The Hasse Principle for Quadratic Forms

Krishanu Sankar

October 17, 2014

In this (minor) thesis, we explore the Hasse local-global principle for quadratic forms over a global field. Sections I, II, and III take us through the proof of the theorem. Section I begins by developing the necessary theory of quaternion algebras, and how they can be used to classify quadratic spaces, all over a general field. Section II restricts our attention to local fields, exploring the structure of quaternion algebras over them, and thereby the structure of norms of quadratic extensions. Here, we specialize some of the ideas of local class field theory. Section III studies global fields, generalizing the ideas of Section II by using the idele group $\mathcal{J}_K$. This section is much more technical! But the results are worth it. We primarily follow [8], but another treatment is given in [6], and a shorter, simpler proof is given in [9]. [4] is cited as a reference to learn about the class field theory, if one wants.

In Sections IV and V, we see the Hasse principle actually fails for the intersection of two quadric surfaces in $\mathbf{P}^3$, or a cubic over $\mathbf{P}^2$. In Section IV, we very concretely treat the example of the intersection of two quadric surfaces, following [1]. In Section V, we explore Selmer's cubic, but opt for a more theoretical approach. Without completely rigorous proofs, we discuss ways to measure how *badly* the Hasse principle fails for abelian varieties when it does fail, using the language of Galois cohomology. We use elliptic curves (the simplest nontrivial case) as an example, following ideas from [3] and [7], and referencing [10]. Another source is [11].

Finally, in the last section (the conclusion), we briefly mention the Hasse principle for *algebraic groups*. One can read more in [2] and [5].

Contents

1 General Fields

1.1 Quadratic Spaces - A brief review

We will briefly recall some definitions. Let k denote an arbitrary field that is not of characteristic 2. A *quadratic space* over k is a finite-dimensional vector space V equipped with a function $q : V \to k$ such that $B(x,y) = \frac{q(x+y)-q(x)-q(y)}{2}$ is a bilinear form. We call (V,q) *nondegenerate* if this bilinear form is nondegenerate, and we call (V,q) *isotropic* if there is some $x \in V$ such that $q(x) = 0$ (we then say x is isotropic). It is also well-known that any finite-dimensional vector space with a symmetric bilinear form has an orthogonal basis.

If (V,q) is a nondegenerate space, and the matrix of the bilinear form in some basis is M, then we may compute $\det(M)$. Of course, if we change our basis according to some matrix P, then the matrix of the bilinear form becomes PMP^T, which has determinant $\det(M)\det(P)^2$. We thus define the *discriminant*, denoted dV, to be the well-defined element of $k^\times/(k^\times)^2$ defined by this determinant.

1.2 Quaternion Algebras

Suppose $\alpha, \beta \in k^\times$. We can define a 4-dimensional algebra over k with basis $\{1, x_1, x_2, x_3)$ such that the following relations hold

$$x_1^2 = \alpha \qquad x_2^2 = \beta \qquad x_3^2 = -\alpha\beta \qquad x_1x_2 = -x_2x_1 = x_3$$

$$x_2x_3 = -x_3x_2 = -\beta x_1 \qquad x_3x_1 = -x_1x_3 = -\alpha x_2$$

Such an algebra is denoted $\langle \alpha, \beta \rangle_k$, and is called the *quaternion algebra* defined by α and β. For example,

- If $\alpha = \beta = -1$, then we get the traditional quaternions.
- If $\alpha = 1, \beta = -1$, then our relations are satisfied by the algebra $M_2(k)$, with the generators

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad x_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad x_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad x_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

It is easy to check that a quaternion algebra has center k and is simple, so by Wedderburn's Theorem on central simple algebras, it is either $M_2(k)$, or is a division algebra. As $\langle\alpha,\beta\rangle_k$ is central simple, we might ask what the reduced norm and reduced trace are. These can be defined explicitly as follows. We can define *conjugates* in $\langle\alpha,\beta\rangle_k$ by

$$\overline{a_0 + a_1x_1 + a_2x_2 + a_3x_3} = a_0 - a_1x_1 - a_2x_2 - a_3x_3$$

and let $N(x) = x\overline{x}, T(x) = x + \overline{x}$. Thus,

$$N(a_0 + a_1x_1 + a_2x_2 + a_3x_3) = a_0^2 - \alpha a_1^2 - \beta a_2^2 + \alpha\beta a_3^2$$

$$T(a_0 + a_1x_1 + a_2x_2 + a_3x_3) = 2a_0$$

In fact, the underlying vector space of the algebra, along with the map N, give it the structure of a quadratic space. The underlying bilinear form, $B(x,y) = \frac{x\overline{y}+y\overline{x}}{2}$, is nondegenerate, with orthogonal basis $1, x_1, x_2, x_3$.

Proposition 1.1. *The following five conditions are equivalent:*

1. $\langle\alpha,\beta\rangle_k \simeq \langle 1,-1\rangle_k$.
2. $\langle\alpha,\beta\rangle_k$ *is not a division algebra.*
3. $\langle\alpha,\beta\rangle_k$ *is isotropic.*
4. *The span of* x_1, x_2, x_3 *within* $\langle\alpha,\beta\rangle_k$ *is isotropic.*
5. $\alpha \in N(k(\sqrt{\beta}))$.

Proof. 1. (1) $\implies$ (2) is obvious because $\langle 1,-1\rangle_k$ is $M_2(k)$.

2. Suppose (2) is true, and that $x \neq 0$ does not have an inverse. If $Nx \neq 0$, then because $N(x^2) = (Nx)^2$, we have x has the inverse $\frac{x\overline{x^2}}{(Nx)^2}$. Hence, $Nx = 0$, and x is our isotropic vector.

3. Suppose (3) is true, and that $N(a_0 + a_1x_1 + a_2x_2 + a_3x_3) = 0$, where $a_0 \neq 0$. After appropriate scaling, we may take $a_0 = 1$. Then $N(a_1x_1 + a_2x_2 + a_3x_3) = -1$. Since $k\{x_1, x_2, x_3\}$ has discriminant $(-\alpha)(-\beta)(\alpha\beta) = 1$ in $k^\times/(k^\times)^2$, the orthogonal complement of $a_1x_1 + a_2x_2 + a_3x_3$ is a 2-dimensional space with discriminant -1. Therefore, it is spanned by two orthogonal vectors v, w such that $Nv = -Nw$, and is isotropic, implying (4).

4. Suppose (4) is true, and $-\alpha a_1^2 - \beta a_2^2 + \alpha\beta a_3^2 = 0$. Then, multiplying by $\alpha\beta$ and rearranging, $\beta(\alpha a_1)^2 + \alpha(\beta a_2)^2 = (\alpha\beta a_3)^2$. Hence, $\alpha = \left(\frac{\alpha a_3}{a_2}\right)^2 - \left(\frac{\alpha a_1}{\beta a_2}\right)^2 \beta$, and so $\alpha \in N(k(\sqrt{\beta}))$.

5. Suppose (5) is true. Then we can construct a quadratic space with basis x_1, x_2, x_3 and with $q(x_1) = -\alpha, q(x_2) = -\beta, q(x_3) = \alpha\beta$, and it is isotropic. If we let x be the isotropic vector, then x defines a nonzero element of $\langle \alpha, \beta \rangle_k$ with norm 0, which is thus non-invertible. Then Wedderburn's theorem tells us that $\langle \alpha, \beta \rangle_k \simeq M_2(k) \simeq \langle 1, -1 \rangle_k$. □

Proposition 1.2. *The following four conditions hold.*

1. $\langle 1, \alpha \rangle_k \simeq \langle 1, -1 \rangle_k \simeq \langle \alpha, -\alpha, \rangle_k \simeq \langle \alpha, 1-\alpha, \rangle_k \simeq M_2(k)$
2. $\langle \alpha, \beta \rangle_k \simeq \langle \beta, \alpha \rangle_k \simeq \langle \alpha\lambda^2, \beta\mu^2 \rangle_k$
3. $\langle \alpha, \alpha\beta \rangle_k \simeq \langle \alpha, -\beta \rangle_k$
4. $\langle \alpha, \beta \rangle_k \otimes_k \langle \alpha, \gamma \rangle_k \simeq \langle \alpha, \beta\gamma \rangle_k \otimes_k \langle 1, -1 \rangle_k$

Proof. (1) is easy to check using the previous proposition. (2) is obvious. (3) is obvious by switching the roles of x_2 and x_3. (4) takes slightly more work, but we can exhibit an explicit isomorphism. Suppose $\langle \alpha, \beta \rangle_k$ has basis $1, x_1, x_2, x_3$ and $\langle \alpha, \gamma \rangle_k$ has basis $1, y_1, y_2, y_3$. Then in the tensor product, the span of $\{1 \otimes 1, x_1 \otimes 1, x_2 \otimes y_2, x_3 \otimes y_2\}$ yields a quaternion algebra isomorphic to $\langle \alpha, \beta\gamma \rangle_k$, while the span of $\{1 \otimes 1, 1 \otimes y_2, x_1 \otimes y_3, -\gamma x_1 \otimes y_1\}$ yields a quaternion algebra isomorphic to $\langle \gamma, -\alpha^2\gamma \rangle_k \simeq \langle 1, -1 \rangle_k$. It is not hard to check that the product of these two quaternion algebras gives the tensor product, so this proves (4). □

In light of (4) of the last proposition, let us say that two central simple k-algebras A and A' are *similar* (denoted $A \sim A'$) if $A \simeq M_n(D), A' \simeq M_{n'}(D)$ for some division algebra D and positive integers n, n'. Then because $D \otimes_k M_2(k) \simeq M_2(D)$, we see that (4) of the last proposition tells us that

$$\langle \alpha, \beta \rangle_k \otimes_k \langle \alpha, \gamma \rangle_k \sim \langle \alpha, \beta\gamma \rangle_k$$

In other words,

Corollary 1.3. *$\langle -, - \rangle_k$ is a symmetric, bilinear form on $k^\times/(k^\times)^2$ which takes values in the similarity classes of central simple k-algebras (with tensor product).*

1.3 The Hasse Algebra and Classification of Quadratic Forms

Let $V \simeq \langle \alpha_1 \rangle \perp \cdots \perp \langle \alpha_n \rangle$ be an n-dimensional quadratic space, where this notation means V has an orthogonal basis $x_1, \ldots, x_n$ with $q(x_i) = \alpha_i$. Then define the *Hasse algebra*

$$SV \simeq \bigotimes_{i \leq j} \langle \alpha_i, \alpha_j \rangle_k$$

We first need to check that this algebra is well-defined up to similarity. This is done by proving two lemmas:

Lemma 1.4. *Let $\mathcal{B} = \{x_1, \ldots, x_n\}$ and $\mathcal{B} = \{y_1, \ldots, y_n\}$ be two orthogonal bases for (V, q). Then there is a finite chain of orthogonal bases*

$$\mathcal{B}_0 \to \mathcal{B}_1 \to \cdots \to \mathcal{B}$$

where each $\mathcal{B}_i$ is obtained from $\mathcal{B}_{i-1}$ by altering only two basis vectors.

Proof. The proof of this statement is by induction on n. The case of $n = 2$ is trivial. For the inductive step, it suffices to show that we can get from $\mathcal{B}_0$ to a basis with one vector equal to y_1. If $y_1 = \alpha_1 x_1 + \cdots + \alpha_p x_p$ for some p, then we can perform a change of basis involving just x_1 and x_p so that now y_1 can be expressed only using $x_1, \ldots, x_{p-1}$. Another inductive argument shows that we can, after a sequence of $p - 1$ changes, get $x_1 = y_1$. □

Lemma 1.5. *Any transformation of orthogonal bases $\mathcal{B} \to \mathcal{B}'$ which changes only two vectors does not change the Hasse algebra.*

Proof. If x_1, x_2 are orthogonal, and $q(x_i) = \alpha_i$, then any linear transformation on these two which preserves orthogonality must have the form

$$x_1 \mapsto x_1' = ax_1 + bx_2 \qquad x_2 \mapsto x_2' = cx_1 - \frac{ac}{b}\frac{\alpha_1}{\alpha_2}x_2$$

Then

$$\alpha_1' := q(x_1') = a^2\alpha_1 + b^2\alpha_2$$

$$\alpha_2' := q(x_2') = c^2\alpha_1 + \frac{a^2c^2}{b^2}\frac{\alpha_1^2}{\alpha_2^2}\alpha_2 \equiv \alpha_1\alpha_2(a^2\alpha_1 + b^2\alpha_2) \pmod{(k^\times)^2}$$

It then obviously follows that, for any d

$$\langle d, \alpha_1'\alpha_2' \rangle_k = \langle d, \alpha_1\alpha_2 \rangle_k$$

Let $c = a^2\alpha_1 + b^2\alpha_2$. Then it suffices to just check

$$\langle \alpha_1, \alpha_1\rangle_k \langle \alpha_1, \alpha_2\rangle_k \langle \alpha_2, \alpha_2\rangle_k \simeq \langle c, c\alpha_1\alpha_2\rangle_k \langle c, c\rangle_k \langle c\alpha_1\alpha_2, c\alpha_1\alpha_2\rangle_k$$

Using bilinearity, and the fact that the (tensor) square of any of these quaternion algebras is trivial, we can cancel out terms to find that we must show

$$\langle \alpha_1, \alpha_2\rangle_k \simeq \langle c, c\alpha_1\alpha_2\rangle_k$$

These two quaternion algebras are isomorphic by an appropriate linear transformation on the pair (x_1, x_2). □

Now that we know the Hasse algebra is well-defined, we use it to classify quadratic spaces.

Theorem 1.6. *Let V, W be nondegenerate n-dimensional quadratic spaces with $1 \leq n \leq 3$. Then V and W are isometric if and only if $dV = dW$ and $SV \sim SW$.*

Proof. We only need to prove these conditions are sufficient to show they are isometric. The $n = 1$ case is trivial. Next, let's consider $n = 3$. If $dV = \alpha$, then consider the quadratic space $(V, \alpha q)$, denoted V'. A simple calculation shows that $dV' = \alpha^4 \equiv 1$, and $SV' \sim SV$. So we can scale both V and W to have discriminant 1. Then we have splittings

$$V \simeq \langle -\alpha\rangle \perp \langle -\beta\rangle \perp \langle \alpha\beta\rangle$$

$$W \simeq \langle -\gamma\rangle \perp \langle -\delta\rangle \perp \langle \gamma\delta\rangle$$

Simply expanding these out, using the fact that $\langle \alpha, \alpha\rangle_k \simeq \langle -1, \alpha\rangle_k$, we find that the first is isomorphic to $\langle \alpha, \beta\rangle_k \otimes \langle -1, -1\rangle_k$, and the second to $\langle \gamma, \delta\rangle_k \otimes \langle -1, -1\rangle_k$. Hence, $\langle \alpha, \beta\rangle_k \simeq \langle \gamma, \delta\rangle_k$, and V and W are just the parts of these algebras orthogonal to 1, so they are isometric. The $n = 2$ case holds by comparing $V \perp \langle 1\rangle$ and $W \perp \langle 1\rangle$, and noting they are isometric by the $n = 3$ case. □

Corollary 1.7. *Let k be a field with the property that every nondegenerate 5-dimensional quadratic space over it is isotropic. Then two nondegenerate quadratic spaces V, W of the same dimension are isometric if and only if $dV = dW$ and $SV \sim SW$.*

Proof. Let n be the dimension. For $n \leq 3$, this follows from the previous theorem. If $n \geq 4$, then $V \perp \langle -1\rangle$ is isotropic by assumption, so V represents 1, and can thus be written in the form $V \simeq V' \perp \langle 1\rangle$. Similarly, $W \simeq W' \perp \langle 1\rangle$. We can easily check that $dV' = dW'$ and $SV' \sim SW'$, so by an inductive argument on n, $V \simeq W$. □

Over some fields, these invariants are enough to fully characterize a quadratic space up to isometry, even for $n \geq 4$, but this is not generally true: for example, consider $k = \mathbb{R}$, $n = 4$, and the quadratic spaces defined by $x_1^2 + x_2^2 + x_3^2 + x_4^2$ and $-x_1^2 - x_2^2 - x_3^2 - x_4^2$.

