_i x_i^2$. We may further suppose that $a_1 = 1$ by scaling appropriately. We will now consider some cases on the number of variables. For $n = 1$, the result is trivial, as $f(x) = x^2$ does not represent 0 over any field.

Case 1. $n = 2$. The proof for this case relies on results about the ramification theory of places, so we will prove this case in a later section.

Case 2. $n = 3$. This case is equivalent to a difficult theorem called the *Hasse norm theorem*. We will discuss a little about this theorem at the end of the paper, but the proof essentially is as follows: we first note that the form $f(x) = x^2 - by^2 - cz^2$ represents 0 if and only if the element c is the norm of an element in the extension $K(\sqrt{b})$. We then invoke the Hasse norm theorem, which tells us that an element is a norm in $K(\sqrt{b})$ if and only if it is a norm in $K_v(\sqrt{b})$ for all places $v \in V$. This immediately establishes this case.

Case 3. $n = 4$. We will show that this case can be reduced to the previous case. To this end, we make the following claim: the form $f(x, y, z, t) = x^2 - by^2 - cz^2 + act^2$ represents 0 if and only if the form $g(x, y, z) = x^2 - by^2 - cz^2$ represents 0 in $K(\sqrt{ab})$. For an outline of the proof of this claim, see ([8], 358). This result is then equivalent to the previous result.

Case 4. $n \geq 5$. We will establish the remaining case via induction. Given a form f in at least 5 variables, we may write $f(x) = ax_1^2 + bx_2^2 - g(x_3, x_4, \ldots, x_n)$. In particular we note that g has at least 3 variables. We next claim that g represents 0 in K_v for all but finitely many places v. This is because the form $x^2 - by^2 - cz^2$ represents 0 if and only if the Hilbert symbol $(b, c)_v$ is equal to $+1$, and by Hilbert reciprocity this is true for all but finitely many places. This means that there exist elements $\alpha_1, \alpha_2 \in K$ such that $c = a\alpha_1^2 + b\alpha_2^2 \neq 0$ is represented by g_v in all but finitely many places. Thus the form $h(y, x_3, \ldots, x_n) = cy^2 - g(x_3, \ldots, x_n)$ represents 0 in all places. By the inductive hypothesis this implies that h represents 0, so in particular we conclude that g also represents 0. This establishes the final case, so the theorem is proven.

□

3.3. **Applications and further results.** We return to the example of a polynomial that we have been revisiting throughout this paper to see how the Hasse-Minkowski theorem can be used in tandem with the Chevalley-Warning theorem and Hensel's lemma to make non-trivial statements about quadratic forms over $\mathbb{Q}$:

Example 3.5. As before, let $f(x, y, z) = 5x^2 + 7y^2 - 13z^2$. We saw before that this has zeroes in $\mathbb{Q}_p$ for any p. Furthermore, this trivially has a zero over $\mathbb{R}$. Thus, by Hasse-Minkowski, we conclude that this has a non-trivial zero over $\mathbb{Q}$. Note

that this does not tell us what such a zero might look like, though explicit testing reveals that $(3, 1, 2)$ is one such zero.

In general, the problem of finding rational zeroes of forms is of great interest. Thus, we would like to generalize the Hasse-Minkowski theorem to forms of higher degree. Unfortunately, one property of the Hasse-Minkowski theorem is that it only holds in general for the case of quadratic forms.

There are some results which move toward generalizing to higher power forms, but they are generally difficult to prove and nowhere near as powerful. For example, the Hasse-Minkowski theorem is known to not hold in general for cubic forms because the form $f(x, y, z) = 3x^3 + 4y^3 + 5z^3$ represents 0 in all local fields of $\mathbb{Q}$ but does not have a rational zero. A theorem of Hooley in [1] states that an analogous result to Hasse-Minkowski does hold for non-singular cubic forms over $\mathbb{Q}$ in at least 9 variables. This is not, however, as powerful as it seems because, as proven by Heath-Brown in [2], every non-singular cubic form over $\mathbb{Q}$ in at least 10 variables represents 0, so Hooley's result is only non-trivial in exactly 9 variables. There are also slight generalizations of Hasse-Minkowski to simultaneous zeroes of systems of forms, but once again they are nowhere near as general. Additionally, in both cases described above, the proofs of these facts are significantly more difficult and rely on powerful results in analytic number theory.

4. Other local-global principles

While the Hasse-Minkowski theorem is one of the most famous examples of a local-global principle, there are countless others throughout algebraic number theory. In this section, we will first explore the ramification theory of places and use this to establish a result about squares in local fields. We will then discuss the theory of quaternion algebras and show how global quaternion algebras are determined entirely by local quaternion algebras.

4.1. The ramification theory of places.

In algebraic number theory, one of the most useful early concepts is to discuss to what extent prime ideals in an algebraic number field split, ramify, or remain inert in certain extensions of that number field. Keeping with the idea of places as a notion of primality, we can ask similar questions about places and apply these ideas in novel ways. We begin with a definition:

Definition 4.1. Let L/K be a field extension. Let $|\cdot|_v$ be an absolute value on K and let $|\cdot|_w$ be an absolute value on L. We say that w *divides* v if $|\cdot|_w$ restricts to $|\cdot|_v$ on K.

