MSc Pure Mathematics - Master's Thesis

Pfister's Local-Global Principle and the u-invariant of Formally Real Fields

April 26, 2020

Benjamin Miles Bullough
Imperial College London
Department of Mathematics
CID: 01045560

Project Supervisor: Dr. Ambrus Pál

Abstract

We present an introduction to Witt's theory of quadratic forms, to accompany a direct proof of Pfister's Local-Global Principle for non-singular quadratic forms over formally real fields. Our approach elaborates on the work of K.J. Becher and T.Y. Lam, employing annihilating Lewis polynomials to recover structures of the Witt ring to prove A. Pfister's result, coupled with the machinery of Pfister forms and ideals of T-hyperbolic quadratic forms. Our thesis culminates in an application of Pfister's celebrated principle to the general u-invariant of formally real fields, as we elucidate a proof of C. Scheiderer concerning the general u-invariant of a residue class field, via the notion of compatibility between field orders and valuations.

Acknowledgements

I would like to thank Dr. Ambrus Pál, whose invaluable guidance allowed me to establish a clear topic, direction and objective for this master's thesis.

Declaration

The work contained in this thesis is my own work, unless stated otherwise.

Contents

Introduction

Pfister's Local-Global principle, first found in A. Pfister's paper 'Quadratische Formen in Beliebigen Korpern' from 1966, establishes a simple characterization of torsion in the Witt ring $W(F)$ in terms of the signature homomorphism, where F is a formally real field of characteristic not equal to 2. Pfister's celebrated result states most importantly that the kernel of the total signature homomorphism is equal to the torsion subgroup of the Witt Ring. The second objective of this thesis is an application of Pfister's local-global principle to the general u-invariant of formally real fields, due to C. Scheiderer [18] in 2000. Defined by R. Elman and T.Y. Lam [8] in 1973, the general u-invariant of a field is the maximum dimension of an anisotropic torsion form of $W(F)$. By providing more detail to Sheiderer's proof, we show that if F is the formally real field of fraction of a henselian valuation ring A, if $\bar{F}$ is the residue class field of F, then $u'(F) = 2u(\bar{F})$.

Typically, going by the standard references for quadratic forms of W. Scharlau [17] and Lam [11] - from 1973 and 1985 respectively - proofs of Pfister's Local-Global principle usually rest on Scharlau's Transfer Lemma, alongside an understanding of Pythageorean fields, Pythagorean extensions and real closures. The novelty of K.J. Becher's proof in [1] is particularly attractive, relying simply on Lewis polynomials and the machinery of Pfister forms. More importantly, the central role played by signature homomorphisms of quadratic preorderings in [1] makes this a compelling approach with regard to Scheiderer's paper [18]. This provides homogeneity to our thesis, which consequently sits at the juncture between quadratic forms and field orderings. Incidentally, this makes Lam's conference notes, 'Orderings, Valuations and Quadratic Forms' [12] from 1983 an interesting complement and source of further reading for our thesis, although we will not use these notes extensively. The proposition we prove from Scheiderer's paper is similarly worthy of note, in as it proves a result which looks very similar to the result found on [11, Page 148, §6] - essentially swapping completeness for the formally real and henselian properties - through greatly contrasting methods. This makes for a fascinating application of Pfister's Local-Global principle, especially as it builds on many of the themes developped in Becher's proof, largely through the use of the Harrison topology.

The aim of this project is to substantiate Pfister's principle, through a direct approach which is as self-contained as possible. This ambition drives the theory and the structure of the first five chapters of our thesis, whereas the final chapter presents an opportunity to expand towards a challenging application. In Chapter 1, we introduce the necessary framework of quadratic forms and quadratic spaces, following an approach which is similar to [11], refering to [17] for some additional colour, as well as frequently using [5] for more relevant and concise explanations. This section is dealt with as succinctly as possible, laying out prerequisites - namely the orthogonal sum, representation, diagonalization and the Kronecker product - for Witt's theory of quadratic forms.

