Quadratic Forms, K-theory and Galois Cohomology

Oliver Daisey

May 2021

Abstract

We present an account of the basic theory of quadratic forms, central simple algebras over a field, and Milnor's K-theory, which culminates in a complete exposition of Alexander Merkurjev's 2006 proof of the norm residue homomorphism of degree two.

Contents

1 Introduction

This is a dissertation dedicated to studying the relationship between different areas of abstract algebra.

In 1970, John Milnor introduced for each field k a graded-commutative ring $K_*^M(k)$ called *Milnor's K-theory* in the hope to study the higher algebraic K-theory in the case of fields. The ring is built on the foundations of a sequence of groups called the *Milnor K-groups* $K_n^M(k)$ of the field k. It was already known that $K_0(k) = \mathbb{Z}$ and $K_1(k) = k^\times$. His definition was established from Matsumuto's computation of the K_2 of a field, which yields

$$K_2(k) = \frac{k^\times \otimes_{\mathbb{Z}} k^\times}{(a \otimes (1-a), a \in k^\times \setminus \{1\})}. \tag{1}$$

Milnor essentially took the relations on the tensor product $k^\times \otimes k^\times$ that define the group K_2 as the *only* relations on his K-theory. It was expected then that relationships to other parts of mathematics such as Galois cohomology and the Grothendieck-Witt ring of quadratic forms would emerge. In particular, he conjectured that there should be a canonical isomorphism

$$K_*^M(k)/2K_*^M(k) \to \mathrm{gr}_{I^\bullet}(k) \tag{2}$$

from Milnor K-theory mod 2, to the graded Witt ring of quadratic forms. Indeed, this conjecture would eventually be proved in 1997 by V. Voevodsky, who also in 2008 completed the proof of the *norm residue isomorphism theorem* (also known as the Bloch-Kato conjecture): For each $n \in \mathbb{N}$ and prime $l \in \mathbb{N}$, there is a canonical isomorphism

$$K_n^M(k)/l \to H_{et}^n\left(k, \mu_l^{\otimes n}\right) \tag{3}$$

from the nth Milnor K-group mod l to the nth Étale cohomology group. The work he did to reach this result earned him the Fields medal in 2002.

Further back in 1981, Alexander Merkurjev proved the following special case of Milnor's conjecture: For every field k of characteristic not 2, the *norm residue homomorphism*

$$h_k : K_2(k)/2K_2(k) \to \mathrm{Br}_2 k \tag{4}$$

taking the class of a symbol $\{a, b\}$ to the class of the quaternion algebra $(a, b)_k$ is an isomorphism. His initial proof of this result involved reducing the problem to the study of a function field of a conic curve and applying results of the higher K-theory of this curve. Much later in 2006, Merkurjev offered a proof of this result that avoids the use of higher K-theory, instead relying on the exactness of the sequence

$$K_2 k \longrightarrow K_2 k(C) \xrightarrow{\partial} \bigoplus_{p \in C} \kappa(p)^\times \xrightarrow{N} k^\times \tag{5}$$

with C a projective conic curve over k, and $\kappa(p)$ the residue field at the scheme-theoretic point p. One purpose of this dissertation is to retell the story of this newer proof in more elementary terms, starting with the basic notions of quadratic forms and central simple algebras, and culminating with a complete proof of the *norm residue isomorphism theorem* in degree 2.

Section 1 of the dissertation is this introduction. Section 2 is a treatment of the theory of quadratic forms over a field of characteristic not 2. The aim is to reach the definition of the graded Witt ring, from which it is possible to state the isomorphism between the former and Milnor K-theory mod 2. Section 3 introduces the notion of finite-dimensional central simple algebras over a field, including some aspects of Artin-Wedderburn theory and the definition of the Brauer group of central simple algebras. We also introduce generalised quaternion algebras and their tensor products, and carefully study certain constructions derived from these algebras. It looks carefully at the algebraic geometry of these algebras, in preparation for the proof of the norm residue isomorphism theorem in degree 2. Section 4 finally introduces Milnor's K-theory, by stating the appropriate definitions and illustrating some of the associated maps on the ring. A particular highlight is the isomorphism between the second Milnor K-group mod 2 and its image in the graded Witt ring, which provides a foundation for the profound connection between Milnor K-theory and quadratic forms. Finally, Section 5 provides a lengthy treatment of an exact sequence on Milnor K-theory and a variant of Hilbert Theorem 90 for Milnor K-theory, which serve as cornerstones for Merkurjev's proof, and ultimately combines these results into a complete proof of the norm residue isomorphism theorem in degree two. This section certainly contains the main result of this dissertation. Section 6 concludes the report with a summary of the material and a brief discussion of mathematics one can study which builds on the topics of the dissertation.

In terms of background, a mastery of basic abstract algebra is essential, since to make arguments shorter I assume complete fluency with common algebraic tricks. I also use routine facts from linear algebra without much comment. A postgraduate with a specialisation in algebra should be able to follow along with this dissertation relatively seamlessly. I myself come from a background in commutative algebra, and so I wrote this dissertation expecting the reader to be completely familiar with group and ring theory, commutative algebra (on the level of Atiyah-Macdonald), basic algebraic geometry up to the Riemann-Roch theorem for algebraic curves, and Galois theory. When noncommutative algebra is required, I develop the theory carefully in light of my own background.

I thank my supervisor Alexander Vishik who over the course of many meetings through the academic year 2020-2021 taught me new mathematics, elaborated on tricky aspects of the present material, and checked my work plenty of times. The advice he gave me will certainly stick with me throughout my mathematical career.

2 Quadratic Forms

I learned the theory of quadratic forms from lecture notes produced by my supervisor for a previous University of Nottingham course. This section is my account of the theory.

2.1 Definitions

Let k be a field of characteristic not equal to 2. We carry this assumption throughout the work, unless otherwise stated. This subsection is intended to swiftly cover the basic definitions and results in the theory of quadratic forms.

There are several equivalent ways to define a quadratic form over a vector space. In this dissertation, we insist that a quadratic form is the diagonal part of a symmetric bilinear form B_q on a finite-dimensional vector space V over k. Hence $B_q : V \times V \to k$ is a map such that such that

1. $B_q(u_1 + u_2, v) = B_q(u_1, v) + B_q(u_2, v)$,
2. $B_q(u, v_1 + v_2) = B_q(u, v_1) + B_q(u, v_2)$,
3. $B_q(\lambda u, v) = \lambda B_q(u, v) = B_q(u, \lambda v)$,
4. $B_q(u, v) = B_q(v, u)$

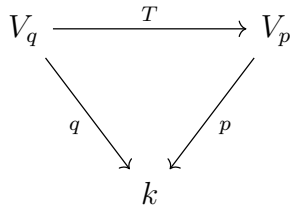
for all $u, v, u_1, u_2, v_1, v_2 \in V$ and $\lambda \in k$, and the corresponding quadratic form q on V is a map $q : V \to k$ such that for any $v \in V$ we have $q(v) = B_q(v, v)$. It is convenient in this discussion to refer to the pair (V, q) as a *quadratic space*, and when the underlying vector space is clear, simply denote the pair by q. We also occasionally slur the distinction between a quadratic space and a quadratic form; provided that the underlying vector spaces are fixed, this convention carries no risk of ambiguity. When we want to recover a quadratic space from a quadratic form q we denote the corresponding vector space by V_q. There is a one-to-one correspondence between quadratic and symmetric bilinear forms, given by

$$q(v) = B_q(v, v), \qquad B_q(u, v) = \frac{q(u + v) - q(u) - q(v)}{2}.$$

This justifies occasionally switching language between that of quadratic forms and that of symmetric bilinear forms.

Given two quadratic spaces (V_q, q) and (V_p, p), we would like to have a good notion of morphisms between them. We will henceforth call a linear map $T : V_q \to V_p$

a *morphism of quadratic spaces* if it makes the diagram



commutative. If we further assume that T is injective, we get the definition of an *isometric embedding* of (V_q, q) into (V_p, p). This notion of maps completes the definition of the category of quadratic spaces over k. For reference, an isomorphism of quadratic spaces is an isomorphism $T : V_q \to V_p$ such that $p \circ T = q$, and such a map is called an *isometry*. When we are considering quadratic forms without reference to the underlying vector space, we write $q \cong p$ if they are isometric.

We now seek a description of quadratic forms in coordinates. Fix a quadratic space (V, q). Since V is a finite-dimensional vector space, we may choose a basis $\mathcal{B} = \{e_1, e_2, \ldots, e_n\}$ for V. Let $u, v \in V$, and let $\overline{u} = (u_1, \ldots, u_n), \overline{v} = (v_1, \ldots, v_n)$ be the coordinates of u and v in this basis. Now the corresponding symmetric bilinear form B_q may be presented in this basis via

$$B_q(u, v) = \overline{u} \cdot A \cdot \overline{v}^t$$

where $A_{i,j} = B(e_i, e_j)$ is a symmetric matrix. What happens if we change bases? Let $\mathcal{B}' = \{e'_1, e'_2, \ldots, e'_n\}$ be a second basis for V, such that $(e_1, \ldots, e_n) \cdot C = (e'_1, \ldots, e'_n)$ for some invertible matrix C. Then, letting $\overline{v}, \overline{v}'$ denote the coordinates of v in the bases $\mathcal{B}$ and $\mathcal{B}'$ respectively, we have $\overline{v}^t = C \cdot (\overline{v}')^t$.

Lemma 1. *Two symmetric matrices A, A' represent isomorphic quadratic forms if and only if there exists an invertible matrix C such that $A' = C^t \cdot A \cdot C$.*

Proof. First, let A, A' represent isomorphic quadratic spaces $(V_q, q), (V_{q'}, q')$ so that in appropriate bases we may write

$$q(v) = \overline{v} \cdot A \cdot \overline{v}^t, \qquad q'(v') = \overline{v'} \cdot A' \cdot \overline{v'}^t$$

where $\overline{v}, \overline{v'}$ are the coordinates of vectors $v \in V_q$ and $v' \in V_{q'}$, and there exists an isomorphism $\phi : V_q \to V_{q'}$ such that

$$q(v) = q'(\phi(v)).$$

From the expressions for q and q' in these coordinates we get that

$$\overline{v} \cdot A \cdot \overline{v}^t = \overline{v'} \cdot A' \cdot \overline{v'}^t$$

where $v' = \phi(v)$. Now let C be the invertible matrix with column i given by $\phi(e_i)$ so that $C \cdot \overline{v}^t = \overline{v'}^t$. With this we have

$$\overline{v} \cdot A \cdot \overline{v}^t = \overline{v'} \cdot A' \cdot C \cdot \overline{v}^t.$$

Since this equation holds for all $\overline{v}^t$, we must have $\overline{v} \cdot A = \overline{v'} \cdot A' \cdot C$. Taking transposes, this implies $A \cdot \overline{v}^t = C^t \cdot A' \cdot \overline{v'}^t$ (note that $A = A^t$ and $A' = A'^t$.) Observing that $\overline{v'}^t = C \cdot \overline{v}^t$, we get that

$$A \cdot \overline{v}^t = C^t \cdot A' \cdot C \cdot \overline{v}^t$$

Since this holds for all $\overline{v'}^t$, we conclude

$$A = C^t \cdot A' \cdot C$$

as required. The converse result is established similarly. □

Letting A, A', C as in Lemma 1, we have

$$\det(A') = \det(A) \cdot \det(C)^2.$$

which permits us to make the following definition: Let (V, q) be a quadratic space. Let A be the matrix representing the quadratic form in a given basis for V. Define the *determinant* $\det(q)$ as $\det(A)$. For this to not depend on the choice of matrix A then we need to consider $\det(q)$ as an element of $k^\times/(k^\times)^2 \cup \{0\}$, where $k^\times/(k^\times)^2$ is the quotient group of the multiplicative group $k^\times$ of the field by the subgroup of squares. If $\det(q) = 0$ then we say that q is *degenerate*.

There is a notion of subobjects in the category of quadratic spaces. Let (V_q, q) be a quadratic space. Suppose (V_p, p) is another quadratic space such that $V_p \subseteq V_q$ is a vector subspace of V_q, and $p = q|_{V_p}$ is the restriction of q to V_p. We then say that (V_p, p) is a *quadratic subspace* of (V_q, q). We often abuse language and just say that p is a subform of q. Within a fixed quadratic space we may take complements, so define the *orthogonal complement* $p^\perp$ to p inside q to be the quadratic subspace $((V_p)^\perp, q|_{(V_p)^\perp})$, where we define $(V_p)^\perp \subset V_q$ to be the linear subspace consisting of all those $v \in V_q$ such that $B_q(u, v) = 0$ for any $u \in V_p$, and $q_{(V_p)^\perp}$ is the restriction of q to this subspace. We may take the orthogonal complement of a quadratic space within itself; we call the orthogonal complement $(V^\perp, 0)$ of (V, q) in itself the *radical* of (V, q).

The notion of orthogonal complements permits a second, equivalent definition to be made for nondegeneracy of forms:

Proposition 1. *A quadratic form q on a vector space V is nondegenerate if and only if the radical of V is trivial.*

Proof. Suppose that q is degenerate. Then letting A be the matrix of the symmetric bilinear form corresponding to q in some basis $\mathcal{B}$ for V, we have $\det(A) = 0$. Hence there exists nonzero $v_0 \in V$ such that $Av_0 = 0$, so that for any $v \in V$, we have

$$B_q(v, v_0) = \overline{v} A \overline{v_0}^t = 0.$$

Hence the orthogonal complement is not trivial. Conversely, suppose q is nondegenerate. Then $\det(A) \neq 0$, meaning A is nonsingular and hence for any $v \in V$ we must have $Av \neq 0$. Hence, letting $n = \dim V$, there exists some $1 \leq i \leq n$ such that the ith coordinate of v in the basis $\mathcal{B}$ is nonzero. Then the corresponding basis element $e_i \in \mathcal{B}$ satisfies

$$B_q(e_i, v) = \overline{e_i} A \overline{v}^t \neq 0.$$

So the orthogonal complement is trivial. □

Note that if (V, q) is a quadratic space with q nondegenerate, then any morphism out of (V, q) is an isometric embedding. This is easy to see directly, for given a quadratic space (W, p), a morphism $T : V \to W$ and any $v, v' \in V$ with $T(v) = 0$,

$$0 = B_p(0, T(v')) = B_p(T(v), T(v')) = B_q(v, v').$$

Hence v belongs to the radical of V which is trivial by nondegeneracy. Hence $v = 0$.

2.2 Operations on quadratic forms

The category of quadratic spaces admits direct sums and tensor products as follows. Given quadratic spaces $(V_q, q), (V_p, p)$ with B_q, B_p the corresponding symmetric bilinear forms to q and p respectively:

1. We define $(V_q, q) + (V_p, p)$ as the quadratic space $(V_q \oplus V_p, q \perp p)$, where the form $q \perp p$ by definition has corresponding symmetric bilinear form

$$B_{q \perp p}((x_1, y_1), (x_2, y_2)) := B_q(x_1, x_2) + B_p(y_1, y_2). \tag{6}$$

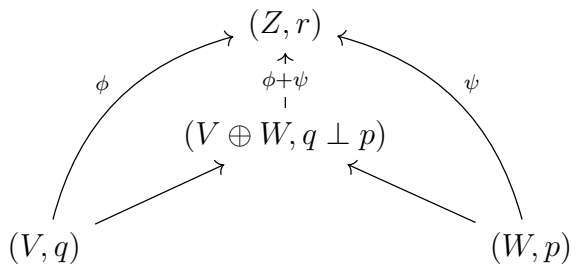
   Alternative notations include $(V_q, q) \perp (V_p, p)$ or even just $q \perp p$ or $q + p$ when the underlying vector spaces are clear. We call this the *orthogonal sum* of the forms q and p.

2. We define $(V_q, q) \otimes (V_p, p)$ as the quadratic space $(V_q \otimes V_p, q \otimes p)$, where again $q \otimes p$ is the quadratic form with corresponding symmetric bilinear form whose action on elementary tensors is given by

$$B_{q \otimes p}(x_1 \otimes y_1, x_2 \otimes y_2) = B_q(x_1, x_2) \cdot B_p(y_1, y_2) \tag{7}$$

with which the bilinear form is determined uniquely on the tensor product, by linearity. We call this the *tensor product* of the forms p and q. It is sometimes the case that we denote the product of forms $q \otimes p$ by qp.

One can easily show that the orthogonal sum is indeed a coproduct in the sense that it satisfies the following universal property: Given quadratic spaces (V, q) and (W, p), there are isometries $(V, q) \to (V \oplus W, q \perp p)$ and $(W, p) \to (V \oplus W, q \perp p)$ such that for any pair of isometries $\phi : (V, q) \to (Z, r)$, $\psi : (W, p) \to (Z, r)$, there exists a unique isometry $\phi + \psi : (V \oplus W, p \perp q) \to (Z, r)$ that makes the diagram



commute. The isometries $(V, q) \to (V \oplus W, q \perp p)$ and $(W, p) \to (V \oplus W, q \perp p)$ are simply those induced by the natural vector space inclusions $V \to V \oplus W$, $W \to V \oplus W$ respectively.

2.3 Diagonalisation of quadratic forms

We can take an arbitrary quadratic space and decompose it into the direct sum of a nondegenerate quadratic space with a quadratic subspace whose form is trivial. Such a decomposition is easy to construct: Let (V_q, q) be a quadratic space, and let $V_q^\perp$ be the radical of V_q. Now let $W \subset V_q$ be any linear complement to $V_q^\perp$. Then we call the quadratic space $(W, q|_W)$ the *nondegenerate part* of q. The left over part $(V_q^\perp, 0)$ is the radical of q. Note that this decomposition is seemingly not canonical since our choice of linear complement W was arbitrary, but the following lemma will show that this choice does not matter:

Proposition 2. *1.* $(V_q, q) = (V_q^\perp, 0) + (W, q|_W)$.

2. The quadratic space $(W, q|_W)$ *is nondegenerate.*

3. The quadratic space $(W, q|_W)$ *does not depend on the choice of* W *(up to unique isomorphism.)*

Proof. 1. By the definition of the linear complement we have that $V_q^\perp \oplus W = V_q$. So we just need to show that the canonical isomorphism $V_q^\perp \oplus W \to V_q$ preserves

the form. Let $(v, w) \in V_q^\perp \oplus W$, then

$$B_{0 \perp q|_W}((v,w),(v,w)) = B_0(v,v) + B_{q|_W}(w,w) = B_q(w,w) = q(w).$$

On the other hand,

$$\begin{aligned} q(v+w) = B_q(v+w, v+w) &= B_q(v,v) + B_q(w,w) + 2B_q(v,w) \\ &= B_q(w,w) = q(w) \end{aligned}$$

since v is orthogonal to everything.

2. By virtue of Proposition 1 we just need to show that the radical of $(W, q|_W)$ is trivial. Let $w \in W^\perp$. Then for any $w' \in W$ we have

$$B_q(w, w') = 0.$$

Furthermore for every $v \in V_q^\perp$ we have $B_q(w, v) = 0$ by definition. So for every $v \in V_q$ we have $B_q(w, v) = 0$, which implies $w \in V_q$. But $V_q \cap W = 0$, which implies $w = 0$.

3. Suppose we have two different choices of linear complement for W. Let us denote them by W_1 and W_2. Then we have the following decompositions for $V_q^\perp$:

$$W_1 \oplus V_q^\perp = V_q = W_2 \oplus V_q^\perp. \tag{8}$$

By inclusion and projection, this induces the following sequence of maps:

$$W_1 \longrightarrow V_q \xrightarrow[\phi]{} W_2, \quad W_2 \longrightarrow V_q \xrightarrow[\psi]{} W_1. \tag{9}$$

One easily verifies that $\phi\psi = \mathrm{id}_{W_1}$ and $\psi\phi = \mathrm{id}_{W_2}$. So we have a canonical isomorphism of vector spaces. We just need to show that quadratic forms are preserved by ϕ, ψ.

Let $w_1 \in W_1$. Then by the inclusion $W_1 \to V_q = W_2 \oplus V_q^\perp$, we may write $w_1 = \phi(w_1) + u$ for some $u \in V_q^\perp$. Hence $q(\phi(w_1)) = q(w_1) - 2B_q(w_1, u) + q(u) = q(w_1)$ since $u \in V_q^\perp$ is orthogonal to every vector. So ϕ is an isomorphism of quadratic spaces.

□

Degeneracy of a quadratic form may also be characterised in terms of how non-injective the corresponding symmetric bilinear form is as a linear map into the dual space. A perfectly nondegenerate quadratic form will yield an isomorphism, as we

now show: Let (V_p, p) be a quadratic space. Then p defines a linear map $f : V_p \to V_p^*$ (here V_p^* is the vector dual space to V_p) given by $v \mapsto B_p(v, -)$, where the image we consider as a $k-$linear map from V_p to k, and call a *linear functional* on V_p. When this map is an isomorphism, the form p is nondegenerate, since only 0 maps to the zero map in V_p^*, and so only $0 \in V_p$ is such that $B_p(v, u) = 0$ for every $u \in V_p$. Conversely, if p is nondegenerate, then the only vector $v \in V_p$ such that $B_p(v, u) = 0$ for every $u \in V_p$ is the zero vector, so the map f is injective. Hence f is also surjective by equality of dimensions, and so f is an isomorphism. Thus we obtain another characterisation of nondegenerate quadratic forms: A quadratic form is nondegenerate if and only if the map f is an isomorphism. In particular, in the nondegenerate case, every linear functional on V_p may be realised as the dual of some $v \in V_p$.

Proposition 3. *Suppose that $p \subset q$ is a nondegenerate subform. Then*

$$q = p + p^{\perp}.$$

This proposition means that nondegenerate subforms always exist as direct summands.

Proof. Let $\phi : V_p \oplus V_{p^\perp} \to V_q$ be the canonical map (so that $\phi(v, v') = v + v'$). We will show that ϕ is an isomorphism. Injectivity is equivalent to $V_p \cap V_{p^\perp} = 0$, which is equivalent to p being nondegenerate. To show surjectivity, let $v \in V_q$, and define $v^* = B_q(v, -) \in V_p^*$. By the above discussion with the fact that p is nondegenerate, we get an identification of V_p with V_p^*, and hence v^* corresponds to some $u \in V_p$. By the construction, it means that $B_q(v, -) = B_q(u, -)$ as linear functionals on V_p. This means that $B_q((v - u), -)$ is the zero map. Hence $(v - u) \in V_p^{\perp}$. So we have $v = u + (v - u) = \phi(u, v - u)$, and hence we have shown surjectivity. Therefore ϕ is an isomorphism of vector spaces.

We just need to show that forms are preserved by ϕ now. Since

$$q(\phi(u, w)) = q(u) + 2B_q(u, w) + q(w) = q(u) + q(w) = (p + p^{\perp})(u, w),$$

this is indeed the case. □

Let $0 \neq v \in V_q$. We say that v is *isotropic* if $q(v) = 0$. Otherwise we say that v is *anisotropic*. We say that the form itself, q, is *anisotropic* if the corresponding vector space V_q has no nonzero isotropic vectors. This definition permits the following: If $v \in V_q$ is an arbitrary isotropic vector, and if we let $l(v)$ denote the line in V_q spanned by v, the quadratic space (V_q, q) decomposes as

$$(V_q, q) = (l(v), q|_{l(v)}) + (l(v)^{\perp}, q|_{l(v)^{\perp}}).$$

The reason for this is clear; we can use Proposition 3 as long as we know $(l(v), q|_{l(v)})$ is nondegenerate, which is indeed the case, since this is equivalent to $q(v) \neq 0$. We now turn to an important structure theorem for quadratic forms.

Theorem 1. *Any quadratic form is diagonalisable - that is, may be written as an orthogonal sum of one-dimensional quadratic forms.*

Proof. We use induction on $\dim(q)$. Clearly the theorem holds for $\dim(q) = 0$. Now let n be some nonnegative integer, and suppose $\dim(q) = n+1$, and that the theorem holds for $\dim(q) \leq n$. Further assume that $q \neq 0$, for otherwise such a decomposition is trivial. Then there exists $v \in V_q$ such that $q(v) \neq 0$. Now use the above discussion to write

$$(V_q, q) = (l(v), q|_{l(v)}) + (l(v)^\perp, q|_{l(v)^\perp})$$

and apply the inductive hypothesis to the form $(l(v)^\perp, q|_{l(v)^\perp})$, which has dimension less than or equal to n. □

We now introduce some new notation. Let us denote the one-dimensional quadratic space $(k, a \cdot x^2)$ by $\langle a \rangle$, and the direct sum $\langle a_1 \rangle + \langle a_2 \rangle + \cdots + \langle a_n \rangle$ by $\langle a_1, a_2, \ldots, a_n \rangle$. We call this the *diagonal decomposition* of a quadratic form. Of course, this needn't be unique. For example, we have $\langle a \rangle = \langle ab^2 \rangle$.

The diagonal presentations behave well under sums and products. We have for orthogonal sums

$$\langle a_1, \ldots, a_n \rangle + \langle b_1, \ldots, b_n \rangle = \langle a_1, \ldots, a_n, b_1, \ldots, b_n \rangle$$

and for tensor products,

$$\langle a_1, \ldots, a_n \rangle \cdot \langle b_1, \ldots, b_n \rangle = \langle a_1 b_1, \ldots, a_1 b_n, a_2 b_1, \ldots, a_2 b_n, \ldots, a_n b_n \rangle.$$

2.4 Orthogonal group & Witt cancellation

Now suppose that q is a nondegenerate quadratic form over a field k., so that k-endomorphisms of quadratic spaces (V_q, q) are isometric embeddings (and hence isometries). We call such a k-endomorphism $\phi : V \to V$ *orthogonal*. If we choose a basis $\mathcal{B}$ for V and for $v \in V$ write $\overline{v} = (v_1, v_2, \ldots, v_n)$ in this basis, then letting B, C be the matrices representing B_q, ϕ in this basis respectively, the orthogonality condition translates to

$$\left(\overline{v^t} \cdot C\right) \cdot B \cdot \left(C^t \cdot \overline{v}\right) = \overline{v^t} \cdot B \cdot \overline{v} \tag{10}$$

which means $C \cdot B \cdot C^t = B$. Along with the facts that inverse isometries are also orthogonal transformations and the composition of two orthogonal transformations is an orthogonal transformation, we deduce that the set of all orthogonal transformations on V_q form a group with respect to composition. We call this group the *orthogonal group* $O(q)$, and it is a subgroup of the general linear group $GL(V_q)$.

A particularly simple class of element of this group are the so called *elementary reflections*, defined for each anisotropic $w \in V_q$ by

$$\begin{aligned} \tau_w : V_q &\to V_q \\ v &\mapsto v - \frac{2B_q(w,v)}{q(w)} \cdot w. \end{aligned}$$

The following proposition shows that τ_w is indeed a reflection.