The motivation for this terminology should be immediately clear: when speaking of prime ideals in the case of number fields, we say that a prime ideal $\mathfrak{q} \subseteq L$ divides a prime ideal $\mathfrak{p} \subseteq K$ if $\mathfrak{q}$ is contained in the unique factorization of $\mathfrak{p}$ into prime ideals in L. An analogous result holds for archimedean places. In order to prove it, we will need the following lemma:

Lemma 4.2. *Let $(K, |\cdot|)$ be a complete field such that $|\cdot|$ is non-archimedean and L/K a finite separable extension. Then there is exactly one absolute value on L dividing $|\cdot|$ and L is complete with respect to this absolute value.*

We will be proving a slightly weaker form of this lemma, which instead posits that there exists *at most* one such absolute value. This weakened version is much simpler to prove and is sufficient for our applications.

Proof. Consider L as a finite dimensional vector space over K. Then any absolute value on L is also a vector space norm. Thus, it suffices to show that all vector space norms are equivalent for finite dimensional vector spaces over a complete valued field. This is true for any complete topological vector space, so we conclude that there is always at most one extension of $|\cdot|$ to L, as desired.

□

Proposition 4.3. *Let K be an algebraic number field and let $|\cdot|_v$ be ann absolute value on K. Let $L = K(\alpha)$ be a finite separable extension such that the minimal polynomial of α is f. Then the places w of L dividing v are in natural one-to-one correspondence with the irreducible factors of f over K_v.*

Proof. Let w be a place dividing v. We then consider the completion L_w of L with respect to this absolute value. We note that L_w is an extension of K_v which is complete, finite, and contains L, so in particular we conclude that it must be equal to $K_v(\alpha)$. Thus, let g be the minimal polynomial of α over K_v. We then have that, because $f(\alpha) = 0$, we must also have $g \mid f$. Thus, to each place w dividing v, we may associate an irreducible factor of f in K_v. To see that this is unique, consider instead an irreducible factor g of f over K_v. Let $K_v' = K_v[x]/(g)$. This is an extension of the complete field K_v, so it must be unique and thus equal to the one described above.

□

We note that this theorem allows for places of L to divide a place v of K with multiplicity.

This correspondence is the key to proving the main classification result described earlier about the places of a number field. Given an algebraic number field $K/\mathbb{Q}$, we can use this result along with Ostrowski's theorem classifying the places on $\mathbb{Q}$ to see exactly what the places on K are. Suppose $K = \mathbb{Q}(\alpha)$ and f is the minimal polynomial of α over $\mathbb{Q}$. Then over $\mathbb{R}$ we see that f has one irreducible factor for each of its real roots and each conjugate pair of complex roots. These correspond to real and complex embeddings of K (which are the maps sending α to each of the roots of its minimal polynomials), so this confirms part of our classification theorem. Suppose instead that we are looking at the p-adic absolute value on $\mathbb{Q}$. Then we need to instead look at the factorization of f over $\mathbb{Q}_p$.

As in the case of prime ideals, the theory of extending places becomes especially interesting when we consider collectively all of the places dividing a given place v. Let L/K be a finite separable extension of an algebraic number field K and let v be a place of K. If there is exactly one place w dividing v and it has multiplicity 1 in the sense described above, we say that v *remains inert* in L. If there exists a place w dividing v with multiplicity greater than 1, we say that v *ramifies* in L. If there are multiple distinct places dividing v, we say that v *splits* in L. If v splits and does not ramify, we say it *totally splits*. We give some examples:

Example 4.4. Let $K = \mathbb{Q}(\sqrt{d})$ for some square-free $d > 0$. We will consider how the places of $\mathbb{Q}$ behave in this extension. We note that the question of how the finite places behave is identical to asking how the ideal (p) factors in K. This is a simple exercise in algebraic number theory. The interesting case is understanding how the Euclidean norm behaves in this extension. We see that the field K has two distinct real embeddings, sending $\sqrt{d} \mapsto \pm\sqrt{d}$. Thus, we conclude that the Euclidean norm splits in this extension.

Suppose instead that $d < 0$. In this case, the embeddings described above are a conjugate pair of complex embeddings, so they only give us one place. Thus, we conclude that the Euclidean norm remains inert in this extension.

The analogy between the ramification theory of ideals and of places can be pushed even one step farther. This can be most succinctly described by the following result:

Theorem 4.5. *Let K be a field and v a place of K. Let L/K be a finite separable extension. Then there are finitely many places $w_1, \dots, w_g$ of L dividing v and the following relation holds:*

$$L \otimes_K K_v \simeq \prod_{i=1}^{g} L_{w_i}$$

Proof. That there are finitely many places dividing v follows immediately from the previous proposition. The product formula also follows fairly easily. Let $L = K(\alpha)$ with minimal polynomial f as before. We then have:

$$\begin{aligned} L \otimes_K K_v &\simeq K[x]/(f) \otimes_K K_v \\ &\simeq K_v[\alpha]/(f) \\ &\simeq \prod K_v[\alpha]/(f_i) \\ &\simeq \prod L_{w_i} \end{aligned}$$

as desired.