In Chapter 2, we delve into Witt's theory of quadratic forms, which originated in 1937, by presenting three main theorems: cancellation, decomposition, chain-equivalence. All three are integral to the subsequent chapters, and we again refer mostly to Lam's proofs of these theorems in [11]. Witt's cancellation theorem is used almost omnipresently, and in particular to define the Witt ring. His decomposition theorem allows us to consider elements of the Witt ring as anisotropic quadratic forms and his chain-equivalence theorem later proves that the signature homomorphism is well-defined on the Witt ring.

The above allows us to define the Witt ring $W(F)$ in Chapter 3, after following [4] to first provide a construction of the Grothendieck-Witt ring $\hat{W}(F)$ and prove its universal property. We also define the fundamental ideal of the Witt ring and prove important properties relating to it. This is interesting to do ahead of Chapter 5 as these facts are somewhat analogous to many of the properties of the ideals of T-hyperbolic quadratic forms.

Chapter 4 is a comprehensive introduction to ordered fields, defining fields orders, quadratic preorderings, and proving the Artin-Schreier's theorem: a field has an order if and only if it is formally real. Lorenz's text [14] is a useful source for most of this chapter, which we conclude by proving ourselves using Witt's chain-equivalence theorem that the signature homomorphism, defined as in [12], is well-defined on the Witt ring.

Our thesis culminates in Chapters 5 and 6, which respectively detail proofs of Pfister and Scheiderer's aforementioned results. In Chapter 5, following the path set out by [1], the remarkable annihilating property of n-th Lewis polynomials on quadratic forms of dimension n helps recover an important structural feature of the Witt ring, namely that its ideals $I_T(F)$ (where T is a quadratic preordering of F) are radical ideals. Defining and proving the multiplicativity of Pfister forms leads to the characterization $I_{\sum F^2}(F) = W(F)_{tors}$, and Pfister's Local-Global principle follows after proving Theorem 5.18, an important theorem of Lorenz and Leicht which incidentally also proves that the u-invariant and general u-invariant of non-formally real fields coincide in Chapter 6.

The Harrison topology, valuations on fields and their compatibility with orderings, discrete valuation rings and finally the Baer-Krull theorem are covered as preliminaries in Chapter 6 to make Scheiderer's proof intelligible. We take the opportunity to prove some interesting facts about the (general) u-invariant, before the climax of Scheiderer's proof - in the formally real case - that $u'(F) = 2u'(\bar{F})$ if the discrete valuation ring A is henselian, and $u(F) \geq 2u'(\bar{F})$ otherwise. We add significant amounts of detail to the author's proof, partly inspired by the work of P.L. Clark in [6] in one step of this endeavour.

Overall, this project is framed so that prerequisite knowledge is kept to a minimum, as we take the time to build up the relevant theory in a way which suits our needs. Nonetheless, familiarity with standard commutative algebra results and discrete valuation rings is helpful, as these topics do not receive an extensively detailed treatment in Chapters 5 and 6.

1 Quadratic Forms and Quadratic Spaces

In this first chapter, we establish the main definitions of the algebraic theory of quadratic forms. We proceed in a detailed way, to emphasise the grounding in homogeneous polynomials of degree 2 and symmetric matrices, which will be useful in proving Witt's theorems on quadratic forms. Let F denote a field of characteristic not equal to 2.

1.1 Quadratic Forms

Definition 1.1 *An <u>n-ary quadratic form</u> $f \in F[X_1, ..., X_n]$ is a homogeneous polynomial of degree 2, in n variables. In other words, an n-ary quadratic form $f \in F[X_1, ..., X_n]$ is a polynomial of the form:*

$$f(X_1, ..., X_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} X_i X_j, \qquad a_{ij} \in F.$$

Remark Define $b_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$ for all $i, j \in [\![1, n]\!]$. Define the $n \times n$ matrix $M_f = (b_{ij})_{i,j=1,\ldots,n}$. The matrix M_f is clearly symmetric by commutativity of the $+$ law in the field F, and we have:

$$f(X_1, ..., X_n) = \sum_{i=1}^{n} \sum_{j=i}^{n} (a_{ij} + a_{ji}) X_i X_j = \sum_{i=1}^{n} \sum_{j=i}^{n} (b_{ij} + b_{ji}) X_i X_j = \begin{pmatrix} X_1 \ldots X_n \end{pmatrix} .M_f. \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}.$$

For a quadratic form f, let $M_f \in \mathcal{M}_n(F)$ denote the associated symmetric matrix of f, as defined above.