Proposition 4. *Let (V_q, q) be a nondegenerate quadratic space. Let $w \in V_q$ be anisotropic, and let τ_w denote the elementary reflection associated to w. Then τ_w is an orthogonal transformation of order 2, with $\tau_w(w) = -w$. Furthermore, τ fixes a hyperplane.*

Proof. We first show τ_w is orthogonal. Let $v \in V_q$. Then

$$\begin{aligned} q\left(v - \frac{2B_q(w,v)}{q(w)} \cdot w\right) &= q(v) - \frac{4(B_q(w,v))^2}{q(w)} + \frac{4(B_q(w,v))^2}{(q(w))^2} \cdot q(w) \\ &= q(v). \end{aligned}$$

The fact that it has order 2 is a calculation of similar style.We have

$$\tau_w(w) = w - \frac{2q(w)}{q(w)} \cdot w = -w.$$

And finally, since $\tau_w(v) = v$ is equivalent to $B_q(w,v) = 0$, and w is anisotropic, all such vectors v form a hyperplane.

□

We now seek to use elementary reflections to prove a fundamental theorem in the theory of quadratic forms, but we need to establish some intermediate results, the first of which is the lemma that states that we may transport two nonzero vectors onto each other by a pair of elementary reflections, provided they are sent to the same nonzero scalar by q. If their difference is anisotropic then one reflection suffices:

Lemma 2. *Let $u, v \in V_q$ be nonzero, and suppose $q(u) = q(v)$ but not 0. Then there exists anisotropic $w \in V_q$ such that $\tau_w(u) = \pm v$. Furthermore, if $u - v$ is anisotropic, then there exists $w \in V_q$ such that $\tau_w(u) = v$.*

Proof. Since $q(v-u)+q(v+u) = 2(q(v)+q(u)) = 4q(u) \neq 0$, one of $v-u, v+u$ must be anisotropic. Denote the anisotropic vector by w. Then

$$\begin{aligned}\tau_w(u) = u - \frac{2B_q(w,u)}{q(w)}w &= u - \frac{2B_q((v\pm u),u)}{B_q(v\pm u, v\pm u)}(v\pm u)\\ &= u - \frac{2(B_q(v,u)\pm B_q(u,u))}{B_q(v,v)+B_q(u,u)\pm 2B_q(v,u)}(v\pm u)\\ &= u \mp \frac{2(B_q(v,u)\pm B_q(u,u))}{2(B_q(v,u)\pm B_q(u,u))}(v\pm u)\\ &= u \mp (v\pm u) = \mp v.\end{aligned}$$

If $v-u$ is anisotropic, just take $w = v-u$ and then $\tau_w(u)$ will be equal to v. □

We can extend this idea further in the following theorem, which shows that *any* orthogonal transformation is composed of a sequence of elementary reflections of finite length.

Theorem 2. *Let (V_q, q) be a nondegenerate quadratic space with $\dim V_q = n$. Let $\phi \in O(q)$ be an orthogonal transformation. Then there is a sequence of anisotropic vectors $v_1, \ldots, v_m \in V_q$ with $1 \leq m \leq 2n$ such that $\phi = \tau_{v_1} \circ \cdots \circ \tau_{v_m}$. Moreover, if q is anisotropic, then $m \leq n$.*

Proof. Induction. For $n = 0$, there is nothing to prove. Next, suppose $n \in \mathbb{N}$ is such that the statement is true for all $k < n$. We are assuming q is nondegenerate, so there exists $x_1 \in V_q$ such that $q(x_1) \neq 0$. Since ϕ is orthogonal, $q(\phi(x_1)) = q(x_1)$. Now using Lemma 2, there exists $v_1 \in V_q$ such that $\tau_{v_1}(\phi(x_1)) = \pm x_1$. If the sign is a plus, then put $\psi = \tau_{v_1} \circ \phi$. Otherwise take $v_2 = x_1$, and set $\psi = \tau_{v_2} \circ \tau_{v_1} \circ \phi$.

In either case, ψ an orthogonal transformation satisfying $\psi(x_1) = x_1$, so that the line $l = k \cdot x_1$ is stable under ψ, and hence $l^\perp$ is also stable. But $\dim l^\perp = n-1$, and so the inductive hypothesis implies that there exists $v_3, \ldots, v_m \in l^\perp$ with $3 \leq m \leq 2n$ such that $\psi|_{l^\perp} = \tau_{v_3}|_{l^\perp} \circ \cdots \circ \tau_{v_m}|_{l^\perp}$. We have $\tau_{v_3}|_l \circ \cdots \circ \tau_{v_m}|_l = id_l = \psi|_l$. Because $V_q = l \oplus l^\perp$, we conclude $\psi = \tau_{v_3} \circ \cdots \circ \tau_{v_m}$. Then either $\phi = \tau_{v_1} \circ \tau_{v_2} \circ \psi$, or $\phi = \tau_{v_1} \circ \phi$, so that ϕ is a product of no more than $2n$ elementary reflections.

For the second part, notice that if q is anisotropic, in the induction step in the argument above, we have that $\phi(x_1) - x_1$ is either zero or anisotropic, so that we can take ψ equal to either ϕ or $\tau_{(\phi(x_1)-x_1)} \circ \phi$ respectively. Passing over from the $n-1$ case to the n case, we get at most one extra reflection. So the total number cannot be more than n. □

We now reach our key theorem of this subsection:

Theorem 3. *(Witt Cancellation.) Let p, q_1, q_2 be quadratic forms such that*

$$q_1 \perp p \cong q_2 \perp p.$$

Then $q_1 \cong q_2$.

Proof. We may assume without loss of generality that $\dim p = 1$, since over a field of characteristic not 2 every quadratic form is diagonalisable. We will show the proposition in the case that q_1, q_2 and p are nondegenerate. Then since $(q_1 \perp p)_{nondeg} = {q_1}_{nondeg} \perp p_{nondeg} = (q_2 \perp p)_{nondeg} = {q_2}_{nondeg} \perp p_{nondeg}$, Witt Cancellation in this case gives that ${q_1}_{nondeg} = {q_2}_{nondeg}$. And since $q_1 = {q_1}_{nondeg} \perp (U, 0)$ and $q_2 = {q_2}_{nondeg} \perp (V, 0)$ with $\dim U = \dim V = \dim q_1 - \dim {q_1}_{nondeg}$, the two forms q_1, q_2 are isomorphic.

Now the proof; since p is nondegenerate, we can write $p = \langle a \rangle$ for some $a \in k^\times$. Let us write $q_1 \perp p = r = q_2 \perp p$. Let $j_1 : p \hookrightarrow r$ and $j_2 : p \hookrightarrow r$ be the respective inclusions of p into r induced by the two decompositions above. Further, let $j_1(V_p) = l_1 \subset V_r$ and $j_2(V_p) = l_2 \subset V_r$. By our initial assumption that $\dim p = 1$, these are one dimensional subspaces. There exist $x_1 \in l_1$, $x_2 \in l_2$ with $r(x_1) = r(x_2) = a$, and $r|_{l_1^\perp} \cong q_1, r|_{l_2^\perp} \cong q_2$. Hence by Lemma 2, there exists anisotropic $w \in V_r$ with $\tau_w(x_1) = \pm x_2$. We have $\tau_w(l_1^\perp) = l_2^\perp$, and it is an orthogonal transformation, so it identifies $r|_{l_1^\perp} = q_1$ with $r|_{l_2^\perp} = q_2$. Hence $q_1 \cong q_2$. □

2.5 Hyperbolic forms

The canonical example of a quadratic form in linear algebra is the form corresponding to the Euclidean inner product on $\mathbb{R}^n$. One key feature of this form is that it is *positive-definite*, so in particular it is anisotropic. In the general theory of quadratic forms over a field, there may exist nonanisotropic subspaces, the simplest example of which being the *hyperbolic plane* $\mathbb{H}$ whose diagonal presentation is given by

$$\mathbb{H} = \langle 1, -1 \rangle.$$

Lemma 3. *Let q be a nondegenerate 2-dimensional quadratic form. The following are equivalent:*

1. $q \cong \mathbb{H}$,
2. *q is isotropic,*
3. $\det(q) = -1$.

Proof. $1 \implies 3$: Immediate.
$3 \implies 2$: Since $\det(q) = -1$, we must have that $q \cong \langle d, -d\rangle$ for some $d \in k^\times$. Then $(1, 1)$ is an isotropic nonzero vector.
$2 \implies 1$: Since q is diagonalisable, we may write $q = \langle a, -b\rangle$ for some $a, b \in k^\times$. Now isotropy implies there exists nonzero (x, y) such that $ax^2 - by^2 = 0$. Then both x and y are nonzero, and $a/b \in (k^\times)^2$. Hence $\langle a, -b\rangle \cong a \cdot \langle 1, -1\rangle$. Now we note that for any $\alpha \in k^\times$ the form $\langle \alpha, -\alpha\rangle = \alpha x^2 - \alpha y^2$ is isometric to xy. The corresponding isometry in coordinates is given by

$$x \mapsto \frac{x + \alpha y}{2\alpha}, \qquad y \mapsto \frac{x - \alpha y}{2\alpha}.$$

Indeed, we have

$$\begin{aligned}\alpha\left(\frac{x+\alpha y}{2\alpha}\right)^2 - \alpha\left(\frac{x-\alpha y}{2\alpha}\right)^2 &= \frac{x^2 + 2\alpha xy + \alpha^2 y^2 - x^2 + 2\alpha xy - \alpha^2 y^2}{4\alpha} \\ &= \frac{4\alpha xy}{4\alpha} = xy,\end{aligned}$$

and so our change of coordinates carries one form over to the other. In particular, this fact implies that $a \cdot \langle 1, -1\rangle \cong \langle 1, -1\rangle = \mathbb{H}$, which is what we wanted. □

We hence see that a (nondegenerate) 2-dimensional isotropic quadratic form is necessarily isometric to the hyperbolic plane. We now generalise this to higher dimensions.

Lemma 4. *Let q be a nondegenerate quadratic form. If q is isotropic, then $q = \mathbb{H} \perp q'$ for some quadratic form q'.*

Proof. Pick an isotropic nonzero vector $v \in V_q$; it is enough to show there exists an embedding $\mathbb{H} \subset q$ such that $v \in V_{\mathbb{H}}$. Since q is nondegenerate, there exists $u \in V_q$ with $B_q(u, v) \neq 0$. Hence u, v are linearly independent, and so generate a two dimensional subspace $U \subset V_q$. Let M be the matrix of the restriction $q|_U$ in the basis $\mathcal{B} = \{u, v\}$. Then

$$M = \begin{pmatrix} 0 & B_q(u, v) \\ B_q(u, v) & q(u) \end{pmatrix}. \tag{11}$$

A direct calculation shows this form is nondegenerate and isotropic. Hence it is isomorphic to $\mathbb{H}$ by Lemma 3. By the construction, $v \in U = V_{\mathbb{H}}$. □

We now introduce an invariant of quadratic spaces which measures in a suitable sense the "degree of isotropy". We say that a subspace consisting entirely of isotropic vectors is called a *totally isotropic* subspace. To describe the maximal size of a totally isotropic subspace we use the following proposition:

Proposition 5. *Let q be a nondegenerate quadratic form. The following conditions are equivalent:*

1. *V_q contains a totally isotropic subspace of dimension m.*
2. *$q = (\perp_{i=1}^{m} \mathbb{H}) \perp q''$ for some quadratic form q''.*

Proof. First, suppose $q = (\perp_{i=1}^{m} \mathbb{H}) \perp q''$. Let us write the corresponding symmetric bilinear form $B_{\perp_{i=1}^{m}\mathbb{H}}$ as $x_1y_1 + \cdots + x_my_m$ for an appropriate choice of basis. Clearly the $m-$dimensional subspace $y_1 = \cdots = y_m = 0$ of $V_{\perp_{i=1}^{m}\mathbb{H}}$ is totally isotropic, and since $V_{\perp_{i=1}^{m}\mathbb{H}} \subset V_q$, the latter contains a totally isotropic subspace of dimension m.

For the other direction, we use induction on m. For $m = 0$ there is nothing to prove. Now suppose that V_q contains contains an m dimensional totally isotropic subspace U. Let $u \in U$ be nonzero, and let $L = k \cdot u$ be the line spanned by u. By Lemma 4, we get an embedding $\mathbb{H} \subset q$ with $u \in V_{\mathbb{H}}$. Then, since q is nondegenerate, we have $q = \mathbb{H} \perp q'$ where q' is the orthogonal complement to $\mathbb{H}$ inside q. We have that q' is nondegenerate, and $V_{q'} = (V_{\mathbb{H}})^{\perp} \subset L^{\perp}$. But on the other hand, $L^{\perp} \supset U^{\perp} \supset U$, since any two $v, w \in U$ are orthogonal, so $V_{q'}$ and U are both subspaces of $L^{\perp}$. Since $\dim(q') = \dim(q) - \dim(\mathbb{H}) = \dim(q) - 2$ and $\dim(L^{\perp}) = \dim(q) - \dim(L) = \dim(q) - 1$, $V_{q'}$ has codimension 1 in $L^{\perp}$. Since the codimension of $V_{q'} \cap U$ inside U is not more than the codimension of $V_{q'}$ inside $L^{\perp}$, we get that $\dim(V_{q'} \cap U)$ is greater than or equal to $(m-1)$, so that in $V_{q'}$ we have a totally isotropic subspace of dimension at least $m-1$. Hence by the inductive assumption, $q' = (\perp_{i=1}^{m-1} \mathbb{H}) \perp q''$ for some quadratic form q''. Hence $q = \mathbb{H} \perp q' = (\perp_{i=1}^{m} \mathbb{H}) \perp q''$. □

We call the form $\perp_{i=1}^{m} \mathbb{H}$ a *hyperbolic form.* Therefore the "degree of isotropy" of the quadratic form q can be measured by the size of the hyperbolic form contained in it. Now we define the *Witt index* $i_W(q)$ of q as the maximal m such that $\perp_{i=1}^{m} \mathbb{H}$ is a direct summand of q. The form q_{an} such that $q = (\perp_{i=1}^{m} \mathbb{H}) \perp q_{an}$ is called the *anisotropic part* or *anisotropic kernel* of q. Of course, this form is anisotropic by Lemma 4 along with the maximality of m. By Witt Cancellation, the form q_{an} is uniquely determined up to isomorphism. And so to each quadratic form we have associated two invariants: The Witt index $i_W(q)$ and the anisotropic part q_{an}. The pair $(i_W(q), q_{an})$ determines the quadratic form q entirely, up to isomorphism. In this way we have "reduced" all nondegenerate forms to anisotropic ones, modulo a nonnegative integer.

2.6 Grothendieck group

Now we wish to construct a commutative ring whose elements are derived from the quadratic spaces over a given field. It is clear that isomorphism classes of quadratic

spaces over a fixed field with the orthogonal sum as an operation form a commutative monoid with the unique 0-dimensional quadratic space as the identity element. But nontrivial elements of this monoid do not have inverses, by dimension considerations. So in our endeavour to assemble a commutative ring of quadratic spaces, we need to somehow complete this monoid to an abelian group. Indeed, given an arbitrary commutative monoid M, one can produce an abelian group $G(M)$ called the *Grothendieck group* out of it in a universal way. Specifically, we define $G(M)$ as the group with a fixed morphism of monoids $i : M \to G(M)$ such that for any abelian group H and morphism of monoids $j : M \to H$, there exists a unique morphism of abelian groups $f : G(M) \to H$ that makes the following commute:

$$\begin{array}{ccc} M & \xrightarrow{i} & G(M) \\ & \searrow^{j} & \downarrow f \\ & & H \end{array}$$

So the Grothendieck group, if it exists, is the smallest abelian group containing M. It is an example of a *free functor* from the category of commutative monoids to the category of abelian groups.

Proposition 6. *The Grothendieck group exists for a given commutative monoid M, and is unique up to isomorphism.*

Proof. We construct the Grothendieck group as follows. Let G be the set of formal differences $[a]-[b]$, where $a, b \in M$. Now let $\sim$ be the equivalence relation defined by

$$[a]-[b] \sim [c]-[d] \iff \exists e \in M \text{ such that } a+d+e = b+c+e.$$

Now let $G(M)$ be the set of equivalence classes of G, with the group operation given by

$$([a]-[b])+([c]-[d]) := [a+c]-[b+d]$$

and inverse given by

$$-([a]-[b]) := [b]-[a].$$

One can check that these operations are well-defined and give $G(M)$ the structure of an abelian group. Then the natural map of monoids $i : M \to G(M)$ is given by $a \mapsto [a]-[0]$.

Let $j : M \to H$ be a morphism of monoids. Let $f : G(M) \to H$ be defined by $[a]-[b] \mapsto j(a)-j(b)$. This homomorphism does not depend on the choice of representatives, since if $[a]-[b] = [c]-[d]$ we have $a+d+e = b+c+e$ for some $e \in M$, so that $f([a]-[b]) - f([c]-[d]) = j(a)-j(b)-j(c)+j(d)+j(e)-j(e) =$

$j(a+d+e)-j(b+c+e) = 0$. And indeed, this choice of f makes the diagram commute.

Let us now show the group $G(M)$ is unique up to isomorphism. Suppose we have two such groups $G(M)$ and $G'(M)$ with natural maps $i : M \to G(M)$, $i' : M \to G'(M)$. Then by the universal property there exists unique homomorphisms $f : G(M) \to G'(M)$, $g : G'(M) \to G(M)$ that make the following commute:

$$\begin{array}{ccc} M & \xrightarrow{\ i\ } & G(M) \\ & \searrow^{i'} & \uparrow{\scriptstyle g} \quad \downarrow{\scriptstyle f} \\ & & G'(M) \end{array} \tag{12}$$

Now observe that the compositions $g \circ f = id_{G(M)}$ and $f \circ g = id_{G'(M)}$ by the universal property applied to the diagrams

$$\begin{array}{ccc} M & \xrightarrow{\ i\ } & G(M) \\ & \searrow^{i} & \uparrow{\scriptstyle id} \quad \downarrow{\scriptstyle id} \\ & & G(M) \end{array} \tag{13}$$

and

$$\begin{array}{ccc} M & \xrightarrow{\ i'\ } & G'(M) \\ & \searrow^{i'} & \uparrow{\scriptstyle id} \quad \downarrow{\scriptstyle id} \\ & & G'(M) \end{array} \tag{14}$$

and so the groups are isomorphic. □

We can characterise the injectivity of the natural map embedding M into $G(M)$ in the following lemma:

Lemma 5. *The natural map i introduced above is injective if and only if the commutative monoid M has the cancellation property, that is for any $a, b, e \in M$,*

$$a + e = b + e \implies a = b.$$

Proof. Suppose i is injective and $a, b, e \in M$ are such that $a + e = b + e$. Then $[a] - [0] = [b] - [0]$, so $i(a) = i(b)$. By injectivity, we have $a = b$.

Conversely, suppose M has the cancellation property. Let $a, b \in M$ and suppose $i(a) = i(b)$. Then $[a] - [0] = [b] - [0]$, which implies $a + e = b + e$ for some $e \in M$. Applying the cancellation property gives $a = b$. □

2.7 Witt ring of quadratic forms

Pulling back to quadratic forms, recall that isomorphism classes of quadratic spaces form a commutative monoid M with respect to the orthogonal sum operation $\oplus$. Furthermore, due to the Witt cancellation theorem, this monoid enjoys the cancellation property. Hence it embeds into its respective Grothendieck group. We denote the Grothendieck group of the monoid of isomorphism classes of quadratic spaces by $\widetilde{W}(k)$. On the set of isomorphism classes of quadratic spaces we have another associative, commutative operation given by the tensor product of quadratic spaces $\otimes$. This is compatible with the monoid structure M and thus induces an associative commutative operation on $\widetilde{W}(k)$, which provides the latter with the structure of a commutative ring, called the *Witt-Grothendieck ring of quadratic forms over k*. The multiplicative identity is the quadratic space $\langle 1 \rangle$. Now consider the element $[\mathbb{H}] - [0]$ in $\widetilde{W}(k)$. By virtue of M embedding into $\widetilde{W}(k)$, we can denote this element simply by $\mathbb{H}$. Let L denote the cyclic subgroup generated by $\mathbb{H}$.

Lemma 6. *The subgroup $L \subset \widetilde{W}(k)$ is an ideal.*

Proof. Let $[p]-[q] \in \widetilde{W}(k)$ be arbitrary. We need to show that $([p]-[q])\cdot\mathbb{H} \in L$. Since $([p]-[q]) \cdot \mathbb{H} = [p \cdot \mathbb{H}] - [q \cdot \mathbb{H}]$, and since $\langle a \rangle \cdot \mathbb{H}$ is a 2-dimensional isotropic form, by the proof of Lemma 3 we have $\langle a \rangle \cdot \mathbb{H} = \mathbb{H}$. Hence we have $p \cdot \mathbb{H} = \mathbb{H} \perp \mathbb{H} \perp \cdots \perp \mathbb{H}$ with number of summands equal to $\dim p$, so that $([p \cdot \mathbb{H}] - [q \cdot \mathbb{H}]) \in L$. Hence L is an ideal. □

We denote the quotient ring $\widetilde{W}(k)/L$ by $W(k)$ and call it the *Witt ring of quadratic forms over k.* Now the following proposition will show that the Witt ring essentially classifies quadratic forms who have the same underlying anisotropic kernel:

Proposition 7. *The following conditions are equivalent:*

1. *Quadratic forms p and q represent the same class in $W(k)$.*
2. *The form $p \perp -q$ is hyperbolic.*
3. *$p_{an} = q_{an}$.*

Proof. (1 $\iff$ 2) We first note that in the Witt ring we have for any form q, $-([q] - [0]) = ([-q] - [0])$, since the form $q \perp -q$ is hyperbolic and hence $[q \perp -q] - [0] = 0$ in $W(k)$. Suppose that forms p and q represent the same class in $W(k)$, so that $([p]-[0])-([q]-[0]) \in L$. Then equivalently we have $([p \perp -q]-[0]) \in L$, so that $p \perp -q$ is hyperbolic.

(3 $\implies$ 1) Suppose p, q are forms such that $p_{an} = q_{an}$. Denote $p_{an} = r = q_{an}$. Then we may write $p = \perp_{i=1}^{n} \mathbb{H} \perp r$, $q = \perp_{i=1}^{m} \mathbb{H} \perp r$, and so

$$[p] - [0] + L = [r] - [0] + L = [q] - [0] + L.$$

(2 $\implies$ 3) Suppose $p \perp -q$ is hyperbolic. We may decompose $p = \perp_{i=1}^{n} \mathbb{H} \perp p_{an}$, $q = \perp_{i=1}^{m} \mathbb{H} \perp q_{an}$ for some $n, m \in \mathbb{N}$. Then we must have

$$(p_{an} \perp -q_{an}) \perp_{i=1}^{n+m} \mathbb{H} = \perp_{j=1}^{l} \mathbb{H}$$

for some $l \geq n + m$.Then applying Witt cancellation, we must have

$$(p_{an} \perp -q_{an}) = \perp_{j=1}^{l-n-m} \mathbb{H}.$$

So $p_{an} \perp -q_{an}$ is hyperbolic. Let us relabel $s = l - n - m$. We see that $\dim p_{an} \leq s$, since by Proposition 5 we have that $\perp_{j=1}^{s} \mathbb{H}$ contains a totally isotropic subspace of dimension s. So if $\dim p_{an} > s$ they would intersect nontrivially, contracting anisotropy of p_{an}. Similarly we see that $\dim q_{an} \leq s$. Then the equality above gives $\dim q_{an} + \dim p_{an} = 2s$, and hence $\dim p_{an} = \dim q_{an} = s$. Now from the equalities

$$p_{an} \perp -q_{an} = \perp_{j=1}^{s} \mathbb{H} = q_{an} \perp -q_{an}$$

and the Witt cancellation theorem, we see that $p_{an} = q_{an}$. □

The above proposition implies that the elements of the Witt ring are in one-to-one correspondence with the isomorphism classes of anisotropic quadratic forms. Hence to calculate the elements of the Witt ring $W(k)$ it is sufficient to list out all of the nonisomorphic anisotropic forms over k. The following examples elaborate on this.

Example 1.

1. Let $k = \mathbb{C}$. Then $W(k) = \mathbb{Z}/2$, since the only anisotropic forms over $\mathbb{C}$ are the zero-dimensional form and the form $\langle 1 \rangle$. There is only one possible ring structure.

2. Let $k = \mathbb{R}$. Then $W(k) = \mathbb{Z}$, since the anisotopic forms over $\mathbb{R}$ are of three types: $0-$dimensional forms, $n-$dimensional forms $\perp_{i=1}^{n} \langle 1 \rangle$, and $n-$dimensional forms $\perp_{j=1}^{n} \langle -1 \rangle$, $n \in \mathbb{N}$. And by identifying these with $0, n$ and $-n$ respectively, we see that the sum and product operations match those in $\mathbb{Z}$.