□

To conclude this section, we will prove the case of Hasse-Minkowski for quadratic forms in two variables. In order to prove this, we will need the following lemma, whose proof is behind the scope of this paper:

Lemma 4.6. *Let K be a field and $L = K(\sqrt{d})$ for some square-free $d \in K$. Then there are infinitely many places of K which do not split completely in L.*

For a proof of this fact, see [8], VIII.8.8. This fact, along with the product formula described above, will be all we need to prove Hasse-Minkowski in two variables. We first recall that this result is equivalent to the statement that an element of K is a square if and only if it is a square in K_v for all places v. One implication is trivial, so suppose that $d \in K$ is not a square. Then we consider the field $L = K(\sqrt{d})$. We then note that, because there are infinitely many places which do not split and there are only finitely many infinite places, there must be a finite place v which does not split. Further, it is a fact that only finitely many places may ramify in any extension. Thus, there must be a finite place which remains inert in L. This immediately implies that d is not a square in K_v, thus establishing this case of the Hasse-Minkowski theorem.

4.2. **Quaternion algebras.** One last example of a local-global principle which we will discuss is related to the theory of *quaternion algebras*. We give first the definition:

Definition 4.7. Let F be a field. A *quaternion algebra* over F is an F-algebra A with basis $\{1, i, j, ij\}$ such that there exist elements $a, b \in F^\times$ satisfying $i^2 = a$, $j^2 = b$, and $ij = -ji$. We will denote this quaternion algebra by $\left(\frac{a,b}{F}\right)$.

The familiar quaternions are then $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$. We will give a few more examples:

Example 4.8. We claim that the matrix ring $M_2(F)$ is isomorphic to $\left(\frac{1,1}{F}\right)$ for any field F. This amounts to choosing matrices i and j which square to the identity and generate the entire algebra. One such choice is the following:

$$i = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$j = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

It can fairly easily be shown that, if $F = \bar{F}$ is algebraically closed, then up to isomorphism this is the only quaternion algebra over F.

This last remark about quaternion algebras over algebraically closed fields actually gets at something more important: that questions about classifying quaternion algebras up to isomorphism are actually questions about squares in the base field. We can make this observation concrete by noting some basic properties of quaternion algebras:

Proposition 4.9. *Let F be any field, $a, b \in F^\times$.*

(1) $\left(\frac{a,b}{F}\right) \simeq \left(\frac{a,-ab}{F}\right) \simeq \left(\frac{b,-ab}{F}\right)$.

(2) For any $u, v \in F^\times$, we have $\left(\frac{a,b}{F}\right) \simeq \left(\frac{au^2,bv^2}{F}\right)$.

Both of these facts follow immediately from the definitions. The second fact is essential to understanding why quaternion algebras will follow some sort of local-global principle.

Suppose that our base field K is actually an algebraic number field. Let A be a quaternion algebra over K. Then, for each place v of K, we can define $A_v = A \otimes_K K_v$. We say that A is *ramified* at v if A_v is a division ring. (For a discussion on why this terminology is used, see [7].) We will denote the set of places where A is ramified by $\mathrm{Ram}(A)$. Then the main classification result is the following theorem:

Theorem 4.10. *Let A and B be quaternion algebras over an algebraic number field K. Then $A \simeq B$ if and only if $\mathrm{Ram}(A) = \mathrm{Ram}(B)$ if and only if $A_v \simeq B_v$ for all places v of K.*

Thus, as with other local-global principles seen throughout the paper, we can entirely discern the global behavior of a quaternion algebra by looking at its behavior in each of the local fields.

Acknowledgments. I would like to thank my mentor, Eric Stubley, for helping me with almost every aspect of this project. His help was invaluable at every step of the process of writing this paper. I would also like to thank Professor Peter May and everyone else involved in the University of Chicago REU program for allowing me to participate in this experience.

References

[1] C. Hooley. *On nonary cubic forms.* Journal für die reine und angewandte Mathematik. 386: 32-98. 1988.

[2] D.R. Heath-Brown. *Cubic forms in ten variables.* Proceedings of the London Mathematical Society. 47: 225-257. 1983.
[3] J. Neukirch. Algebraic Number Theory. Springer-Verlag. 1999.
[4] J.-P. Serre. A Course in Arithmetic. Springer-Verlag. 1973.
[5] J.-P. Serre. Local Fields. Springer-Verlag. 1979.
[6] J. S. Milne. Algebraic Number Theory. http://www.jmilne.org/math/CourseNotes/ANT.pdf.
[7] J. Voight. The arithmetic of quaternion algebras. https://math.dartmouth.edu/ jvoight/crmquat/book/quat-modforms-041310.pdf.
[8] J. W. S. Cassels and A. Frölich. Algebraic Number Theory. Academic Press. 1967.
[9] R. Sridharan. *On the theorem of Hasse-Minkowski.* http://www.bprim.org/cyclotomicfieldbook/sri.pdf.