2 Local Fields

2.1 Preliminaries and definitions

Definition 2.1. *A* **non-archimedean local field** k *is a field that is complete with respect to a discrete valuation, and whose residue field is finite.*

The prototypical example of a local field is a completion of $\mathbb{Q}$ with respect to the p-adic norm, for some prime p (this takes a rational number x and returns $p^{-\nu_p(x)}$, where $\nu_p(x)$ is the power of p in the prime factorization of x). This yields $\mathbb{Q}_p$, the p-adics. This same procedure can be done for any finite extension of $\mathbb{Q}$ to yield a finite extension of some $\mathbb{Q}_p$.

We shall completely classify isomorphism classes of quadratic spaces over non-archimedean local fields, and answer the question of when a quadratic space is isotropic. This will require a study of squares and quadratic extensions, and in the process we shall prove the following well-known result of local class field theory:

Proposition 2.2. *If L is a quadratic extension of a local field k, then $k^\times / N_{L/k} L^\times$ is a group of order 2.*

Let us establish some notation. If $(k, |\cdot|_v)$ is a non-archimedean local field, let $\mathcal{O}_k$ denote the ring of elements with norm less than or equal to 1. Then $\mathcal{O}_k$ is a discrete valuation ring with maximal ideal $\mathfrak{p}$ which is generated by a *uniformizer* π (so $\mathfrak{p} = (\pi)$). The residue field $\mathcal{O}_k / \mathfrak{p}\mathcal{O}_k$ is finite of some characteristic p, so normalize the absolute value such that $|\pi|_v = 1/p$, and similarly define a discrete valuation ord on k such that $\mathrm{ord}(x) = -\log_p(|x|_v)$. (Note that (π^n) is the fractional ideal of elements with order greater than n, so because $\mathcal{O}_k$ is complete, it is isomorphic to $\lim\limits_{\leftarrow} \mathcal{O}_k / \mathfrak{p}^n \mathcal{O}_k$, and so is *profinite*.)

Suppose that L/k is an extension of degree n. Then recall L is local as well, the valuation uniquely extends to L, and so we can define $\mathcal{O}_L$ and $\mathfrak{B} \subset \mathcal{O}_L$ generated by a uniformizer β. $\mathcal{O}_k / \mathfrak{p} \to \mathcal{O}_L / \mathfrak{B}$ is injective, and so is also a field extension, of some degree f. Also, $\mathfrak{p}$ is generated by some power of the uniformizer β - let this power be β^e. It is then easy to see that $\mathcal{O}_L/\mathfrak{p}\mathcal{O}_L$ is ef-dimensional as a vector space over $\mathcal{O}_k/\mathfrak{p}\mathcal{O}_k$. We can then see $\mathcal{O}_L/\mathfrak{p}^m\mathcal{O}_L$ is ef-dimensional as a free module over $\mathcal{O}_k/\mathfrak{p}^m\mathcal{O}_k$, and by taking an inverse limit, we see that $n = ef$. e is called the *ramification degree* of the extension: it accounts for how the valuation changes (for example, in the valuation of β, the uniformizer π has order e). f is called the *residue degree* for obvious reasons.

We will call a local field k *dyadic* if its residue field $\mathcal{O}_k/\mathfrak{p}\mathcal{O}_k$ has characteristic 2, and *non-dyadic* otherwise. In the next two sections, we will prove that over a local field k, there are only two quaternion algebras, up to isomorphism. For this statement, we will treat the non-dyadic case and the dyadic case separately.

2.2 Quaternion Algebras: the Non-dyadic case

Let $\mathcal{O} = \mathcal{O}_k$, and let $\tilde{k} = \mathcal{O}/\mathfrak{p}\mathcal{O}$ be the residue field. In this subsection, we will prove the following theorem.

Theorem 2.3. *Let k be a non-dyadic local field, and let $\Delta \in \mathcal{O}_k^\times$ be a quadratic nonresidue. Then $\langle \pi, \Delta \rangle_k$ is a division algebra, and every quaternion algebra over k is isomorphic to either this division algebra, or to $\langle 1, -1 \rangle_k \simeq M_2(k)$. In particular, there are only two quaternion algebras, up to isomorphism.*

(*Note:* This implies that, for any nontrivial extension L of k, $NL^\times$ is an index 2 subgroup of $k^\times$. More generally, it is true that if L/k is any finite Galois extension, then

$$k^\times/NL^\times \simeq \mathrm{Gal}(L/k)^{\mathrm{ab}}$$

This is a key result of local class field theory!)

First, we prove some simple lemmas about lifting.

Lemma 2.4. *If $x \in \mathcal{O}^\times$ is a square in $\tilde{k}^\times$, then it's a square in $\mathcal{O}^\times$.*

Proof. It is sufficient to show that if x is a square mod π^n, then it is a square mod π^{n+1}: the result will then follow by induction and the fact that $\mathcal{O}^\times$ is profinite. This is a simple lifting argument:

$$x \equiv (a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1})^2 + d\pi^n \pmod{\pi^{n+1}}$$

$$x \equiv (a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + \frac{d}{2a_0}\pi^n)^2 \pmod{\pi^{n+1}}$$

□

Corollary 2.5. *The group $(\mathcal{O}^\times)^2 \subset \mathcal{O}^\times$ is a subgroup of index* 2.

This is obvious, because this holds for the squares in the residue field.

Corollary 2.6. *If $\alpha, \beta \in \mathcal{O}^\times$, then $\langle \alpha, \beta \rangle_k \simeq \langle 1, -1 \rangle_k$.*

Proof. First, we show that $\alpha x^2 + \beta y^2 = z^2$ has a solution in $\tilde{k}$. If β is a quadratic residue, we are done, so assume it is a quadratic nonresidue. Fix $z = 1$. We want to show that $f(x) = \frac{1-\alpha x^2}{\beta}$ is a square for at least one nonzero x. It is well known that the multiplicative group of $\tilde{k}$ is cyclic of order $q-1$, so if $f(x)$ is a nonsquare for every $x \in \tilde{k}$, then $f(x)^{\frac{q-1}{2}} + 1 = 0$ has q roots. But this polynomial is of degree $q-1$: hence, at least one $x \in \tilde{k}^\times$ is not a root. (0 is automatically a root, as $\beta^{-\frac{q-1}{2}} = -1$, because β is a quadratic nonresidue.)

Now pick a solution (x, y) to $\alpha x^2 + \beta y^2 = 1$ in $\tilde{k}$, and lift x to an arbitrary element of $\mathcal{O}$. Then since $\frac{1-\alpha x^2}{\beta}$ is a square in $\tilde{k}$, it is a square in k, as desired. □

Proof of the Theorem: Let us consider the quaternion algebra $\langle \alpha\pi^e, \beta\pi^f \rangle_k$, where $\alpha, \beta \in \mathcal{O}^\times$. Using the bilinearity of this symbol, we find that

$$\langle \alpha\pi^e, \beta\pi^f \rangle_k \sim \langle \alpha, \beta \rangle_k \otimes \langle \alpha, \pi^f \rangle_k \otimes \langle \pi^e, (-1)^f \beta \rangle_k \otimes \langle \pi^e, (-\pi)^f \rangle_k$$

Because $\langle \pi, -\pi \rangle_k \sim 1$ and $\langle \alpha, \beta \rangle_k \sim 1$, we see that any quaternion algebra is similar to a tensor power of $\langle \pi, \Delta \rangle_k$. Now it only remains to show that this is a nontrivial quaternion algebra. It is equivalent to show that there is no solution to $\pi\alpha^2 + \Delta\beta^2 = 1$ in $k^\times$.

Suppose that there is such a solution. It is obvious, by looking at powers of π, that $\beta \in \mathcal{O}^\times$, and then it is clear that $\alpha \in \mathcal{O}^\times$ as well. Let us look at both sides of the equation modulo $\mathfrak{p} = (\pi)$. The left side is then Δ times a square, which is then a nonsquare, but the right side is 1, which is a square! We then get a contradiction, and so there was no solution. Hence, by Proposition 1.1, $\langle \pi, \Delta \rangle_k$ is a nontrivial quaternion algebra. ■

Denote the trivial quaternion algebra by **1**, and the nontrivial one by $-\mathbf{1}$. We have shown that $\langle \gamma, \Delta \rangle_k \simeq \mathbf{1}$ for any quadratic nonresidues γ, Δ,

$\langle \pi, \Delta \rangle \simeq -\mathbf{1}$, and $\langle \pi, \pi \rangle_k \simeq \langle \pi, -1 \rangle_k$ which is $\pm\mathbf{1}$ depending on whether the characteristic of $\tilde{k}$ is $\pm 1 \pmod 4$. This explicitly tells us the structure of the map $\langle -, - \rangle_k$ on $k^\times/(k^\times)^2 \times k^\times/(k^\times)^2$.

2.3 Quaternion Algebras: The Dyadic case

In the dyadic case, the structure of the squares is a more complicated, and so the calculation is more involved. First, we must make a definition.

Definition 2.7. *Let $\xi \in k^\times$. Define $\mathfrak{d}(\xi)$, the* **quadratic defect** *of ξ, to be the largest power $\mathfrak{p}^d$ of the maximal ideal such that ξ is a quadratic residue mod $\mathfrak{p}^d$.*

The theorem we seek to prove is almost the same:

Theorem 2.8. *Let k be a dyadic local field, and let $\Delta \in \mathcal{O}_k^\times$ have quadratic defect $4\mathcal{O}$. Then $\langle \pi, \Delta \rangle_k$ is a division algebra, and every quaternion algebra over k arising from a tensor product of algebras of the form $\langle \alpha, \beta \rangle_k$ is isomorphic to either this division algebra, or to $\langle 1, -1 \rangle_k \simeq M_2(k)$. In particular, there are only two quaternion algebras, up to isomorphism.*

In the non-dyadic case, if ξ was a square mod $\mathfrak{p}$, then it was automatically a square, so the quadratic defect was always either 0 or $\mathcal{O}$. But in the dyadic case, there are many more possibilities. For example, with $\mathbb{Q}_2$, where $\mathfrak{p} = (2)$, we can have quadratic defect $(1), (2)$, or (4) (and then, if $\xi \in \mathbb{Z}_2^\times$ is a square mod 8, it is a square, so no other quadratic defects are possible).

Proposition 2.9. *$\mathfrak{d}(\epsilon)$ is one of the ideals*

$$0 \subset 4\mathcal{O} \subset 4\mathfrak{p}^{-1} \subset 4\mathfrak{p}^{-3} \subset 4\mathfrak{p}^{-5} \subset \cdots \subset \mathfrak{p}^3 \subset \mathfrak{p}$$

That is, if we have $\mathfrak{p}^e = (2)$ (which holds for some e), then $\mathfrak{d}(\epsilon)$ can be one of the ideals $\mathfrak{p}, \mathfrak{p}^3, \ldots, \mathfrak{p}^{2e-1}, \mathfrak{p}^{2e}, 0$.

Proof. Suppose $\mathfrak{d}(\epsilon) \subseteq \mathfrak{p}^{2e+1}$. Then, after multiplying by an appropriate square, ϵ can be written in the form $1 + 4\pi\alpha$, for some $\alpha \in \mathcal{O}$. We can then solve the equation $1 + 4\pi\alpha = (1 + 2\pi\beta)^2$: we find it is equivalent to solving $\alpha = \beta + \pi\beta^2$. If $\alpha = \sum\limits_{i=0}^{\infty} \alpha_i \pi^i$ and $\beta = \sum\limits_{i=0}^{\infty} \beta_i \pi^i$, where each $\alpha_i, \beta_i \in \mathcal{O}$, we can easily solve for the β_i's inductively. Hence, $\mathfrak{d}(\epsilon) = 0$.

It then only remains to consider ϵ with $\mathfrak{d}(\epsilon) = \mathfrak{p}^d$ for $1 \leq d \leq 2e - 1$ (the case $d = 0$ happens for a nonsquare, and the case $d = 2e$ happens for the number 5). We must prove that d has to be odd; equivalently, we must show that if ϵ is a square mod $\mathfrak{p}^{2r}$, then it is a square mod $\mathfrak{p}^{2r+1}$. By scaling by an appropriate square, we may assume $\epsilon = 1+\epsilon_1\pi^{2r}$ i.e., that is it 1 (mod $\mathfrak{p}^{2r}$). The residue field $\tilde{k}$ is a finite extension of $\mathbf{F}_2$, and so its multiplicative group is of odd order: hence, every element of $\tilde{k}$ is a square. Hence, there is some δ_1 such that $\delta_1^2 \equiv \epsilon_1 \pmod{\pi}$ But

$$1+\epsilon_1\pi^{2r} \equiv 1+\delta_1^2\pi^{2r} \equiv (1+\delta_1\pi^r)^2 \pmod{\pi^{2r+1}}$$

because $2\pi^r \equiv 0 \pmod{\pi^{2r+1}}$. This completes the proof. □

Proposition 2.10. *$k^\times/(k^\times)^2 \simeq (\mathbb{Z}/2)^{n+2}$, where n is the degree of k as an extension over $\mathbb{Q}_2$.*

Proof. It is clearly equivalent to show that $\mathcal{O}^\times/(\mathcal{O}^\times)^2 \simeq (\mathbb{Z}/2)^{n+1}$. Let e be the ramification index over $\mathbb{Q}_2$ (so that $(\pi^e) = (2)$), and let f be the degree of the field $\mathcal{O}/\mathfrak{p}\mathcal{O}$ over $\mathbf{F}_2$ (remember that $ef = n$). We showed that the possible quadratic defects are

$$\mathfrak{p} \subset \mathfrak{p}^3 \subset \ldots \subset \mathfrak{p}^{2e-1} \subset \mathfrak{p}^{2e} \subset 0$$

and we know that every element of $\mathcal{O}^\times$ is a square mod $\mathfrak{p}$. We will show that in the above sequence of inclusions, the group of elements of $\mathcal{O}^\times$ which are a square modulo any one of these ideals is an index 2^f subgroup of the group of elements which are a square modulo the previous ideal. That is, 2^{-f} of the residues mod $\mathfrak{p}^3$ are squares, 2^{-2f} of the residues mod $\mathfrak{p}^5$, 2^{-3f} of the residues mod $\mathfrak{p}^7$, and so on.