3. For $k = \mathbb{F}_q$ in odd characteristic, the Witt ring always consists of 4 elements. We have
$$W(k) = \begin{cases} \mathbb{Z}/2\mathbb{Z}[t]/(t^2), & q \equiv 1 \pmod 4, \\ \mathbb{Z}/4\mathbb{Z}, & q \equiv -1 \pmod 4. \end{cases} \tag{15}$$
This is due to the following:

Lemma 7. *A quadratic form over $\mathbb{F}_q$ of dimension at least 3 is isotropic.*

Proof. It is sufficient to show that a quadratic form over $\mathbb{F}_q$ of dimension exactly 3 is isotropic. So let $p = \langle a, b, c\rangle$ with $a, b, c \in \mathbb{F}_q^\times$ be a quadratic form, and let (x, y, z) be an isotropic vector for p. Then we have

$$ax^2 + by^2 + cz^2 = 0. \tag{16}$$

Any scalar multiple of (x, y, z) is also a solution of Equation 16, so we may assume, reordering coordinates if necessary, that $z = 1$. Then it is sufficient to find some $t \in (\mathbb{F}_q)^2$ such that we have $at = -bt - c$. But now observe that since $\mathbb{F}_q$ is a finite field, the multiplicative group $\mathbb{F}_q^\times$ has order $q - 1$ and thus the subgroup of squares $(\mathbb{F}_q^\times)^2$ has order $(q - 1)/2$. So including zero we have $(q + 1)/2$ such elements. Now observe that the sets

$$A := \{at \mid t \in (\mathbb{F}_q^\times)^2 \cup \{0\}\}, \qquad B := \{-bt - c \mid t \in (\mathbb{F}_q^\times)^2 \cup \{0\}\}$$

each have cardinality $(q + 1)/2$ and are subsets of $\mathbb{F}_q$, hence their intersection must be nonempty. So indeed we have $t \in (\mathbb{F}_q^\times)^2 \cup \{0\}$ such that $at = -bt - c$. Then choosing $s \in \mathbb{F}_q^\times$ with $s^2 = t$, the nonzero vector $(s, s, 1)$ is isotropic, and we are done. □

Now there is only one zero-dimensional form over $\mathbb{F}_q$, the quadratic form 0. We know that one-dimensional forms are in bijection with square classes in $\mathbb{F}_q^\times$, that is, elements of $\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2 = \mathbb{Z}/2\mathbb{Z}$. So there are only two forms up to isomorphism, the form $\langle 1\rangle$ and the form $\langle \alpha\rangle$, where α is not a square in $\mathbb{F}_q^\times$. Clearly all of the one-dimensional forms are anisotropic. Finally, given a two-dimensional quadratic form r, the form $r \perp \langle -1\rangle$ is three-dimensional, hence isotropic by Lemma 7 and thus $\langle 1\rangle$ is a subform of r. So we may write $r = \langle 1, -d\rangle$ for some $d \in k^\times$, which gives rise to two separate isomorphism classes of quadratic forms: Either $r = \langle 1, -1\rangle$ is hyperbolic, or $r = \langle 1, -\alpha\rangle$ is anisotropic. So in total we have four nonisomorphic anisotropic quadratic forms over $\mathbb{F}_q$, namely

$$0, \langle 1\rangle, \langle \alpha\rangle, \langle 1, -\alpha\rangle.$$

There are two possible ring structures on this set. We list the cases:

(a) $q \equiv 1 \pmod 4$. Then -1 is a square in $\mathbb{F}_q$, and hence $W(k)$ has characteristic two, since $\langle 1\rangle + \langle 1\rangle = \langle 1, 1\rangle = \langle 1, -1\rangle = 0 \in W(k)$. Hence $W(k)$ is a two-dimensional $\mathbb{Z}/2\mathbb{Z}$-vector space, and denoting $1 = \langle 1\rangle, t = \langle \alpha\rangle$, we

may choose the basis $\langle 1, t\rangle$. Now due to the relation $t^2 = \langle \alpha^2\rangle = \langle 1\rangle = 1$ and the fact that 1 is a unit, we see that

$$W(k) = \mathbb{Z}/2\mathbb{Z}[t]/(t^2 - 1)$$

in this case. And clearly we have an isomorphism $\mathbb{Z}/2\mathbb{Z}[t]/(t^2 - 1) \to \mathbb{Z}/2\mathbb{Z}[t]/(t^2)$ by swapping t and $t + 1$.

(b) $q \equiv -1 \pmod 4$. Then -1 is not a square in $\mathbb{F}_q$. So our unit for multiplication $\langle 1\rangle$ has order 4, since $\langle 1\rangle + \langle 1\rangle = \langle 1, 1\rangle \neq \langle 1, -1\rangle$, we see $\langle 1\rangle$ has order greater than 2, and, since the underlying abelian group of $W(k)$ must have order 4 and the order of $\langle 1\rangle$ divides 4, we see that the order of $\langle 1\rangle$ is exactly 4. So the underlying abelian group is cyclic of order 4, with generator equal to the unit for multiplication. It follows that

$$W(k) = \mathbb{Z}/4\mathbb{Z}.$$

in this case.

2.8 Graded Witt ring & Pfister forms

By considering powers of even-dimensional quadratic forms in $W(k)$, we obtain a multiplicative filtration, from which we may define a ring auxiliary of $W(k)$ whose structure is easier to study. First, let $\dim : \widetilde{W}(k) \to \mathbb{Z}$ be such that $[p] - [q] \mapsto \dim(p) - \dim(q)$, where dimensions are of the underlying vector spaces of the forms p, q. One can check that dim is a well-defined ring homomorphism. Notice that $L = \langle \mathbb{H}\rangle$ consists of even-dimensional forms only, since $\mathbb{H}$ has dimension 2. This means that there exists a unique homomorphism $\dim_{\mathbb{Z}/2} : W(k) \to \mathbb{Z}/2$ that makes the diagram

$$\begin{array}{ccc} \widetilde{W}(k) & \xrightarrow{\dim} & \mathbb{Z} \\ \downarrow & & \downarrow \\ W(k) & \xrightarrow{\dim_{\mathbb{Z}/2}} & \mathbb{Z}/2 \end{array}$$

commutative. We let I denote the kernel of the homomorphism $\dim_{\mathbb{Z}/2}$, and call it the *fundamental ideal* of the Witt ring. It consists of classes of even-dimensional quadratic forms. Taking successive powers I^n for $n \in \mathbb{N}$ of the ideal I introduces a multiplicative filtration

$$W(k) \supset I \supset I^2 \supset \cdots \supset I^n \supset \ldots$$

on $W(k)$. That is, $I^n \cdot I^m \subset I^{n+m}$ for all $n, m \in \mathbb{N}$. From here, we introduce a new ring. Let I, $W(k)$ be as above. Introduce the *associated graded ring* to $W(k)$ as the ring

$$\mathrm{gr}_{I^\bullet}(k) = \bigoplus_{n=0}^{\infty} I^n/I^{n+1} = W(k)/I \oplus I/I^2 \oplus I^2/I^3 \oplus \dots$$

with the inherited addition and multiplication from $W(k)$.

We now introduce a class of quadratic forms called *Pfister forms*. First, we define a *1-fold Pfister form* as the form $\langle\langle a \rangle\rangle$ for $a \in k^\times$, where

$$\langle\langle a \rangle\rangle := \langle 1, -a \rangle.$$

Then we define an *n-fold Pfister form* $\langle\langle a_1, a_2, \dots, a_n \rangle\rangle$ by

$$\langle\langle a_1, a_2, \dots, a_n \rangle\rangle = \langle a_1 \rangle \cdot \langle a_2 \rangle \cdot \dots \cdot \langle a_n \rangle.$$

A remarkable property of these forms is the following:

Theorem 4. *If an n-fold Pfister form is isotropic, then it is hyperbolic.*

Proof. A proof is found in [5]. □

Now we define the *Albert form* $A_{\{a,b\}+\{c,d\}}$ in diagonal presentation as the form

$$A_{\{a,b\}+\{c,d\}} := \langle c, d, -cd, -a, -b, ab \rangle.$$

It can be easily seen that in the Witt ring, we have $A_{\{a,b\}+\{c,d\}} = \langle\langle a, b \rangle\rangle - \langle\langle c, d \rangle\rangle$. We will revisit these forms later in the dissertation.

Any binary form $\langle a, b \rangle \in W(k)$ can be written as a difference of 1-fold Pfister forms $\langle\langle -a \rangle\rangle, \langle\langle b \rangle\rangle$ since

$$\langle a, b \rangle = \langle 1, -(-a) \rangle - \langle 1, -b \rangle$$

and hence I is additively generated by $1-$fold Pfister forms. So I^2 is additively generated by $2-$fold Pfister forms.

Proposition 8. *Let $gr_{I^\bullet}(k)_n$ denote the nth component of $gr_{I^\bullet}(k)$.*

1. $gr_{I^\bullet}(k)_1 = \mathbb{Z}/2$.
2. $gr_{I^\bullet}(k)_2 = k^\times/(k^\times)^2$.

Proof. 1. We need to show that $W(k)/I \cong \mathbb{Z}/2$. Since $\dim_{\mathbb{Z}/2}$ is surjective and has kernel equal to I, the result follows.

2. First, define $\phi_1 : k^\times/(k^\times)^2 \to I/I^2$ by $a \mapsto \langle\langle a\rangle\rangle \mod I^2$. Let us show this map only depends on the square class of a. We have

$$\phi_1(a \cdot b^2) = \langle\langle a \cdot b^2\rangle\rangle = \langle 1, -a \cdot b^2\rangle = \langle 1, -a\rangle = \langle\langle a\rangle\rangle \pmod{I^2}.$$

Next, let us show that ϕ_1 is a homomorphism from $k^\times/(k^\times)^2$ to the underlying abelian group of I/I^2. We have

$$\begin{aligned}\phi_1(a) + \phi_1(b) - \phi_1(a \cdot b) &= \langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle - \langle\langle a \cdot b\rangle\rangle \pmod{I^2} \\ &= \langle 1, -a\rangle + \langle 1, -b\rangle - \langle 1, -ab\rangle \\ &= \mathbb{H} + \langle 1, -a, -b, ab\rangle \\ &= \langle 1, -a, -b, ab\rangle = \langle\langle a, b\rangle\rangle \in I^2.\end{aligned}$$

We get that ϕ_1 is surjective since I is additively generated by 1-fold Pfister forms. Now we claim that ϕ_1 is an isomorphism. To show this, we produce the inverse map.

Let q be a quadratic form. We define the *signed discriminant* $\det_\pm(q)$ of q by the formula

$$\det_\pm(q) = (-1)^{[\dim(q)/2]} \cdot \det(q).$$

This is a well-defined function on $W(k)$, since we have the function on the Grothendieck-Witt ring

$$\begin{aligned}\det_\pm : \widetilde{W}(k) &\to k^\times/(k^\times)^2, \\ [p] - [q] &\mapsto (-1)^{\left[\frac{\dim(p)-\dim(q)}{2}\right]} \cdot \frac{\det(p)}{\det(q)},\end{aligned}$$

which is clearly well-defined and coincides with the above definition for the classes of the form $([p] - [0])$ (note we take $\det(0) = 1$). We see that $\det_\pm(x + y) = \det_\pm(x) \cdot \det_\pm(y)$ if at least one of the forms x, y is even-dimensional. In particular it is additive on L, since every form on L has even dimension. Furthermore, since we have $\det_\pm(\mathbb{H}) = (-1)^1 \cdot \frac{(-1)}{1} = 1$, the map is trivial on all of L. Hence for any $x \in \widetilde{W}(k)$ and $y \in L$ we have

$$\det_\pm(x + y) = \det_\pm(x) \cdot \det_\pm(y) = \det_\pm(x)$$

and so $\det_\pm$ descends to a well-defined function on $W(k)$ as was first claimed. The descent is additive when we restrict it to $I \subset W(k)$, since by definition every element of I has even dimension.

Now we claim that $\det_\pm : I/I^2 \to k^\times/(k^\times)^2$ is a well-defined group homomorphism, inverse to the map ϕ_1. We already know it is additive. To show it is well-defined, we need to show it is trivial on I^2. But since I^2 is additively generated by 2-fold Pfister forms, we only need to show it is trivial on $\langle\langle a, b\rangle\rangle$. We have

$$\begin{aligned}\det_\pm(\langle\langle a, b\rangle\rangle) = \det_\pm(\langle 1, -a, -b, ab\rangle) &= (-1)^2 \cdot 1 \cdot (-a) \cdot (-b) \cdot (ab) \\ &= (ab)^2 \\ &= 1 \pmod{(k^\times)^2}.\end{aligned}$$

Hence $\det_\pm : I/I^2 \to k^\times/(k^\times)^2$ is a well-defined group homomorphism. To show it is inverse to ϕ_1, let us compute the composition in both ways. On the one hand,

$$\det_\pm \circ \phi_1(a) = \det_\pm(\langle\langle a\rangle\rangle) = (-1) \cdot 1 \cdot -a = a.$$

On the other hand, since ϕ_1 is surjective, the composition $\phi_1 \circ \det_\pm = id_{I/I^2}$, and so $\phi_1, \det_\pm$ are inverse isomorphisms.

□

The isomorphism constructed above lets us characterise the forms inside I^2: They have even dimension (since $I^2 \subset I$) and they have trivial signed discriminant.

Example 2. Let us see some examples of the associated graded ring to $W(k)$ for some choices of field k.

1. Let $k = \mathbb{R}$. Then $W(k) = \mathbb{Z}$ and by this isomorphism, $I = 2\mathbb{Z}$. So $I^n = 2^n \cdot \mathbb{Z} \subset \mathbb{Z}$. Hence
$$\mathrm{gr}_{I^\bullet}\mathbb{R} = \bigoplus_{n=0}^{\infty}(2^n\mathbb{Z}/2^{n+1}\mathbb{Z}) = \bigoplus_{n=0}^{\infty}(\mathbb{Z}/2) \cdot t^n$$
where $t = 2$; hence $\mathrm{gr}_{I^\bullet}\mathbb{R} = \mathbb{Z}/2[t]$.

2. Let $k = \mathbb{F}_q$ be a finite field of odd characteristic. Again, assume that $\alpha \in \mathbb{F}_q$ is not a square. Then $W(k)$ consists of only one non-trivial even-dimensional anisotropic form $\langle\langle\alpha\rangle\rangle$, in which case $I = \{0, \langle\langle\alpha\rangle\rangle\}$, and thus $I^2 = 0$. Hence all the graded components $\mathrm{gr}_{I^\bullet}(k)_n$ are trivial for $n \geq 2$. We see that
$$\mathrm{gr}_{I^\bullet}\mathbb{F}_q = \mathbb{Z}/2 \oplus \mathbb{Z}/2$$
as an abelian group.

Pfister forms are especially important since they appear as the norm forms for an important class of algebras called *quaternion algebras*. Furthermore, Albert forms appear as norm forms for so-called *biquaternion algebras*. We shall meet both of these algebras later in the next section, which introduces the notion of *central simple algebras* over a field.

2.9 Witt Chain Equivalence

This subsection introduces a technique that is useful in later proofs. Suppose $\langle a_1, \ldots, a_n\rangle$, $\langle b_1, \ldots, b_n\rangle$ are two quadratic forms. We say these two forms are *elementary equivalent* if we can choose two (not necessarily distinct) indices $1 \leq i, j \leq n$ such that $a_l = b_l$ for any $l \neq i, j$, and $\langle a_i, a_j\rangle \cong \langle b_i, b_j\rangle$. And we say $\langle a_1, \ldots, a_n\rangle$ and $\langle b_1, \ldots, b_n\rangle$ are *chain equivalent*, denoted $\overset{\text{c}}{\sim}$, if there exists a sequence of elementary equivalences that takes $\langle a_1, \ldots, a_n\rangle$ to $\langle b_1, \ldots, b_n\rangle$. Chain equivalence is an equivalence relation, and for quadratic forms chain equivalent implies isomorphic. Immediately we get:

Theorem 5 (Witt Chain Equivalence)**.** *Any two diagonalisations of the same non-degenerate quadratic form are chain equivalent.*

Proof. Let q be a nondegenerate quadratic form. We induct on $n = \dim q$. For $n \leq 2$, there is nothing to prove. Suppose any two diagonalisations of a non-degenerate $(\dim q - 1)$-form are chain equivalent and suppose $\langle a_1, \ldots, a_n\rangle$ and $\langle b_1, \ldots, b_n\rangle$ are two diagonal presentations of the same quadratic form; we must show that they are chain equivalent. First, a_1 is a value of q, so we may write it as $a_1 = b_1x_1^2 + \cdots + b_nx_n^2$ for some choice of $x_1, \ldots, x_n \in k$. Assume that, among all such $(x_1, \ldots, x_n)$, our choice has the minimal number s of nonzero components. Then, ignoring the zero terms, we can write $a_1 = b_{i_1}x_{i_1}^2 + \cdots + b_{i_s}x_{i_s}^2$. Next, since the group S_n is generated by transpositions, any diagonalisation $\langle b_{\sigma(1)}, \ldots, b_{\sigma(n)}\rangle$ is chain equivalent to the form $\langle b_1, \ldots, b_n\rangle$. In our situation, this means we can assume that $i_l = l$ for all $1 \leq l \leq s$. Now we claim that $s = 1$ (and we will prove this soon). We have $a_1 = b_1 \cdot x_1^2$ and so $\langle b_1, b_2, \ldots, b_n\rangle \overset{\text{c}}{\sim} \langle a_1, b_2, \ldots, b_n\rangle$. Hence by Witt Cancellation, the forms $\langle b_2, \ldots, b_n\rangle$ and $\langle a_2, \ldots, a_n\rangle$ are isomorphic. By the inductive hypothesis on n, we have $\langle b_2, \ldots, b_n\rangle \overset{\text{c}}{\sim} \langle a_2, \ldots, a_n\rangle$. So $\langle a_1, \ldots, a_n\rangle \overset{\text{c}}{\sim} \langle a_1, b_2, \ldots, b_n\rangle \overset{\text{c}}{\sim} \langle b_1, \ldots, b_n\rangle$. Now suppose for contradiction that $s \geq 2$. Then letting $d = b_1x_1^2 + b_2x_2^2$, we have $d \neq 0$. Hence $\langle x_1, x_2\rangle \cong \langle d, x_1x_2d\rangle$, since $\det(\langle x_1, x_2\rangle) = \det(d, x_1x_2d\rangle)$ and d is a common value of both forms. So $\langle b_1, b_2, b_3, \ldots, b_n\rangle \overset{\text{c}}{\sim} \langle d, dx_1x_2, b_3, \ldots, b_n\rangle$. Now $a_1 = d + b_3x_3^2 + \cdots + b_nx_n^2 = d + b_3x_3^2 + \cdots + b_sx_s^2$. But this contradicts the minimality of s. □

Chain equivalence lets us describe the Witt-Grothendieck ring $\widetilde{W}(k)$ in terms of generators and relations.

Proposition 9. *The ring $\widetilde{W}(k)$ is isomorphic to the quotient of the free associative algebra generated by the formal symbols $\langle a\rangle$, $a \in k^*$, with the following relations:*

1. $\langle x^2\rangle = 1$,

2. $\langle a\rangle + \langle b\rangle = \langle c\rangle + \langle d\rangle$ *for all* $a, b, c, d \in k^*$ *with* $abcd \in (k^*)^2$ *and there exists* $x, y \in k$ *with* $c = ax^2 + by^2$.

3. $\langle a\rangle \cdot \langle b\rangle = \langle ab\rangle$.

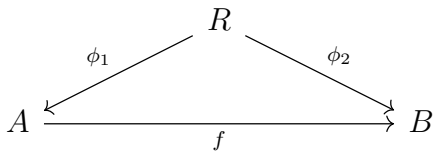
Proof. Denote this ring by R. Let $\phi : R \to \widetilde{W}(k)$ be defined by $\langle a\rangle \mapsto [a]-[0]$. Clearly this homomorphism is well-defined, since all the relations in R are respected in $\widetilde{W}(k)$. Clearly ϕ is surjective. Let us show ϕ is injective. Let $\sum_{i=1}^{s}\langle a_i\rangle - \sum_{j=1}^{l}\langle b_j\rangle = u \in \ker\phi$. Then $\phi(u) = [\langle a_1, \ldots, a_s\rangle] - [\langle b_1, \ldots, b_l\rangle] = 0$. Using the relations in $\widetilde{W}(k)$ and Witt Cancellation, this means $\langle a_1, \ldots, a_s\rangle$ and $\langle b_1, \ldots, b_l\rangle$ are isomorphic; in particular, this means $l = s$. Using Witt Chain Equivalence, we have that $\langle a_1, \ldots, a_s\rangle$ and $\langle b_1, \ldots, b_s\rangle$ are chain equivalent. Each elementary equivalence in this chain equates (possibly two) pairs $\langle a_i\rangle$ and $\langle b_j\rangle$ due to the relations in R, and so we have $\langle a_{i_n}\rangle = \langle b_{j_n}\rangle$ for all $1 \leq i_n, j_n \leq s$. So $u = 0$. □

3 Central simple algebras

We now turn away from the general theory of quadratic forms to present the theory of central simple algebras.

3.1 Definitions

The definition of an algebra over a ring abstracts familiar setups likes the complex numbers $\mathbb{C}$ with scalar multiplication taken from $\mathbb{R}$, or the polynomial ring $\mathbb{Z}[x, y]$ viewed as a $\mathbb{Z}$-module. Fix a unital ring A and a commutative unital ring R with a homomorphism $\phi : R \to A$ such that $\phi(R) \subset Z(A)$. Then we say A is an (associative) *R-algebra*. When $R = k$ is a field, A has the structure of a vector space over k. A homomorphism of R-algebras $f : A \to B$ is a ring homomorphism such that the diagram



(17)

commutes, where ϕ_1, ϕ_2 are the canonical homomorphisms mapping R into A, B respectively.

In this dissertation, we focus our attention on k-algebras with k a field; then the inclusion $k \to A$ is an injection and hence k-algebra homomorphisms $A \to B$ are ring homomorphisms that are also k-linear maps that preserve the image of k in A.

We say a k-algebra A is *simple* if it possesses no non-trivial 2-sided ideals. It is *central* if $Z(A) = k$. Then we reach our key definition of this section: A *central simple algebra* over k is a k-algebra A which is both central and simple.

3.2 Normed algebras

To gain a substantial taste of the behaviour of k-algebras before we develop the general theory, in this subsection we will consider a family of $\mathbb{R}$-algebras which will serve as a foundational example from here on.

Consider the complex numbers $\mathbb{C} = \mathbb{R} \oplus \mathbb{R} \cdot i$ as an $\mathbb{R}-$vector space, with product

$$(x_1 + y_1 i) \cdot (x_2 + y_2 i) = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + y_1 x_2) i.$$

This makes $\mathbb{C}$ an associative, commutative $\mathbb{R}$-algebra with unit $1 = 1 + 0 \cdot i$.

The nontrivial element of the Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acts in the usual way as complex conjugation, that is defined by $z = a + bi \mapsto a - bi = \overline{z}$. Clearly $z = \overline{z}$ if and only if $z \in \mathbb{R}$.

Since $\mathbb{C}/\mathbb{R}$ is a finite Galois extension, we may define the *norm* in the usual way, by setting $N_{\mathbb{C}/\mathbb{R}} : \mathbb{C} \to \mathbb{R}$ by $z \mapsto z \cdot \overline{z}$, or equivalently in $\mathbb{R}$-coordinates by $x + iy \mapsto x^2 + y^2$. The norm is a quadratic form isomorphic to $\langle 1, 1\rangle$, and it is also multiplicative, since

$$N_{\mathbb{C}/\mathbb{R}}(z_1 \cdot z_2) = N_{\mathbb{C}/\mathbb{R}}(z_1) \cdot N_{\mathbb{C}/\mathbb{R}}(z_2).$$

Since $\langle 1, 1\rangle$ is an anisotropic form, we may invert an arbitrary nonzero $z \in \mathbb{C}$ by the rule

$$z^{-1} = \frac{\overline{z}}{N_{\mathbb{C}/\mathbb{R}}(z)},$$

and hence $\mathbb{C}$ is a field. This point of view is generalised later.

As a further example of a normed algebra, consider Hamilton's quaternions $\mathbb{H} = \mathbb{C} \oplus \mathbb{C} \cdot j$ as a $\mathbb{C}-$algebra with the product

$$(u_1 + v_1 j)(u_2 + v_2 j) = (u_1 u_2 - v_1 \overline{v_2}) + (u_1 v_2 + v_1 \overline{u_2})j.$$

Here this product is associative, but it is not commutative. In the quaternions we have the conjugation $\overline{u + vj} = \overline{u} - vj$, where $\overline{u}$ is the normal complex conjugate. We can give Hamilton's quaternions $\mathbb{H}$ real coordinates by specifying $i \cdot j = k$, and writing an arbitrary $z \in \mathbb{H}$ as

$$z = a + bi + cj + dk$$

where $a, b, c, d \in \mathbb{R}$. Then the multiplication in $\mathbb{H}$ just corresponds to expanding the product in real coordinates, with the rules $i \cdot j = k, j \cdot i = -k, j \cdot k = i, k \cdot j = -i$, $k \cdot i = j, i \cdot k = -j$. In these real coordinates, conjugation looks like

$$\overline{a + bi + cj + dk} = a - bi - cj - dk.$$

As expected, quaternion conjugation is an involution, and it is an *anti-isomorphism*, meaning $\overline{a \cdot b} = \overline{b} \cdot \overline{a}$. And clearly $w = \overline{w}$ if and only if $w \in \mathbb{R}$.

For an arbitrary quaternion $w = u + vj \in \mathbb{H}$, define its *reduced norm* $N : \mathbb{H} \to \mathbb{R}$ by $N(w) = w \cdot \overline{w} = N_{\mathbb{C}/\mathbb{R}}(u) + N_{\mathbb{C}/\mathbb{R}}(v)$. In real coordinates this looks like $N(x + yi + zj + tk) = x^2 + y^2 + z^2 + t^2$.

Lemma 8. *The reduced norm N is multiplicative:*

$$N(w_1 \cdot w_2) = N(w_1) \cdot N(w_2).$$

Proof. Let $w_1, w_2 \in \mathbb{H}$. Then

$$\begin{aligned} N(w_1 \cdot w_2) &= (w_1 \cdot w_2) \cdot \overline{(w_1 \cdot w_2)} \\ &= (w_1 \cdot w_2) \cdot (\overline{w_2} \cdot \overline{w_1}) \\ &= w_1 \cdot (w_2 \cdot \overline{w_2}) \cdot \overline{w_1} \\ &= w_1 \cdot N(w_2) \cdot \overline{w_1} \\ &= (w_1 \cdot \overline{w_1}) \cdot N(w_2) \\ &= N(w_1) \cdot N(w_2). \end{aligned}$$

□

Once again, the reduced norm N in $\mathbb{R}$-coordinates is a quadratic form isomorphic to $\langle 1, 1, 1, 1\rangle$. And since $\langle 1, 1, 1, 1\rangle$ is anisotropic, we get that $\mathbb{H}$ is a division algebra, that is, for any non zero $w \in \mathbb{H}$, there exists an inverse $w^{-1} = \overline{w} \cdot N(w)^{-1}$.

We can follow a similar construction with the *octonions* $\mathbb{O} = \mathbb{H} \oplus \mathbb{H} \cdot l$. We consider the octonions as an $\mathbb{H}-$algebra with the product

$$(u_1 + v_1 l) \cdot (u_2 + v_2 l) = (u_1 u_2 - \overline{v_2} v_1) + (v_2 u_1 + v_1 \overline{u_2}) l. \tag{18}$$

This product is neither commutative nor associative. This means that, strictly speaking, $\mathbb{H}$ is not an $\mathbb{R}$-algebra in the way we have defined them. But it is useful nonetheless to see how things like the reduced norm operate in this higher dimensional algebra. As before, we have conjugation given by $\overline{u + vl} = \overline{u} - vl$, and it is again an anti-automorphism.

We will similarly define a reduced norm $Nrd : \mathbb{O} \to \mathbb{R}$ given by $Nrd(w) = w \cdot \overline{w}$. It is additive, that is for $w = u + vl$, we have $Nrd(w) = Nrd(u) + Nrd(v)$, which shows that Nrd as a quadratic form on the octonions is equal to the direct sum of two copies of $\langle 1, 1, 1, 1\rangle$. But to show it is multiplicative, we need a few results.