Definition 1.2 *The <u>quadratic map</u> q defined by the quadratic form f over F^n, with the standard canonical basis $\{e_1, ..., e_n\}$ of F^n, is the map:*

$$q : \left| \begin{array}{ccc} F^n & \longrightarrow & F \\ \sum_{i=1}^{n} x_i.e_i & \longmapsto & f(x_1, ..., x_n) \end{array} \right.$$

where $x_i \in F$ are scalars.

The following theorem from [5, p.3] sums up all of the above succinctly, and explains why in this project will use the notions of quadratic maps, quadratic forms, symmetric matrices and symmetric bilinear pairings interchangeably.

Theorem 1.3 *Let $n \in \mathbb{N}$. There are canonical 1-to-1 correspondences between the following:*

1. *The set of homogeneous polynomials of degree two in n variables over F.*
2. *The set of quadratic maps $q : F^n \to F$.*
3. *The set of symmetric $n \times n$ matrices with values in F.*
4. *The set of symmetric bilinear forms $B : F^n \times F^n \to F$.*

Proof:

- (1) $\leftrightarrow$ (3) : We have already seen that f is entirely defined by its associated symmetric matrix.

- (2) $\leftrightarrow$ (4) : We have the two inverse constructions:

$$q \to B(x,y) = \frac{1}{2}(q(x+y) - q(x) - q(y))$$

$$q(x) = B(x,x) \leftarrow B$$

  By bilinearity of B and the fact that for all $a \in F, x \in F^n, q(a.x) = a^2.q(x)$, these are easily seen to be well-defined maps, and inverse of each other.

- (3) $\leftrightarrow$ (4) : If $M \in \mathcal{M}_n(F)$ is a symmetric matrix, then the function:

$$B : \left| \begin{array}{ccc} F^n \times F^n & \longrightarrow & F \\ (x,y) & \longmapsto & x^t.M.y \end{array} \right.$$

  is symmetric and is also clearly bilinear. Conversely, if we are given a symmetric bilinear function $B : F^n \to F^n$, then define the symmetric matrix: $M = (B(e_i, e_j))_{i,j=1,\dots,n}$. From the fact that $e_i^t.M.e_j = [M]_{i,j}$, it is clear that these constructions are inverse of each other, as the values $B(e_i, e_j)$, for $i, j \in [\![1, \dots, n]\!]$ determine entirely the symmetric bilinear form B on $F^n \times F^n$.

$\square$

Remark Let V be an n-dimensional F-vector space. We can define, on V, a quadratic map $q : V \to F$ by simply identifying V with F^n by a coordinatization of V, ie: taking $\{f_1, \dots, f_n\}$ a basis of V and considering vectors $v \in V$ as n-tuples of coordinates with respect to this basis. This idea motivates the notion of 'equivalence' in the following section, as two different coordinatizations of V could give two different quadratic maps.

1.2 Equivalence of Quadratic Forms

Definition 1.4 *Let $f, g \in F[X_1, \dots, X_n]$ be n-ary quadratic forms. Denote $X = \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}$ for the n-tuple of indeterminates, and write $f(X) = f(X_1, \dots, X_n)$. We say that f and g are equivalent if there exists an $n \times n$ matrix $C \in GL_n(F)$ such that: $f(X) = g(C.X)$. Finally, we say that quadratic maps q_f and q_g are equivalent when their associated quadratic forms f and g are equivalent.*

The following proposition is obtained immediately from the above definition, and we use it to prove Proposition 1.6, which can be found as a remark in [11, p.5].