Suppose that $\epsilon \in \mathcal{O}/\mathfrak{p}^{2d+1}\mathcal{O}$ is a nonzero square when reduced mod $\mathfrak{p}^{2d-1}$, where $1 \leq d \leq n-1$. Then write $\epsilon \equiv x^2 \pmod{\mathfrak{p}^{2d-1}}$, where $x \in \mathcal{O}/\mathfrak{p}^d\mathcal{O}$. x only has to be defined mod $\mathfrak{p}^d$, because

$$(x+a\pi^d)^2 \equiv x^2+ax(2\pi^d)+a^2\pi^{2d} \equiv x^2+ax\pi^{d+n}+a^2\pi^{2d} \equiv x^2 \pmod{\mathfrak{p}^{2d-1}}$$

We can see that any two squares mod $\mathfrak{p}^{2d+1}$ which reduce to $x^2 \pmod{\mathfrak{p}^{2d-1}}$ differ by something of the form $a^2\pi^{2d}$, where $a \in \mathcal{O}/\mathfrak{p}\mathcal{O}$. Every element of $\mathcal{O}/\mathfrak{p}\mathcal{O}$ can be written in the form a^2, so we see that the elements of the form $x^2+a^2\pi^{2d}$ hit precisely 2^{-f} of the residues mod $\mathfrak{p}^{2d+1}$ which are congruent to $x^2 \pmod{\mathfrak{p}^{2d-1}}$.

When $d = e$, we use the same approach. We see that $(x+a\pi^e)^2 \equiv x^2+4(a^2+ax) \pmod{\mathfrak{p}^{2e+1}}$ for $a \in \mathcal{O}/\mathfrak{p}\mathcal{O}$. But only half of the residues in

$\mathcal{O}/\mathfrak{p}\mathcal{O}$ can be written in the form a^2+ax for $a \in \mathcal{O}/\mathfrak{p}\mathcal{O}$: indeed two residues a, b of $\mathcal{O}/\mathfrak{p}\mathcal{O}$ have $a^2+ax \equiv b^2+bx$ if and only if $a+b \equiv -x$. Hence, 2^{-f-1} of the residues of $\mathcal{O}/\mathfrak{p}^{2e+1}\mathcal{O}$ lying above $x^2 \pmod{\mathfrak{p}^{2e-1}}$ are squares. Combining this with repeated application of the previous argument gives that $2^{-ef-1} = 2^{-n-1}$ of the nonzero residues mod $\mathfrak{p}^{2e+1}$ are squares. Any nonzero square mod $\mathfrak{p}^{2e+1}$ can be lifted to a square in $\mathcal{O}^\times$, so this completes the proof. □

Note that by the above argument, there are units of every quadratic defect possible, because each 'level' lowers the density by a factor of 2^{-f}. Concretely, we could say that a $1-2^{-f}$ proportion of the units have defect $\mathfrak{p}$, $2^{-f}(1-2^{-f})$ have defect $\mathfrak{p}^3$, $2^{-2f}(1-2^{-f})$ have defect $\mathfrak{p}^5$, and so on.

Corollary 2.11. *There is a unit Δ with quadratic defect $4\mathcal{O}$. Any other such Δ' lies in $\Delta(\mathcal{O}^\times)^2$.*

This holds because the group of unit squares is an index 2 subgroup of the group of units which are squares mod $4\mathcal{O}$, and the elements of quadratic defect 2 are the nontrivial coset of this subgroup.

Proposition 2.12. *Let V be a binary quadratic space such that $dV \in \mathfrak{p}$, and let Δ have quadratic defect $4\mathcal{O}$. Then for any nonzero γ, V represents precisely one of $\gamma, \gamma\Delta$.*

Proof. By appropriately scaling the quadratic form on V, we can assume $\gamma = 1$. Write $V \simeq \langle \epsilon \rangle \perp \langle \delta\pi \rangle$, where δ, ϵ are units. ϵ can be chosen to be any unit of V - let it be the unit of smallest quadratic defect represented by V (i.e., as close as possible to being a square). Without loss of generality, $\epsilon \equiv 1 \pmod{\mathfrak{d}(\epsilon)}$.

1. If ϵ is a square, it can be chosen to be 1, and then V represents 1. Suppose V also represents Δ, so that $x^2 + \delta\pi y^2 = \Delta$. Clearly x is a unit and y is an integer (by looking at powers of π in each term). Then $\Delta/x^2 = 1+\delta\pi(y/x)^2$ has quadratic defect $4\mathcal{O}$. However, this expression cannot be a square mod π^2 because $(a+b\pi)^2 \equiv a^2+b^2\pi^2+ab(2\pi) \equiv a^2 \pmod{\pi^2}$, so we have a contradiction! So V cannot represent Δ.

2. If $\mathfrak{d}(\epsilon) = 4\mathcal{O}$, then V represents Δ (and not 1 by assumption).

3. Suppose $\mathfrak{d}(\epsilon) = \mathfrak{p}^{2d-1} \supsetneq 4\mathcal{O}$. Let $\epsilon = 1 + \epsilon_1\pi^m$, where ϵ_1 is a unit, and $\mathfrak{d}(\epsilon) = \mathfrak{p}^m$. Then we can find some $y \in \mathcal{O}/\mathfrak{p}\mathcal{O}$ such that $1 + \epsilon_1\pi^m + y^2\delta\pi^m \equiv 1 \pmod{\mathfrak{p}^{m+1}}$, and so V represents something of smaller quadratic defect, which is a contradiction! Hence, this case is impossible.

□

Proposition 2.13. *Let $\epsilon, \Delta \in \mathcal{O}^\times$, where Δ has quadratic defect $4\mathcal{O}$. Then $\langle \pi, \Delta \rangle_k \nsim \langle 1, -1 \rangle_k \sim \langle \epsilon, \Delta \rangle_k$.*

Proof. The first inequality follows directly from the previous proposition. Let's prove the second. There is some $x \in \mathcal{O}^\times$ such that $\Delta x^2 \equiv 1 \pmod 4$. Write $\Delta x^2 \equiv 1 - 4t\epsilon \pmod{4\pi}$, where $t \in \tilde{k}$. Then since $\tilde{k}$ has characteristic 2, t is a square, and so we have some y such that $\Delta x^2 + \epsilon y^2 \equiv 1 \pmod{4\pi}$. The sum on the left hence has quadratic defect 0, and is a square. □

2.4 The Hilbert Symbol: an explicit calculation

Definition 2.14. *Let $a, b \in k^\times$. We define the* **Hilbert symbol** (a, b) *to be* $+1$ *if* $ax^2 + by^2 = z^2$ *has a nonzero solution over* k*, and* -1 *if it does not.*

It is clear that (a, b) is just a specialization of $\langle a, b, \rangle_k$, equal to 1 if this quaternion algebra is trivial, and -1 otherwise. Moreover, the results classifying quaternion algebras from the previous two sections tell us that the Hilbert symbol is bilinear.

Theorem 2.15.

1. *If $k = \mathbb{R}$, $(a, b) = 1$ if either a or b is positive, and $(a, b) = -1$ if both are negative.*
2. *If $k = \mathbb{Q}_p$ with $p \neq 2$ and we write $a = p^\alpha a_1$ and $b = p^\beta b_1$ with a_1, b_1 having valuation 0,*
$$(a, b) = (-1)^{\alpha\beta\left(\frac{p-1}{2}\right)} \left(\frac{a_1}{p}\right)^\beta \left(\frac{b_1}{p}\right)^\alpha$$
3. *If $k = \mathbb{Q}_2$ with $p = 2$ and the same notation as above,*
$$(a, b) = (-1)^{\left(\frac{a_1 - 1}{2}\right)\left(\frac{b_1 - 1}{2}\right)} \left(\frac{a_1}{2}\right)^\beta \left(\frac{b_1}{2}\right)^\alpha$$

Here, if p is odd, $\left(\frac{x}{p}\right)$ denotes the Legendre symbol which is $+1$ if x is a quadratic residue mod p, and -1 if it is not. Meanwhile, $\left(\frac{x}{2}\right)$ is $+1$ if $x \equiv \pm 1 \pmod 8$, and -1 if $x \equiv 3, 5 \pmod 8$.

Proof. This is clear from (Theorem 2.3) and (Theorem 2.8). □

Since $k^\times/(k^\times)^2$ is a $\mathbf{F}_2$-vector space, it may be interesting to compute what it looks like for each possible field k.

1. $k = \mathbb{R}$. $(\mathbb{R}^\times)^2$ is just all positive reals, so $\boxed{\mathbb{R}^\times/(\mathbb{R}^\times)^2 \simeq \mathbb{Z}/2}$. The generator is -1, and the matrix of the bilinear form is (1).

2. $k = \mathbb{Q}_p$, $p \neq 2$. Then $\mathbb{Q}_p^\times \simeq \mathbb{Z} \times \mathbb{Z}_p^\times$, where the copy of $\mathbb{Z}$ encodes the valuation of an element. Now

$$\mathbb{Z}_p^\times \simeq \varprojlim (\mathbb{Z}/p^n)^\times \simeq \varprojlim (\mathbb{Z}/p^{n-1}) \times (\mathbb{Z}/(p-1))$$

The maps are surjections, so they can be arranged to be the identity away from the p-primary part. Hence, $\mathbb{Z}_p^\times \simeq \mathbb{Z}_p \times \mathbb{Z}/(p-1)$. More explicitly, the $\mathbb{Z}/(p-1)$ coordinate encodes the residue modulo p (multiplicatively), and the $\mathbb{Z}_p$ is topologically generated by $1+p$ (since $1+p$ has order p^{n-1} in $(\mathbb{Z}/p^n)^\times$). Given this isomorphism, since $\mathbb{Z}_p/2\mathbb{Z}_{\shortmid} = \{1\}$ and $(\mathbb{Z}/(p-1))/2(\mathbb{Z}/(p-1)) \simeq \mathbb{Z}/2$, it follows that $\boxed{\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \simeq (\mathbb{Z}/2)^2}$. A basis is $\{p, u\}$ (where u is a lift of a quadratic nonresidue of $(\mathbb{Z}/p)^\times$), and the matrix of the form is

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad p \equiv 1 \pmod 4$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \qquad p \equiv 1 \pmod 4$$

3. $k = \mathbb{Q}_2$. As before,

$$\mathbb{Q}_2^\times \simeq \mathbb{Z} \times \mathbb{Z}_2^\times \simeq \mathbb{Z} \times \varprojlim (\mathbb{Z}/2^n\mathbb{Z})^\times$$

However, $(\mathbb{Z}/2^n\mathbb{Z})^\times \simeq \mathbb{Z}/2 \times \mathbb{Z}/2^{n-2}\mathbb{Z}$, generated by -1 (which is a quadratic nonresidue modulo 2^n) and an element of order 2^{n-2} (say, any element which is not $1 \mod 8$). So $\mathbb{Q}_2^\times \simeq \mathbb{Z} \times \mathbb{Z}/2 \times \mathbb{Z}_2$, and so $\boxed{\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \simeq (\mathbb{Z}/2)^3}$. If we pick generators $\{2, -1, 5\}$, the matrix of the form is $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

2.5 Classification and Existence of Quadratic Spaces

We now classify quadratic spaces over local fields. For this section, let Δ denote a fixed units of quadratic defect $4\mathcal{O}$ (in the non-dyadic case, this just means a quadratic nonresidue).

Theorem 2.16. *Let k be a local field. Then two nondegenerate quadratic spaces W and V over k of the same dimension are isometric if and only if $dW = dV$ and $SW \simeq SV$.*

We showed in the previous chapter that, if every rank 5 quadratic space is isotropic over a field, then the above theorem holds for that field. Hence, we will seek to prove this for local fields.

Proposition 2.17. *If (V, q) is binary and anisotropic, then $q(V)$ is a coset of an order 2 subgroup of $k^\times$.*

Proof. Scale q so that $1 \in q(V)$. Write $V \simeq \langle 1\rangle \perp \langle -\alpha\rangle$. The map

$$\gamma \mapsto (\alpha, \gamma)_k$$

is a homomorphism $k^\times \to \{\pm 1\}$ with kernel $q(V)$. Since V is anisotropic, α is a nonsquare, so this map is surjective (since the Hilbert symbol is nondegenerate). □

Proposition 2.18. *If (V, q) and (W, p) are binary spaces with $q(V) = p(W)$, then $V \simeq W$.*

Proof. By scaling, suppose both represent 1. Write $V \simeq \langle 1\rangle \perp \langle -\alpha\rangle$ and $W \simeq \langle 1\rangle \perp \langle -\beta\rangle$. Then $(\alpha, \gamma) = (\beta, \gamma)$ for all γ, and hence, α/β is a square. □

Proposition 2.19. *If $V = \langle 1\rangle \perp \langle -\Delta\rangle$, then $q(V) = \mathcal{O}^\times (k^\times)^2$.*

Proof. Let $\epsilon \in \mathcal{O}^\times$. Then by (Theorem 2.3) and (Theorem 2.8), $(\epsilon, \Delta) = 1$, meaning $\epsilon \in q(V)$. So $\mathcal{O}^\times \subset q(V)$, and thus the result. □

Proposition 2.20. *Let V be an anisotropic quaternary space. Then*

$$V \simeq \langle 1\rangle \perp \langle -\Delta\rangle \perp \langle \pi\rangle \perp \langle -\pi\Delta\rangle$$

where Δ is any unit of quadratic defect $4\mathcal{O}$.

Proof. First, suppose V has a binary subspace U with $q(U) \subseteq \mathcal{O}^\times (k^\times)^2$ (and thus $q(U) = \mathcal{O}^\times (k^\times)^2$ by (Proposition 2.17)). Then if U^* is the orthogonal complement, $q(U^*) = \pi\mathcal{O}^\times (k^\times)^2$, since V is anisotropic. By combining the previous two propositions, we see V has the desired form.

Now take an arbitrary splitting $V = W \perp W^*$ into binary subspaces. We can assume both W and W^* represent both units and prime elements. We can use these to split W and W^*, so that V splits as

$$\langle \epsilon_1 \rangle \perp \langle \epsilon_2 \pi \rangle \perp \langle ? \rangle \perp \langle ? \rangle$$

i.e., with two of the components being a unit and a prime. By (Proposition 2.12) , $\langle \epsilon_1 \rangle \perp \langle \epsilon_2 \pi \rangle$ represents Δ_1, where Δ_1 is either 1 or Δ. Writing $V = \langle \Delta_1 \rangle \perp V'$, we see that V' represents some units and some primes. If dV' is prime, then V' breaks into an orthogonal sum of a prime and two units, and if dV' is a unit, then V' breaks into an orthogonal sum of two primes and a unit. Either way, V' again has a subspace which is the orthogonal sum of a unit and a prime, so this binary subspace represents $-\Delta_2$, where Δ_2 is either 1 or Δ. So now V looks like

$$V \simeq \langle \Delta_1 \rangle \perp \langle -\Delta_2 \rangle \perp \langle ? \rangle \perp \langle ? \rangle$$

This gives us a binary subspace U with discriminant either $-\Delta$ or -1. The second is impossible, as then, U is isotropic, so we have the first case, and so by (Proposition 2.19) , $q(U) = \mathcal{O}^\times (k^\times)^2$, which completes the proof. □

Proof of Theorem: From here, it is easy to see that, over a local field, any nondegenerate quadratic space V of dimension at least 5 is isotropic. Split $V = U \perp W$, where W is quaternary. If W is anisotropic, then $W \simeq \langle 1 \rangle \perp \langle -\Delta \rangle \perp \langle \pi \rangle \perp \langle -\pi\Delta \rangle$. The first two components of this space together represent $\mathcal{O}^\times (k^\times)^2$, while the last two components represent $\pi\mathcal{O}^\times (k^\times)^2$, so this quaternary space represents every nonzero element. Hence, V is isotropic, as desired.