Lemma 9. *Given $w \in \mathbb{O}$,*

$$\overline{w} = w \iff w \in \mathbb{R}.$$

Proof. Write $w = u + vl$. Then siince $\overline{u + vl} = \overline{u} - vl$, we have $w = \overline{w}$ if and only if $u = \overline{u}$ and $v = -v$, or equivalently $v = 0$. Now from the case of quaternions it is clear that this is equivalent to $u \in \mathbb{R}$, $v = 0$, so that $w \in \mathbb{R}$. □

Lemma 10. *$\mathbb{O}$ is central. That is,*

$$Z(\mathbb{O}) = \mathbb{R}.$$

Proof. It is clear that $\mathbb{R} \subset Z(\mathbb{O})$, so we will just show the other inclusion. Let $w = u + vl \in Z(\mathbb{O})$. Then for an arbitrary $u' \in \mathbb{H}$ (which we will fix later) and $w' = u' + 0l$ we have $w \cdot w' = w' \cdot w$, which is equivalent to $uu' + v\overline{u'}l = u'u + vu'l$. Hence $uu' = u'u$ and $v\overline{u'} = vu'$. Since $uu' = u'u$ is in the quaternion case, we get to deduce that $u \in \mathbb{R}$. Finally, we may fix u' so that $\overline{u'} - u' \neq 0$. From here we deduce that $v = 0$ (recall that $\mathbb{H}$ is a division ring and hence has no zero divisors.) Hence $w = u + vl \in \mathbb{R}$. □

Proposition 10. *The reduced norm Nrd on the octonions is multiplicative.*

Proof. Write $w_1 = u_1 + v_1 l$, $w_2 = u_2 + v_2 l$. Then

$$w_1 \cdot w_2 = (u_1 u_2 - \overline{v_2} v_1) + (v_2 u_1 + v_1 \overline{u_2})l, \tag{19}$$

and since conjugation on quaternions is an anti-automorphism,

$$\overline{(w_1 \cdot w_2)} = (\overline{u_2 u_1} - \overline{v_1} v_2) + (-v_2 u_1 - v_1 \overline{u_2})l. \tag{20}$$

Since $Nrd(w) \in \mathbb{R}$ for all $w \in \mathbb{O}$, we need only compute the first component of $(w_1 \cdot w_2) \cdot \overline{(w_1 \cdot w_2)}$. So

$$\begin{aligned} Nrd(w_1 \cdot w_2) &= (w_1 \cdot w_2) \cdot \overline{(w_1 \cdot w_2)} \\ &= (u_1 u_2 - \overline{v_2} v_1)(\overline{u_2 u_1} - \overline{v_1} v_2) - \overline{(-v_2 u_1 - v_1 \overline{u_2})}(v_2 u_1 + v_1 \overline{u_2}). \end{aligned}$$

Further expanding, this is equal to

$$\begin{aligned} &u_1 u_2 \overline{u_2 u_1} - u_1 u_2 \overline{v_1} v_2 - \overline{v_2} v_1 \overline{u_2 u_1} + \overline{v_2} v_1 \overline{v_1} v_2 + \overline{u_1 v_2} v_2 u_1 \\ &+ \overline{u_1 v_2} v_1 \overline{u_2} + u_2 \overline{v_1} v_2 u_1 + u_2 \overline{v_1} v_1 \overline{u_2}. \end{aligned}$$

Now applying the observation that $a \cdot \overline{a} = \overline{a} \cdot a = Nrd(a) \in \mathbb{R}$ commutes with everything, we may write $u_1 u_2 \overline{u_2 u_1}$ as $u_1 Nrd(u_2)\overline{u_1} = Nrd(u_1)Nrd(u_2)$, and other monomials similarly, to obtain

$$\begin{aligned} &(Nrd(u_1)Nrd(u_2) + Nrd(v_1)Nrd(v_2) + Nrd(u_1)Nrd(v_2) + Nrd(u_2)Nrd(v_1)) \\ &+ (\overline{u_1 v_2} v_1 \overline{u_2} + u_2 \overline{v_1} v_2 u_1 - u_1 u_2 \overline{v_1} v_2 - \overline{v_2} v_1 \overline{u_2 u_1}). \end{aligned}$$

Factoring the terms in the first brackets as $(Nrd(u_1)+Nrd(v_1))(Nrd(u_2)+Nrd(v_2)) = Nrd(w_1)Nrd(w_2)$, it remains to show that

$$\overline{u_1 v_2} v_1 \overline{u_2} + u_2 \overline{v_1} v_2 u_1 - u_1 u_2 \overline{v_1} v_2 - \overline{v_2} v_1 \overline{u_2 u_1} = 0. \tag{21}$$

To do this, we will introduce a new tool. We define the *reduced trace* $Trd : \mathbb{H} \to \mathbb{R}$ according to the formula $Trd(w) = w + \overline{w}$. Since $\overline{Trd(w)} = Trd(w)$, we have that $Trd(w) \in \mathbb{R}$ for any $w \in \mathbb{H}$.

Lemma 11. *Given $a, b \in \mathbb{H}$,*

$$Trd(a \cdot b) = Trd(b \cdot a).$$

Proof. We have $Trd(a \cdot b) = a \cdot b + \overline{b} \cdot \overline{a}$, and $Trd(b \cdot a) = b \cdot a + \overline{a} \cdot \overline{b}$. It is sufficient to check that $Trd(a \cdot b) \cdot c = Trd(b \cdot a) \cdot c$ for some nonzero $c \in \mathbb{H}$. If a or b is zero, then both sides are zero, so there is nothing to prove. Otherwise we may take $c = a$ and compute

$$\begin{aligned} Trd(a \cdot b) \cdot a &= a \cdot b \cdot a + \overline{b} \cdot \overline{a} \cdot a \\ &= a \cdot b \cdot a + \overline{b} \cdot Nrd(a) \\ &= a \cdot b \cdot a + Nrd(a) \cdot \overline{b} \\ &= a \cdot b \cdot a + a \cdot \overline{a} \cdot \overline{b} = a \cdot Trd(b \cdot a) = Trd(b \cdot a) \cdot a, \end{aligned}$$

where we used the fact that $\mathbb{H}$ is associative and that Nrd, Trd belong to the centre. Hence the lemma is proved. □

To finish off the proof of the proposition, we just need to observe that the left hand side of Equation 21 is equal to $Trd(a \cdot b) - Trd(b \cdot a)$, where $a = u_2\overline{v_1}v_2$ and $b = u_1$, and so by the lemma must be zero. □

3.3 Tensor product of k-algebras

Now let A, B be k-algebras. We define the *tensor product* of A and B to be the k-algebra $A \otimes_k B$ (this is the tensor product of vector spaces) with the unique multiplication whose action on elementary tensors is given by

$$(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) = (a_1 \cdot a_2) \otimes (b_1 \cdot b_2). \tag{22}$$

An important result is:

Theorem 6 (Product of CSAs is CSA)**.** *Let A, B be central simple algebras over a field k. Then the tensor product $A \otimes_k B$ is a central simple algebra over k.*

Proof. To show the product is central, it is enough to show the stronger result

Lemma 12 (Centres distribute over tensor product)**.** *Let A, B be algebras over a field k. Then $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$.*

Proof. We first show the inclusion $Z(A) \otimes_k Z(B) \subset Z(A \otimes_k B)$. If $\sum_{i=1}^n a_i \otimes b_i \in Z(A) \otimes_k Z(B)$, then given any $\sum_{j=1}^k a'_j \otimes b'_j \in A \otimes_k B$, we have

$$\begin{aligned}\left(\sum_{i=1}^n a_i \otimes b_i\right)\left(\sum_{j=1}^k a'_j \otimes b'_j\right) &= \sum_{i,j=1}^{i=n,j=k} (a_i a'_j) \otimes (b_i b'_j) \\ &= \sum_{i,j=1}^{i=n,j=k} (a'_i a_j) \otimes (b'_i b_j) \\ &= \left(\sum_{i=1}^n a'_i \otimes b'_i\right)\left(\sum_{j=1}^k a_j \otimes b_j\right).\end{aligned}$$

where we exploited the centrality of the a_i, b_i. To demonstrate the inclusion $Z(A \otimes_k B) \subset Z(A) \otimes_k Z(B)$, let $z = \sum_{i=1}^n a_i \otimes b_i \in Z(A \otimes_k B)$. Consider the subspace B' of B spanned by the b_i. Choose a basis for B'. By writing the b_i in this basis, expanding the tensors and absorbing coefficients, we justify the assumption that we may write $z = \sum_{i=1}^n a_i \otimes b_i$ where the b_i are linearly independent. Repeating this for the a_i, we can assume further that the a_i are linearly independent too. Then given any z' of the form $z' = a \otimes 1 \in A \otimes_k B$, we have

$$\begin{aligned}zz' &= \sum_{i=1}^{i=n} (a_i a) \otimes (b_i) \\ = z'z &= \sum_{i=1}^{i=n} (a a_i) \otimes (b_i).\end{aligned}$$

and, taking the difference and using linear independence of the b_i, we get $a_i a = a a_i$ for all i. Hence $a_i \in Z(A)$. A similar argument on the b_i lets us deduce that $b_i \in Z(B)$ too. □

Lemma 13 (Product of simple algebras is simple)**.** *Let A, B be simple algebras over a field k, and assume A is central. Then $A \otimes_k B$ is a simple algebra.*

Proof. Choose a nontrivial two-sided ideal I in $A \otimes_k B$. Choose a nonzero element $x = \sum_{i=1}^n a_i \otimes b_i$ with n minimal amongst all possible choices, so that the b_i are linearly independent. By minimality of n, we see that $a_1 \neq 0$, so the ideal

$$J = \left\{ \sum_{finite} a a_1 a' \mid a, a' \in A \right\} = A.$$

Hence there exists a set of $a, a' \in A$ such that $\sum aa_1a' = 1$. By forming the products $(a \otimes 1)x(a' \otimes 1)$ in I for each pair a, a' and adding, we get an element of the form $y = 1 \otimes b_1 + \sum_{i=2}^{n} a_i' \otimes b_i$. So we justify the assumption that we can choose

$$x = 1 \otimes b_1 + a_2 \otimes b_2 + \cdots + a_n \otimes b_n \in I$$

with the same n as above. Let $a \in A$ be arbitrary. Then

$$(a \otimes 1)x - x(a \otimes 1) = \sum_{i=2}^{n} (aa_i - a_ia) \otimes b_i \in I.$$

By the minimality of n, we get that each $aa_i - a_ia = 0$, so that $a_i \in Z(A) = k$ for each i. Hence

$$x = \sum_{i=1}^{n} 1 \otimes (a_ib_i) = 1 \otimes \left(\sum_{i=1}^{n} a_ib_i \right) = 1 \otimes b$$

for some $b \in B$ (note we get $n = 1$ as a consequence). So, on the one hand,

$$(1 \otimes_k B)(1 \otimes b)(1 \otimes_k B) = 1 \otimes_k (BbB) = 1 \otimes_k B \subseteq I$$

by the simplicity of B, and on the other hand

$$(A \otimes_k 1)(1 \otimes_k B) = A \otimes_k B \subseteq I.$$

Hence $I = A \otimes_k B$, and so $A \otimes_k B$ is simple. □

Now combine the above facts to two central simple algebras A, B over k to get the theorem. □

By virtue of this theorem, the set of all isomorphism classes of central simple algebras may be endowed with the structure of a commutative monoid, denoted M, with the product given by the tensor product $\otimes_k$, and the identity given by k viewed as an algebra over itself. Not every element of M is invertible (and hence M is not a group), but we can form a quotient of M by so-called *Brauer equivalence*, where the class of each element of M is invertible. The resulting group is called the *Brauer group* of k.

3.4 Brauer equivalence

This subsection walks through the construction of Brauer equivalence on M. We start with a theorem of Wedderburn that gives a general description of finite-dimensional central simple algebras over a field. From now on, we assume all algebras are finite-dimensional.

Theorem 7 (Wedderburn)**.** *Let A be a finite-dimensional central simple algebra over a field k. Then $A \cong M_n(D)$ for some integer $n > 0$ and division algebra D. Moreover, the integer n here is unique, and D is unique up to isomorphism.*

The division algebra D appearing in this theorem is called the *underlying division algebra* of A. Its proof requires some easy lemmas.

Lemma 14 (Schur)**.** *Let M be a simple module over a k-algebra A, with k a field. Then $\mathrm{End}_A(M)$ is a division algebra.*

Proof. Let $\phi \in \mathrm{End}_A(M)$. Then $\ker\phi$ and $\mathrm{Im}\,\phi$ are A-submodules of M. Then either $\ker\phi = 0$, $\mathrm{Im}\,\phi = M$, in which case ϕ is invertible, or $\ker\phi = M$, $\mathrm{Im}\,\phi = 0$, in which case $\phi = 0$. So every nonzero ϕ is invertible and so $\mathrm{End}_A(M)$ is a division algebra. □

Lemma 15 (Rieffel)**.** *Let L be a nonzero left ideal in the finite-dimensional simple k-algebra A, with k a field. Put $D = \mathrm{End}_A(L)$. Then the map*

$$\begin{aligned} \lambda_L : A &\to \mathrm{End}_D(L), \\ a &\mapsto \phi_a \end{aligned}$$

with $\phi_a(x) = ax$, is an isomorphism.

Proof. Injectivity: Any non-trivial ring homomorphism from a simple k-algebra is injective.
Surjectivity: Let $\phi \in \mathrm{End}_D(L)$ be arbitrary. By simplicity of A, the two-sided ideal LA is equal to A. Hence we may write $1 = \sum_i l_i a_i$ for finitely many $a_i \in A, l_i \in L$. Now

$$\phi = \phi \cdot \lambda_L(1) = \sum_i \phi\lambda_L(l_i)\lambda_L(a_i).$$

It suffices to show that $\phi\lambda_L(l_i) \in \lambda_L(L)$ for each i, because then $\phi \in \lambda_L(A)$ and hence the map is surjective. We will show that $\lambda_L(L)$ is a left ideal of $\mathrm{End}_D(L)$. Let $\psi \in \mathrm{End}_D(L)$ and $l \in L$. We have attached to l the map $\lambda_L(l) : x \mapsto lx$. Using the fact that ψ is a D-endomorphism, we have $\psi \cdot \lambda_L(l) : x \mapsto \psi(lx) = \psi(l)x = \lambda_L(\psi(l))(x)$. So we have $\psi \cdot \lambda_L(l) = \lambda_L(\psi(l))$, and hence $\lambda_L(L)$ absorbs multiplication from the left. □

Proof of Wedderburn's theorem. Existence. Choose a minimal left ideal L of A (since A is finite-dimensional, any descending chain of left ideals must stabilise. so we can always make such a choice). We may then regard L as a simple A-module. By Schur's lemma, $D = \mathrm{End}_A(L)$ is a division algebra. Hence every D-module is free, that is, we can choose a basis. By Rieffel's lemma, we have $A \cong \mathrm{End}_D(L)$. Now choosing a basis for the D-module L, we get an isomorphism $\mathrm{End}_D(L) \cong M_n(D)$, where $n = \dim_D(L)$

is finite due to the finite dimensionality of A over k.
Uniqueness. First, note that we have the direct sum decomposition

$$M_n(D) = \bigoplus_s I_s$$

where the I_s, $1 \leq s \leq n$ are ideals of $M_n(D)$ defined by $m_{ij} \in I_s \iff m_{ij} = 0$ for $j \neq s$. Further note that each of the I_s are simple left $M_n(D)$-modules, i.e. are minimal ideals with respect to inclusion. Since any simple left $M_n(D)$-module can be realised as a quotient of $M_n(D)$ by a maximal ideal, and the I_s are mutually isomorphic to D^n, we get that every simple left $M_n(D)$-module is isomorphic to D^n.

Now, to show uniqueness. Suppose we have $A \cong M_n(D) \cong M_m(D')$ for division algebras D, D' and integers n, m. The ideal L in the proof of existence is a simple left $M_n(D)$-module. Hence we have $D^n \cong L \cong D'^m$. Choosing a basis for D^n and D'^m respectively, we obtain isomorphisms $A \cong \mathrm{End}_A(D^n) \cong \mathrm{End}_A(D'^m)$. We have $A \cong \mathrm{End}_D(D^n)$ and $A \cong \mathrm{End}_{D'}(D'^m)$. Now apply Rieffel's lemma to get a chain of isomorphisms $D \cong \mathrm{End}_A(D^n) \cong \mathrm{End}_A(D'^m) \cong D'$. So $D \cong D'$ and hence $n = m$. □

As a corollary, we obtain

Proposition 11. *Let A be a central simple algebra over k. Then $\dim_k A = n^2$ for some $n \in \mathbb{N}$.*

Proof. By Wedderburn's theorem, we see that $A \cong M_m(D)$ for some $m \in \mathbb{N}$ and division algebra D, and clearly $\dim_k A = m^2 \cdot \dim_k D$, so it is enough to show that any division algebra over k has square dimension. First, there are no nontrivial finite dimensional division algebras over the algebraic closure $\overline{k}$ of k, since if K is such an algebra and $x \in K$, then since $\overline{k} \subset Z(K)$, we have that $\overline{k}[x]$ is a commutative, finite dimensional subring of D over $\overline{k}$, and is hence a finite (so algebraic) field extension of $\overline{k}$. But then algebraic closure implies $\overline{k}[x] = \overline{k}$ and thus $x \in \overline{k}$.

Extending scalars to $\overline{k}$, we see that the $\overline{k}$-algebra $\overline{D} = D \otimes_k \overline{k}$ is simple by Lemma 13, and it is central by a similar argument to before. Now Wedderburn's theorem gives

$$\overline{D} = M_l(D')$$

for some finite dimensional division algebra D' over $\overline{k}$, whence $D' = \overline{k}$ by our previous discussion and so $\dim_{\overline{k}}(\overline{D}) = l^2$. Now we only need to observe that $\dim_{\overline{k}}(\overline{D}) = \dim_k(D)$, and hence $n = ml$ proves the proposition. □

We now turn to the crucial definition: We say that central simple algebras A, B over k are *Brauer equivalent* if they have the same underlying division algebras. This forms an equivalence relation compatible with the tensor product operation, so that

the quotient of the monoid M from earlier by this equivalence relation is well-defined. The quotient is a group $\mathrm{Br}(k)$ with identity $[k]$, and the inverse of the algebra A is the algebra A^{op}, the *opposite algebra* of A, defined to have the same elements and addition as A, but multiplication

$$a \cdot b = ba$$

where the multiplication on the right is performed in A. It is easy to see that A^{op} is a central simple algebra over k if and only if A is.

Lemma 16. *Let A be a CSA over k. Then*

$$A \otimes_k A^{op} = M_n(k).$$

where $n = \dim_k A$.

Proof. Define the k-linear map

$$\begin{aligned} T : A \otimes_k A^{op} &\to \mathrm{End}_k(A), \\ \sum a_i \otimes a_i' &\mapsto \left(x \mapsto \sum a_i x a_i' \right). \end{aligned}$$

This map is obviously nonzero, and since $A \otimes_k A^{op}$ is simple, we see it is injective. Since both sides have the same dimension, the map is necessarily surjective. Now choose a k-basis for A to get the isomorphism. □

So $A \otimes_k A^{op} \sim k$ in the Brauer group, and so indeed A^{op} is inverse to A.

For each finite field extension L/k, we have a well-defined *norm map* $N_{L/k}$ on the Brauer group $\mathrm{Br}(L)$, defined in terms of Galois cohomology (a detailed exposition is found in [4]). In this dissertation, we will treat the norm map as a black box. One property is that given the class of a central simple algebra Q in $\mathrm{Br}(k)$, we have

$$Q = N_{L/k}(Q_L)$$

where $Q_L := Q \otimes_k L$ is considered as an L-algebra. The other properties we need will be introduced later.

3.5 Generalised quaternion algebras

One important class of central simple algebras are the (generalised) *quaternion algebras*. Here we present a theory of these algebras that will be invoked throughout the sequel. Let k be a field with char $k \neq 2$. First, we introduce the notation $k\langle i, j \rangle$ for the free associative k-algebra on the indeterminates i, j. This is the "freest" algebra

generated by i and j over k, meaning no relations hold on i, j other than those forced by the definition of k-algebra. Fix $a, b \in k^\times$, and define

$$(a,b)_k := \frac{k\langle i,j\rangle}{(i^2-a, j^2-b, ij+ij)}. \tag{23}$$

We call $(a,b)_k$ the *quaternion algebra* attached to a, b. It is clear that $(a,b)_k$ is a four-dimensional k-algebra, where $1, i, j, ij$ form a basis. Given $q = x + yi + zj + wij \in (a,b)_k$, we define the *conjugate* $\overline{q} := x - yi - zj - wij$. We define the *reduced norm* of q as the product

$$N(q) := q\overline{q} = x^2 - ay^2 - bz^2 + abw^2.$$

This is a nondegenerate quadratic form on $(a,b)_k$ equal to the Pfister form $\langle\langle a, b\rangle\rangle$. Since $N(q_1q_2) = q_1q_2\overline{(q_1q_2)} = q_1q_2\overline{q_2}\overline{q_1} = q_1N(q_2)\overline{q_1} = q_1\overline{q_1}N(q_2) = N(q_1)N(q_2)$, we see that N is a multiplicative function. Furthermore we see that $N(q) \neq 0$ if and only if q is invertible (the inverse is $\overline{q}/N(q)$). Similarly to the reduced norm, we define the k-linear *reduced trace* $Tr(q) := q + \overline{q}$. The kernel of this map is a 3-dimensional vector subspace $V = ki \oplus kj \oplus kij$ of $(a,b)_k$. Given any $v \in V$, we have $v^2 = -N(v)$. We define the *associated conic* C to $(a,b)_k$ as the smooth projective conic curve whose defining polynomial is is the restriction $N|_V$ of the reduced norm to V. We have

$$C: \qquad aX^2 + bY^2 = abZ^2.$$

Example 3. 1. By inspecting the definition, we see that $(a,b)_k \cong (b,a)_k$.

2. Fixing $a = b = -1$, we have $(a,b)_\mathbb{R} \cong \mathbb{H}$, the classical Hamilton quaternions over $\mathbb{R}$. The associated conic C is the projective curve with equation $X^2+Y^2+Z^2 = 0$. Note that C has no $\mathbb{R}$-rational points.

3. Fixing $a = -1, b = 1$, we obtain the classical split-quaternions. We have an isomorphism $(a,b)_k \cong M_2(k)$, the k-algebra of 2×2 matrices with entries in k, by
$$i \mapsto I := \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \qquad j \mapsto J := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$
The matrices id, I, J, IJ form a k-basis for $M_2(k)$, and furthermore one has the relations $I^2 = -\mathrm{id}$, $J^2 = \mathrm{id}$, $IJ = -JI$.

4. Generalising the above, we have an isomorphism $(1,b)_k \cong M_2(k)$ via the map
$$i \mapsto I := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \qquad j \mapsto J := \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}.$$
One can check that id, I, J, IJ forms a basis for $M_2(k)$ and that all the necessary relations in the image hold.

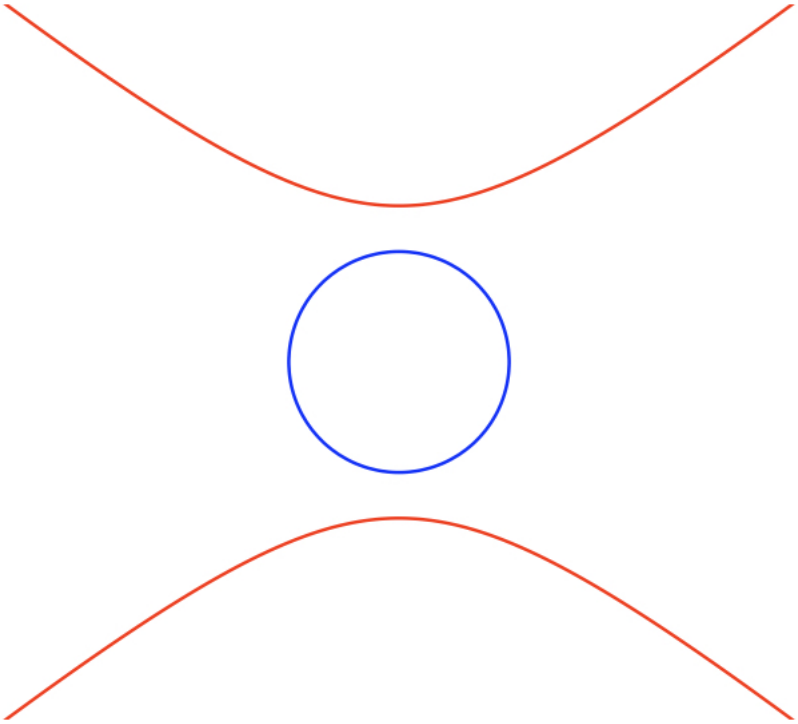


Figure 1: The restriction to an affine patch of the associated conics for the quaternion algebras $(1,1)_{\mathbb{R}}$ and $(2,-3)_{\mathbb{R}}$. We get a circle and a hyperbola, respectively.

5. We can visualise associated conics with $\mathbb{R}$-rational points (see Figure 1).

Motivated by this last example, we call a quaternion algebra over k *split* if it is isomorphic to $M_2(k)$ as a k-algebra.

Lemma 17. *The following conditions are equivalent:*

1. $(a,b)_k$ *is split.*
2. $(a,b)_k$ *is not a division algebra.*
3. N *is isotropic.*
4. b *is a norm in the quadratic extension* $k(\sqrt{a})/k$.
5. C *has a* k*-rational point.*

Proof. The implication $1 \implies 2$ follows since $M_2(k)$ is never a division algebra, and $2 \iff 3$ follows since $N(q) \neq 0$ if and only if q is invertible. To show $3 \implies 4$, suppose $q = x+yi+zj+wij$ satisfies $N(q) = 0$. Then we have $(z^2-aw^2)b = x^2-ay^2$.