Proposition 1.5 *Two quadratic forms are equivalent if and only if their associated symmetric matrices are congruent (in the traditional linear algebra sense).*

Proposition 1.6 *Let $B : V \times V \to F$ be a symmetric bilinear form, let V be an n-dimensional F-vector space. Two quadratic forms f, f', obtained from B by different coordinatizations of V, are equivalent.*

Proof: We follow the proof from [11]. Let $\{e_1, ..., e_n\}$ and $\{f_1, ..., f_n\}$ be different bases for f, f' respectively. Then, for each $i \in [\![1, n]\!]$, we have: $f_i = \sum_{k=1}^{n} c_{ki} e_k$ for some $c_{1i}, ..., c_{ni} \in F$. We have from the proof of Theorem 1.3 that $M_f = (B(e_i, e_j))_{i,j=1,...,n}$ and $M_{f'} = (B(f_i, f_j))_{i,j=1,...,n}$, and therefore:

$$[M_{f'}]_{i,j} = B(f_i, f_j) = B(\sum_{k=1}^{n} c_{ki} e_k, \sum_{l=1}^{n} c_{lj} e_l) = \sum_{k,l} c_{ki} B(e_k, e_l) c_{lj} = [C^t.M_f.C]_{i,j},$$

where $C = (c_{kl})_{k,l=1,...,n}$. It is clear from the definition of C and elementary linear algebra that it is invertible. This shows that M_f and $M_{f'}$ are congruent, and we conclude by Proposition 1.5. □

Remark This solves the issue raised at the end of Section 1.1. The above definition also tells us that two quadratic maps $q, q' : V \to F$ are equivalent if and only if there exists a linear isomorphism $\phi \in \mathrm{End}(V)$ such that: $\forall v \in V, q(v) = q'(\phi(v))$. The isomorphism ϕ is precisely left multiplication by the invertible matrix $C \in GL_n(F)$ which gives equivalence of f and f'.

1.3 Quadratic Spaces

Definition 1.7 *Let V be a finite-dimensional F-vector space, let $B : V \times V \to F$ be a symmetric bilinear form on V. A* <u>*quadratic space*</u> *is a pair (V, B), which, by Theorem 1.3, can also be denoted by (V, q) where $q(v) = B(v, v)$ for all $v \in V$.*

Definition 1.8 *Let $(V, B), (V', B')$ be two quadratic spaces. We say that (V, B) and (V', B') are* <u>*isometric*</u> *(denoted as: $(V, B) \simeq (V', B')$) if there exists a linear isomorphism $\tau \in \mathcal{L}(V, V')$ such that: $\forall x, y \in V, B(x, y) = B'(\tau(x), \tau(y))$.*

By Theorem 1.3 and the final remark of Section 1.2, we have the following important theorem from [11, p.5], which allows us to consider equivalences of quadratic forms synonymously with isometries of quadratic spaces:

Theorem 1.9 *Let (V, B) and (V', B') be quadratic spaces. Then $(V, B) \simeq (V', B')$ if and only if f_B and $f_{B'}$ are equivalent. There is a 1-to-1 correspondence between isometry classes of n-dimensional quadratic spaces and equivalence classes of n-ary quadratic forms.*

We will need the following definitions. Let (V, B) be a quadratic space, let S be a subspace of V, which is also a quadratic space, with symmetric bilinear form $B_{|S \times S}$. The <u>orthogonal complement in V</u> of S is as usual $S^{\perp} = \{x \in V \mid B(x, S) = 0\}$. We say that

(V, B) is regular if its radical, defined by $rad(V) = V^{\perp}$, is equal to 0, or equivalently if B is non-degenerate on V. It is easy to see that B is non-degenerate if and only if the map:

$$\rho : \left| \begin{array}{ccc} V & \longrightarrow & V^* \\ x & \longmapsto & B(\cdot, x) \end{array} \right.$$

is an isomorphism of vector spaces, if and only if the associated symmetric matrix M_B of B is non-singular. In the above case, we say that the quadratic map $q_B : x \mapsto B(x, x)$ is a non-singular quadratic map.