Now that we know two quadratic spaces are isomorphic if they have the same dimension, discriminant, and Hasse algebra, we can ask: **given a dimension, discriminant, and Hasse algebra, is there a quadratic space with these invariants?** This leads us to our second theorem.

Theorem 2.21. *Given $n_0 \in \mathbb{N}, d_0 \in k^\times/(k^\times)^2, s_0 \in \{\pm 1\}$, the necessary and sufficient conditions for there to exist a quadratic space V over k with dim$(V) = n_0$, $d_0 = dV$, $s_0 = SV$ are that $s_0 = (d_0, -1)$ when $n_0 = 1$ or $n_0 = 2, d_0 \in -(k^\times)^2$, and no conditions otherwise.*

Let us first deal with the cases where conditions are stipulated.

1. For a quadratic space of dimension 1, say, $\langle d \rangle$, the Hilbert symbol is $(d, d) = (-1, d)$. So it is clear that the condition is necessary, and is satisfied for any space of dimension 1.

2. Consider quadratic spaces of dimension 2, and suppose $d_0 \in -(k^\times)^2$. Suppose $V \simeq \langle a \rangle \perp \langle b \rangle$. Then $dV = ab$, and $SV = (-1, ab)(a, b) = (-1, ab)(a, -ab)$. If V has discriminant d_0 and Hilbert symbol s_0, and $ab = d_0 \in -(k^\times)^2$, then $-ab$ is a square, and $SV = (-1, d_0)$.

All other cases will follow from the following proposition.

Proposition 2.22. *Let V be a nondegenerate quadratic space over k which is neither a line nor the space $\langle 1 \rangle \perp \langle -1 \rangle$. Then there exists a quadratic space V' of the same dimension and discriminant, but with $SV' = -SV$.*

Proof. First we consider the case of $\dim(V) \geq 3$. Let $V \simeq \langle \alpha_1 \rangle \perp \cdots \langle \alpha_n \rangle$. If we replace α_i, α_{i+1} by $\Delta\alpha_i, \Delta\alpha_{i+1}$, it leaves the discriminant unchanged, and multiplies the Hilbert symbol by $(\Delta, \Delta\alpha_i\alpha_{i+1}) = (\Delta, \alpha_i\alpha_{i+1}$. This is 1 if $\alpha_i\alpha_{i+1}$ is prime. So as long as the α_i's can be chosen so that at least one is prime and at least one is not, this proves the proposition.

First, note that any quadratic space V of dimension at least 3 represents both primes and units. For example, if $\langle a \rangle \perp \langle b \rangle$ represents $\mathcal{O}^\times (k^\times)^2$ and $\langle a \rangle \perp \langle b \rangle \perp \langle c \rangle$ represents the same set, then $\langle a \rangle \perp \langle b \rangle \perp \langle c \rangle \perp \langle c \rangle \perp \langle c \rangle$ is anisotropic, which is a contradiction. Now for any V of dimension at least 3, let $W \subseteq V$ have dimension 3. Then W represents both primes and units. dW cannot be both a unit and a prime, so it has an orthogonal decomposition with at least one prime and one unit, as desired. This proves the proposition for dimension $n \geq 3$.

Finally, we need to prove the proposition for $\dim(V) = 2$ when the discriminant is not -1. Suppose $V \simeq \langle a \rangle \perp \langle b \rangle$ has discriminant d and Hasse algebra s. The Hasse algebra of $\langle ax \rangle \perp \langle bx \rangle$ is $s(x, xd) = s(x, -d)$. Since $-d$ is not a square, there is some x such that $(x, -d) = -1$, and then $\langle ax \rangle \perp \langle bx \rangle$ has Hasse algebra $-s$, as desired. □

3 Global Fields

3.1 Preliminaries and definitions

The term *global field* is used to refer to one of two possible types of fields:

1. An algebraic number field (i.e., a finite extension of $\mathbb{Q}$). These are the global fields of characteristic 0.
2. The function field of an algebraic curve over a finite field (i.e., a finite extension of $\mathbf{F}_q(T)$, the field of rational functions in one variable over a finite field of q elements). These are the global fields of positive characteristic.

The reason for the term 'global' is because a global field K comes equipped with a set of valuations Ω, called *places* of K. We can consider, for each place $\mathfrak{p}$, the completion $K_\mathfrak{p}$, and most of these are local fields. For example,

1. When $K = \mathbb{Q}$, the places correspond to the primes p, along with another place we call ∞. The associated valuations are $|\cdot|_p$ and $|\cdot|$, and the corresponding local field for $|\cdot|_p$ is $\mathbb{Q}_p$. Completion at ∞ gives $\mathbb{R}$.
2. When $K = \mathbf{F}_q(T)$, the places correspond to points $a \in \mathbf{F}_q$. The valuation corresponding to a is precisely the order of a in a function (positive for a zero, negative for a pole), and the local field is the completion with respect to the ideal $(T - a)$ (so, Laurent series in $(T - a)$).

(We will primarily be thinking about the number field case, although these methods hold for function fields as well.) The objective of this section is to study and classify quadratic spaces over a global field K by using the results of the previous section at the local completions, and then developing a *local-global principle* to path together the local data into global structure. The imagery from the function field case motivates this idea, because in that case, the places correspond exactly to the points of the algebraic curve, and so we can imagine the idea of patching together local sections to get a global one!

3.2 The Group of Ideles

3.2.1 Introduction and Preliminaries

Fix a global field K, and let Ω denote its set of places. We defined the *adele ring* to be the collection of sequences

$$\{(x_\mathfrak{p})_{\mathfrak{p}\in\Omega} : x_\mathfrak{p} \in K_\mathfrak{p} \ \forall \mathfrak{p} \text{ and } \operatorname{ord}_\mathfrak{p}(x_\mathfrak{p}) \geq 0 \text{ for a.a. } \mathfrak{p} \in \Omega\}$$

Because each $K_\mathfrak{p}$ is a ring, this becomes a ring with componentwise addition and multiplication, and has a topology induced from the product topology on the product of the $K_\mathfrak{p}$'s. $\mathcal{J}_K$, the *group of ideles*, is the group of invertible elements of this ring (namely, adeles where each coordinate is nonzero). It turns out that inversion is not continuous on $\mathcal{J}_K$, and so the topology needs to be made finer, but we will not need to explore this point. Let $\mathbb{P}_K \simeq K^\times$ (the group of *principal ideles*) be the image of $K^\times$ in $\mathcal{J}_K$ (we will sometimes denote it by $K^\times$ as an abuse of notation).

As an aside, let us mention one major motivation for the study of ideles. In local class field theory on a local field k, one finds a direct correspondence between abelian extensions L of k and open subgroups of $k^\times$. The correspondence is given by the norm map, and if L is an arbitrary finite Galois extension of k, then $G(L/k)^{\mathrm{ab}} \simeq k^\times / N_{L/K}(L^\times)$. One might wonder if such a beautiful and clean structure theorem can be given in the (much more complicated) global case, and it turns out that $\mathcal{J}_K/\mathbb{P}_K$ is precisely the group whose open subgroups correspond to abelian extensions of K (and in a functorial way: there is a map $\mathcal{J}_K/\mathbb{P}_K \to G_K^{\mathrm{ab}}$, where any open subgroup of $\mathcal{J}_K/\mathbb{P}_K$ is the kernel of the projection onto some $G(L/K)$). Developing the entire theory would take us too far astray, but we will mimic some ideas of global class field theory in the case of quadratic extensions.)

Although $\mathcal{J}_K$ seems huge in comparison to K, we have that any finite set of coordinates of an idele can be approximated arbitrarily well by elements of K. More precisely,

Lemma 3.1. *(Weak Approximation) Let T be a finite set of places of K. Then $K \hookrightarrow \prod_{\mathfrak{p}\in T} K_\mathfrak{p}$ has dense image.*

Proof. The idea of the proof lies in the Chinese Remainder Theorem. For any $(x_\mathfrak{p})_{\mathfrak{p}\in T}$ with each $x_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}$ for each $\mathfrak{p}$, and any n, ϵ, we can find an element $x \in \mathcal{O}_K$ such that $\mathrm{ord}_\mathfrak{p}(x - x_\mathfrak{p}) \geq n$ for all non-Archimedean $\mathfrak{p}$ and $|x - x_\mathfrak{p}|_\mathfrak{p} < \epsilon$ for all Archimedean $\mathfrak{p}$. □

3.2.2 S-ideles

Let $S \subset \Omega$ be a cofinite set consisting of only non-Archimedean, non-dyadic places. We then let

$$\mathcal{J}_K^S := \{(x_\mathfrak{p}) : \mathrm{ord}_\mathfrak{p}(x_\mathfrak{p}) = 0 \ \forall \mathfrak{p} \in S\}$$

and let $\mathbb{P}_K^S = \mathbb{P}_K \cap \mathcal{J}_K^S$. These are the ideles (and principal ideles) where all of the interesting stuff valuation-wise is happening on the complement of

S (which is a much more manageable set). On the non-idelic side, we can define $\mathfrak{u} = \mathfrak{u}_K^S$, the group of *$S$-units*, to be the set of elements $x \in K^\times$ with $\mathrm{ord}_\mathfrak{p}(x) = 0$ for $\mathfrak{p} \in S$ (so that $\mathfrak{u}_K^S \simeq \mathbb{P}_K^S$). We can say, in a very definite way, what this group looks like.

Theorem 3.2. *(Dirichlet Unit Theorem) Let $\Omega - S$ have s places. Then $\mathfrak{u}_K^S$ is a direct product of $s-1$ copies of $\mathbb{Z}$ with the group of absolute units, which is a finite group consisting of the roots of unity in $K^\times$.*

Proof. It turns out that $\mathfrak{u}_K^S$ is isomorphic to $\mathbb{Z}^{s-1}$ times the group of roots of unity (which are the absolute units). A complete proof is given in [8], page 77. The proof hinges on two ideas:

1. The product formula, which states that if $\alpha \in K^\times$, then $|\alpha|_\mathfrak{p} = 1$ for almost all $\mathfrak{p}$, and $\prod\limits_{\mathfrak{p}} |\alpha|_\mathfrak{p} = 1$.

2. The construction of elements $\epsilon_\mathfrak{q}$, for each $\mathfrak{q} \in \Omega - S$, such that $|\epsilon_\mathfrak{q}|_\mathfrak{q} > 1$, and $|\epsilon_\mathfrak{q}|_\mathfrak{p} < 1$ for all other $\mathfrak{p} \in \Omega - S$. Any subset of $s-1$ of these then forms an independent generating set for the free abelian subgroup of $\mathfrak{u}_K^S$ (this is easy to show). Uniformizers at each place, after some minor modification, give such a generating set.

□

Moreover, we have the following result, which allows us to study $\mathcal{J}_K$ via the much more manageable group $\mathcal{J}_K^S$. The computations we will do will take advantage of this fact.

Proposition 3.3. *There is a cofinite set S consisting of non-Archimedean, non-dyadic places such that $\mathcal{J}_K = K^\times \mathcal{J}_K^S$.*

Again, a proof is given in [8], section 33. Fix such a set S for the rest of this section.

3.2.3 The Idelic Norm

Let L/K be a finite Galois extension, and suppose $\mathfrak{B}$ is a place of L lying over $\mathfrak{p} \in \Omega$. Then $L_\mathfrak{B}/K_\mathfrak{p}$ is Galois, so we have a norm map $N_{\mathfrak{B}/\mathfrak{p}} : L_\mathfrak{B} \to K_\mathfrak{p}$. Since $L \otimes_K K_\mathfrak{p} \simeq \prod\limits_{\mathfrak{B}|\mathfrak{p}} L_\mathfrak{B}$, we have

$$\prod_{\mathfrak{B}|\mathfrak{p}} N_{L_\mathfrak{B}/K_\mathfrak{p}}(x) = N_{L/K}(x)$$

So it makes sense to define an *idelic norm* $N_{L/K} : \mathcal{J}_L \to \mathcal{J}_K$ defined by

$$N_{L/K}(x_\mathfrak{p}) = (\prod_{\mathfrak{B}|\mathfrak{p}} N_{\mathfrak{B}/\mathfrak{p}} x_\mathfrak{p})$$

This map satisfies a commutative diagram

$$\begin{tikzcd}
L^\times \arrow[r] \arrow[d, "N_{L/K}"'] & \mathcal{J}_L \arrow[d, "N_{L/K}"] \\
K^\times \arrow[r] & \mathcal{J}_K
\end{tikzcd}$$

and is functorial in extensions.

3.2.4 The Structure of Quadratic Extensions

Let θ be a nonsquare in $K^\times$, and let $L = K(\sqrt{\theta})$. Let S' denote the set of places of L lying above S (sometimes denoted S for simplicity of notation), and let $\mathfrak{U} = \mathfrak{U}_L^{S'}$ denote the S'-units of L. Clearly, $N_{L/K}\mathcal{U} \subseteq \mathfrak{u} \subseteq \mathfrak{U}$.

Consider a place $\mathfrak{p}$. Since $L \otimes_K K_\mathfrak{p} = \prod_{\mathfrak{B}|\mathfrak{p}} L_\mathfrak{B}$ there are two possibilities for the behavior at $\mathfrak{p}$:

1. There are two primes $\mathfrak{B}_1, \mathfrak{B}_2$ over $\mathfrak{p}$, and each has local degree $n_\mathfrak{p} = 1$ (i.e., $L_\mathfrak{B} = K_\mathfrak{p}$). In this case, $\theta \in (K_\mathfrak{p}^\times)^2$. Let a be the number of $\mathfrak{p} \notin S$ such that $n_\mathfrak{p} = 1$.

2. There is one prime $\mathfrak{B}$ over $\mathfrak{p}$ with local degree $n_\mathfrak{p} = 2$ (either unramified or totally ramified). Let b be the number of $\mathfrak{p} \notin S$ such that $n_\mathfrak{p} = 2$.

Let us say that $\alpha \in K_\mathfrak{p}^\times$ is a *local norm* at $\mathfrak{p}$ if $\alpha \in N_{\mathfrak{B}/\mathfrak{p}} L_\mathfrak{B}^\times$ for all $\mathfrak{B}|\mathfrak{p}$. Then if $n_\mathfrak{p} = 1$, every element of $K_\mathfrak{p}^\times$ is a local norm, whereas if $n_\mathfrak{p} = 2$, then the local norms form a subgroup of index 2.

3.3 The Hasse Norm Theorem

In this section, we will seek to prove the following key theorem.