Now suppose that a is not a square in k, for otherwise $k(\sqrt{a}) = k$ and thus b is a norm. Then we see that $N(z + \sqrt{a}w)b = N(x + \sqrt{a}y)$, and since $N(z + \sqrt{a}w) \neq 0$, we have $b = N((x+\sqrt{a}y)/(z+\sqrt{a}w))$. We show 4 $\implies$ 1 to get statements 1-4 equivalent. To do this, we exhibit an isomorphism $(a, b)_k \cong (1, 4a^2)$, which with Example 3 the result follows. Suppose 4, then b^{-1} is also a norm and hence we may write $b^{-1} = s^2 - at^2$ for some $s, t \in k$. Put $c = sj + tij$. Then $c^2 = bs^2 - abt^2 = b(s^2 - at^2) = bb^{-1} = 1$. Put $d = (1+a)i+(1-a)ci$. Since $ci = -ic$, we have $d^2 = (1+a)^2a-(1-a)^2a = 4a^2$, and moreover $cd = (1+a)ci+(1-a)i = -dc$. So we have an isomorphism $(a, b)_k \cong (1, 4a^2)_k$ by $i \mapsto c$, $j \mapsto d$. Finally, we show 4 $\iff$ 5. To show 4 $\implies$ 5, let $b = s^2 - at^2$ for some $s, t \in k$. We see that $P = (x_0, y_0, z_0) = (a^{-1}, b^{-1}t, a^{-1}b^{-1}s)$ is a k-rational point, since multiplying the equation of C by $ab \neq 0$ and substituting in P, we have the calculation

$$ab(a(a^{-1})^2 + b(b^{-1}t)^2 - ab(a^{-1}b^{-1}s)^2) = b + at^2 - s^2 = 0$$

and hence $ax_0^2 + by_0^2 = abz_0^2$. Now to show 5 $\implies$ 4, suppose (x_0, y_0, z_0) is a k-rational point of C. Then at least one of x_0, y_0 are nonzero. If $x_0 \neq 0$, then the point $(u_0, v_0, w_0) := (a^{-1}y_0, b^{-1}x_0, z_0)$ is a k-rational point of the curve

$$C' : \qquad aX^2 + bY^2 = Z^2$$

and since $v_0 \neq 0$, we have $b = (z_0/v_0)^2 - a(u_0/v_0)^2$, so b is a norm in the quadratic extension $k(\sqrt{a})/k$. If $x_0 = 0$ then $y_0 \neq 0$ and similar reasoning lets us deduce that a is a norm in the quadratic extension $k(\sqrt{b})/k$, which is equivalent. □

As a remark, we note that if C has a k-rational point, then it is isomorphic to the projective line $\mathbb{P}^1(k)$. Conversely, it is clear that if $C \cong \mathbb{P}^1(k)$, then C has a k-rational point. So we may add this on as a further equivalent condition to the above. In fact, two generalised quaternion algebras $(a, b)_k, (c, d)_k$ are isomorphic if and only if their associated conics are isomorphic.

Example 4. Fix $a \in k^\times \setminus \{1\}$, then the quaternion algebra $(a, 1 - a)_k$ splits since the associated conic has equation $aX^2 + (1 - a)Y^2 = a(1 - a)Z^2$ and so it is easy to check that $(a^{-1}, (1 - a)^{-1}, a^{-1}(1 - a)^{-1})$ is a k-rational point.

Lemma 18. *The quaternion algebra $(a, b)_k$ is a central simple algebra over k.*

Proof. Centrality: Clearly $k \subset Z((a, b)_k)$. Let $q = x + yi + zj + wij \in Z((a, b)_k)$. Then $qi - iq = -2zij - 2awj = 0$, so $z = 0, w = 0$. And $qj - jq = 2yij = 0$, so $y = 0$. We hence see that $q \in k$.

Simplicity: If $(a, b)_k$ is a division algebra, this is trivial. By virtue of Lemma 17, we may therefore assume that $(a, b)_k$ is split. It is sufficient to show that $M_2(k)$ is

simple. Let $I \subset M_2(k)$ be a nonzero two-sided ideal, and let $0 \neq m \in I$. Then m has a nonzero entry. Denote by E_{ij} the elementary matrix with 1 in the i,jth entry and 0 everywhere else. By applying successive row/column operations to m, we may turn m into E_{ij} for any i, j. This corresponds to multiplying m on the left/right by matrices, so each $E_{ij} \in I$. Since the E_{ij} for $1 \leq i, j \leq 2$ form a basis for $M_2(k)$, we see $I = M_2(k)$. □

3.6 Biquaternion algebras

It follows from Lemma 18 that the tensor product $(a, b)_k \otimes_k (c, d)_k$ is a central simple algebra over k. We refer to such a product as a *biquaternion algebra* over k.

Lemma 19. *Let $(a, b)_k, (a, b')_k$ be quaternion algebras. Then $(a, b)_k \otimes_k (a, b')_k \cong (a, bb')_k \otimes_k M_2(k)$.*

Proof. Choose quaternion bases $\{1, i, j, ij\}$ and $\{1, i', j', i'j'\}$ for $(a, b)_k$ and $(a, b')_k$ respectively.We define two k-subspaces Q_1, Q_2 of $(a, b)_k \otimes_k (a, b')_k$ with bases $\{1 \otimes 1, i \otimes 1, j \otimes j', ij \otimes j'\}$ and $\{1 \otimes 1, 1 \otimes j', i \otimes i'j', (-b'i) \otimes i'\}$ respectively. Since the k-vector spaces generated by these bases are closed under products, it is clear that Q_1, Q_2 are k-subalgebras of $(a, b)_k \otimes_k (a, b')_k$. We have the following:

1. $Q_1 \cong (a, bb')_k$ since we have $(i \otimes 1)^2 = a \otimes 1 = a(1 \otimes 1)$ and $(j \otimes j')^2 = b \otimes b' = bb'(1 \otimes 1)$.

2. $Q_2 \cong (b', -a^2b')_k$ since we have $(1 \otimes j')^2 = 1 \otimes b' = b'(1 \otimes 1)$ and $(i \otimes i'j')^2 = a \otimes (-ab') = -a^2b'(1 \otimes 1)$.

Furthermore, it is easy to see that $(b', -a^2b')_k \cong (b', -b')_k$ via the map $i \mapsto i$, $j \mapsto aj$. And $(b', -b')_k$ is split, since the associated conic has a k-rational point $(1, 1, 0)$.So we see $Q_2 \cong M_2(k)$. Finally, we have the commutator $[Q_1, Q_2] = 0$, which may be verified by computing commutators of basis elements of Q_1 with basis elements of Q_2.

Define

$$\begin{aligned} \phi : Q_1 \times Q_2 &\to (a, b)_k \otimes_k (a, b')_k \\ (x, y) &\mapsto xy. \end{aligned}$$

This induces, by the universal property of the tensor product and the fact that $[Q_1, Q_2] = 0$, a k-algebra homomorphism $Q_1 \otimes_k Q_2 \to (a, b)_k \otimes_k (a, b')_k$. One can check that the induced map is surjective (every element of the induced basis on $(a, b)_k \otimes_k (a, b')_k$ can be attained), and hence the map is an isomorphism by equality of dimensions. □

As a corollary, we obtain

Lemma 20. *Given a quaternion algebra $(a,b)_k$, we have $(a,b)_k \otimes_k (a,b)_k \cong M_4(k)$.*

Proof. Set $b = b'$ in the previous lemma, and observe that $(a,b^2) \cong (a,1)$ by $i \mapsto i, j \mapsto bj$. By item 4 of Example 3, we have $(a,b^2) \cong M_2(k)$. Observing that $M_2(k) \cong M_2(k)^{op}$ by taking a matrix to its transpose, Lemma 16 lets us deduce $M_2(k) \otimes_k M_2(k) \cong M_4(k)$. □

We note that the biquaternion algebra $A = (a,b)_k \otimes_k (c,d)_k$ has a conjugation induced by the conjugations on $(a,b)_k$ and $(c,d)_k$. Specifically, for $q \in (a,b)_k, p \in (c,d)_k$, we let

$$\sigma(q \otimes p) = \overline{q} \otimes \overline{p}$$

and extend to the whole tensor product by linearity. This induced conjugation is not canonical since it depends on the choice of generalised quaternion algebras in the tensor product above. Now let $V \subset A$ be the kernel of the map $a \mapsto a + \sigma(a)$. Let $W \subset A$ be the kernel of the map $a \mapsto a - \sigma(a)$. Then the biquaternion algebra A decomposes into k-subspaces as

$$A = V \oplus W$$

since $V \cap W = 0$, and taking the basis of A induced by products of basis elements of $(a,b)_k$ and $(c,d)_k$ respectively and evaluating the conjugation σ on this basis, we see that V is a 6-dimensional subspace of A and W is a 10-dimensional subspace of A. So the dimensions of V and W correctly add to the dimension of A.

Now given a biquaternion algebra $A = (a,b)_k \otimes_k (c,d)_k$ as before, define the quadratic form

$$A_{\{a,b\}+\{c,d\}} = N_{(a,b)} - N_{(c,d)}$$

where $N_{(a,b)}, N_{(c,d)}$ are the subforms given by the restriction to $V_{(a,b)}, V_{(c,d)}$ of the reduced norms $\langle\langle a,b\rangle\rangle$, $\langle\langle c,d\rangle\rangle$ on $(a,b)_k$ and $(c,d)_k$ respectively, and the underlying vector space for $A_{\{a,b\}+\{c,d\}}$ is the space V defined above. We call such a form an *Albert form*. Note that it depends on the choice of quaternion algebras as before, but any two Albert forms for A are k-scalar multiples of each other. In diagonal presentation, we have

$$A_{\{a,b\}+\{c,d\}} = \langle a, b, -ab, -c-d, cd\rangle$$

(contrast this with the definition given in subsection 2.8).

3.7 Geometry of quaternion algebras

In this subsection, we explore the algebraic geometry of the associated conic to a quaternion algebra. We fix a field k of characteristic not 2 and a quaternion algebra $Q = (a,b)_k$, so that the associated conic C has equation $aX^2 + bY^2 = abZ^2$. Now

consider the ring $R = k[X, Y, Z]/(aX^2 + bY^2 - abZ^2)$. It is a graded ring, so we have a topological space $\mathrm{Proj}(R)$ whose elements correspond to homogeneous prime ideals of R not containing the irrelevant ideal (X, Y, Z). The space $\mathrm{Proj}(R)$ is glued out of three affine patches $\mathbb{A}_X, \mathbb{A}_Y, \mathbb{A}_Z$ which correspond to the localisations at X, Y, Z respectively. To present the following definitions, let us restrict to the affine patch $\mathbb{A}_Z$. By a *closed point* of C we mean a scheme-theoretic point corresponding to a maximal ideal p of $R_{Z,0} := k[X, Y]/(aX^2 + bY^2 - ab)$. We consider the *local ring* $\mathcal{O}_p(C)$ of C at p, which is by definition the localisation of $R_{Z,0}$ at p. The *degree* of a closed point p is the dimension of the residue field $\mathcal{O}_p(C)/p\mathcal{O}_p(C)$ over k. This is finite by a geometric formulation of Hilbert's Nullstellensatz. Clearly a point p is k-rational if and only if it has degree 1. If the scheme-theoretic point does not belong to the affine patch $\mathbb{A}_Z$, then we can simply restrict to a different affine patch in which it does, and then work in that corresponding localisation for the definitions above.

Recall that the kernel of the reduced trace Tr is a 3-dimensional vector subspace V of Q. For every $q \in Q$ we define the linear functional $l_q \in V^*$ by $l_q(x) := Tr(qx)$. Attached to l_q is the line in the projective plane $\mathbb{P}(V)$ defined by the equation $l_q(x) = 0$.

Lemma 21. *Let $p, q \in Q$ and $c_1, c_2 \in k$. Then*

1. *$l_p = l_q$ if and only if $p - q \in k$,*
2. *$l_{c_1 p + c_2 q} = c_1 l_p + c_2 l_q$,*
3. *$l_{\overline{p}} = -l_p$,*
4. *$l_{p^{-1}} = -(N(p))^{-1} l_p$, provided p is invertible.*

Proof. 1. If $l_p = l_q$, then for any $x \in V$ we have $px + \overline{(px)} = qx + \overline{(qx)}$, hence $px + \overline{x}\overline{p} - qx - \overline{x}\overline{q} = 0$ and so along with the fact that since $x \in V$ we have $\overline{x} = -x$, it follows

$$(p - q)x = x(\overline{p - q}). \tag{24}$$

Write $p - q = \alpha + \beta i + \gamma j + \delta ij$. Then set $x = i \in V$. From Equation 24, we get

$$\alpha i + a\beta - \gamma ij - a\delta j = \alpha i - a\beta - \gamma ij - a\delta j$$

which implies $2a\beta = 0$, so $\beta = 0$. Writing down similar equations for $x = j$ and $x = ij$ gives $\gamma = \delta = 0$ too, and hence $p - q \in k$. The converse is clear.

2. This follows from k-linearity of Tr.

3. We have $l_{\overline{p}}(x) + l_p(x) = \overline{p}x + \overline{(\overline{p}x)} + px + \overline{(px)} = \overline{p}x + \overline{x}p + px + \overline{x}\overline{p} = \overline{p}x - xp + px - x\overline{p} = (p + \overline{p})x - x(p + \overline{p}) = 0$ since $p + \overline{p} \in k$ commutes with all $x \in V$.

4. Assume p is invertible. Then $p^{-1} = \overline{p} \cdot N(p)^{-1}$. So for $x \in V$ we have $l_{p^{-1}}(x) = p^{-1}x + \overline{(p^{-1}x)} = \overline{p} \cdot N(p)^{-1}x + \overline{x} \cdot \overline{(\overline{p} \cdot N(p)^{-1})} = N(p)^{-1}(\overline{p}x - \overline{x}p) = N(p)^{-1} \cdot l_{\overline{p}}(x) = -(N(p))^{-1} l_p(x)$ by 3.

□

Lemma 22. *There is a bijective correspondence between quadratic subalgebras of Q and lines in $\mathbb{P}(V)$.*

Proof. Given a quadratic subalgebra K of Q, let $p \in K \setminus k$, so that we may write $K = k[p] := k \oplus kp$. Then given some other choice $q \in K \setminus k$ we have $p = \lambda q + \mu$ for some $\lambda \in k^\times, \mu \in k$, hence $l_p = l_{\lambda q + \mu} = \lambda l_q + l_\mu = \lambda l_q$ by Lemma 21 and therefore l_p, l_q determine the same line in $\mathbb{P}(V)$. So there is a well-defined map taking quadratic subalgebras to lines in $\mathbb{P}(V)$. Conversely, since Tr is a nondegenerate bilinear form on Q, every linear functional on V can be expressed as l_q for some $q \in Q$. Hence every line in $\mathbb{P}(V)$ is given by $l_q(x) = 0$ for some $q \in Q$. We see that $q \notin k$ since otherwise l_q is trivial. So q generates a quadratic subalgebra of Q. It is easy to see that these maps are mutually inverse. □

3.8 Divisors on the associated conic

Now we briefly introduce divisors. A more detailed treatment of them is given in Fulton's book [3]. By a *divisor* on C we mean a $\mathbb{Z}$-valued function on the closed points of C with finite support. Hence a divisor is equivalent to a formal finite sum $D := n_1 p_1 + n_2 p_2 + \cdots + n_k p_k$ for some $k \in \mathbb{N}$, where the p_i are closed points on C and the n_i are integers. We define the *degree* of D as the sum $\sum_{i=1}^{k} n_i \cdot \deg(p_i)$. We say D is *effective* if each of the $n_i \geq 0.$, and in this case we write $D \geq 0$. Given a rational function $f \in k(C)$, we define the *divisor of poles and zeros* for f as the divisor $\operatorname{div}(f) := \sum_{p \in C} \operatorname{ord}_p(f) \cdot p$, where the sum is indexed over all closed points p of C, and $\operatorname{ord}_p(f)$ is equal to the order of f in the discrete valuation ring $\mathcal{O}_p(C)$. Since C is projective, it is easy to see that $\deg \operatorname{div}(f) = 0$.

Given a divisor D on C, we define the *Riemann-Roch space* $L(D)$ attached to D as the vector space

$$L(D) := \{f \in k(C) \mid D + \operatorname{div}(f) \geq 0\} \cup \{0\}.$$

Hence, writing $D = \sum n_p p$, $L(D)$ consists of all those rational functions whose zeroes at each p with negative coefficient have order at least $-n_p$, and whose poles at each p with positive coefficient have order at most n_p. Attached to C is a divisor ω, called a *canonical divisor* of C.

Example 5. If Q is split, then C is isomorphic to $\mathbb{P}^1(k)$ as a projective curve, and hence we may choose $\omega = -2(\infty)$ where (∞) is the point at infinity of $\mathbb{P}^1(k)$. Then the Riemann-Roch theorem gives the equality of dimensions

$$\dim_k L(D) - \dim_k L(\omega - D) = \deg(D) - g + 1$$

with $g = 0$. We have two cases: If $\deg(D) \geq 0$, then for any $f \in k(C)$ we have $\deg(\mathrm{div}(f)+\omega-D) < 0$, and so $\mathrm{div}(f)+\omega-D$ is not effective. Hence $\dim_k L(\omega-D) = 0$ and so we have $\dim_k L(D) = \deg(D) + 1$. If $\deg(D) < 0$, then $\mathrm{div}(f) + D$ is not effective and so clearly $\dim_k L(D) = 0$. So in summary we have

$$\dim_k L(D) = \begin{cases} \deg(D) + 1, & \deg(D) \geq 0, \\ 0, & \deg(D) < 0. \end{cases}$$

In particular, if $\deg(D) = 0$, then $\dim_k L(D) = 1$, and so we may choose nonzero $f \in L(D)$ such that $\mathrm{div}(f) + D \geq 0$. Since the left hand side has degree zero, it follows that $\mathrm{div}(f) + D = 0$. But then $D = -\mathrm{div}(f) = \mathrm{div}(1/f)$. So every divisor of degree zero on C is principal.

Since the canonical divisor is stable under field extensions (since the tangent bundle of C is), the degree of the canonical divisor ω on C is the same as that on $\mathbb{P}^1$. So the degree of ω on C is -2, and the same argument as above still works to show that in the nonsplit case too, every divisor on C of degree zero is principal.

Lemma 23. *There is a bijective correspondence between lines in $\mathbb{P}(V)$ and degree two effective divisors on C.*

Proof. Taking the intersection of the line defined by l_q with the associated conic C, we get a degree two effective divisor on C. Conversely, given a degree two effective divisor D on C, we have two cases: Either $D = p_1 + p_2$ with p_1, p_2 k-rational points, or $D = p$, with p a degree two closed point of C. In the first case it is clear that we get a line in $\mathbb{P}(V)$ by assigning the unique line that passes through p_1 and p_2 (this is a tangent to C in the case $p_1 = p_2$). In the second case, we get a line by passing to the splitting field K of p, where p splits into two k-rational points p_1, p_2 which are distinct since the characteristic of k is not two. Then the $\mathrm{Gal}(K/k)$-action which swaps p_1 and p_2 preserves the line between them, and so this line must exist over the base field k. □

3.9 Nonsplit conics

We now specialise to the case when Q is a division algebra, with which the geometry of the associated conic becomes simpler. Hence, we will assume Q is a division algebra until we state otherwise.

Lemma 24. *A k-subalgebra K of Q of dimension 2 is a quadratic (maximal) subfield of Q.*

Proof. Since K contains a copy of k we can write $K = k \oplus kx$ for some $x \in K \setminus k$. Then given two elements $a + bx, c + dx \in K$, we have

$$(a + bx)(c + dx) = ac + bdx^2 + (ad + bc)x,$$
$$(c + dx)(a + bx) = ca + dbx^2 + (da + cb)x,$$

which are equal since $a, b, c, d \in k$. So K is commutative. Now to show it is a subfield, it is sufficient to show that the (left or right) inverse $x^{-1} \in K$. Indeed, we have $x^{-1} = \overline{x}/N(x)$, and since $\overline{x} \in K$, it follows $x^{-1} \in K$. □

Since Q is nonsplit, C does not have any k-rational points. It follows that an effective divisor D on C of degree two must be prime, i.e. $D = p$ for a closed point p of degree two. Hence Lemmas 22 and 23 specialise to

Lemma 25. *There is a bijective correspondence between quadratic subfields of Q and closed points of degree 2 in C.*

We would then expect there to be a relationship between the quadratic subfield K of Q and the residue field of the corresponding closed point p in C. Indeed, we have the following result:

Theorem 8 (Correspondence between subfields and residue fields)**.** *Let K be a quadratic subfield of Q, let p be the corresponding closed point of degree 2 in C, and let $\kappa(p)$ be the residue field at p. Then we have a canonical isomorphism*

$$\phi : K \to \kappa(p).$$

The isomorphism operates as follows: Choose a quadratic subfield K of Q. First,choose $q \in Q \setminus K$, so that we can write $Q = K \oplus qK$. Then given any $c \in Q$, write $c = a + bq$ for unique $a, b \in K$. We identify the linear forms l_c, l_b with their corresponding linear homogeneous polynomials; then

$$\phi : b \mapsto \frac{l_c}{l_b}(p) \in \kappa(p).$$

The map ϕ as defined may be verified to a well-defined ring homomorphism from K to $\kappa(p)$, which is surjective and injective. A proof of this can be found in Merkurjev's paper [6].

4 Milnor K-theory of fields

4.1 Construction

Let k be a field. Then we can consider the multiplicative group $k^\times$ as a $\mathbb{Z}-$module. Let $T_\mathbb{Z}(k^\times)$ denote the tensor algebra of $k^\times$ over $\mathbb{Z}$ - this is the $\mathbb{Z}_{\geq 0}$-graded algebra

$$T_\mathbb{Z}(k^\times) = \oplus_{n=0}^\infty k^* \otimes_\mathbb{Z} \cdots \otimes_\mathbb{Z} k^\times = \mathbb{Z} \oplus k^\times \oplus (k^\times \otimes_\mathbb{Z} k^\times) \oplus \dots$$

with the product

$$(v_1 \otimes \cdots \otimes v_m) \cdot (w_1 \otimes \cdots \otimes w_n) = (v_1 \otimes \cdots \otimes v_m \otimes w_1 \otimes \cdots \otimes w_n).$$

The *Milnor K-theory* of k is the quotient algebra

$$K_*^M(k) = T_\mathbb{Z}(k^\times)/(a \otimes (1-a), a \in k \setminus \{0,1\}).$$

We have the direct sum decomposition

$$K_*^M(k) = \bigoplus_{i=0}^\infty K_i^M(k)$$

where $K_0^M(k) = \mathbb{Z}, K_1^M(k) = k^\times$. By the very definition of $K_*^M(k)$, it is generated by $K_1^M(k)$. We identify each $a \in k^\times$ with $\{a\} \in K_1^M(k)$, and the product $\{a_1\} \cdot \cdots \cdot \{a_n\} \in K_n^M(k)$ is denoted $\{a_1, \dots, a_n\}$ and is called a *pure symbol*. Below are some basic algebraic properties of K^M:

Lemma 26. *For any $a \in k^\times$, we have $\{a, a\} = \{a, -1\}$.*

Proof. If $a = 1$, then on the one hand $\{a, a\} = 1 \otimes_\mathbb{Z} 1 = 0$ (we are regarding 1 as the neutral element of $k^\times$), and on the other hand $\{a, -1\} = 1 \otimes_\mathbb{Z} -1 = 0$. If $a \in k^\times \setminus \{1\}$, then $-\{a\} = \{1/a\}$,and hence

$$\begin{aligned} 0 = \{1/a, 1-1/a\} = -\{a, 1-1/a\} &= -\{a, (1-a)/(-a)\} \\ &= -\{a, 1-a\} + \{a, -a\} = \{a, -a\} \end{aligned}$$

So $0 = \{a, -a\} = \{a, a/(-1)\} = \{a, a\} - \{a, -1\}$, which means $\{a, a\} = \{a, -1\}$. □

Lemma 27. *For any $a, b \in k^\times$, we have $\{a, b\} = -\{b, a\}$.*

Proof. We have for any $a, b \in k^\times$, using bilinearity, $\{ab, ab\} = \{a, a\} + \{b, b\} + (\{a, b\} + \{b, a\})$. It remains to show that $\{a, a\} + \{b, b\} = \{ab, ab\}$. Using Lemma 26, we get $\{a, a\} + \{b, b\} = \{a, -1\} + \{b, -1\} = \{ab, -1\} = \{ab, ab\}$. □

From this proposition with the fact that $K_*^M(k)$ is generated by the first-degree component, it follows that for any $x \in K_n^M(k), y \in K_m^M(k)$, we have $xy = (-1)^{nm}yx$. So $K_*^M(k)$ is *skew-commutative*. Of course, the relations $\{a, 1-a\} = 0$ and $\{a, -a\} = 0$ generalise easily: We have for $a_1, \ldots, a_n \in k^\times$ $\{a_1, \ldots, a_n\} = 0$ if $a_1 + \cdots + a_n = 1$ or $a_1 + \cdots + a_n = 0$.

Example 6. 1. We compute $K_*^M(\mathbb{F}_q)$ where $\mathbb{F}_q$ is a finite field of q elements. Clearly $K_1^M(\mathbb{F}_q) = \mathbb{Z}/(q-1)$. Choose a generator a for $\mathbb{F}_q^\times$. Then since we have a surjective homomorphism $F_q^\times \otimes F_q^\times \to K_2^M(\mathbb{F}_q)$, it follows $K_2^M(\mathbb{F}_q)$ is cyclic with generator $\{a, a\}$. Since $\{a, a\} = \{a, -1\}$, this generator has order no more than 2, which means $K_2^M(\mathbb{F}_q)/2 = K_2^M(\mathbb{F}_q)$. The equation $x^2 + y^2 = a$ has a solution in $\mathbb{F}_q$ by a counting argument: The number of elements of the form x^2 is $1+(q-1)/2$ and the number of elements of the form $a-y^2$ is also $1+(q-1)/2$ for $x, y \in \mathbb{F}_q$. Since the sum is greater than q, there must exist an element that can be presented both as x^2 and $a - y^2$. Since a generates a cyclic group, it is not a square, and so we must have $x, y \neq 0$. Hence we have $(y/x)^2 - a/x^2 = -1$. Now working in $K_2^M(\mathbb{F}_q)/2$, we see that $\{1/(x^2), -1\} = -\{x^2, -1\} = 0$ and $\{a/(x^2), (y/x)^2\} = 0$, so that we have the following:

$$\begin{aligned}\{a, -1\} &= \{a, -1\} + \{1/(x^2), -1\} + \{a/(x^2), (y/x)^2\} \\ &= \{a/(x^2), -1\} + \{a/(x^2), (y/x)^2\} \\ &= \{a/(x^2), -(y/x)^2\} = 0.\end{aligned}$$

Hence $K_2^M(\mathbb{F}_q)$ is zero, and so $K_n^M(\mathbb{F}_q)$ is zero for $n \geq 2$.