Definition 1.10 *Let $(V_1, B_1), (V_2, B_2)$ be two quadratic spaces. Their orthogonal sum is the quadratic space (V, B), denoted by $V_1 \perp V_2 = V$, defined by:*

$$V = V_1 \oplus V_2 \quad , \qquad B : \left| \begin{array}{ccc} V \times V & \longrightarrow & F \\ ((x_1, x_2), (y_1, y_2)) & \longmapsto & B_1(x_1, y_1) + B_2(x_2, y_2) \end{array} \right.$$

B is indeed symmetric and bilinear, B restricted to V_i is B_i, and considering V_1 and V_2 as subspaces of V by the canonical inclusion, $B(V_1, V_2) = 0$.

Notation For any two quadratic spaces $(V, B, q), (V', B', q')$, we can denote their orthogonal sum as $V \perp V', B \perp B', q \perp q'$, or $(V, q) \perp (V', q')$ all equivalently and interchangeably.

1.4 The Representation Criterion and Diagonalization

We will need the following proposition - which can be found in [5, p.10] - to prove the Representation Criterion. We provide a proof which is largely similar to [5, p.10].

Proposition 1.11 *Let (V, B) be a quadratic space, and let $W \subset V$ be a regular subspace of V. Then:*

$$V = W \perp W^{\perp}.$$

Proof: We know that W is regular if and only if B is non-degenerate when restricted to W. So we have: $W \cap W^{\perp} = 0$, because if $y \in W \cap W^{\perp}$, then $B(x, y) = 0$ for all $x \in W$, so $y = 0$ by non-degeneracy of B on W. Let $z \in V$. Consider $\phi \in W^*$, the dual of W, defined by: $\forall x \in W, \phi(x) = B(x, z)$. We know that B is non-degenerate on W if and only if $x \mapsto B(x, \cdot)$ is an isomorphism from W to W^*. Therefore, since $\phi \in W^*$, there exists $y \in W$ such that $\phi = B(y, \cdot) = B(z, \cdot)$. So $B(z - y, \cdot) \equiv 0$, therefore $z - y = a \in W^{\perp}$. So $z = y + a$, with $y \in W, a \in W^{\perp}$, which gives us: $V = W \oplus W^{\perp}$. W and $W^{\perp}$ inherit the (restricted) bilinear form B, and because $B(W, W^{\perp}) = 0$, we can conclude that $V = W \perp W^{\perp}$. $\square$

Definition 1.12 *We say that a quadratic form $f \in F[X_1, ..., X_n]$ is diagonal if one of the following two equivalent conditions is satisfied:*

1. $f(X) = \sum_{i=1}^{n} a_i X_i^2$ *, for some $a_i \in F$.*
2. M_f *is a diagonal matrix.*

We say that an n-dimensional quadratic space (V, B) is <u>*diagonalizable*</u> *if there exists n 1-dimensional quadratic spaces $W_1, ..., W_n$ such that: $V \simeq W_1 \perp ... \perp W_n$.*

Notation For $d \in F$, let $\langle d \rangle$ denote the isometry class of the 1-dimensional quadratic space corresponding to the quadratic form dX^2.

We want to describe when a quadratic space is diagonalizable, as this form will clearly be easier to work with. In fact, it turns out that all quadratic spaces are diagonalizable. This will be a corollary of the Representation Criterion, as found in [11, p.9]. We first need to define what it means for a quadratic form to represent an element of F^*.

Definition 1.13 *We say that a quadratic form $f \in F[X_1, ..., X_n]$* <u>*represents*</u> *an element $d \in F^*$ if there exists $x_1, ..., x_n \in F$ such that $f(x_1, ..., x_n) = d$. Let $D(f) = \{d \in F \mid f \text{ represents } d\}$. Similarly, for a quadratic space (V, B), we define $D(V) = \{d \in F^* \mid \exists v \in V, q_B(v) = d\}$.*

Remark Suppose that $a, d \in F^*$. Then $d \in D(f)$ if and only if $a^2 d \in D(f)$. This fact is immediate from the that $q_f(a.v) = a^2 q_f(v)$ for all $v \in V, a \in F$. This allows us to consider $D(f)$ as a well-defined subset of $F^*/(F^*)^2$, the group of square classes of F^*. Moreover, it is important to remark for future reference that $\langle a^2 d \rangle \simeq \langle d \rangle$ for all $d \in F, a \in F^*$, via the isometry given by left-multiplication by a. Finally, by the definition of an isometry, it is clear that the set of elements represented by a quadratic form is invariant under isometry.