Theorem 3.4. *(Hasse Norm Theorem) Let L/K be a quadratic extension. Then $\alpha \in K^\times$ is a global norm if and only if it is a norm locally at every place.*

3.3.1 Index Computations

As before, let S denote a cofinite set of non-Archimedean, non-dyadic places such that $\mathcal{J}_K = K^\times \mathcal{J}_K^S$. Let $s = |\Omega - S|$, let a, b be defined as in the previous section, and let $L = K(\sqrt{\theta})$, where $\theta \in K^\times$ is a nonsquare, and a unit at all places $\mathfrak{p} \in S$. In this section, we will seek to prove the inequality

$$2 \leq (\mathcal{J}_K : K^\times N_{L/K}\mathcal{J}_L) < \infty$$

namely, that the $K^\times$-span of the group of norms is a nontrivial subgroup of $\mathcal{J}_K$, but is of finite index. This will allow us to prove key local-to-global statements about the norm in the next section. Along the way, we will prove that $(\mathcal{J}_K^S : N_{L/K}\mathcal{J}_L^S) = 2^b$, which we can think of as analogous to the statement that if we take a quadratic extension of a local field, then the norms form an index 2 subgroup of the nonzero elements of the base field.

Lemma 3.5. *Let $G \subset K^\times$ be a finitely generated group of rank r (i.e., the free part has dimension r). Then*

$$G/G^2 \simeq \begin{cases} (\mathbb{Z}/2)^{r+1} & \text{if } \; -1 \in G \\ (\mathbb{Z}/2)^r & \text{if } \; -1 \notin G \end{cases}$$

Proof. This is quite easy. Let $G \simeq \mathbb{Z}^r \oplus G_0$, where G_0 is the finite part. If $g \in G_0$ is such that $g^2 = 1$, then $g = \pm 1$, and so -1 is the only element of order 2. Therefore, G_0/G_0^2 is $\mathbb{Z}/2$ if $-1 \in G_0$, and $\{1\}$ otherwise. The result follows immediately. □

Proposition 3.6. $(\mathbb{P}_K^S : (\mathbb{P}_K^S)^2) = (\mathfrak{u}_K^S : (\mathfrak{u}_K^S)^2) = 2^s$.

Proof. The first two are equal by definition. Recall that, by the Dirichlet Unit Theorem, $\mathfrak{u}_K^S$ is a product of $\mathbb{Z}^{s-1}$ with the group of roots of unity of $K^\times$. The result follows from (Lemma 3.5). □

Proposition 3.7. *Let $(\mathcal{J}_K^S)^2$ denote the set of ideles $(x_\mathfrak{p}) \in \mathcal{J}_K^S$ such that $x_\mathfrak{p} \in (K_\mathfrak{p}^\times)^2$ for all $\mathfrak{p} \notin S$. Then*

$$(\mathcal{J}_K^S : (\mathcal{J}_K^S)^2) = 4^s$$

Proof. $(\mathcal{J}_K^S)^2$ only differs from $\mathcal{J}_K^S$ in that it has additional restrictions at the places not in S (that the elements at these places are squares). So we have an isomorphism

$$\mathcal{J}_K^S/(\mathcal{J}_K^S)^2 \to \prod_{\mathfrak{p}\notin S} K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^2$$

The result now follows from careful accounting of the value of $(K_\mathfrak{p}^\times : (K_\mathfrak{p}^\times)^2)$. At non-Archimedean, non-dyadic places, it is 4. At real places, it is 2. At complex places, it is 1. At dyadic places $\mathfrak{p}$, it is 4 times $|2|_\mathfrak{p}^{-1}$. The number of real places plus half the number of complex places (when we perform a degree 2 extension, a real place either splits into two real places, or becomes a complex place) equals the number of dyadic places weighted by the value above. □

Proposition 3.8. *If θ is a unit at all places of S,*

$$(\mathcal{J}_K^S : N_{L/K}\mathcal{J}_L^S) = 2^b$$

(where b is the number of places $\mathfrak{p} \notin S$ where θ is a nonsquare)

Proof. Consider the map $\mathcal{J}_K^S \to \prod_{\mathfrak{p}\notin S} K_\mathfrak{p}^\times$, and let $\mathbb{K}_K^S$ denote the kernel. This is the group of ideles $(x_\mathfrak{p})$ with $x_\mathfrak{p} = 1$ for $\mathfrak{p} \notin S$.

We claim $\mathbb{K}_K^S \subset N_{L/K}\mathcal{J}_L^S$. For $\mathfrak{p} \notin S$, there is nothing to check, as 1 is a norm. For $\mathfrak{p} \in S$, we're asking whether arbitrary elements $\epsilon \in \mathcal{O}_\mathfrak{p}^\times$ are norms of units. But this is true because θ is a unit, and we showed that $(\epsilon, \theta)_\mathfrak{p} = 1$ at a non-dyadic place.

The image of $N_{L/K}\mathcal{J}_L^S$ under the above map is

$$\prod_{n_\mathfrak{p}=1} K_\mathfrak{p}^\times \times \prod_{n_\mathfrak{p}=2} N_{\mathfrak{B}/\mathfrak{p}} L_\mathfrak{B}^\times$$

This is true because $n_\mathfrak{p} = 1$ precisely when θ is a square at $\mathfrak{p}$, and $n_\mathfrak{p} = 2$ precisely when θ is a nonsquare at $\mathfrak{p}$. Therefore,

$$\mathcal{J}_K^S/(N_{L/K}\mathcal{J}_L^S) \simeq (\prod_{\mathfrak{p}\notin S} K_\mathfrak{p}^\times)/(\prod_{n_\mathfrak{p}=1} K_\mathfrak{p}^\times \times \prod_{n_\mathfrak{p}=2} N_{\mathfrak{B}/\mathfrak{p}} L_\mathfrak{B}^\times) \simeq (\mathbb{Z}/2)^b$$

This last isomorphism holds because if k is a local field, and ℓ is a quadratic extension, then $k^\times/N_{\ell/k}\ell^\times \simeq \mathbb{Z}/2$. □

Let us reiterate that this is analogous to the statement that for a quadratic extension of a local field, the norm subgroup has index 2. Now from here, to prove the inequality we initially wanted, we will need a general tool.

Lemma 3.9. *(Herbrand's Lemma) Let G be an abelian group, and let $\Phi \subset G$ have finite index. Suppose we have maps $N, T : G \to G$, such that both act as maps $\Phi \to \Phi$, and NT and TN are trivial maps. That is, we have the inclusion of chain complexes $\Phi_\bullet \hookrightarrow G_\bullet$ given by*

$$\begin{tikzcd}
\cdots \arrow[r, "N"] & G \arrow[r, "T"] & G \arrow[r, "N"] & G \arrow[r, "T"] & \cdots \\
\cdots \arrow[r, "N"] & \Phi \arrow[u] \arrow[r, "T"] & \Phi \arrow[u] \arrow[r, "N"] & \Phi \arrow[u] \arrow[r, "T"] & \cdots
\end{tikzcd}$$

where the vertical arrows are all the inclusion of groups. Then we have the equation

$$\frac{|H_0(G_\bullet)|}{|H_1(G_\bullet)|} = \frac{|H_0(\Phi_\bullet)|}{|H_1(\Phi_\bullet)|}$$

Proof. Let G_T denote the kernel of the map $T : G \to G$. Similarly define G_N, Φ_T, Φ_N. Then

$$(G : \Phi)(\Phi_T : N\Phi) = (TG : T\Phi)(G_T : \Phi_T)(\Phi_T : N\Phi)$$

$$= (TG : T\Phi)(G_T : N\Phi) = (TG : T\Phi)(G_T : NG)(NG : N\Phi)$$

Interchanging T and N to obtain a similar equation, and then divide. □

Proposition 3.10. *$b \geq 1$, and*

$$(\mathbb{P}_K^S : N_{L/K}\mathbb{P}_L^S) = (\mathfrak{u}_K^S : N_{L/K}\mathfrak{U}_L^S) = 2^{b-1}$$

Proof. We will write $\mathfrak{U} = \mathfrak{U}_L^S$ and $\mathfrak{u} = \mathfrak{u}_K^S$. Let $x \mapsto \overline{x}$ be the nontrivial K-automorphism $L \to L$ (sending $a + b\sqrt{\theta} \mapsto a - b\sqrt{\theta}$). Define $T : L^\times \to L^\times$ by $Tx = x/\overline{x}$, and let N be the norm map. We can check that

$$\begin{cases} Nx = x^2, \quad Tx = 1 \ \ \forall x \in K^\times \\ Tx = x^2, \quad Nx = 1 \ \ \forall x \in TL^\times \end{cases}$$

Hence, $TN = NT = 1$, and $T\mathfrak{U} \subseteq \mathfrak{U}$ and $N\mathfrak{U} \subseteq \mathfrak{u}$. By the Dirichlet Unit Theorem, $\mathfrak{u} = \mathfrak{u}_0 \times \mathfrak{u}_1$, where $\mathfrak{u}_0$ is finite and $\mathfrak{u}_1 \simeq \mathbb{Z}^{s-1}$. We define

$$\Phi = \mathfrak{u}_1(T\mathfrak{U}) \subset \mathfrak{U}$$

(Any element Tx has all valuations equal to 1, as $G(L/K)$ preserves all valuations. Also, $\mathfrak{u}_1$ is generated by uniformizers. Therefore, $\mathfrak{u}_1$ and $T\mathfrak{U}$ are disjoint, so Φ is the direct product of these two.)

For any $x \in \mathfrak{U}$, $x^2 = Nx * Tx$. So

$$\mathfrak{U}^2 \subseteq (N\mathfrak{U})(T\mathfrak{U}) \subseteq \mathfrak{u}(T\mathfrak{U}) = \mathfrak{u}_0\Phi$$

Thus,

$$(\mathfrak{U} : \Phi) = (\mathfrak{U} : \mathfrak{u}_0\Phi)(\mathfrak{u}_0\Phi : \Phi) \leq (\mathfrak{U} : \mathfrak{U}^2)(\mathfrak{u}_0 : \mathfrak{u}_0 \cap \Phi)$$

Since $\mathfrak{u}_0$ is finite, Φ has finite index in $\mathfrak{U}$. So Φ and $\mathfrak{U}$ have the same rank. $\mathfrak{U}$ has rank $a + s - 1$, by the Dirichlet Unit Theorem, so Φ does as well. Since $\mathfrak{u}_1$ has rank $s - 1$, it follows that $T\mathfrak{U}$ has rank a.

We now apply Herbrand's Lemma to $\Phi \subset \mathfrak{U}$ to compute that

$$(\mathfrak{u} : N\mathfrak{U}) = (\mathfrak{U}_T : N\mathfrak{U}) = \frac{(\mathfrak{U}_N : T\mathfrak{U})(\Phi_T : N\Phi)}{(\Phi_N : T\Phi)}$$

Let us compute the three indices on the right to finish the proof.

1. $T\Phi = T(\mathfrak{u}_1)T(T(\mathfrak{U}))$. If $x \in T\mathfrak{U}$, then $Tx = x^2$. Also, obviously $T\mathfrak{u}_1 = \{1\}$. So $\boxed{\Phi_T = \{\pm 1\}\mathfrak{u}_1}$. Next, because $NT\mathfrak{U} = \{1\}$, we have $N\Phi = N\mathfrak{u}_1 = \mathfrak{u}_1^2 = \Phi_T^2$. So

$$\Phi_T / N\Phi \simeq \Phi_T/\Phi_T^2 \simeq (\mathbb{Z}/2)^s$$

by applying (Lemma 3.5) and using the fact that $\mathfrak{u}_1$ has rank $s - 1$.

2. By analogous reasoning, $\Phi_N = \{\pm 1\}T\mathfrak{U}$, and $T\Phi = \Phi_N^2$. So $\Phi_N/T\Phi \simeq (\mathbb{Z}/2)^{a+1}$, because $T\mathfrak{U}$ has rank a.

3. We just need to show that $(\mathfrak{U}_N : T\mathfrak{U}) = 1$. That is, we must show that if $x \in \mathfrak{U}$ and $Nx = 1$, then $x = y/\overline{y}$ for some $y \in \mathfrak{U}$. First, we'll there is such a $y \in L^\times$. If $x \neq -1$, then $\frac{1+x}{1+\overline{x}} = x$ (because $N(x) = x\overline{x} = 1$), and if $x = -1$, then $\sqrt{\theta}/\overline{\sqrt{\theta}} = -1$.

   Now for every $\mathfrak{p} \in S$, there is some $\alpha_\mathfrak{p} \in K^\times$ such that $|\alpha_\mathfrak{p}|_\mathfrak{P} = |y|_\mathfrak{P}$. This holds because the extension is unramified at every place of S, and so the valuations $||_\mathfrak{p}, ||_\mathfrak{P}$ are the same on K. Since $\mathcal{J}_K = K^\times \mathcal{J}_K^S$, there is some $\alpha \in K$ so that $|\alpha|_\mathfrak{p} = |\alpha_\mathfrak{p}|_\mathfrak{p}$ for all $\mathfrak{p} \in S$. Then y/α works. T is trivial on $K^\times$, so the required condition is still satisfied, and it is easily checked that $y/\alpha \in \mathfrak{U}$.

□

Corollary 3.11. *Let $\alpha \in K$ be a square at all $\mathfrak{p} \notin S$, and a unit at all $\mathfrak{p} \in S$. That is, in the inclusion $K^\times \to \mathcal{J}_K$, α lands in $(\mathcal{J}_K^S)^2$. Then α is a square in K. (In other words,*

$$P_K^S \cap (\mathcal{J}_K^S)^2 = (\mathbb{P}_K^S)^2$$

Proof. By the previous proposition, $b \geq 1$ for $L = K(\sqrt{\theta})$. That is, any S-unit θ which is a non-square in K must be a nonsquare at some $\mathfrak{p} \notin S$. The contrapositive statement is the result. □

Proposition 3.12. $(\mathcal{J}_K : K^\times(\mathcal{J}_K^S)^2) = (\mathcal{J}_K^S : \mathbb{P}_K^S(\mathcal{J}_K^S)^2) = 2^s$.