2. Next, we compute $K_*^M(\mathbb{R})/2K_*^M(\mathbb{R})$. We have $K_*^M(\mathbb{R})/2K_*^M(\mathbb{R}) = (T_{\mathbb{Z}}(\mathbb{R}^\times)/2T_{\mathbb{Z}}(\mathbb{R}^\times))/(a \otimes (1-a)\ a \in \mathbb{R}\backslash\{0,1\})$. But $T_{\mathbb{Z}}(\mathbb{R}^\times)/2T_{\mathbb{Z}}(\mathbb{R}^\times) = T_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{R}^\times/(\mathbb{R}^\times)^2)$, and $\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \mathbb{Z}/2\mathbb{Z}$. So $T_{\mathbb{Z}/2\mathbb{Z}}(\mathbb{R}^\times/(\mathbb{R}^\times)^2) = \mathbb{Z}/2\mathbb{Z}[t]$, where $t = -1$. Any element of the form $a \otimes (1-a)$ is zero in $(\mathbb{R}^\times/(\mathbb{R}^\times)^2)^{\otimes 2}$, since either a or $1-a$ is positive. It follows that

$$K_*^M(\mathbb{R})/2 = T_{\mathbb{Z}/2}(\mathbb{R}^\times/(\mathbb{R}^\times)^2) = \mathbb{Z}/2[t].$$

4.2 Functoriality

We now fix fields F, L. We may regard K_*^M as a (covariant) functor from the category of fields to the category of graded abelian groups. This is because a field extension L/F induces a group homomorphism $K_*^M(F) \to K_*^M(L)$ defined by sending a symbol $\{a_1, \ldots, a_n\}$ to itself. It is easy to see that a trivial field extension F/F induces the identity map on the corresponding Milnor K-theories, and that K_*^M respects towers $K \supset L \supset F$ of field extensions. Given $u \in K_*^M(F)$, we write u_L for the image of u in $K_*^M(L)$.

4.3 Residue map

Give F a discrete valuation $v : F^\times \to \mathbb{Z}$, that is to say a group homomorphism satisfying $v(x+y) \geq \min\{v(x), v(y)\}$. Let $\overline{F}$ denote the residue field. We may regard v as a group homomorphism

$$v : K_1^M(F) \to K_0^M(F),$$

which extends uniquely to a *residue homomorphism*

$$\partial : K_n^M(F) \to K_{n-1}^M(F),$$

defined as follows. Choose a prime element t (that is $t \in F^\times$ such that $v(t) = 1$) and let $\overline{u}$ denote the image of u in $\overline{F}$. Given a symbol $\{a_1, a_2, \ldots, a_n\}$, write each $a_i = u_i \cdot t^{k_i}$ for some unit u_i and integer k_i. Then, using linearity of the symbols and the identity $\{a, a\} = \{a, -1\}$, we get that we may write $\{a_1, a_2, \ldots, a_n\}$ as a sum of symbols of the form $\{t, u_2, \ldots, u_n\}$ and $\{u_1, u_2, \ldots, u_n\}$. Now define

$$\begin{aligned} \partial : \{t, u_2, \ldots, u_n\} &\mapsto \{\overline{u_2}, \ldots, \overline{u_n}\}, \\ \{u_1, \ldots, u_n\} &\mapsto 0. \end{aligned}$$

This specifies ∂ completely, so if such a map exists, it is unique. A construction of the residue map due to Serre is found in [7].

When we set $F = k(C)$, the function field of the associated conic to a quaternion algebra, then given a closed point $p \in C$ there is a residue homomorphism

$$\partial_p : K_2^M(F) \to K_1^M(\overline{F}) = K_1^M(\kappa(p)) = \kappa(p)^\times$$

induced by the discrete valuation of the local ring $\mathcal{O}_p(C)$.

4.4 Norm map

Let L/F be a field extension. Suppose that L/F is finite. Then there is the classical norm homomorphism

$$N_{L/F} : L^\times \to F^\times$$

given for each $a \in L^\times$ by the determinant of the F-linear transformation $x \mapsto ax$. When L/F is Galois, we have

$$N_{L/F}(a) = \prod_{\sigma \in \mathrm{Gal}(L/F)} \sigma(a).$$

Similarly to before, the norm map may be viewed as a group homomorphism

$$N_{L/F} : K_1^M(L) \to K_1^M(F).$$

The induced homomorphism $K_*^M(F) \to K_*^M(L)$ endows $K_*^M(L)$ with the structure of a $K_*^M(F)$-module. It is true that $N_{L/F}$ extends uniquely to a $K_*^M(F)$-linear *norm residue map* defined in any degree

$$N_{L/F} : K_*^M(L) \to K_*^M(F)$$

by the residue map defined above, and Milnor's computation of Milnor's K-theory for a function field in one variable., also given in [7]. A theorem of Kato characterises the norm homomorphisms associated with L/F on Milnor K-theory. The properties we need are:

1. The induced homomorphism $K_*^M F \to K_*^M L$ composes with the norm map in the following way: For $u \in K_*^M F$ we have

$$N_{L/F}(u_L) = [L : F] \cdot u.$$

2. If L/F is Galois with Galois group G, then

$$(N_{L/F}(u))_L = \sum_{\sigma \in G} \sigma u$$

where σu is the natural action (see the discussion following Lemma 38 for the description for $K_2^M(k)$, the only component we consider the norm map on).

4.5 Milnor K-theory mod 2 and the graded Witt ring

The induced grading on the quotient $K_*^M(k)/2K_*^M(k) = \bigoplus_{n \geq 0} K_n^M(k)/2K_n^M(k)$ lets us define the *nth Milnor K-group mod 2* $k_n^M(k) := K_n^M(k)/2K_n^M(k)$. We have $k_0^M(k) = \mathbb{Z}/2\mathbb{Z}$ and since for any $a \in k^\times$ we have $2\{a\} = \{a^2\}$, it follows that $k_1^M(k) = k^\times / (k^\times)^2$. The second degree component $k_2^M(k)$ of $K_*^M(k)/2K_*^M(k)$ admits the following description by generators and relations: It is generated as an $\mathbb{F}_2$-vector space by symbols $\{a, b\}$ with $a, b \in k^\times$, subject to the relations $\{aa', b\} = \{a, b\} + \{a', b\}$, $\{a, bb'\} = \{a, b\} + \{a, b'\}$ and $\{a, b\} = 0$ if $a + b = 1$.

Revisiting the graded Witt ring and Pfister forms introduced in Subsection 2.8, we will now introduce a map from Milnor K-theory mod 2 to the graded Witt ring.

Proposition 12. *There is a well-defined surjective homomorphism*

$$\phi : k_*^M(k) \to gr_{I^\bullet}(k)$$

which takes the class of a pure symbol $\{a\}$ *to the corresponding 1-fold Pfister form* $\langle\langle a \rangle\rangle$.

Proof. Recalling the definition of Milnor K-theory, we see that $k_*^M(k)$ is the quotient of the tensor algebra over $\mathbb{Z}/2$ of the $\mathbb{F}_2$-vector space $k^\times/(k^\times)^2$ by the ideal generated by elements $a \otimes (1-a)$ for all $a \in k^\times \setminus \{1\}$. Since we have the identifications

$$k_0^M(k) \quad = \quad \mathbb{Z}/2\mathbb{Z} \quad = \quad \mathrm{gr}_{I^\bullet}(k)_0$$

$$k_1^M(k) \quad = \quad k^\times/(k^\times)^2 \quad = \quad \mathrm{gr}_{I^\bullet}(k)_1$$

we get an induced $\mathbb{F}_2$-algebra homomorphism $\phi : T_{\mathbb{Z}/2}(k^\times/(k^\times)^2) \to \mathrm{gr}_{I^\bullet}(k)$. We now need to check that ϕ descends to a well-defined homomorphism on the quotient, for which it is sufficient to check that elements of the shape $a \otimes (1-a)$ are mapped to zero. We have $\phi(a \otimes (1-a)) = \langle\langle a, 1-a\rangle\rangle \in I^2/I^3 = \mathrm{gr}_{I^\bullet}(k)_0$. Expanding, we see

$$\langle\langle a, 1-a\rangle\rangle = \langle\langle a\rangle\rangle \cdot \langle\langle 1-a\rangle\rangle = \langle 1, -a\rangle \cdot \langle 1, a-1\rangle = \langle 1, -a, a-1, a-a^2\rangle.$$

To check that this form is zero in $\mathrm{gr}_{I^\bullet}(k)$, it is sufficient to show that it is hyperbolic. But by Theorem 4, it is enough to show that $\langle 1, -a, a-1, a-a^2\rangle$ is isotropic, which is true since $(1,1,1,0)$ is an isotropic vector. By definition, the graded algebra $\mathrm{gr}_{I^\bullet}(k)$ is generated by the first degree component, and clearly this is contained in the image of ϕ by the identifications above. Hence it follows that ϕ descends to a well-defined surjective ring homomorphism . □

In fact, ϕ is an isomorphism, however showing the injectivity of ϕ is a terribly difficult endeavour. It is a result of Voevodsky that ϕ turns out to be an isomorphism (see [8] for a proof). In particular, this implies there is an isomorphism

$$\begin{aligned} k_2^M(k) &\to I^2/I^3 \\ \{a, b\} &\mapsto \langle\langle a, b\rangle\rangle. \end{aligned}$$

We are going to prove this degree two isomorphism by elementary means. To do this, it is sufficient to introduce a group homomorphism from I^2/I^3 to $k_2^M(k)$, which is left-inverse to ϕ_2.

4.6 Stiefel-Whitney classes

Let us introduce the notation $\overline{k^M}(k)/2$ for the product $\prod_{n\geq 0} k_n^M(k)$. Let q be a quadratic form, and let $\langle a_1, \ldots, a_n\rangle$ be a diagonalisation of q. We define the *total Stiefel-Whitney class* $sw_\bullet$ of this diagonalisation as the element

$$\left(\prod_{i=1}^{n}(1+\{a_i\})\right)^{-1} \cdot (1+\{-1\})^{[n/2]} \in \overline{k^M}(k)/2.$$

Then we define the *individual Stiefel-Whitney classes* $sw_i \in k_i^M(k)$ of the diagonalisation $\langle a_1, \ldots, a_n \rangle$ as the ith graded component of the total class $sw_\bullet$. For $sw_\bullet$ to be an invariant of the quadratic form q, it shouldn't depend on the choice of diagonalisation. Indeed, this is the case:

Proposition 13. *Let q be a quadratic form. Then the Stiefel-Whitney class $sw_\bullet$ of any two diagonalisations of q are equal.*

Proof. Recalling the Witt Chain Equivalence theorem of Subsection 2.9, it is sufficient to demonstrate the equality for any two chain equivalent diagonalisations, for which it is sufficient to demonstrate equality for two diagonalisations of the same 2-dimensional form. So let $\langle a, b \rangle \cong \langle c, d \rangle$ be two isomorphic forms. Then we have

$$\begin{aligned} sw_\bullet(\langle a, b \rangle) &= ((1 + \{a\}) \cdot (1 + \{b\}))^{-1} \cdot (1 + \{-1\}) \\ &= (1 + \{a\} + \{b\} + \{a, b\})^{-1} \cdot (1 + \{-1\}) \end{aligned}$$

and thus $sw_\bullet(\langle a, b \rangle) = sw_\bullet(\langle c, d \rangle)$ if and only if

$$\{ab\} + \{a, b\} = \{cd\} + \{c, d\}.$$

By computing determinants of the forms, we see that $ab/cd \neq 0$ is a square in k, and so it follows that $\{ab\} = \{cd\}$ in $k_1^M(k)$. Hence we are left to showing that $\{a, b\} = \{c, d\}$ in $k_2^M(k)$. Because c is a value of $\langle a, b \rangle$ we have $c = ax^2 + by^2$ for some $x, y \in k$. Since $c \neq 0$ we may assume first that $x \neq 0$. Furthermore, because ab, cd are equal modulo $(k^\times)^2$, we have $d = abcl^2$, where $l \in k^\times$. Hence in $k_2^M(k)$ we have

$$\begin{aligned} \{c, d\} &= \{c, abl^2 c\} \\ &= \{c. - abl^2\} + \{c, -c\} \\ &= \{c, -abl^2\} \\ &= \{ax^2 + by^2, -ab\} \\ &= \{ax^2(1 + by^2/(ax^2)), -ab\} \\ &= \{ax^2, -ab\} + \{1 - (-by^2/(ax^2)), -ab\} \\ &= \{a, -ab\} + \{1 - (-by^2/(ax^2)), -ab(y/ax)^2\} \\ &= \{a, -a\} + \{a, b\} \\ &= \{a, b\} \end{aligned}$$

as required. □

By virtue of the above proposition, we may simply define the Stiefel-Whitney class of q as the Stiefel-Whitney class of any one of its diagonalisations.

Proposition 14. *Let p and q be quadratic forms. Suppose that* $\dim(p)$ *is even. Then*

$$sw_\bullet(q) \cdot sw_\bullet(p) = sw_\bullet(p \perp q).$$

Proof. Choose diagonalisations $p = \langle a_1, \ldots, a_n \rangle$, $q = \langle b_1, \ldots, b_{2m} \rangle$. Then we have

$$\begin{aligned} sw_\bullet(q) \cdot sw_\bullet(p) &= \left(\prod_{i=1}^{n} (1 + \{a_i\}) \right)^{-1} \cdot (1 + \{-1\})^{[n/2]} \cdot \left(\prod_{i=1}^{2m} (1 + \{b_i\}) \right)^{-1} \cdot (1 + \{-1\})^{[2m/2]} \\ &= \left(\prod_{i=1}^{n} (1 + \{a_i\}) \prod_{i=1}^{2m} (1 + \{b_i\}) \right)^{-1} \cdot (1 + \{-1\})^{[n/2]+[m]} \\ &= sw_\bullet(q \perp p) \end{aligned}$$

since $[n/2] + [m] = [(n + 2m)/2]$. □

The above proposition along with the following lemma implies that taking Stiefel-Whitney classes descends to a well-defined group homomorphism from I to $\overline{k^M}_2(k)$:

Lemma 28. *The Stiefel-Whitney class* $sw_\bullet(\mathbb{H}) = 1$.

Proof. Direct calculation:

$$sw_\bullet(\mathbb{H}) = ((1 + \{1\}) \cdot (1 + \{-1\})^{-1} \cdot (1 + \{-1\})^{[2/2]} = 1.$$

□

Hence by Proposition 14, $sw_\bullet(q)$ depends only on the class of q in $W(k)$. Since all elements of the fundamental ideal I have even dimension, the claim that $sw_\bullet$ descends to a well-defined group homomorphism

$$sw_\bullet : I \to (\overline{k^M}(k))^\times$$

follows.

Lemma 29. *Let q be a quadratic form. The first Stiefel-Whitney class $sw_1(q)$ coincides with the signed discriminant* $\det_\pm(q)$ *introduced in Subsection 2.8.*

Proof. Write $q = \langle a_1, \ldots, a_n \rangle$ for some $a_i \in k^\times$, $1 \leq i \leq n$. Then

$$\begin{aligned} sw_1(q) &= \left(\left(\prod_{i=1}^{n} (1 + \{a_i\}) \right)^{-1} \cdot (1 + \{-1\})^{[n/2]} \right)_1 \\ &= -\sum_{i=1}^{n} \{a_i\} + [n/2]\{-1\} \\ &= \left\{ (-1)^{[n/2]} \cdot \prod_{i=1}^{n} a_i \right\} = \{\det_\pm(q)\} \end{aligned}$$

in $k_1^M(k) = k^\times/(k^\times)^2$. □

The above lemma along with the characterisation of forms in I^2 given in Subsection 2.8 implies that quadratic forms q in I^2 have the property that $sw_1(q) = 1$ is trivial.

Lemma 30. *Let $p, q \in I$. Then:*

1. $sw_1(p+q) = sw_1(p) + sw_1(q)$.
2. $sw_2(p+q) = sw_2(p) + sw_2(q) + sw_1(p) \cdot sw_1(q)$.

Proof. Recalling that for $p, q \in I$ we have $sw_\bullet(p+q) = sw_\bullet(p) \cdot sw_\bullet(q)$, it follows

$$1+sw_1(p+q)+sw_2(p+q)+\cdots = (1+sw_1(p)+sw_2(p)+\dots)(1+sw_1(q)+sw_2(q)+\dots).$$

Expanding the right hand side, we get

$$1 + (sw_1(p) + sw_1(q)) + (sw_2(p) + sw_2(q) + sw_1(p)sw_1(q)) + \dots,$$

from which the result follows. □

We now consider the second individual Stiefel-Whitney class $sw_2(q)$ of a quadratic form q.

Proposition 15. *The Stiefel-Whitney map sw_2 is left-inverse to the restriction*

$$\begin{aligned} \phi_2 : k_2^M(k) &\to I^2/I^3 \\ \{a, b\} &\mapsto \langle\langle a, b\rangle\rangle \end{aligned}$$

of the map ϕ introduced in Proposition 12 to $k_2^M(k)$. Hence ϕ is an isomorphism in degree two.

Proof. First, by Lemmas 29 and 30, we see that if $p, q \in I^2$, then $sw_2(p+q) = sw_2(p) + sw_2(q)$, which shows that $sw_2 : I^2 \to k_2^M(k)$ is additive. Secondly, we have

$$sw_2(\langle\langle a, b\rangle\rangle) = \{a, b\}$$

since

$$\begin{aligned} sw_\bullet(\langle\langle a\rangle\rangle) &= (1 + \{-a\})^{-1} \cdot (1 + \{-1\}) \\ &= (1 + \{-a\} + \{-a, -a\} + \{-a, -a, -a\} + \dots) \cdot (1 + \{-1\}) \\ &= (1 + \{-a\} + \{-a, -1\} + \{-a, -1, -1\} + \dots) \cdot (1 + \{-1\}) \\ &= (1 + \{-a\} \cdot (1 + \{-1\} + \{-1, -1\} + \dots)) \cdot (1 + \{-1\}) \\ &= (1 + \{-a\} \cdot (1 + \{-1\}^{-1}) \cdot (1 + \{-1\}) \\ &= 1 + \{-1\} + \{-a\} = 1 + \{a\} \end{aligned}$$

shows that $sw_1(\langle\langle a\rangle\rangle) = \{a\}$ and $sw_2(\langle\langle a\rangle\rangle) = 0$, and since $\langle\langle a,b\rangle\rangle + \langle\langle ab\rangle\rangle = \langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle$ in the Witt ring, we have the equality of the expressions

$$sw_2(\langle\langle a,b\rangle\rangle) + sw_2(\langle\langle ab\rangle\rangle) + sw_1(\langle\langle a,b\rangle\rangle) \cdot sw_1(\langle\langle ab\rangle\rangle)$$

and

$$sw_2(\langle\langle a\rangle\rangle) + sw_2(\langle\langle b\rangle\rangle) + sw_1(\langle\langle a\rangle\rangle) \cdot sw_1(\langle\langle b\rangle\rangle),$$

from which we see $sw_2(\langle\langle a,b\rangle\rangle) = sw_1(\langle\langle a\rangle\rangle) \cdot sw_1(\langle\langle b\rangle\rangle) = \{a,b\}$.

We now check that sw_2 descends to a well-defined group homomorphism $I^2/I^3 \to k_2^M(k)$. We want to show that $sw_2(I^3) = 0$, for which it is sufficient to show that for any 3-fold Pfister form $\langle\langle a,b,c\rangle\rangle$, $sw_2(\langle\langle a,b,c\rangle\rangle) = 0$ (since they generated I^3). Since in the Witt ring we have $\langle\langle a,b\rangle\rangle = \langle\langle a\rangle\rangle + \langle\langle b\rangle\rangle - \langle\langle ab\rangle\rangle$, it follows that

$$\langle\langle a,b,c\rangle\rangle = \langle\langle a,c\rangle\rangle + \langle\langle b,c\rangle\rangle - \langle\langle ab,c\rangle\rangle$$

whence

$$\begin{aligned} sw_2(\langle\langle a,b,c\rangle\rangle) &= \{a,c\} + \{b,c\} - \{ab,c\} \\ &= \{ab,c\} - \{ab,c\} = 0. \end{aligned}$$

Now to show sw_2 is left-inverse to ϕ_2, it is sufficient to show that $sw_2 \circ \phi_2$ is the identity map when restricted to pure symbols (since they generate $k_2^M(k)$. Let $\{a,b\} \in k_2^M(k)$. Then

$$(sw_2 \circ \phi_2)(\{a,b\}) = sw_2(\langle\langle a,b\rangle\rangle) = \{a,b\}$$

as required. □

5 Norm residue isomorphism theorem in degree two

Let $\mathrm{Br}_2(k)$ denote the subset of elements of $\mathrm{Br}(k)$ with order at most 2; this is clearly a subgroup. We have a map

$$h_k : k_2^M(k) \to \mathrm{Br}_2(k)$$

defined on the classes of pure symbols by $\{a,b\} + 2K_2^M(k) \mapsto (a,b)_k$, and extended to the whole of $k_2^M(k)$ as a group homomorphism. This map is well-defined: The Brauer-equivalence class of $(a,b)_k$ is bilinear with respect to a and b by Lemma 19 and the easy fact that $(a,b)_k \cong (b,a)_k$. By the lemma following after, it has order at most two in the Brauer group. And $(a,b)_k$ is split if $a+b=1$, by Example 4.

Theorem 9 (Norm-residue, Merkurjev [6])**.** *The norm residue homomorphism*

$$h_k : k_2^M(k) \to Br_2(k)$$

taking a pure symbol $\{a,b\}$ mod $2K_2^M(k)$ to the Brauer-equivalence class of $(a,b)_k$, is an isomorphism.

The rest of the dissertation is dedicated to the proof of Theorem 9. For the record, we note the fact that the norm map on Milnor K-theory and the norm residue homomorphism just introduced commute as follows: We have

$$N_{L/F}\left(h_L(u)\right) = h_F(N_{L/F}(u)).$$

It also commutes with the induced homomorphism $K_2^M F \to K_2^M L$ as follows: We have for $u \in K_2^M F$

$$h_F(u)_L = h_L(u_L).$$

Proofs of these facts are found in [2].

5.1 Key exact sequence

The proof of Theorem 9 will follow easily once we have proved the exactness of the sequence given in the introduction in Equation (5). For the sake of convenience, we restate:

Theorem 10 (Key exact sequence)**.** *Let C be a smooth conic curve over a field k of characteristic not 2. Then the sequence*

$$K_2^M(k) \longrightarrow K_2^M(k(C)) \xrightarrow{\partial} \bigoplus_{p\in C} \kappa(p)^\times \xrightarrow{N} k^\times$$

where $\partial = \bigoplus \partial_p$ and N is given by the norm maps $N_{\kappa(p)/k}$, is exact.

Following an approach similar to Milnor in [7], we will define an ascending filtration on $K_2^M(k(C))$ by Milnor K-groups associated to a sequence of Riemann-Roch spaces. Then we will demonstrate the key exact sequence for each of these intermediate spaces, from which the main result follows by taking a direct limit.

We now introduce these spaces: Fix a closed point p_0 of C of degree 2. Given an integer $n \in \mathbb{Z}$, we let $L_n := L(np_0)$. Thus L_n consists of 0, and all of those $f \in k(C)$ that have a pole at p_0 of order at most n, and no poles anywhere else. We treat p_0 as the point at infinity. Clearly

$$\cdots \subset L_{-3} \subset L_{-2} \subset L_{-1} \subset L_0 = k \subset L_1 \subset L_2 \subset L_3 \subset \ldots,$$

and $L_n \cdot L_m \subset L_{n+m}$ for all $n, m \in \mathbb{Z}$. We have the natural inclusion maps $i_{n,m} : L_n \to L_m$ for every $m \geq n$.

We now assume that C is nonsplit, since in the split case Theorem 10 is covered by Milnor's exact sequence for the computation of the Milnor K-theory of the function field of $\mathbb{P}^1$, given in [7]. Then by Example 5, for each $n \geq 0$ the Riemann-Roch space L_n has dimension $2n + 1$, and otherwise L_n has dimension 0. Also, every point on C has even degree, since in this case Q is a division algebra, and thus the degree of every finite splitting field extension is even. Furthermore, given a closed point p on C of degree $2n$, we may find a nonzero function $\pi_p \in L_n$ such that $\operatorname{div}(\pi_p) = p - np_0$.

Now for each $n \in \mathbb{Z}$, we let M_n be the subgroup generated by symbols $\{f, g\}$ where $f, g \in L_n^\times$. So $M_n := \{L_n^\times, L_n^\times\}$, where $L_n^\times := L_n \setminus \{0\}$. Each M_n is a subgroup of $K_2^M(k(C))$. Indeed, M_0 may be identified with the image of the induced homomorphism $K_2^M(k) \to K_2^M(k(C))$, and $M_{-1} = 0$. We have the filtration

$$0 = M_{-1} \subset M_0 \subset M_1 \subset \cdots \subset K_2^M(k(C)).$$

Lemma 31. *We have*

$$K_2^M k(C) = \bigcup_{n \in \mathbb{Z}} M_n.$$

Proof. Given some $f \in k(C)$, split $\operatorname{div}(f)$ into its poles and zeros, so that we can write

$$\operatorname{div}(f) = D_+ - D_-$$

where D_+ and D_- are effective divisors on C with $\deg(D_+) = \deg(D_-) = 2l$ for some integer l (recall we assume that C is nonsplit, so the degree of every point is even). Then choose functions $g, h \in k(C)$ with divisors

$$\operatorname{div}(g) = D_+ - lp_0, \qquad \operatorname{div}(h) = D_- - lp_0.$$

Then $g, h \in L_l$ and $\operatorname{div}(f) = \operatorname{div}(g/h)$, so we see that $f = \lambda g/h$ for some $\lambda \in k^\times$. Let $f' \in k(C)$ be arbitrary and apply the above to get $f' = \lambda' g'/h'$ for some $\lambda' \in k^\times$ and

$g', h' \in L_l$. Then we have

$$\{f, f'\} = \{\lambda g/h, \lambda' g'/h'\} = \{\lambda g, \lambda' g'\} + \{h, h'\} - \{\lambda g, h'\} - \{h, \lambda' g'\} \in M_l.$$

Hence $K_2^M k(C) \subset \bigcup_{n\in\mathbb{Z}} M_n$. The other inclusion is immediate. □

5.2 The first connecting isomorphism

Suppose $g \in L_n^\times$. Then the support of $\mathrm{div}(g)$ does not contain any closed points p of degree strictly greater than $2n$. Hence given a closed point p of degree $2n$, the subgroup M_{n-1} is contained in the kernel of the residue homomorphism ∂_p. Hence ∂ descends to a well-defined homomorphism

$$\partial_n : M_n/M_{n-1} \to \bigoplus_{\deg p = 2n} \kappa(p)^\times.$$

Lemma 32. *For each $n \geq 2$, ∂_n is an isomorphism.*

Proof. For each $p \in C$ of degree $2n > 2$, denote by ϵ_p the k-linear map

$$\epsilon_p : L_{n-1} \to \kappa(p)$$

given for each $f \in L_{n-1}$ by $f \mapsto f(p)$. Since p has degree $2n$, it does not belong to the support of a divisor in L_{n-1}. So it follows that if $f(p) = 0$ in $\kappa(p)$ for some $f \in L_{n-1}$, then $f = 0$. Hence ϵ_p is injective.