Theorem 1.14 *(*<u>*Representation Criterion*</u>*): Let (V, B) be a quadratic space, and let $d \in F^*$. Then:*

$$d \in D(V) \iff \exists (V', B'), V \simeq \langle d \rangle \perp V'.$$

Proof: ($\Longleftarrow$): The quadratic form of V is given by $f_B(x_1, ..., x_n) = f_{B'}(x_1, ..., x_{n-1}) + dx_n^2$. Then $(0, 0, ..., 0, 1)$ gives $d \in D(V)$.

($\Longrightarrow$): Let $d \in D(V)$. There exists $v \in V$ such that $q(v) = d$. Since $d \neq 0$ and $v \neq 0$, $F.v$ is a 1-dimensional regular subspace of V. So $F.v \perp (F.v)^\perp = V$ by Proposition 1.11. We have that $F.v \simeq \langle d \rangle$, via the isometry $\lambda.v \mapsto \lambda$, because as $q(\lambda.v) = \lambda^2 d$ on $F.v$, whereas on $\langle d \rangle$, dX^2 also gives $\lambda^2 d$. We can conclude, as required, that: $V \simeq \langle F.v \rangle \perp (F.v)^\perp \simeq \langle d \rangle \perp (F.v)^\perp$. $\square$

Notation We will sometimes also write $\langle v \rangle$ instead of $\langle d \rangle$ when v and d are as in the proof above.

Corollary 1.15 *Let (V, B) be a quadratic space of dimension n over the field F. Then (V,B) is diagonalizable, ie: $V \simeq \langle d_1 \rangle \perp ... \perp \langle d_n \rangle$ for some $d_1, ..., d_n \in F$. By 1.9, this means that any n-ary quadratic form is equivalent to a diagonal quadratic form, namely $d_1 X_1^2 + ... + d_n X_n^2$. We also write this diagonalization as $V \simeq \langle d_1, ..., d_n \rangle$ for compactness.*

Proof: Let (V, q) be a quadratic space of dimension n. If $D(V) = \emptyset$, then $V = \langle 0, ..., 0\rangle$ and we are done. If there exists $d_1 \in D(V)$, then by Theorem 1.14, we have that $V \simeq \langle d_1\rangle \perp V_1$, where V' is a quadratic space of dimension $n-1$. By induction, V' has a diagonalization $V' = \langle d_2, ..., d_n\rangle$ so that $V \simeq \langle d_1, ..., d_n\rangle$, as required. The base case for this induction is trivial. □

1.5 Determinant of a Non-Singular Quadratic Form

Definition 1.16 *The* <u>*determinant*</u> *of a non-singular quadratic form f is an element of the group of square classes $F^*/(F^*)^2$ and is defined by:*

$$d(f) = \det(M_f).(F^*)^2$$

Proposition 1.17 *The determinant of a non-singular quadratic form is an invariant of the equivalence class of f, and therefore also of the isometry class of a quadratic space.*

Proof: Let g be a quadratic form which is equivalent to f. There exists $C \in GL_n(F)$ such that $M_g = C^t.M_f.C$ by Proposition 1.5. Therefore: $d(g) = \det(C^t.M_f.C).(F^*)^2 = \det(C)^2.\det(M_f).(F^*)^2 = \det(M_f).(F^*)^2 = d(f)$. □

Proposition 1.18 *Let f, g be two non-singular quadratic forms. Then: $d(f\perp g) = d(f)d(g)$.*

Proof: We have that: $M_{f\perp g} = \begin{pmatrix} M_f & (0) \\ (0) & M_g \end{pmatrix}$, and therefore $\det(M_{f\perp g}) = \det(M_f).\det(M_g)$, as required. □

Remark The above proposition can be found in [17, p.11]. Using the notation of Corollary 1.15, it shows via an easy induction that $d(V) = d(f) = d_1...d_n.(F^*)^2$ for a diagonalized quadratic space and quadratic form.