Proof.

$$\begin{aligned}(\mathcal{J}_K : K^\times(\mathcal{J}_K^S)^2) &= (K^\times\mathcal{J}_K^S : K^\times(\mathcal{J}_K^S)^2) = (\mathcal{J}_K^S(K^\times(\mathcal{J}_K^S)^2) : K^\times(\mathcal{J}_K^S)^2) \\ &= (\mathcal{J}_K^S : \mathcal{J}_K^S \cap K^\times(\mathcal{J}_K^S)^2) = (\mathcal{J}_K^S : \mathbb{P}_K^S(\mathcal{J}_K^S)^2) \\ &= \frac{(\mathcal{J}_K^S : (\mathcal{J}_K^S)^2)}{(\mathbb{P}_K^S(\mathcal{J}_K^S)^2 : (\mathcal{J}_K^S)^2)} = \frac{4^s}{(\mathbb{P}_K^S : \mathbb{P}_K^S \cap (\mathcal{J}_K^S)^2)} \\ &= \frac{4^s}{(\mathbb{P}_K^S : (\mathbb{P}_K^S)^2)} = 2^s\end{aligned}$$

□

Proposition 3.13. *If θ is a unit at all places of S, and $\mathcal{J}_L = L^\times\mathcal{J}_L^S$, then*

$$(\mathcal{J}_K : K^\times N_{L/K}\mathcal{J}_L) = 2(\mathbb{P}_K^S \cap N_{L/K}\mathcal{J}_L^S : N_{L/K}\mathbb{P}_L^S) < \infty$$

Proof. Let $N = N_{L/K}$. We know from Proposition (Proposition 3.8) that $\mathcal{J}_K^S : N\mathcal{J}_L^S) = 2^b < \infty$. Therefore,

$$\begin{aligned}(\mathcal{J}_K : K^\times N\mathcal{J}_L) &= (K^\times\mathcal{J}_K^S : K^\times N(L^\times\mathcal{J}_L^S)) = (K^\times\mathcal{J}_K^S : K^\times N\mathcal{J}_L^S) \\ = (\mathcal{J}_K^S(K^\times N\mathcal{J}_L^S) &: K^\times N\mathcal{J}_L^S) = (\mathcal{J}_K^S : \mathcal{J}_K^S \cap K^\times N\mathcal{J}_L^S) = (\mathcal{J}_K^S : \mathbb{P}_K^S N\mathcal{J}_L^S) \\ &= \frac{(\mathcal{J}_K^S : N\mathcal{J}_L^S)}{(\mathbb{P}_K^S N\mathcal{J}_L^S : N\mathcal{J}_L^S)} = \frac{2^b}{(\mathbb{P}_K^S : \mathbb{P}_K^S \cap N\mathcal{J}_L^S)}\end{aligned}$$

But

$$2^{b-1} = (\mathbb{P}_K^S : N\mathbb{P}_L^S) = (\mathbb{P}_K^S : \mathbb{P}_K^S \cap N\mathcal{J}_L^S)(\mathbb{P}_K^S \cap N\mathcal{J}_L^S : N\mathbb{P}_L^S)$$

Hence, the result follows. □

Corollary 3.14. $2 \leq (\mathcal{J}_K : K^\times N_{L/K}\mathcal{J}_L) < \infty$

3.3.2 Squares and Norms

Here, we use the final few results from the last section to deduce some local-global facts about squares and norms. Our first key local-global theorem is the so-called Global Square Theorem.

Theorem 3.15. *(Global Square Theorem) If $\theta \in K^\times$ is a square at almost all places, then it is a square.*

Proof. Suppose, for a contradiction, that θ is a nonsquare that is a square at almost all places. Let S be a cofinite set of non-Archimedean, non-dyadic places such that θ is a square and a unit at all $\mathfrak{p} \in S$. Let $L = K(\sqrt{\theta})$. We will deduce that $\mathcal{J}_K = K^\times N\mathcal{J}_L$, which is of course impossible because we showed $(\mathcal{J}_K : K^\times N_{L/K}\mathcal{J}_L) \geq 2$. Consider any $x \in \mathcal{J}_K$. By Weak Approximation, there some $\alpha \in K^\times$ so that $\alpha^{-1}x$ is arbitrarily close to 1 at all $\mathfrak{p} \notin S$. Since $(\mathcal{O}_\mathfrak{p}^\times)^2$ is open in $\mathcal{O}_\mathfrak{p}^\times$, α can be chosen so that $\alpha^{-1}x$ is a local square. So $\alpha^{-1}x$ is a local norm at all $\mathfrak{p} \notin S$, and since θ is a square at all $\mathfrak{p} \in S$, $\alpha^{-1}x$ is trivially a norm at all $\mathfrak{p} \in S$. So $\alpha^{-1}x \in N_{L/K}\mathcal{J}_L$. Hence, $\mathcal{J}_K \subseteq K^\times N\mathcal{J}_L$, and we have a contradiction. □

Next, we will generate the necessary theory to prove that not only is $(\mathcal{J}_K : K^\times N_{L/K}\mathcal{J}_L \geq 2$, but $(\mathcal{J}_K : K^\times N_{L/K}\mathcal{J}_L = 2$. Recall from (Lemma 3.5) and the Dirichlet Unit Theorem that $\mathfrak{u}_K^S/(\mathfrak{u}_K^S)^2 \simeq (\mathbb{Z}/2)^s$. Pick generators $\epsilon_1, \ldots, \epsilon_s$ for this group, and define

$$K(\sqrt{\mathfrak{u}}) = K(\sqrt{\epsilon_1}, \ldots, \sqrt{\epsilon_s})$$

Clearly this field has dimension 2^s over K.

Proposition 3.16. *There are infinitely many $\mathfrak{p} \in S$ such that $\epsilon_1 \notin (K_\mathfrak{p}^\times)^2$, but $\epsilon_i \in (K_\mathfrak{p}^\times)^2$ for $2 \leq i \leq s$.*

Proof. Let $H = K(\sqrt{\epsilon_2}, \ldots, \sqrt{\epsilon_s})$. By the Global Square Theorem, there are infinitely many places of H where ϵ_1 is not a square. Hence, $\epsilon_1\epsilon_i$ is a nonsquare at infinitely many places as well, for $2 \leq i \leq s$. So ϵ_1 and $\epsilon_1\epsilon_i$ are nonsquares at the places $\mathfrak{p}$ of K lying under these: there are infinitely many such $\mathfrak{p}$. Meanwhile, since $K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^2 \simeq \mathbb{Z}/2$, it follows that ϵ_i is a square at all of these $\mathfrak{p}$, for $2 \leq i \leq s$. □

Corollary 3.17. *There are places $\mathfrak{p}_1, \ldots, \mathfrak{p}_s \in S$ where ϵ_i is a nonsquare at $\mathfrak{p}_i$, and a square at all $\mathfrak{p}_j$ for $i \neq j$.*

Corollary 3.18. *Let $\theta \in K$ be a square at all $\mathfrak{p} \notin S$ and a unit at all $\mathfrak{p} \in S' := S - \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Then θ is a square.*

Proof. Suppose θ is not a square, and let $L = K(\sqrt{\theta})$. We will obtain a contradiction by concluding that $\mathcal{J}_K \subseteq K^\times N_{L/K}\mathcal{J}_L$, which contradicts Proposition . Since $\mathcal{J}_K = K^\times \mathcal{J}_K^S$, it is enough to show $\mathcal{J}_K^S \subseteq K^\times N_{L/K}\mathcal{J}_L$. Pick an idele $x \in \mathcal{J}_K^S$. Define $c_1, \ldots, c_s$ where $c_i = 0$ if x is a square at $\mathfrak{p}_i$, and $c_i = 1$ if x is a nonsquare at $\mathfrak{p}_i$. Then let ϵ be the S-unit

$$\epsilon = \epsilon_1^{c_1} \cdots \epsilon_s^{c_s}$$

ϵ is a square at precisely the $\mathfrak{p}_i$ where x is a square. Since the $\mathfrak{p}_i$'s are nondyadic, $x\epsilon$ is a square at each $\mathfrak{p}_i$. Hence, it is in $N_{L/K}\mathcal{J}_L$. (At the places $\mathfrak{p}_i$, it is a square. At the places not in S, the extension is trivial. And at places $\mathfrak{p}$ of S', the extension is unramified, so if the extension is nontrivial, it is nontrivial on the residue fields, and thus the norm map induces a surjection $\mathfrak{U}_{\mathfrak{B}} \to \mathfrak{u}_{\mathfrak{p}}$.) □

Proposition 3.19. $(\mathcal{J}_K : K^\times N_{L/K}\mathcal{J}_L) = 2$.

Proof. It will suffice to show that $(\mathcal{J}_K : K^\times N_{L/K}\mathcal{J}_L \leq 2$. Let S be a set of places satisfying the previously mentioned conditions, and so that θ is a unit at all $\mathfrak{p} \in S$. Proposition tells us that $(\mathcal{J}_K : K^\times(\mathcal{J}_K^S)^2) = 2^s$, and clearly $K^\times(\mathcal{J}_K^S)^2 \subseteq K^\times N_{L/K}\mathcal{J}_L$, so it would suffice to show that $(K^\times N_{L/K}\mathcal{J}_L : K^\times(\mathcal{J}_K^S)^2) = 2^{s-1}$. We already know this index is a power of 2 that is at most 2^{s-1}, so it suffices to find a strictly ascending tower of subgroups

$$K^\times(\mathcal{J}_K^S)^2 = \Phi_1 \subsetneq \Phi_2 \subsetneq \cdots \subsetneq \Phi_s = K^\times N_{L/K}\mathcal{J}_L$$

We generate the tower as follows. Let $\theta, \epsilon_2, \ldots, \epsilon_s$ be a set of generators of $\mathfrak{u}/\mathfrak{u}^2$, and pick places $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ satisfying the conditions of (Corollary 3.17). Let $\Phi_1 = K^\times(\mathcal{J}_K^S)^2$, and let $\Phi_j = K_{\mathfrak{p}_j}^\times \Phi_{j-1}$ for all j. Since θ is a square at $\mathfrak{p}_2, \ldots, \mathfrak{p}_s$, these are all subgroups of $K^\times N_{L/K}\mathcal{J}_L$, so we just need to show that $\Phi_{j-1} \subsetneq \Phi_j$.

Suppose for a contradiction that $K_{\mathfrak{p}_j}^\times \subset \Phi_{j-1}$. Let π be a uniformizer at $\mathfrak{p}_j$, and let x be the idele $(1, \ldots, \pi, \ldots)$. By assumption,

$$x \in \Phi_{j-1} = K_{\mathfrak{p}_1}^\times \cdots K_{\mathfrak{p}_{j-1}}^\times K^\times(\mathcal{J}_K^S)^2$$

So there's some $y \in K_{\mathfrak{p}_1}^\times \cdots K_{\mathfrak{p}_{j-1}}^\times(\mathcal{J}_K^S)^2$ and $\alpha \in K^\times$ so that $x = \alpha y$. y is a square at all $\mathfrak{p} \notin S$, so α is as well. Also, y is a unit at all $\mathfrak{p} \in S'$, and so α is as well. Then α is a square, by (Corollary 3.18). But this is impossible, because α is prime at $\mathfrak{p}_j$! Hence, we have a contradiction, and so $\Phi_{j-1} \subsetneq \Phi_j$, as desired. □

Corollary 3.20. *If θ is a unit at all places of S and $\mathcal{J}_L = L^\times \mathcal{J}_L^S$, then $\mathbb{P}_K^S \cap N_{L/K}\mathcal{J}_L^S = N_{L/K}\mathbb{P}_L^S$.*

This follows by combining the previous proposition with (Proposition 3.13).

Theorem 3.21. *(Hasse Norm Theorem) Let L/K be quadratic. $\alpha \in K$ is a norm if and only if it is a local norm at all places.*

Proof. It suffices to show the 'if' direction. Let $L = K(\sqrt{\theta})$, and let S be a set of places satisfying the same assumptions as before and such that θ, α are units at all $\mathfrak{p} \in S$, and so that $\mathcal{J}_L = L^\times \mathcal{J}_L^S$. Then the idele (α) is in $\mathbb{P}_K^S$, and it is in $N_{L/K}\mathcal{J}_L^S$ by the ramification argument at the end of the proof of (Corollary 3.18). . Therefore, $(\alpha) \in N_{L/K}\mathbb{P}_L^S$. So $\alpha \in N_{L/K}\mathfrak{U}_L^S$ is a global norm. □

It turns out that the above statement holds for all cyclic extensions L/K. All of our proofs could be modified to account for this more general case. In fact, this is closely related to the general statement (the Albert-Brauer-Hasse-Noether theorem) that $\mathrm{Br}(K) \to \prod_{\mathfrak{p}} \mathrm{Br}(K_\mathfrak{p})$ is injective, where $\mathrm{Br}(K) = H^2(K, \mathbb{G}_m)$ is the group of central simple algebras over K up to similarity, with the operation of tensor product.

3.4 Isotropy of Quadratic Forms

For a quadratic space V over K, and a place $\mathfrak{p}$, let $V_\mathfrak{p} = V \otimes_K K_\mathfrak{p}$ be the obvious completion, where q is extended by continuity.

Theorem 3.22. *A nondegenerate quadratic space over K is isotropic if and only if it is isotropic at all places.*

We first prove some general facts about quadratic forms over an arbitrary field. We will begin by proving some preliminary general facts about quadratic forms over an arbitrary field.

Proposition 3.23. *Let V be a nondegenerate quaternary space of discriminant 1, and let $U \subset V$ be a dimension 3 subspace. Then V is isotropic if and only if U is.*

Proof. It suffices to show that if V is isotropic, then U is. Write $V = U \perp \langle\alpha\rangle$ for $\alpha \neq 0$. Then U represents $-\alpha$, so write $V = P \perp \langle -\alpha\rangle \perp \langle\alpha\rangle$. Thus, $dP = -1$, and so $P \simeq \langle\beta\rangle \perp \langle -\beta\rangle$ for some β, and is thus isotropic. □

Proposition 3.24. *Every nondegenerate isotropic quadratic space is split by a hyperbolic plane, and therefore represents every element of the base field.*

Proof. Let x be an isotropic vector in the space. Then since the bilinear form is nondegenerate, there is some y such that $B(x, y) \neq 0$. Then the span of x and y is nondegenerate and isotropic, and is therefore a hyperbolic plane. $\square$

Corollary 3.25. *Let V be a nondegenerate quadratic space, and let $\alpha \neq 0$. Then V represents α if and only if $\langle -\alpha \rangle \perp V$ is isotropic.*

Proof. It clearly suffices to show the 'if' direction. If V is isotropic, then it represents every scalar, and we are done by the previous proposition. If not then by simply considering an isotropic element of $\langle -\alpha \rangle \perp V$, we find that V represents α. $\square$

Proposition 3.26. *Let V be a nondegenerate quaternary space of discriminant d, and let $L = k(\sqrt{d})$. Then V is isotropic if and only if V_L is.*

Proof. Suppose V is anisotropic. Then d is a nonsquare, so L is quadratic over k. Then elements of V_L have the form $x + y\sqrt{d}$ with $x, y \in V$. Pick an isotropic vector of this form. Then $q(x) + dq(y) + 2B(x, y)\sqrt{d} = 0$. Hence, $q(x) = -dq(y)$ and $B(x, y) = 0$. Write $q(y) = \epsilon, q(x) = -d\epsilon$. Then $V \simeq \langle \epsilon \rangle \perp \langle -d\epsilon \rangle \perp P$. Computing the discriminant, we see $dP = -1$, and so P is a hyperbolic plane. So V is isotropic. $\square$

Proof of the Theorem: We only need to prove the 'if' part. We proceed by considering dimension $2, 3, 4$, and ≥ 5 separately.

1. Dimension 2. Write $V \simeq \langle a_1 \rangle \perp \langle a_2 \rangle$. Then, every $V_\mathfrak{p}$ has discriminant -1, so $-a_1a_2 \in (K_\mathfrak{p}^\times)^2$ for every $\mathfrak{p}$. Then by the Global Square Theorem, $-a_1a_2 \in (K^\times)^2$, and so V is isotropic.