We now show how to get an element of $\kappa(p)$ from the evaluation at p of a function in the Riemann-Roch space L_{n-1}. Fix nonzero $u \in \kappa(p)$. Define the k-linear map

$$L_1 \to \kappa(p)/\operatorname{Im}\epsilon_p, \qquad h \mapsto u \cdot \epsilon_p(h) + \operatorname{Im}\epsilon_p.$$

The dimension on the right hand side is

$$\dim_k \kappa(p)/\operatorname{Im}\epsilon_p = \dim_k \kappa(p) - \dim_k L_{n-1} = 2n - 2(n-1) + 1 = 1.$$

The dimension on the left hand side is $\dim_k L_1 = 3$. Hence this map is noninjective, so there exists a nonzero $h \in L_1$ such that $u \cdot h(p) \in \operatorname{Im}\epsilon_p$. We have $h(p) \neq 0$ in $\kappa(p)$ since $\deg(p) > 2$. Hence for some $f \in L_{n-1}$, we have $u = \left(\frac{f}{h}\right)(p)$.

Now the above allows us to define an inverse

$$\phi_n : \bigoplus_{\deg p = 2n} \kappa(p)^\times \to M_n/M_{n-1}$$

to ∂_n by setting $\phi_n = \sum \phi_p$ with

$$\begin{aligned} \phi_p : \kappa(p)^\times &\to M_n/M_{n-1} \\ u &\mapsto \left\{\pi_p, \frac{f}{h}\right\} + M_{n-1} \end{aligned}$$

where f, h are functions derived as in the above such that $u = \left(\frac{f}{h}\right)(p)$, and π_p is a function in L_n with $\operatorname{div}(\pi_p) = p - np_0$. We know such a function exists since $p - np_0$ is a divisor of degree zero, and every divisor of degree zero on C is principal. To prove this association does not depend on the choice of f, h, we need to introduce a lemma characterising Riemann-Roch functions vanishing at p.

Lemma 33. *Fix $p \in C$ of degree $2n$, with $p \neq p_0$. Let*

$$\epsilon_p : L_m \to \kappa(p)$$

be the evaluation map, $\epsilon_p(f) = f(p)$. Pick a function $f \in L_m$ such that $f \in \operatorname{Ker} \epsilon_p$. Then $f = \pi_p g$ for some $g \in L_{m-n}$.

Proof. The case $m < n$ was considered previously. Suppose $m \geq n$. Consider the restriction to L_n of ϵ_p, and let $f \in \operatorname{Ker} \epsilon_p \cap L_n$.Then we see $\operatorname{div}(f) = p - np_0 = \operatorname{div}(\pi_p)$, so $f = \lambda \pi_p$ for some nonzero $\lambda \in k$. In particular, we see $\operatorname{Ker} \epsilon_p \cap L_n$ is one-dimensional. So rank-nullity on ϵ_p restricted to L_n gives

$$\dim_k \operatorname{Im}(\epsilon_p|_{L_n}) = 2n + 1 - 1 = 2n = \dim_k \kappa(p).$$

In particular, we see that ϵ_p is surjective, since it is so when restricted to a subspace. Then applying rank-nullity again we see

$$\dim_k \operatorname{Ker} \epsilon_p = \dim_k L_m - \dim_k \kappa_p = 2m - 2n + 1.$$

Consider the map $L_{m-n} \to L_m$ induced by multiplication by π_p. Since $\pi_p(p) = 0$ the image is contained in $\operatorname{Ker} \epsilon_p$. Also this map is injective, so the image has dimension $\dim_k L_{m-n} = 2m - 2n + 1$. Hence $\operatorname{Ker} \epsilon_p = \pi_p L_{m-n}$. This proves the lemma. □

Now we will show that ϕ_p is well-defined. It clearly doesn't depend on the choice of scalar multiple for π_p. So let f, h be as before and suppose $f' \in L_{n-1}, h' \in L_1$ are nonzero functions such that $\left(\frac{f'}{h'}\right)(p) = u$. Then clearly $f'h - fh' \in L_n$, and $f'h - fh'$ vanishes at p. Then since p is degree $2n$, we must have $f'h - fh' = \lambda \pi_p$ for some $\lambda \in k$. There are two cases.

1. $\lambda = 0$. Then $f/h = f'/h'$, so $\{\pi_p, f/h\} + M_{n-1} = \{\pi_p, f'/h'\} + M_{n-1}$.

2. $\lambda \neq 0$. A computation yields

$$\left\{\frac{\lambda\pi_p}{f'h}, \frac{fh'}{f'h}\right\} + M_{n-1} = \left\{\pi_p, \frac{f}{h}\right\} - \left\{\pi_p, \frac{f'}{h'}\right\} + M_{n-1}$$

Then since we have $1 = \frac{\lambda\pi_p}{f'h} + \frac{fh'}{f'h}$, it follows that $\left\{\pi_p, \frac{f}{h}\right\} + M_{n-1} = \left\{\pi_p, \frac{f'}{h'}\right\} + M_{n-1}$.

Next, we will show that ϕ_p is a group homomorphism. So suppose $u, v \in \kappa(p)^\times$. Then we may choose functions f_u, f_v, f_{uv} and h_u, h_v, h_{uv} as before such that

$$\left(\frac{f_u}{h_u}\right)(p) = u, \qquad \left(\frac{f_v}{h_v}\right)(p) = v, \qquad \left(\frac{f_{uv}}{h_{uv}}\right)(p) = uv.$$

Then the function $f_u f_v h_{uv} - f_{uv} h_u h_v \in L_{2n-1}$ vanishes at p, so by Lemma 33, we have $f_u f_v h_{uv} - f_{uv} h_u h_v = \pi_p g$ for some $g \in L_{n-1}$. Then an analogous computation to before yields

$$0 = \left\{\frac{\pi_p g}{f_u f_v h_{uv}}, \frac{f_{uv} h_u h_v}{f_u f_v h_{uv}}\right\} \equiv \left\{\pi_p, \frac{f_{uv}}{h_{uv}}\right\} - \left\{\pi_p, \frac{f_u}{h_u}\right\} - \left\{\pi_p, \frac{f_v}{h_v}\right\}$$

modulo M_{n-1}. Hence

$$\left\{\pi_p, \frac{f_{uv}}{h_{uv}}\right\} + M_{n-1} = \left\{\pi_p, \frac{f_u}{h_u}\right\} + M_{n-1} = \left\{\pi_p, \frac{f_v}{h_v}\right\} + M_{n-1},$$

so $\phi_p(uv) = \phi_p(u) + \phi_p(v)$. Clearly ϕ_p preserves the identity (we can take $f = h = 1$).

By the above we get that ϕ_n is a homomorphism. We now show that it is the inverse to ∂_n.

1. $\partial_n \circ \phi_n = id$. Let p be a point of degree $2n > 2$ and let $u \in \kappa(p)^\times$. Choose nonzero $f \in L_{n-1}$, $h \in L_1^\times$ such that $\left(\frac{f}{h}\right)(p) = u$. Then since p is the only point of degree $2n$ at which the symbol $\{\pi_p, f/h\}$ has nontrivial residue, we have

$$\partial_n \circ \phi_n(u) = \sum_{\deg(x)=2n} \partial_x \left(\left\{\pi_p, \frac{f}{h}\right\}\right) = \left(\frac{f}{h}\right)(p) = u.$$

Hence $\partial_n \circ \phi_n$ is the identity.

2. $\phi_n \circ \partial_n = id$. It is sufficient to show that ϕ_n is surjective. We do this by showing we may achieve two types of element. First, given $f \in L_{n-1}^\times$, we see that all classes of symbols of the form $\{\pi_p, f\}$ are of the form $\phi_n(f)$. Second, we aim to show all classes of symbols of the form $\{\pi_p, \pi_q\}$ are achievable, where

p, q are distinct points of degree $2n$. So let $g \in L_{n-1}^{\times}, h \in L_1^{\times}$ be functions such that $\pi_p(q) = \left(\frac{g}{h}\right)(q)$. Then the function $\pi_p h - g \in L_{n+1}^{\times}$ vanishes at q, and so by Lemma 33 we have $\pi_p h - g = \pi_q r$ for some function $r \in L_1^{\times}$. Then another analogous computation to the proof of well-definedness / the homomorphic property of ϕ_p yields

$$0 = \left\{ \frac{\pi_q r}{\pi_p h}, \frac{g}{\pi_p h} \right\} + \mathrm{Im}(\phi_n) = \{\pi_p, \pi_q\} + \mathrm{Im}(\phi_n).$$

Hence $\{\pi_p, f\}, \{\pi_p, \pi_q\} \in \mathrm{Im}(\phi_n)$. It remains to show that classes of elements of these forms generate the quotient group M_n/M_{n-1}. Let $\{f, g\} + M_{n-1} \in M_n/M_{n-1}$ with $f, g \in L_n^{\times}$. Then we may write f, g as finite products of the form

$$f = \lambda_f \pi_{p_1} \pi_{p_2} \dots \pi_{p_l}, \qquad g = \lambda_g \pi_{q_1} \pi_{q_2} \dots \pi_{q_m}$$

where $\lambda_f, \lambda_g \in k^{\times}$ and the p_i, q_i are closed points of degree at most $2n$. Then we may write $\{f, g\} = \{\lambda_f \pi_{p_1} \pi_{p_2} \dots \pi_{p_l}, \lambda_g \pi_{q_1} \pi_{q_2} \dots \pi_{q_m}\}$, and using bilinearity of symbols this splits into a sum of symbols of the form $\{\pi_{p_i}, \pi_{p_j}\}$ and $\{\lambda, \pi_x\}$.

□

5.3 The second connecting isomorphism

The filtration

$$M_{-1} \subset M_0 \subset M_1 \subset M_2 \subset M_3 \subset \dots \subset K_2^M k(C)$$

may be refined further by adding an extra subgroup $M_0 \subset M' \subset M_1$, defined by $M' = \{L_1^{\times}, L_0^{\times}\} = \{L_1^{\times}, k^{\times}\}$. We denote by A' the subgroup of $\bigoplus_{\deg(p)=2} \kappa(p)^{\times}$ consisting of those elements (x_p) such that $x_p \in k^{\times}$ for all closed points p of degree 2, and $\prod_p x_p = 1$.

Lemma 34. *The subgroup M' is generated by M_0 and symbols of the form $\{\pi_p, x\}$ with $x \in k^{\times}$. and $p \neq p_0$ closed points of degree 2.*

Proof. Simply write any $\{f, x\} \in M'$ as $\{\lambda \pi_p, x\} = \{\lambda, x\} + \{\pi_p, x\}$ with $\lambda \in k^{\times}$ and p the closed point of degree 2 where f vanishes. Then since elements of the shape $\{f, x\}$ are additive generators for M', the claim follows. □

By virtue of this lemma and the fact that every symbol $\{\pi_p, x\}$ has residues x, x^{-1} at p, p_0 respectively and no other nontrivial residues at closed points of degree 2, we see that $\partial_1(M'/M_0) \subset A'$.

Lemma 35. *The restriction $\partial' : M'/M_0 \to A'$ of the homomorphism ∂_1 is an isomorphism.*

Proof. It is sufficient to exhibit an inverse isomorphism. Let

$$\begin{aligned}\psi : A' &\to M'/M_0,\\ (x_p) &\mapsto \sum_{\deg p=2, p\neq p_0} \{\pi_p, x_p\} + M_0.\end{aligned}$$

Clearly this is a surjective homomorphism, since M'/M_0 is generated by classes of elements of the form $\{\pi_p, x\}$ with $x \in k^\times$ and $p \neq p_0$ a closed point of degree 2., and hence to achieve the class of the symbol $\{\pi_q, x\}$ we send the family (x_p) with $x_p = x$ for $p = q$, $x_{p_0} = x^{-1}$ and $x_p = 1$ otherwise. Hence to show ψ is inverse to ∂', it is enough to show $\partial' \circ \psi = id$. Let $(x_p) \in A'$. Then

$$\partial'(\psi((x_p))) = \partial_1 \left(\sum_{\deg p=2, p\neq p_0} \{\pi_p, x_p\} + M_0 \right).$$

Fix $p \neq p_0$. The only symbol in the sum above with nontrivial residue at p is $\{\pi_p, x_p\}$ with residue x_p. At p_0 each symbol $\{\pi_p, x_p\}$ with $p \neq p_0$ has residue x_p^{-1}. Hence $\partial' \circ \psi((x_p))$ is the family (y_p) such that $y_p = x_p$ for $p \neq p_0$ and $y_{p_0} = \prod_{p\neq p_0} x_p^{-1}$. But then $(y_p) = (x_p)$ in light of the relation $\prod_p x_p = 1$. □

5.4 Joining the connecting isomorphisms

We will now use the previous two isomorphisms to build a chain complex of short exact sequences. To achieve this we need the following "bridging" exact sequence:

Lemma 36. *The sequence*

$$0 \longrightarrow M_1/M' \xrightarrow{\partial_1} \left[\bigoplus_{\deg p=2} \kappa(p)^\times\right] / A' \xrightarrow{N} k^\times$$

is exact.

Proof. (Sketch of proof.) By Theorem 8, we have

$$\bigoplus_{\deg p=2} \kappa(p)^\times \cong \bigoplus_{K\subset Q} K^\times,$$

where the direct sum is taken over all quadratic subfields $K \subset Q$. By this isomorphism we get a canonically isomorphic induced norm map

$$N : \bigoplus_{K\subset Q} K^\times \to k^\times$$

whose action on each K in the direct sum equals the restriction to $K^\times$ of the reduced norm $N_{K/k} : K^\times \to k^\times$. Now we denote by $A(Q)$ the kernel of this norm homomorphism in Q. By Theorem 8, A' corresponds to the subgroup of $A(Q)$ formed by those families (a_K) such that $a_K \in k^\times$ for every $K \subset Q$. In other words we have $A' = A(Q) \cap \bigoplus k^\times$. Now Lemma 36 is equivalent to the statement that the induced homomorphism

$$\partial_1 : M_1/M' \to A(Q)/A'$$

is an isomorphism. To prove ∂_1 is an isomorphism, Merkurjev writes the quotient $A(Q)/A'$ as an abstract group G given in terms of generators and relations, and then proves M_1/M' is isomorphic to G. This process is quite lengthy to present in this dissertation however, and the details are deferred to Merkurjev.

We now prove Theorem 10. To do this we need:

Lemma 37. *For each $n \geq 1$, the sequence*

$$0 \longrightarrow M_n/M_0 \xrightarrow{\partial} \bigoplus_{\deg p \leq 2n} \kappa(p)^\times \xrightarrow{N} k^\times. \tag{25}$$

is exact.

Proof. We prove it by induction. For the case $n = 1$, Lemmas 36 and 35 (i.e. the connecting isomorphisms) imply the exactness of the sequences

$$0 \longrightarrow M'/M_0 \xrightarrow{\partial_1} A' \longrightarrow 0$$

and

$$0 \longrightarrow M_1/M' \xrightarrow{\partial_1} \left[\bigoplus_{\deg p=2} \kappa(p)^\times\right]/A' \xrightarrow{N} k^\times.$$

Hence we have a diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M'/M_0 & \longrightarrow & A' & \longrightarrow & 0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_1/M_0 & \longrightarrow & \bigoplus_{\deg p=2} \kappa(p)^\times & \longrightarrow & k^\times & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_1/M' & \longrightarrow & \left[\bigoplus_{\deg p=2} \kappa(p)^\times\right]/A' & \longrightarrow & k^\times & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

in which all rows and columns bar the middle row are exact. Clearly the middle row is a complex, hence by a general result the middle row is exact, proving (25) for $n = 1$.

For the induction step, we construct a similar diagram. Lemma 32 gives an exact sequence

$$0 \longrightarrow M_n/M_{n-1} \longrightarrow \bigoplus_{\deg p=2n} \kappa(p)^\times \longrightarrow 0.$$

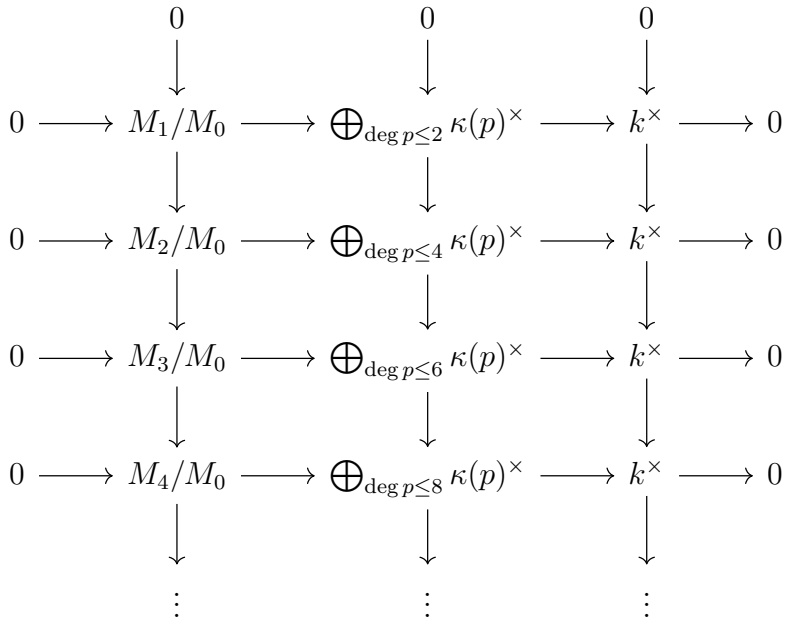
Hence assuming (25) holds for $n-1$ we have a diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_{n-1}/M_0 & \longrightarrow & \bigoplus_{\deg p\leq 2(n-1)} \kappa(p)^\times & \longrightarrow & k^\times & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_n/M_0 & \longrightarrow & \bigoplus_{\deg p\leq 2n} \kappa(p)^\times & \longrightarrow & k^\times & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_n/M_{n-1} & \longrightarrow & \bigoplus_{\deg p=2n} \kappa(p)^\times & \longrightarrow & 0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where all rows and columns bar the middle row are exact. By the same reasoning as before, the middle row is therefore exact. This concludes the induction step. □

We know from Lemma 31 that $K_2^M k(C) = \bigcup M_n$, and so taking a direct limit over

the system



yields the sequence

$$0 \longrightarrow K_2^M k(C)/M_0 \longrightarrow \bigoplus_{p \in C} \kappa(p)^\times \longrightarrow k^\times \longrightarrow 0$$

which is exact by Lemma 37 and the fact that direct limits preserve exactness. Hence by identifying $M_0 = K_2^M(k)$ we have proved the theorem. □

5.5 Hilbert Theorem 90 for K_2^M

In this subsection we use a variant of Hilbert's Theorem 90 for Milnor K-theory to reduce elements in $2K_2^M(k)$ that are equal to 0 to one pure symbol. The theorem we aim to achieve is

Theorem 11. *Let $u \in K_2^M(k)$. If $2u = 0$, then $u = \{-1, a\}$ for some $a \in k^\times$.*

We begin with a lemma which will help us later:

Lemma 38. *Let L/k be a quadratic extension. Then the group $K_2^M L$ is generated by symbols of the form $\{x, a\}$ with $x \in L^\times$ and $a \in k^\times$.*

Proof. See [1], Corollary 5.3 and apply to the case $n = 2$. □

From now on we let L/k be a quadratic Galois extension with Galois group G, and denote by $\sigma \in G$ the nontrivial conjugation. There is a natural action of σ on $K_2^M(L)$ defined on pure symbols by $\sigma\{a,b\} = \{\sigma a, \sigma b\}$. Given a field extension E/k linearly disjoint to L/k, then the tensor product $L \otimes_k E$ is a quadratic Galois field extension of E, with Galois group naturally isomorphic to G. We denote $LE := L \otimes_k E$.

Let

$$V(E) := K_2^M(LE)/(\sigma - 1)K_2^M(LE).$$

Then for every homomorphism

$$E \to E'$$

of field extensions of k linearly disjoint with L/k, there is an induced homomorphism

$$V(E) \to V(E')$$

defined in the natural way.

Proposition 16. *Given a smooth projective conic curve C over k such that C splits over L, the induced homomorphism*

$$\psi : V(k) \to V(k(C))$$

is injective.

Proof. We have

$$V(k) = K_2^M(L)/(\sigma - 1)K_2^M(L), \qquad V(k(C)) = K_2^M(L(C))/(\sigma - 1)(K_2^M(L(C)).$$

Suppose $u \in K_2^M(L)$ is such that $\psi(u) = 0$, so that

$$u_{L(C)} = (\sigma - 1)v,$$

where $v \in K_2^M(L(C))$. Now for each closed point $p \in C$, we define the L-algebra

$$\kappa(p)_L := L \otimes_k \kappa(p)$$

as the extension of scalars of the residue field $\kappa(p)$ to L. Then it is clear that for each $p \in C$, $\kappa(p)_L$ is isomorphic to the product of the residue fields $\kappa(q)$ for all closed points $q \in C_L$ over p. Hence, let us denote

$$\partial_p(v) = \prod \partial_q(v) \in \kappa(p)_L^\times,$$

where the product of the $\partial_q(v) \in \kappa(q)^\times$ is taken over all closed points q over p. Furthermore, we have

$$\begin{aligned}\partial_p(v)/\sigma(\partial_p(v)) &= \partial_p((1-\sigma)v) \\ &= \partial_p(u_{L(C)}) \\ &= 1,\end{aligned}$$

hence $\partial_p(v) = \sigma(\partial_p(v))$, which shows that $\partial_p(v) \in \kappa(p)^\times$. Now we have

$$\prod_{p\in C} N_{\kappa(p)/k}(\partial_p(v)) = N_{L/k}\left(\prod_{q\in C_L} N_{\kappa(q)/L}(\partial_q(v))\right),$$

and the key exact sequence of Theorem 10 applied to C_L yields

$$\prod_{q\in C_L} N_{\kappa(q)/L}(\partial_q(v)) = 1$$

so that $\prod_{p\in C} N_{\kappa(p)/k}(\partial_p(v)) = 1$. Now using the key exact sequence for C, we see that there exists some $w \in K_2^M k(C)$ with $\partial_p(w) = \partial_p(v)$ for every $p \in C$. Now let

$$v' = v - w_{L(C)} \in K_2^M(L(C)).$$

Then applying ∂_p to both sides, we see

$$\partial_p(v') = \partial_p(v)\partial_p(w)^{-1} = \partial_p(v)\cdot\partial_p(v)^{-1} = 1.$$

Hence again applying the key exact sequence, we have $s \in K_2^M L$ with $s_{L(C)} = v'$. Now

$$(\sigma-1)s_{L(C)} = (\sigma-1)v' = (\sigma-1)v = u_{L(C)}$$

which means $((\sigma-1)s-u)_{L(C)} = 0$. Now $L(C)/L$ is a purely transcendental extension, and by reasoning to be justified later in the proof of injectivity of the norm residue homomorphism, the induced map

$$K_2^M(L) \to K_2^M(L(C))$$

is injective. In particular, this implies $(\sigma-1)s-u = 0$. So $u = (\sigma-1)s$, which proves the proposition. □

This proposition implies

Lemma 39. *Given any finitely generated subgroup $H \subset k^\times$, there is a field extension K/k such that:*

1. *K/k is linearly disjoint with L/k.*

2. *The natural homomorphism $V(k) \to V(K)$ is injective.*

3. *We have $H \subset N_{L'/K}(L'^{\times})$ where $L' = LK$.*

Proof. We proceed by induction on the number of generators n for H. For the base step, assume $H = \langle b \rangle$ is generated by one element. We set $K = k(C)$, where C is the associated conic to the quaternion algebra $Q = (a, b)_k$, where $a \in k^{\times}$ is such that $L = k(\sqrt{a})$. Now certainly Q splits over $k(C) = K$, and thus $b \in N_{L'/K}(L'^{\times})$ by Lemma 17. Since C splits over L, Proposition 16 gives that the natural homomorphism $V(k) \to V(K)$ is injective.

For the induction step, let us assume the claim holds for a subgroup generated by $n-1$ elements, and write

$$H = G + \langle a_n \rangle,$$

where G is generated by $n-1$ elements. By induction, we may find a field extension K'/k such that K'/k is linearly disjoint with L/k, the induced homomorphism $V(k) \to V(K')$ is injective, and

$$G \subset N_{LK'/K'}(L'^{\times}).$$

Now consider $\langle a_n \rangle_{K'} \subset (K')^{\times}$. By the base step $n = 1$, we get a field extension K''/K' with properties 1-2, and such that

$$\langle a_n \rangle_{K''} \subset N_{LK''/K''}((LK'')^{\times}).$$

But then also $G_{K''} \subset N_{LK''/K''}((LK'')^{\times})$, which completes the induction step. □

We now introduce a short interlude to present a classical theorem in algebra:

Theorem 12 (Hilbert Theorem 90, classical.)**.** *Suppose L/F is a finite Galois extension of degree n, such that the Galois group $G = Gal(L/F)$ is cyclic with generator σ. Then if $a \in L$ is such that $N_{L/F}(a) = 1$, then there exists $b \in L$ with*

$$a = \sigma(b)/b.$$

Proof. Suppose $a \in L$ has norm

$$N_{L/F}(a) = \prod_{i=0}^{n-1} \sigma^i(a) = 1.$$

Then to prove the theorem, it is sufficient to show that the map

$$a\sigma(\cdot) : L \to L$$

has eigenvalue 1. Now we extend $a\sigma(\cdot)$ to the tensor product of L-vector spaces by defining

$$\begin{aligned} 1_L \otimes a\sigma(\cdot) : L \otimes_F L &\to L \otimes_F L, \\ \ell \otimes \ell' &\mapsto \ell \otimes a\sigma(\ell'). \end{aligned}$$

The primitive element theorem of field theory lets us write $L = F(\alpha)$, where $\alpha \in L$ has minimal polynomial

$$f(t) = \prod_{i=0}^{n-1} (t - \sigma^i(\alpha)),$$

whence a chain of isomorphisms

$$L \otimes_F L \cong L \otimes_F F(\alpha) \cong L \otimes_F (F[t]/f(t)) \cong L[t]/f(t) \cong L^n$$

so that we identify

$$\ell \otimes p(\alpha) = \ell(p(\alpha), p(\sigma\alpha), \ldots, p(\sigma^{n-1}\alpha))$$

where we wrote the second factor of the tensor as a polynomial in α. But by this isomorphism, the map $a\sigma(\cdot)$ becomes

$$\begin{aligned} a\sigma(\cdot) : L^n &\to L^n, \\ \ell(p(\alpha), \ldots, p(\sigma^{n-1}\alpha)) &\mapsto \ell(ap(\sigma\alpha), \ldots, \sigma^{n-1}ap(\sigma^n\alpha)). \end{aligned}$$

Thus

$$a\sigma((\ell_1, \ldots, \ell_n)) = (a\ell_n, \sigma a\ell_1, \ldots, \sigma^{n-1}a\ell_{n-1}).$$

Hence we see that $(1, \sigma a, \sigma a\sigma^2 a, \ldots, \sigma a \cdots \sigma^{n-1}a)$ is an eigenvector with eigenvalue 1. □

Now given any two elements $x, y \in L^\times$, let us denote by $\langle x, y \rangle$ the image of the symbol $\{x, y\} \in K_2^M(L)$ in $V(k)$.