1.6 Kronecker Product

We have already defined and discussed the orthogonal sum $'\perp'$, which will allow us to define the additive law of the Witt ring. We now define the Kronecker product $'\otimes'$ of two quadratic spaces, following the definitions of [11], which will help us define the multiplicative law of the Witt ring in Chapter 3.

Definition 1.19 *Let (V_1, B_1) and (V_2, B_2) be two quadratic spaces. We define the vector space $V = V_1 \otimes V_2$, the linear span of the ordered basis $\{e_1 \otimes f_1, e_1 \otimes f_2, ..., e_n \otimes f_m\}$, where $\{e_1, ..., e_n\}$ is an ordered basis of V_1 and $\{f_1, ..., f_m\}$ is an ordered basis of V_2. We define the symmetric bilinear map on V:*

$$B : \left| \begin{array}{ccc} V \times V & \longrightarrow & F \\ (v_1 \otimes v_2, v_1' \otimes v_2') & \longmapsto & B_1(v_1, v_1')B_2(v_2, v_2') \end{array} \right.$$

(V, B) is indeed a quadratic space, and is called the <u>*Kronecker product*</u> *of both quadratic spaces, as it is easy to see that B is symmetric and bilinear.*

Proposition 1.20 *The symmetric matrix of B is given by the Kronecker product of the symmetric matrices of B_1 and B_2.*

Proof: Let M, M_1, M_2 be the symmetric matrices of B, B_1, B_2 respectively. Suppose that $M_1 = (a_{ij})_{i,j=1,\ldots,n}$ and $M_2 = (b_{kl})_{k,l=1,\ldots,m}$. Let $i, j \in [\![1, n]\!]$, let $k, l \in [\![1, m]\!]$. Then:

$$[M]_{i.k,j.l} = B(e_i \otimes f_k, e_j \otimes f_l) = B_1(e_i, e_j)B_2(f_k, f_l) = a_{ij}.b_{kl},$$

so this gives precisely the Kronecker product of M_1 and M_2. □

Proposition 1.21 *The Kronecker product satisfies commutative, associative, and distributive laws on quadratic forms, the latter with respect to the orthogonal sum operation.*

Proof: The proof is a series of straightforward checks from the definitions of the Kronecker product and orthogonal sum of two quadratic spaces and the resulting quadratic form. □

Proposition 1.22 *For all $a, b \in F^*$, $\langle a\rangle \otimes \langle b\rangle \simeq \langle ab\rangle$.*

Proposition 1.23 *Let q_1, q_2 be two quadratic forms over F. Then:* $\dim(q_1 \otimes q_2) = \dim(q_1). \dim(q_2)$.

The proof of Proposition 1.22 is immediate using Proposition 1.20, and the fact that the symmetric matrix for $\langle a\rangle$ is just the scalar a. This, along with the distributivity of the Kronecker product over the orthogonal sum as stated in Proposition 1.21, shows us that for two diagonal forms $\langle a_1, ..., a_n\rangle \otimes \langle b_1, ..., b_m\rangle \simeq \langle a_1b_1, ..., a_1b_m, a_2b_1, ..., a_nb_m\rangle$. Proposition 1.23 comes directly from the definition of the Kronecker product, and shows in Chapter 3 that dim is a semi-ring homomorphism.

2 Witt's Theorems

Let F be a field of characteristic not equal to 2. From now on, we will freely refer to quadratic maps $q : V \to F$ as quadratic forms, as there is no longer a need to make a strong distinction between q_f and f, given how we pass from one form to the other using Theorem 1.3, as we did throughout Chapter 1.

2.1 The Hyperbolic Plane

The following terms are central to Witt's theory of quadratic forms, and can be found in any standard text on quadratic forms, ie: [17] or [11], for example.