2. Dimension 3. By scaling V so that it represents 1, it has a splitting $V = L \perp P$ such that

$$L \simeq \langle -\alpha \rangle \qquad\qquad P \simeq \langle 1 \rangle \perp \langle -\theta \rangle$$

   If θ is a square in $K^\times$, then we are done, so assume it is not. Since each $V_\mathfrak{p}$ is isotropic, each $P_\mathfrak{p}$ represents α. Hence, α is a local norm of $K(\sqrt{\theta})$ at every $\mathfrak{p}$. By the Hasse Norm Theorem, α is therefore a global norm, which implies V is isotropic.

3. Dimension 4. First suppose $dV = 1$. Pick a nondegenerate ternary $U \subset V$. Then each $V_{\mathfrak{p}}$ has discriminant 1, so by (Proposition 3.23), $U_{\mathfrak{p}}$ is isotropic. Then by the dimension 3 case, U is isotropic, and we are done.

   Now suppose $dV \neq 1$. Write $V \simeq \langle a_1 \rangle \perp \langle a_2 \rangle \perp \langle a_3 \rangle \perp \langle a_4 \rangle$. Let $L = K(\sqrt{dV})$, and consider the extension of scalars $V_L = V \otimes_K L$. Each $(V_L)_{\mathfrak{B})}$ is isotropic, because it contains $V_{\mathfrak{p}}$ (where $\mathfrak{B}|\mathfrak{p}$). The discriminant of this space is 1 (as $dV \in (L^\times)^2$), and so by the previous argument, V_L is isotropic. Then by (Proposition 3.26), V is isotropic.

4. Dimension $n \geq 5$. We proceed by induction on n. Decompose $V = U \perp W$, where U is binary. Let $T = \{\mathfrak{p} | W_{\mathfrak{p}} \text{ anisotropic}\}$. We claim T is finite. Indeed, it suffices to consider the case where W ternary (if not, replace it by a ternary subspace). Let $W = \langle \epsilon_1 \rangle \perp \langle \epsilon_2 \rangle \perp \langle \epsilon_3 \rangle$. Then, for all $\mathfrak{p}$ but finitely many, the ϵ_i's are units at $\mathfrak{p}$. If $\mathfrak{p}$ is finite and nondyadic, and the ϵ_i's are units, then $SV = 1$ over $K_{\mathfrak{p}}$. So T consists of at most the archimedean places, the dyadic places, and a finite number of non-dyadic places, making it finite.

   If T is empty, then we are done by the inductive hypothesis, so suppose T is nonempty. Then for every $\mathfrak{p}$, there is some $\mu_{\mathfrak{p}} \in K_{\mathfrak{p}}^\times$ such that $\mu_p \in q(U_{\mathfrak{p}})$, $-\mu_{\mathfrak{p}} \in q(W_{\mathfrak{p}})$. Let $U = \langle a_1 \rangle \perp \langle a_2 \rangle$. Then for every $\mathfrak{p} \in T$, we have $\xi_{\mathfrak{p}}, \eta_{\mathfrak{p}}$ such that

   $$\xi_{\mathfrak{p}}^2 a_1 + \eta_{\mathfrak{p}}^2 a_2 = \mu_{\mathfrak{p}}$$

   By Weak Approximation, we can find $\xi, \eta \in K$ which are close to $\xi_{\mathfrak{p}}$ and $\eta_{\mathfrak{p}}$, respectively, at each $\mathfrak{p} \in T$. Let $\mu = \xi^2 a_1 + \eta^2 x_2$. By taking arbitrarily good approximations, we can make μ arbitrarily close to the μ_p. Since $(K_{\mathfrak{p}}^\times)^2 \subset K$ is open, we can then make it so that $\mu \in \mu_{\mathfrak{p}}(K_{\mathfrak{p}}^\times)^2$ for each $\mathfrak{p} \in T$. Then because $-\mu_{\mathfrak{p}} \in q(W_{\mathfrak{p}})$ for each $\mathfrak{p} \in T$, we have that $\langle \mu \rangle \perp W$ is isotropic at all $\mathfrak{p} \in T$. Since it is isotropic at all places, $\langle \mu \rangle \perp W$ is then isotropic, and so is V.

3.5 Equivalence and Classification of Quadratic Forms

Theorem 3.27. *Let U and V be nondegenerate quadratic spaces over a global field K. Then U is isometric to a subspace of V if and only if $U_{\mathfrak{p}}$ is isometric to a subspace of $V_{\mathfrak{p}}$ for all places $\mathfrak{p}$.*

Proof. We proceed by induction on the dimension of U. First, consider $\dim(U) = 1$, and let $U = \langle\alpha\rangle$. Then $\langle-\alpha\rangle \perp V$ is isotropic at all $\mathfrak{p}$. Hence, it is isotropic by (Theorem 3.22), and so V represents α. Thus, $U \hookrightarrow V$.

Now for the inductive step. Pick a nonzero $\alpha \in q(U)$. Then $V_\mathfrak{p}$ represents α for every $\mathfrak{p}$, and so V represents α (by the dimension 1 case). So then we have splittings

$$V \simeq \langle\alpha\rangle \perp V' \qquad U \simeq \langle\alpha\rangle \perp U'$$

It's clear that $U'_\mathfrak{p} \hookrightarrow V'_\mathfrak{p}$ for every $\mathfrak{p}$, so by the inductive hypothesis, $U' \hookrightarrow V'$. So then $U \hookrightarrow V$, and this completes the induction. □

As a special case where U and V have the same dimension, we have

Corollary 3.28. *(Hasse-Minkowski Theorem) Two nondegenerate quadratic spaces over a global field are isometric if and only if they are isometric at every place.*

Using our earlier classification of quadratic forms over local fields using local invariants, we find that a quadratic form over a global field is classified by

1. The dimension.
2. The discriminant.
3. The Hasse symbols $S_\mathfrak{p}V$ at the non-archimedean places $\mathfrak{p}$.
4. The signature at real $\mathfrak{p}$. (for a symmetric bilinear form, this counts the dimension of the largest positive definite subspace.)

The reason for (4), the signature, is because we need to consider the localization at real places. We have not included the argument here, but any real quadratic form is equivalent to one of the form $x_1^2 + \ldots + x_m^2 - x_{m-1}^2 - \ldots - x_n^2$, and these $(n+1)$ different forms (depending on the number of $+1$'s and -1's) are nonisomorphic.

We can then proceed to ask: what relations hold on these global invariants, i.e., what combinations of values are achieved by actualy quadratic forms? Although it would take too long to prove, it turns out that the following two statements holds:

Theorem 3.29. *(Hilbert Reciprocity, or Product Formula) If each $S_{\mathfrak{p}}V$ is regarded as ± 1, then*

$$\prod_{\mathfrak{p}} S_{\mathfrak{p}}V \sim 1$$

Theorem 3.30. *Let $a_1, \ldots, a_n \in K^\times$, and let $(\epsilon_{i,v})$, $v \in \Omega$, $i = 1, \ldots, n$ be numbers equal to ± 1. Then there exists $x \in K^\times$ such that $(a_i, K)_v = \epsilon_{i,v}$ for all i, v if and only if the following three conditions hold:*

1. *$\epsilon_{i,v} = 1$ for almost all i, v.*
2. *For all i, $\prod_v \epsilon_{i,v} = 1$.*
3. *For all v, there exists $x_v \in K_v^\times$ such that $(a_i, x_v)_v = \epsilon_{i,v}$ for all i.*

The key 'local-to-global' idea in the proof is the Weak Approximation Theorem.

4 Concrete Counterexample: Intersection of Two Quadrics

In light of the Hasse-Minkowski theorem (both the equivalence of forms and the isotropy) for number fields, we can naturally ask whether the same local-global principles hold in cases other than quadratic equations. More concretely, we can ask, for k a global field:

1. If V is a smooth, projective variety over k such that V_{k_v} has a k_v-rational point for every place v, then does V have a k-rational point?
2. If V and W are smooth projective varieties over k such that V_{k_v} and W_{k_v} are isomorphic for each place v of k, then is V isomorphic to W?

It turns out that the answer to both of these questions is no, in the next simplest cases after a quadric: the case of the intersection of two quadrics, and the case of a cubic. In this section, we will present the first of these two cases, in a very concrete way.

4.1 Preliminary Reduction

We consider the simultaneous equations

$$aU^2 + bV^2 + cW^2 = dZ^2 \qquad ; \qquad UW = V^2$$

with $a, b, c, d \in \mathbb{Z}$, d squarefree, a, c, d nonzero, and $b^2 - 4ac \neq 0$. Nontrivial solutions over $\mathbb{Z}$ to this quaternary system (resp. primitive solutions over $\mathbb{Z}_p$) are in correspondence with nontrivial solutions over $\mathbb{Z}$ to the ternary equation

$$aX^4 + bX^2Y^2 + cY^4 = dZ^2$$

(resp. primitive solutions over $\mathbb{Z}_p$). First, let's prove this over $\mathbb{Z}$. Obviously, a solution to the second equation yields a solution to the first. Given a solution (u, v, w, z) to the first equation, then (v, w, zw) and (u, v, zu) are solutions to the second equation, and at least one is nontrivial. Moreover, this same argument holds for $\mathbb{R}$, as well.

Now let's look at primitive solutions over $\mathbb{Z}_p$ (i.e., not all divisible by p). Again, a primitive solution to the second equation gives one for the first equation. Suppose (u, v, w, z) is a primitive solution to the first equation. Then both (v, w, zw) and (u, v, zu) are solutions to the second equation. We claim that at least one of u, v, w is not divisible by p. Suppose to the contrary. Then z is not divisible by p, and so $p^2|d$, contradicting the fact that d is squarefree. Hence, one of u, v, w is prime to p, and thus has an inverse in $\mathbb{Z}_p$. Depending on which is invertible, one of the following is a primitive solution:

$$(1, vu^{-1}, zu^{-1}) \qquad (vw^{-1}, 1, zw^{-1}) \qquad (1, wv^{-1}, zwv^{-2})$$

The above arguments allow us to study the ternary equation instead.

4.2 Parametrizing Conics

Suppose $ax^2 + by^2 = 1$ is a conic over a field k. Given an initial solution (x_0, y_0), we can parametrize solutions to the equation as follows. Construct the line through (x_0, y_0) of slope T: it has equation $y - y_0 = T(x - x_0)$. Plugging this into the conic and solving gives us the relation

$$a(bx_0T^2 - 2by_0T - ax_0)^2 + b(-by_0T^2 - 2ax_0T + ay_0)^2 = (bT^2 + a)^2$$

As T varies over the elements of k, this gives us all other solutions to the equation. For example, if $k = \mathbb{R}$, $a = b = 1$, and $x_0 = -1, y_0 = 0$, then this parametrization allows us to generate Pythagorean triples if T is chosen to be a positive rational number. Call the first polynomial above $q_1(T)$ and the second $q_2(T)$, and let $q_3(t) = bT^2 + a$.

4.3 $aX^4 + bY^4 = Z^2$ over Finite Fields

For this section, let p be an odd prime. We will use the above tool to construct solutions to $aX^4 + bY^4 = Z^2$ in any finite field k of characteristic p. But we first need a lemma.

Lemma 4.1. *Let $\mathbf{F}_q$ be a field with q elements. Let f, g be polynomials over $\mathbf{F}_q$ with degree at most two. If $f(t)^{\frac{q-1}{2}} = g(t)^{\frac{q-1}{2}}$ for all t, then $f(t)/g(t)$ is a constant.*

Proof. Suppose $f(t)^{\frac{q-1}{2}} - g(t)^{\frac{q-1}{2}} = 0$ for all 0. This is a polynomial of degree at most $q-1$, with q roots: hence, it is identically zero. Thus, $f^{\frac{q-1}{2}} = g^{\frac{q-1}{2}}$ (as polynomials). Since $\mathbf{F}_q[X]$ is a unique factorization domain, it follows that f/g is a constant polynomial. □

Proposition 4.2. *$aX^4 + bY^4 = Z^2$ has a nontrivial solution in k.*

Proof. Let q_1, q_2, q_3 be the polynomials as above, generated from an initial solution (x_0, y_0) to the equation $ax^2 + by^2 = 1$ (which we proved must exist in the proof of Hasse-Minkowski). Since q_1 and q_2 are not constant multiples of one another (clear by inspection), neither are q_1 and rq_2, where r is any nonsquare in $k^\times$. Then there is some t such that $q_1(t)^{\frac{q-1}{2}} \neq (rq_2(t))^{\frac{q-1}{2}} = -q_2(t)^{\frac{q-1}{2}}$. Hence, $q_1(t)^{\frac{q-1}{2}} = q_2(t)^{\frac{q-1}{2}}$, and so $q_1(t)q_2(t)$ is a quadratic residue: call it c^2. Then either $(q_1(t), c, q_1(t)q_3(t))$ is a solution to $aX^4 + bY^4 + Z^2$ (if $q_1(t) \neq 0$), or $(c, q_2(t), q_2(t)q_3(t))$ is a solution (if $q_2(t) \neq 0$). □

4.4 p-adic solutions

Proposition 4.3. *Let p be an odd prime not dividing a, c, d. Then $aX^4 + cY^4 = dZ^2$ has a primitive solution in $\mathbb{Z}_p$.*

Proof. d has an inverse $d^{-1} \in \mathbb{Z}_p$. By the previous subsection, $d^{-1}aX^4 + d^{-1}cY^4 = Z^2$ has a nontrivial solution (x_1, y_1, z_1) modulo p.

If $p \nmid z_1$, then $d^{-1}(ax_1^4 + cy_1^4)$ is a square modulo p, and hence equals some n^2 in $\mathbb{Z}_p$. If $p \nmid x_1$, then $(1, y_1x_1^{-1}, nx_1^{-2})$ is a primitive solution in $\mathbb{Z}_p$, and if $p | x_1$, take $(x_1y_1^{-1}, 1, ny_1^{-2})$ instead.

If $p | z_1$, then $-ac^{-1}$ is a fourth power modulo p, and hence equals n^4 in $\mathbb{Z}_p$. Then $(1, n, 0)$ is a primitive solution in $\mathbb{Z}_p$. □

Now suppose we have the system of equations

$$U^2 - qW^2 = dZ^2 \qquad ; \qquad UW = V^2$$

where

1. $q \equiv 1 \pmod{16}$ is a prime.
2. d is squarefree.
3. d is a nonzero square mod q.
4. q is a fourth power mod p for every odd p dividing d.

Proposition 4.4. *This system has a primitive p-adic solution for every prime p, as well as a real solution.*

$(q^{1/2}, q^{1/4}, 1, 0)$ is a real solution. To find the p-adic solutions (i.e., the primitive solutions modulo p^m for every m), it suffices to find a p-adic solution to the equation $X^4 - qY^4 = dZ^2$ for every m. If $p \nmid 2dq$, then we've already shown this.

Suppose $p = q$. By condition 3 above, $d = n^2$ in $\mathbb{Z}_q^\times$, and $(1, 0, n^{-1})$ is a primitive p-adic solution. Suppose $p|d$, p odd. Then $q = n^4$ in $\mathbb{Z}_p^\times$ for some n, and $(n, 1, 0)$ is a primitive p-adic solution. Suppose $p = 2$. Since $q \equiv 1 \pmod{16}$, $q = n^4$ in $\mathbb{Z}_2^\times$, for some n, and $(n, 1, 0)$ is a primitive solution.