Lemma 40. *There is a well-defined group homomorphism*

$$\begin{aligned} f = f_k : N_{L/k}(L^\times) \otimes k^\times &\to V(k), \\ N_{L/k}(x) \otimes a &\mapsto \langle x, a \rangle. \end{aligned}$$

Proof. Let us first show the map is well-defined. Given $x, y \in L^\times$ with $N_{L/k}(x) = N_{L/k}(y)$, then $N_{L/k}(x/y) = 1$, and thus by the classical variant of Hilbert Theorem 90 introduced above, we have

$$y = xz\sigma(z)^{-1}$$

for some $z \in L^\times$. Then since

$$\{y, a\} = \{xz\sigma(z)^{-1}, a\} = \{x, a\} + \{z, a\} - \{\sigma(z), a\} = \{x, a\} - (\sigma - 1)\{z, a\}$$

we see that $\langle y, a \rangle = \langle x, a \rangle$. □

Lemma 41. *Suppose $b \in N_{L/k}(L^\times)$. Then*

$$f(b \otimes (1-b)) = 0.$$

Proof. There are two cases:

1. b is a square in $k^\times$. Put $b = c^2$ for some $c \in k^\times$. Then

$$\begin{aligned} f(b \otimes (1-b)) = \langle c, 1-c^2 \rangle = \langle c, (1-c)(1+c) \rangle &= \langle c, 1-c \rangle + \langle c, 1+c \rangle \\ &= \langle c, 1+c \rangle \\ &= \langle -1, 1+c \rangle = 0, \end{aligned}$$

since we may write $-1 = z\sigma(z)^{-1}$ for some $z \in L^\times$, whence

$$\begin{aligned} \langle -1, 1+c \rangle = \langle z\sigma(z)^{-1}, 1+c \rangle &= \langle z, 1+c \rangle - \langle \sigma(z), 1+c \rangle \\ &= \langle z, 1+c \rangle - \langle z, 1+c \rangle = 0. \end{aligned}$$

2. b is not a square in k. Then we have a quadratic field extension

$$K = k[t]/(t^2 - b).$$

Let

$$L' = L[t]/(t^2 - b).$$

Then L' is either a field or the direct sum of two copies of K. Let us denote by $u \in K$ the image of the polynomial t, so that we have $u^2 = b$. Let $x \in L^\times$ be such that $N_{L/k}(x) = b$. Then we have the equalities

$$N_{L'/K}(x/u) = b/u^2 = 1,$$

thus $N_{L'/L}(1-u) = 1-b$.We get an automorphism of L' over K by extending σ in the natural way. Thus by again applying the classical variant of Hilbert Theorem 90, we may find $v \in L'^\times$ with

$$v\sigma(v)^{-1} = x/u.$$

Hence

$$\begin{aligned} f(b \otimes (1-b)) = \langle x, 1-b \rangle &= \langle x, N_{L'/L}(1-u) \rangle \\ &= N_{L'/L} \langle x, 1-u \rangle \\ &= N_{L'/L} \left\langle \frac{x}{u}, 1-u \right\rangle \\ &= N_{L'/L} \langle v\sigma(v)^{-1}, 1-u \rangle \\ &= -(\sigma - 1) N_{L'/L} \langle v, 1-u \rangle = 0. \end{aligned}$$

□

We are now finally prepared to introduce the powerhouse results of this dissertation, beginning with a variant of Hilbert Theorem 90 for $K_2^M(k)$:

Theorem 13 (Hilbert Theorem 90 for $K_2^M(k)$.)**.** *The sequence*

$$K_2^M L \xrightarrow{\sigma-1} K_2^M L \xrightarrow{N_{L/k}} K_2^M k$$

is exact.

Proof. Suppose $u \in K_2^M(L)$ is such that $N_{L/k}(u) = 0$. By Lemma 38, we may write

$$u = \sum_{i=1}^{n} \{x_i, a_i\}$$

where the $x_i \in L^\times$ and $a_i \in k^\times$. Furthermore, we have

$$N_{L/k}(u) = \sum_{i=1}^{n} \{N_{L/k}(x_i), a_i\} = 0.$$

Hence turning back to the very definition of $K_2^M k$, we see that $u \in (b \otimes (1-b) \mid b \in k^\times \setminus \{1\})$, and thus we may write

$$\sum_{i=1}^{n} N_{L/k}(x_i) \otimes a_i = \sum_{i=1}^{m} b_i \otimes (1 - b_i) \tag{26}$$

for some $b_i \in k^\times$.

Let H be the subgroup of $k^\times$ generated by the $N_{L/k}(x_i)$ and b_i. Then Equation 26 holds in $H \otimes k^\times$, and Lemma 39 tells us that there is a field extension K/k linearly disjoint from L/k such that the natural homomorphism $V(k) \to V(K)$ is injective, and $H \subset N_{L'/K}(L'^\times)$ with $L' = LK$. Hence Equation 26 also holds in $N_{L'/K}(L'^\times) \otimes K^\times$. Applying the map f_K of Lemma 40 to both sides of Equation 26 and keeping Lemma 41 in mind, we see

$$\sum_{i=1}^{m} \langle x_i, a_i \rangle = f_K \left(\sum_{i=1}^{n} N_{L/k}(x_i) \otimes a_i \right) = \sum_{i=1}^{m} f_K(b_i \otimes (1 - b_i)) = 0.$$

Hence $u_{L'} \in (\sigma - 1) K_2^M L'$. We have that the map $V(k) \to V(K)$ is injective. It follows that $u \in (\sigma - 1) K_2^M L$. □

We are now ready to prove Theorem 11. Let $G = \mathbb{Z}/2\mathbb{Z}$ and denote by $\sigma \in G$ the nontrivial element. Let $L = k((x))$ be the field of Laurent power series with coefficients in k, and let G act on L by $\sigma(x) = -x$. Then letting

$$E = L^G = \{f \in L \mid \sigma(f) = f\}$$

be the fixed field of G in L, we get a quadratic Galois extension L/E. The canonical discrete valuation on L with uniformising parameter x yields a residue homomorphism $\partial : K_2^M(L) \to k^\times$. There is also a specialisation homomorphism $s_x : K_2^M L \to K_2^M k$ defined by $s(u) := \partial(\{-x\} \cdot u)$.

Lemma 42. *The diagram*

$$\begin{array}{ccc} K_2^M L & \xrightarrow{\sigma-1} & K_2^M L \\ \downarrow{\scriptstyle \partial} & & \downarrow{\scriptstyle s_x} \\ k^\times & \xrightarrow{\cdot\{-1\}} & K_2^M L \end{array}$$

where the bottom map is multiplication by the pure symbol $\{-1\}$, is commutative.

Proof. Let $u \in K_2^M L$. We consider two cases:

1. $u = \{f, g\}$ for power series $f, g \in k[[t]]$ with nonzero constant term. Then $s_x(u) = \{f(0), g(0)\}$ and $(\sigma f)(0) = f(0), (\sigma g)(0) = g(0)$. Hence

   $$s_x \circ (\sigma - 1)\{f, g\} = s_x(\{\sigma f, \sigma g\}) - s_x(\{f, g\}) = \{(\sigma f)(0), (\sigma g)(0)\} - \{f(0), g(0)\} = 0.$$

   On the other hand, since $\partial\{f, g\} = 0$, we have $\{-1\} \cdot \partial\{f, g\} = 0$. So the maps commute for this element.

2. $u = \{x, g\}$ with g as before. Then $\{-1\} \cdot \partial(u) = \{-1, g(0)\}$, and

   $$s_x \circ (\sigma - 1)\{x, g\} = s_x(\{-x, \sigma(g)\} - \{x, g\}) = s_x(\{-x, \sigma(g)\}) - s_x(\{x, g\}).$$

   We have $s_x(\{x, g\}) = \partial(\{-x, x, g\}) = 0$ since $\{-x, x\} = 0$, and

   $$\begin{aligned} s_x(\{-x, \sigma(g)\}) = \partial(\{-x, -x, \sigma(g)\}) &= \partial(\{x, -1, \sigma(g)\} + \{-1, -1, \sigma(g)\}) \\ &= \{-1, \sigma(g)(0)\} + 0 = \{-1, g(0)\}. \end{aligned}$$

   So the maps commute for this element too.

It remains to observe that the symbols $\{f, g\}$ and $\{x, g\}$ generate the group $K_2^M L$, and hence the diagram commutes. □

To finish the proof of Theorem 11, let $u \in K_2^M(k)$ be such that $2u = 0$. Then $2u_E = 0$, and so $N_{L/E}(u_L) = 2u_E = 0$. Then Theorem 13 gives that $u_L = (\sigma - 1)v$ for some $v \in K_2^M(L)$. Then Lemma 42 implies

$$u = s_x(u_L) = s_x((\sigma - 1)v) = \{-1, \partial(v)\}.$$

One further result will be useful in the proof of the main theorem. Let L/k be a quadratic extension, and denote by σ the nontrivial element of the Galois group of L/K.

Lemma 43. *The sequence*

$$k_2^M k \longrightarrow k_2^M L \xrightarrow{N_{L/k}} k_2^M k$$

is exact.

Proof. Let $u \in K_2^M(L)$ with $N_{L/k}(u) = 2v$, where $v \in K_2^M k$. Then by linearity we have $N_{L/k}(u - v_L) = N_{L/k}(u) - N_{L/k}(v_L) = 2v - 2v = 0$. By Theorem 13 we then have $u - v_L = (\sigma - 1)w$ where $w \in K_2^M L$. Therefore

$$\begin{aligned} u = v_L + (\sigma - 1)w &= v_L - (w + \sigma w) + 2\sigma w \\ &= (v - N_{L/k}(w))_L + 2\sigma w \in (v - N_{L/k}(w))_L + 2K_2^M(L) \end{aligned}$$

as required. □

5.6 Injectivity of the norm residue homomorphism

Equipped with Theorem 10 and the consequences of Hilbert's Theorem 90 for $K_2^M(k)$ we are now going to provide the injectivity part of the proof of Theorem 9. The proof is by induction on n. For $n = 1$ and $n = 2$ it follows by

Proposition 17. *Let $a, b, c, d \in k^\times$. Then $0 = \{a, b\} + \{c, d\} \in k_2^M(k)$ if and only if the Albert form $A_{\{a,b\}+\{c,d\}}$ is hyperbolic.*

Proof. Suppose $\{a, b\} + \{c, d\} = 0$. Then since $\{c, d\} = -\{c, d\}$ in $k_2^M(k)$, we have $\{a, b\} = \{c, d\}$, which from Proposition 15 it follows $\langle\langle a, b\rangle\rangle = \langle\langle c, d\rangle\rangle$. Hence, in the Witt ring $W(k)$, we have $\langle\langle a, b\rangle\rangle - \langle\langle c, d\rangle\rangle = 0$. But this just means $A_{\{a,b\}+\{c,d\}}$ is hyperbolic. The converse may be established similarly. □

Now suppose $h_k(\{a, b\} + \{c, d\}) = 0$. Then $(a, b)_k \otimes_k (c, d)_k \sim k$ in the Brauer group, from which it follows $(a, b)_k \sim (c, d)_k$. Then these must be isomorphic as central simple algebras, so in particular, their reduced norms are isomorphic. Hence

$\langle\langle a,b\rangle\rangle = \langle\langle c,d\rangle\rangle$. In other words, $\{a,b\} = \{c,d\}$ in $k_2^M(k)$, hence $\{a,b\} + \{c,d\} = 0$. This concludes the base step.

Now, the induction step: Assume that h_k is injective when restricted to sums of n symbols. Suppose $h_k(\{a,b\} + v) = 0$ where v is a sum of n symbols., and $\{a,b\} \neq 0$. Consider the field extension L/k where $L = k(C)$ is the function field of the associated conic $C : aX^2 + bY^2 = abZ^2$ to the quaternion algebra $(a,b)_k$. We see that C is anisotropic. Make the change of variables $x = X/Z, y = Y/Z$. Then since $x^2/b + y^2/a = 1$, in $K_2^M(L)$ one has

$$\begin{aligned}\left\{\frac{x^2}{b}, \frac{y^2}{a}\right\} &= -\{a,b\} + \left\{x^2, y^2\right\} - \{b, y^2\} - \{x^2, a\} \\ &= 2\left\{x, \frac{y^2}{a}\right\} - 2\{b,y\} - \{a,b\}.\end{aligned}$$

Denote $r = \{x, y^2/a\} - \{b,y\}$. The above computation shows that $\{a,b\} = 2r$ in $K_2^M(L)$.

By definition, $(a,b)_k$ is split over L. Hence $h_L((a,b)_k + v_L) = h_L(v_L) = 0$. By our inductive hypothesis we have $v_L = 2w$, where $w \in K_2^M L$. Now set $c_p = \partial_p(w)$ for each $p \in C$. Since $\partial_p(v_L) = 1$ for every $p \in C$, we have $c_p^2 = \partial_p(2w) = 1 \in k^\times$, so $c_p = (-1)^{n_p}$ where $n_p = 0$ or $n_p = 1$. Now set p_0 to be the closed point of degree two given by the equation $Z = 0$ (the point at infinity in the $\mathbb{A}_Z$ affine chart). Then we may define the divisor

$$D := \sum_{p \in C} n_p p$$

which clearly has finite support, and degree $2m$ by the fact that every point of C is even, since C is anisotropic. Now the divisor $D - mp_0$ is degree zero, hence principal, so we may choose $f \in L^\times$ with $\mathrm{div} f = D - mp_0$. Now we set

$$w' = w + \{-1, f\} + lr.$$

with $l = m + n_{p_0}$. We now compute the residues of w' at each $p \in C$. There are two cases.

1. $p = p_0$. Then

$$\begin{aligned}\partial_{p_0}(r) &= \partial_{p_0}\left(\left\{x, \frac{y^2}{a}\right\} - \{b,y\}\right) \\ &= \partial_{p_0}\left(\left\{\frac{Y}{Z}, b\right\}\right)\partial_{p_0}\left(\left\{\frac{X}{Z}, \frac{Y^2}{Z^2}\right\}\right)\partial_{p_0}\left(\left\{\frac{X}{Z}, a^{-1}\right\}\right) \\ &= \frac{\overline{a}}{\overline{b}}\partial_{p_0}\left(\left(\left\{\frac{X}{Z}, \frac{Y}{Z}\right\}\right)\right)^2,\end{aligned}$$

and

$$\begin{aligned}\left\{\frac{X}{Z},\frac{Y}{Z}\right\} &= \{X,Y\}+\{X,Z^{-1}\}+\{Z^{-1},Y\}+\{Z^{-1},Z^{-1}\}\\ &= \{Z,X\}+\{Z^{-1},Y\}+\{Z^{-1},-1\}\end{aligned}$$

modulo the kernel of ∂_{p_0}. So

$$\partial_{p_0}\left(\left\{\frac{X}{Z},\frac{Y}{Z}\right\}\right) = -\frac{\overline{X}}{\overline{Y}}.$$

Therefore

$$\partial_{p_0}(r) = \frac{\overline{a}\overline{X}^2}{\overline{b}\overline{Y}^2} = -1.$$

By definition we have $\partial_{p_0}(\{-1,f\}) = (-1)^m$ and $\partial_{p_0}(w) := c_{p_0} = (-1)^{n_{p_0}}$, we see

$$\partial_{p_0}(w') = \partial_{p_0}(w)\cdot\partial_{p_0}\left(\{-1,f\}\right)\cdot\left(\partial_{p_0}(r)\right)^l = (-1)^{n_{p_0}+m+l} = 1.$$

2. $p \neq p_0$. Then if p corresponds to the degree 2 point given by $X=0$, then

$$\begin{aligned}\partial_p(r) &= \partial_p(\{X/Z, Y^2/aZ^2\})\cdot\partial_p(\{b, Y/Z\})\\ &= \overline{Y}^2/\overline{a}\overline{Z}^2 = 1.\end{aligned}$$

If p corresponds to the degree 2 point given by $Y=0$, then

$$\begin{aligned}\partial_p(r) &= \partial_p(\{Y^2/aZ^2, X/Z\})\cdot\partial_p(\{Y/Z, b\})\\ &= (\overline{X}/\overline{Z})^2\cdot\overline{b} = 1.\end{aligned}$$

If p corresponds to any other point then r has no poles or zeroes and thus $\partial_p(r)=1$. Hence in any case r has no nontrivial residue at p, and By definition $\{-1,f\}$ has residue $(-1)^{n_p}$. Hence

$$\partial_p(w') = (-1)^{n_p}\cdot(-1)^{n_p} = 1.$$

Hence we see that $\partial_p(w')=1$ for every $p\in C$, so $w'\in\operatorname{Ker}\partial$. Hence by the key exact sequence of Theorem 10 we have $w' = s_L$, where $s\in K_2^M k$. So

$$v_L = 2w' - 2lr = 2s_L - \{a^l, b\}_L.$$

Now consider the diagram of fields

$$\begin{array}{ccc} k & \longrightarrow & E \\ \downarrow & & \downarrow \\ L & \longrightarrow & E(C) \end{array}$$

where $E = k(\sqrt{a})$ is a splitting field for $(a,b)_k$. Write $v' = v - 2s + \{a^l, b\} \in K_2^M k$. Then

$$v'_L = v_L - 2s_L + \{a^l, b\}_L = 2s_L - \{a^l, b\}_L - 2s_L + \{a^l, b\}_L = 0.$$

Hence $v'_{E(C)} = 0$, too. We now want to show that $v'_E = 0$. To do this we observe that the function field $E(C)$ is isomorphic to the field of rational functions $E(t)$ in one variable. The irreducible polynomial t induces a discrete valuation on $E(t)$, so t has valuation $\nu(t) = 1$. Hence the image $v'_{E(C)}$ of v'_E in the inclusion of fields $E \subset E(C)$ satisfies

$$\partial_t(\{-t\} \cdot v'_{E(C)}) = v'_E$$

where ∂_t is the residue homomorphism induced by the discrete valuation induced by t, and so we see that the induced homomorphism $K_*^M(E) \to K_*^M(E(C))$ is injective. In particular, we see that $v'_E = 0$ as required. Now the norm map yields $0 = N_{E/F}(v'_E) = 2v'$. Hence Theorem 11 gives $v' = \{-1, d\}$ where $d \in k^\times$. So in $k_2^M(k)$ we have $v = \{a^l, b\} + \{-1, d\}$, which reduces us back to the case $n = 2$. □

5.7 Surjectivity of the norm residue homomorphism

It remains to prove surjectivity. Let Q be a central simple algebra of order 2 in the Brauer group. We proceed in two cases:

1. Assume k admits no nontrivial odd degree extensions. Then we proceed by induction on the Schur index $\mathrm{ind}(Q)$ of Q, which is by definition the square root of the dimension of the corresponding division algebra to Q given by Wedderburn's theorem (which is a Brauer equivalence invariant, of course). Such a square root is integral due to the proof of Proposition 11. In the base step $\mathrm{ind}(Q) = 1$, we have that Q is Brauer equivalent to zero, so clearly $Q \in \mathrm{Im}\, h_k$. Now we proceed with the induction step. Suppose $\mathrm{ind}(Q) > 1$. Then the underlying division algebra D of Q is nontrivial, and so it contains a nontrivial maximal subfield M/k, which contains a nontrivial subfield K/k of degree equal to a power of 2, since k has no odd degree extensions. This field is contained in a Galois extension N/k, with the Galois group $\mathrm{Gal}(N/k)$ a 2-group. By the Galois correspondence, L corresponds to a subgroup H of G. Since 2-groups have nontrivial centres, it follows that H is contained in a normal subgroup of index 2 in G. Applying the Galois correspondence again, we see that K/k contains a quadratic subextension, and hence we may choose a quadratic extension L/k such that the Schur index of $Q_L := Q \otimes_k L$ is strictly less than the Schur index of Q. Then by induction we have $Q_L = h_L(u)$, where $u \in k_2^M L$. Hence

$$h_k(N_{L/k}(u)) = N_{L/k}(h_L(u)) = N_{L/k}(Q_L) = 0.$$

By the injectivity of the norm residue homomorphism we therefore have $N_{L/k}(u) = 0$, and by Lemma 43, it follows $u = v_L$ for some $v \in k_2^M k$. Then since

$$h_k(v)_L = h_L(v_L) = h_L(u) = Q_L,$$

we see that $Q - h_k(v)$ splits over a quadratic extension, and so denoting $s = \mathrm{ind}(Q - h_k(v))$, it follows by [2] Corollary 98.5 that s divides $[L : k] = 2$, hence either $s = 2$ or $s = 1$. Clearly if $s = 1$ then $Q - h_k(v)$ is split, and hence the class of a quaternion algebra. If $s = 2$ then $Q - h_k(v)$ is Brauer-equivalent to a four-dimensional central division algebra over k, so is a two-dimensional vector space over $L = k(\sqrt{d})$ for some $d \in k^\times$, and is thus the class of a quaternion algebra. In either case we have that $Q - h_k(v)$ is the class of a quaternion algebra, and hence $Q - h_k(v) = h_k(w)$ where $w \in k_2^M k$ is a pure symbol. So $Q = h_k(w + v) \in \mathrm{Im}(h_k)$.

2. We now pass to the general case. Let k' be the maximal subfield of the algebraic closure $\overline{k}$ such that every finite subextension of k' has odd degree. Such a field k' exists by the axiom of choice, and clearly there does not exist any nontrivial extensions of k' of odd degree. Then by the first part of the proof, in the Brauer group we have

$$Q_{k'} = h_{k'}(v') = \sum Q'$$

for some $v' \in k_2^M(k')$ and classes of quaternion algebras Q' defined over k'. But observing that k' is the union of all finite odd degree extensions L/k, we see that we may choose a nontrivial odd degree extension L/k with each Q' in the sum above defined over L and thus with $Q_L = h_L(v)$ for some $v \in k_2^M L$. Then we have

$$Q = N_{L/k}(Q_L) = N_{L/k}(h_L(v)) = h_k(N_{L/k}(v)) \in \mathrm{Im}\, h_k.$$

as required. □

Combining the proofs of injectivity and surjectivity, this completes the proof of Theorem 9. □

6 Conclusions & Further Study

The moral of this dissertation is that there can exist deep connections between ostensibly different areas of mathematics. The primary result of this dissertation, the norm residue isomorphism theorem in degree two, is important as it allows one to use the properties of Milnor K-theory to characterise and understand central simple algebras of order 2 in the Brauer group. As a key example of this idea, we easily deduce the following result, purely on the side of central simple algebras:

Corollary 1. *Suppose D is a central division algebra such that $D \otimes_k D$ is isomorphic to a matrix algebra over k. Then there exists $m, m', n \in \mathbb{N}$ and quaternion algebras $Q_1, \ldots, Q_n$ defined over k such that there is an isomorphism*

$$D \otimes_k M_m(k) \cong Q_1 \otimes_k Q_2 \otimes_k \cdots \otimes_k Q_n \otimes_k M_{m'}(k).$$

Proof. By hypothesis $D \in \mathrm{Br}_2(k)$. Hence D is in the codomain of the norm residue homomorphism, and by Theorem 9 we see D is the image of a sum of pure symbols, i.e, Brauer equivalent to a product of quaternion algebras. The result follows. □

The connection between quadratic forms and Milnor K-theory is also advantageous, since one can understand quadratic forms in the Witt ring through the associated graded ring with which Milnor K-theory gives a description by generators and relations (although we did not prove Voevodsky's innovative result that shows the nth graded component of the Witt ring and the nth Milnor K-group agree for $n > 2$).

One may pursue a ubiquitous number of further topics to supplement the material of this dissertation. The most natural choice would be to study the Chow groups of algebraic geometry. Specifically, given a smooth variety X over a field k, there are the Chow groups $CH_i(X)$ which give strong information about the subvarieties of X. One may generalise these groups to the *motivic cohomology* groups $H^{a,b}_{\mu}(X, \mathbb{Z})$ of X, which simultaneously capture both the Chow groups and Milnor K-theory. In fact, Voevodsky's proof of the Milnor conjecture makes extensive use of techniques from motivic cohomology. So perhaps one could also go on to try and understand this proof after learning the theory of motives. I studied many more mathematical ideas that failed to make it into the final report as I felt they would distract the reader from the core story that I wanted to tell. Nonetheless, you can see the influence of larger overarching ideas throughout the text.

As a final closing remark, I'd like to again thank my supervisor, Alexander Vishik, for the time and effort he sacrificed towards supervising my project. Without his guidance I would surely be lost in the high levels of abstraction and sophistication that some of the ideas I dealt with in this dissertation entailed. It was certainly thanks to him that I was able to tackle such an ambitious project.

References

[1] Hyman Bass and John Tate. "The Milnor ring of a global field". In: *"Classical" Algebraic K-Theory, and Connections with Arithmetic*. Springer, 1973, pp. 347–446.

[2] Richard S Elman, Nikita Karpenko, and Alexander Merkurjev. *The algebraic and geometric theory of quadratic forms*. Vol. 56. American Mathematical Soc., 2008.

[3] William Fulton. "Algebraic curves". In: *An Introduction to Algebraic Geom* (2008), p. 54.

[4] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*. Vol. 165. Cambridge University Press, 2017.

[5] Tsit-Yuen Lam. *Introduction to quadratic forms over fields*. Vol. 67. American Mathematical Soc., 2005.

[6] Alexander Merkurjev. "On the norm residue homomorphism of degree two". In: *Translations of the American Mathematical Society-Series 2* 219 (2006), pp. 103–124.

[7] John Milnor. "Algebraic K-theory and quadratic forms". In: *Inventiones mathematicae* 9.4 (1970), pp. 318–344.

[8] Dmitri Orlov, Alexander Vishik, and Vladimir Voevodsky. "An exact sequence for with applications to quadratic forms". In: *Annals of mathematics* (2007), pp. 1–13.