4.5 Counterexamples

Consider the equation $X^4 - qY^4 = dZ^2$, where $q \equiv 1 \pmod 8$ is prime, d is squarefree, and $(d, q) = 1$. Suppose (x, y, z) is a primitive integer solution. We may assume x, y, and z are all pairwise prime: suppose p divides exactly two of these. Then it must divide x. If it divides z, then $p^2|q$, which is a contradiction. If it divides y, then $p^4|dz^2$, which is a contradiction because d is squarefree.

Suppose p is an odd prime dividing z (and thus not dividing x or y. Then taking the congruence modulo p implies that $\left(\frac{q}{p}\right) = 1$. By Quadratic Reciprocity, $\left(\frac{p}{q}\right) = 1$. Because $q \equiv 1 \pmod 8$, $-1, 2$ are quadratic residues mod q. Therefore, z_1, being a product of quadratic residues, is a quadratic residue mod q. Since $d = z_1^{-2} x_1^4 \pmod q$, d is a fourth power mod q.

Hence, if we construct a system of equations

$$U^2 - qW^2 = dZ^2 \qquad ; \qquad UW = V^2$$

where

1. $q \equiv 1 \pmod{16}$ is prime.

2. d is squarefree.

3. Taken mod q, d is a nonzero square, but not a fourth power.

4. q is a fourth power mod p for every odd p dividing d. then our system has solutions in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every prime p, but has no solution in $\mathbb{Q}$. For example, when $q = 17, d = 2$, we get the equivalent equation $X^4 - 17Y^4 = 2Z^2$ - this famous example is due to Lind and Reichardt.

5 Measuring how badly the Hasse Principle fails

5.1 Selmer's cubic

Selmer provided a famous example of a counterexample to the Hasse principle over $\mathbb{Q}$ in $\mathbb{P}^2$: namely, the cubic curve

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

Not only does it have local solutions at every place but no rational solution, but it has four nonisomorphic *companion curves*:

$$\mathcal{C}_1 : 3X^3 + 4Y^3 + 5Z^3 = 0$$

$$\mathcal{C}_2 : 12X^3 + Y^3 + 5Z^3 = 0$$

$$\mathcal{C}_3 : 15X^3 + 4Y^3 + Z^3 = 0$$

$$\mathcal{C}_4 : 3X^3 + 20Y^3 + Z^3 = 0$$

$$\mathcal{C}_5 : 60X^3 + Y^3 + Z^3 = 0$$

That is, these five curves are isomorphic over $\mathbb{R}$ and over $\mathbb{Q}_p$ for every prime p, but are nonisomorphic over $\mathbb{Q}$. All of these curves have local solutions at every place, and none have a solution in $\mathbb{Q}$ except for $\mathcal{C}_5$ (the *Jacobian* of the family), which has $(0, 1, -1)$ as a solution. It turns out that if $\mathcal{C}$ is any curve of genus 1 in $\mathbb{P}^2$ (over $\mathbb{Q}$), then $\mathcal{C}$ has a nonisomorphic companion curve if and only if it (or one of its companions) has a nontrivial $\mathbb{Q}_p$-point for every p and a nontrivial $\mathbb{R}$-point, but no nontrivial $\mathbb{Q}$-point. That is, the two possible 'Hasse principles' we have been considering fail in exactly the same cases for genus 1 curves.

We could explicitly show, just as for the intersection of two quadrics, why this equation has local solutions but no global solutions. However, the methods are much the same in flavor, and not very enlightening. Instead, we will mention some more powerful theory and discuss groups which measure *how badly* the Hasse principle fails (just as the ideal class group of a number field measures how badly unique factorization fails). For example, although the Hasse principle fails for Selmer's curve, there are only five companion curves - the situation, a priori, could have been far worse. In this section, we will not present concrete proofs of the results.

In the interest of honesty, let's hint towards how to construct $\mathbb{Q}_p$-points for Selmer's curve. The following lemma narrows our search for solutions over $\mathbb{Q}_p$ to a search for solutions over $\mathbf{F}_p$:

Lemma 5.1. *(Hensel's Lemma) Let $G(T) \in \mathbb{Z}_p[T]$, and let $t_0 \in \mathbb{Z}_p$ be such that*

$$p | G(t_0) \qquad\qquad p \nmid G'(t_0)$$

where G' is the formal derivative of G. Then there is some $t \in \mathbb{Z}_p$ such that $G(t) = 0$ and $|t - t_0|_p \leq G(t_0)$.

The technique to prove this is quite standard: suppose we have a solution $t_n \pmod{p^n}$. Then we can consider the p different lifts of t_n modulo p^{n+1}, and because $p \nmid G'(t)$, these p different lifts give p different outputs modulo p^{n+1} when plugged into G. It then follows that one (and precisely one) of them is a solution modulo p^{n+1}. Repeating ad infinitum takes us from a mod p solution to a $\mathbb{Z}_p$-solution. A similar statement holds for a multivariable G, but the derivative condition needs to be replaced by an appropriate condition on the partial derivatives.

It is not hard to find nontrivial solutions to Selmer's cubic mod p for every p and check that it satisfies the conditions of Hensel's lemma. Obviously it has a nontrivial $\mathbb{R}$-solution. The process of proving that Selmer's cubic has no $\mathbb{Q}$-solution is rather tedious - a proof is provided in

5.2 Galois Cohomology

The language of cohomology is a more modern, cleaner way to state many of these results. We recall some notions here (for a more thorough treatment, see [10]).

5.2.1 Nonabelian Cohomology

If G is a topological group and A is a G-group (a group on which G acts continuously), then recall that we can define $H^0(G, A) = A^G$, the group of invariants. Recall that a 1-cocycle is a map $a : G \to A$ such that $a_{st} = a_s{}^s a_t$. Two cocycles a, a' are said to be cohomologous if there is some $b \in A$ such that $a'_s = b^{-1} a_s{}^s b$. We define $H^1(G, A)$ to be the set of cocycles modulo the relation of cohomology. If A is an abelian group, then this agrees with the usual definition of the cohomology groups $H^*(G, A)$.

Principal Homogeneous Spaces: $H^1(G, A)$ can also be identified with the set of isomorphism classes of *principal homogeneous spaces* over A. These are G-sets P on which A acts transitively on the right, making P into an affine space over A. A principal homogeneous space P can be obtained from any cocycle a by 'twisting' the action of G on A via the cocycle.

5.2.2 Forms of a variety, and Galois cohomology

A natural group we might apply this theory to is a Galois group $G(L/K)$. It is also well-known that if V is a variety defined over a field K, then $H^1(G(L/K), \mathrm{Aut}_V(L))$ parametrizes (up to K-isomorphism) the K-varieties which become isomorphic to V upon extending scalars to L. Here, Aut_V is the algebraic group whose L-points are the L-automorphisms of V. If we let $L = \overline{K}$, then we denote this cohomology group by $H^1(K, \mathrm{Aut}_V)$, and it parametrizes K-varieties which are isomorphic over the algebraic closure.

Example: Consider the case where V is a quadratic space (V, q) over the field K. Then the group $H^1(K, \mathbf{O}(V, q))$ parametrizes quadratic spaces which are isomorphic to (V, q) over $\overline{K}$, but not over K. It is not hard to show that any two quadratic spaces of the same rank over an algebraically closed field are isomorphic. So then in the case where K is a global field, if we look at the map

$$H^1(K, \mathbf{O}(V, q)) \to \prod_v H^1(K_v, \mathbf{O}(V, q))$$

we see that the Hasse-Minkowski theorem is precisely equivalent to the injectivity of this map. The map is constructed by noting that the inclusion $K \to K_v$ induces a map $G_{K_v} \to G_k$, and taking cohomology reverses the direction of the map once more.

Example: If $\mathcal{C}$ is any variety over K, then $\ker(H^1(K, \mathrm{Aut}_{\mathcal{C}}) \to \prod_v H^1(K_v, \mathrm{Aut}_{\mathcal{C}}))$ is precisely the set of *companions* to $\mathcal{C}$. Here, the kernel is the fiber of the basepoint (these are *pointed* sets, where the basepoint is the class of the trivial cocycle). It is known, for example, that if $\mathcal{C}$ is a curve of genus ≥ 2, then $\mathrm{Aut}_{\mathcal{C}}$ is finite, and so $\mathcal{C}$ has to have a finite number of companions.

5.3 Elliptic Curves

Definition 5.2. *An elliptic curve is a smooth projective curve of genus* 1 *(i.e., the Euler characteristic of cohomology for the structure sheaf is* 0*), with an exceptional point O.*

5.3.1 Group structure

Any elliptic curve $(\mathcal{E}, O)$ moreover comes with a *group structure* which is commutative: i.e., it is an abelian variety. The group structure is such that $\mathcal{E}(L)$ is the abelian group generated by the L-points, subject to the relations that

1. Any three collinear points sum to 0. (If a line is tangent to the elliptic curve, the tangency point is counted twice.)
2. O is the identity.

Example: For example, it turns out that if a cubic curve in $\mathbb{P}^2_K$ has a K-rational point, then it defines an elliptic curve. It is not hard to see the group structure is well-defined for cubics (because a line generically intersects a cubic three times). The hard part is associativity, but we will not prove this. For example, with any cubic of the form $X^3 + Y^3 + dZ^3 = 0$, we may pick $(1, -1, 0)$ as the identity element. In fact, making the change of coordinates

$$X_1 = -6dZ \quad Y_1 = 18d(X - Y) \quad Z_1 = (X + Y)/2$$

we get our cubic into the standard Weierstrass form

$$Y_1^2 Z_1 = X_1^3 - 2^4 3^3 d^2 Z_1^3$$

5.3.2 The Jacobian

In general, a cubic curve may not have a K-rational point (for example, Selmer's curve does not), and so may not have the structure of an elliptic curve. However, the situation is not so grim - it turns out that if $\mathcal{D}$ is any curve of genus 1 over $\mathbb{Q}$, then we can construct an elliptic curve $\mathcal{C}$ over $\mathbb{Q}$, along with a birational map $\mathcal{D} \to \mathcal{C}$. More of the structure of $\mathcal{C}$ is described in [3], chapter 20. $\mathcal{C}$ is called the *Jacobian* of $\mathcal{D}$ (because it turns out that it, miraculously, parametrizes line bundles over $\mathcal{C}$ with degree 0).

5.3.3 Companion Curves and the Tate-Shafarevich Group

Let A be an abelian variety over $\mathbb{Q}$. Now the cohomology $H^1(G_{\mathbb{Q}}, A(\overline{\mathbb{Q}}))$ is a *group*, and parametrizes equivalence classes of principal homogeneous spaces over A. If $A = \mathcal{E}$ is an elliptic curve, then this group consists of genus one curves with a principal homogeneous action of $\mathcal{E}(\overline{\mathbb{Q}})$. These curves must have genus one because a principal homogeneous action determines a birational map $\mathcal{E} \to \mathcal{D}$, and birational maps preserve genus. The group $H^1(G_{\mathbb{Q}}, \mathcal{E}(\overline{\mathbb{Q}}))$ is called the *Weil-Châtelet group*.

More concretely: given a cocycle representing $\mathcal{D}$, recall from the section on cohomology that $\mathcal{D}$ is constructed by 'twisting' the action of $G_{\mathbb{Q}}$. In other words, $\mathcal{D}(\overline{\mathbb{Q}})$ and $\mathcal{E}(\overline{\mathbb{Q}})$ are abstractly isomorphic, but not isomorphic as $G_{\mathbb{Q}}$-modules, and therefore, can have different K-points for K a finite extension of $\mathbb{Q}$! In some sense, the Jacobian can be thought of as the 'untwisted' version of the genus one curve. In Selmer's example, the last of the five curves was the Jacobian.

As we did before with $\mathrm{Aut}_{\mathcal{C}}$, we can consider the group

$$\ker(H^1(G_{\mathbb{Q}}, \mathcal{E}(\overline{\mathbb{Q}})) \to \prod_v H^1(G_{\mathbb{Q}_v}, \mathcal{E}(\overline{\mathbb{Q}})))$$

This group is called the *Tate-Shafarevich group* and is denoted $Ш(\mathcal{E}/\mathbb{Q})$. It parametrizes the set of isomorphism classes over $\mathbb{Q}$ of companion curves $\mathcal{C}$ of $\mathcal{E}$ endowed with the additional structure of a principal homogeneous group action $\mathcal{E} \times \mathcal{C} \to \mathcal{C}$. It is easy to see that this is an abelian group, being the kernel of a homomorphism of abelian groups. The following conjecture is a source of much current research:

Conjecture: (Tate-Shafarevich) For any abelian variety A over $\mathbb{Q}$, $Ш(A/\mathbb{Q})$ is finite.

$Ш(A/\mathbb{Q})$ is closely related to the set of companions: $Ш(A/\mathbb{Q})$ provides more resolution among the companion varieties, because there is the additional structure of a principal homogeneous action associated to each element. So proving the finiteness of $Ш(A/\mathbb{Q})$ would show that the Hasse principle fails *only up to finite obstruction* (i.e., that there are only finitely many companions). But $Ш(A/\mathbb{Q})$ is nicer in that there is a group structure.

6 Another direction - Algebraic Groups

Let K be a global field, and let $\mathbb{G}$ be an algebraic group defined over K (for example, the algebraic group of automorphisms of a variety). We could ask: *for what K and what $\mathbb{G}$ is the map $H^1(K, \mathbb{G}) \to \prod_v H^1(K_v, \mathbb{G})$ injective?* It has been shown that

Theorem 6.1. *(Kneser and others) If $\mathbb{G}$ is a simply connected algebraic group over a global field K, then the map above is injective.*

Theorem 6.2. *(Kneser and others) If $\mathbb{G}$ is a connected semisimple algebraic group and K is a number field, then the map above is surjective.*

A proof is given in [5]. This result is used in proofs of strong approximation (which asks for which algebraic groups $\mathbb{G}$ is $\prod_{s \in S} G(K_s)$ dense in $G(\mathbb{A}_K)$, for S a finite set of places), and computations of Tamagawa numbers of algebraic groups. This is a rich and fascinating direction for research, but unfortunately, one I didn't have time to explore too deeply. Giving these results justice is well beyond the scope of this project, but is a natural extension!

References

[1] W. Aitken, F. Lemmermeyer, *Counterexamples to the Hasse Principle: An Elementary Introduction*

[2] A. Borel, G. D. Mostow, *Algebraic Groups and Discontinuous Subgroups*, Symposium on Algebraic Groups, Boulder, Colorado, 1965

[3] J. W. S. Cassels, *Lectures on Elliptic Curves*

[4] J. W. S Cassels, A. Frohlich, *Algebraic Number Theory*

[5] M. Kneser, *Lectures on Galois Cohomology of Classical Groups*

[6] T. Y. Lam, Introduction to Quadratic Forms overs Fields

[7] B. Mazur, *On the Passage from Local to Global in Number Theory*

[8] O. T. O'Meara, *Introduction to Quadratic Forms*

[9] J. P. Serre, *A Course in Arithmetic*

[10] J. P. Serre, *Galois Cohomology*

[11] J. Silverman, *The Arithmetic of Elliptic Curves*