Definition 2.1 *Let (V, B) be a quadratic space. Let $v \in V$. We say that v is an isotropic vector if $q_B(v) = B(v, v) = 0$, and anisotropic otherwise. We say that (V, B) is isotropic if it contains an isotropic vector, and anisotropic otherwise. We say that (V, B) is totally isotropic if every $v \in V$ is an isotropic vector.*

Before getting to Witt's Decomposition Theorem, we first need to define a special isometry class of quadratic forms which will play a key role in Witt's theory of quadratic forms. To this end, we use the following theorem from [11, p.12].

Definition-Theorem 2.2 *Let (V, q) be a 2-dimensional quadratic space. Then the following are equivalent:*

1. *V is regular and isotropic.*
2. *V is regular, with $d(V) = -1.(F^*)^2$.*
3. *V is isometric to $\langle 1, -1\rangle$.*
4. *V corresponds to the equivalence class of the binary quadratic form X_1X_2.*

The isometry class of any 2-dimensional quadratic space satisfying one of the equivalent conditions above is called the hyperbolic plane, and is denoted by $\mathbb{H}$. An orthogonal sum of hyperbolic planes is called a hyperbolic space.

Proof:

- (1) $\implies$ (2): Consider a diagonal basis for V, $\{v_1, v_2\}$, as V is diagonalizable. Then $q(v_1) = d_1 \neq 0$ and $q(v_2) = d_2 \neq 0$, by regularity of V. The associated quadratic form f of (V, q) is $d_1X_1^2 + d_2X_2^2$. We also know that V has an isotropic vector, so there exists $w = av_1 + bv_2 \in V$ such that $q(w) = 0$. So: $q(av_1 + bv_2) = f(a, b) = a^2.d_1 + b^2.d_2 = 0$, so: $d_1 = -(\frac{b}{a})^2 d_2$ and: $d(V) = d(f) = d_1.d_2.(F^*)^2 = -d_2^2(\frac{b}{a})^2.(F^*)^2 = -1.(F^*)^2$.

- (2) $\implies$ (3) : We can write $V = \langle a, b\rangle$, for $a, b \in F^*$ as V is regular. Since $d(V) = -1.(F^*)^2$, we have that $ab.(F^*)^2 = -1.(F^*)^2$ so: $-(a^{-1})b \in (F^*)^2$, and therefore $b = (-a).c$ where c is a square in F^*. So $V \simeq \langle a, b\rangle \simeq \langle a, -a\rangle$ by the remark on page

7. So V is defined by the quadratic form $f(X_1, X_2) = aX_1^2 - aX_2^2$ which is equivalent to the quadratic form $g(X_1, X_2) = aX_1X_2$ via the invertible matrix:

$$C = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

because: $g(C.X) = a(X_1 + X_2)(X_1 - X_2) = aX_1^2 - aX_2^2 = f(X)$. We have $1 \in D(V)$ from $g(a^{-1}, 1) = 1$ and therefore by the Representation Criterion, $V \simeq \langle 1, b\rangle$ for some $b \in F^*$. Then $D(V) = 1.b.(F^*)^2 = -1.(F^*)^2$ by our assumption, and therefore b is equal to -1 up to multiplication by a square. We conclude that $V \simeq \langle 1, b\rangle \simeq \langle 1, -1\rangle$ thanks to our remark on page 7.

- (3) $\Longrightarrow$ (4) : We showed above that $f(X) = X_1^2 - X_2^2$ and $g(X) = X_1X_2$ are equivalent quadratic forms.
- (4) $\Longrightarrow$ (1) : Consider the quadratic space (V, q) whose associated quadratic form is $g(X) = X_1X_2$. Then $M_g = \begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix}$, which is invertible, and therefore (V, q) is a regular quadratic space. The coordinates $(1, 0)$ give an isotropic vector.

$\square$

We obtain the following important theorem via a modified proof from [11, p.14].

Theorem 2.3 *Let (V, B) be a regular quadratic space. V is isotropic if and only if V contains a hyperbolic plane as an orthogonal summand.*

Proof: $(\Longleftarrow)$: We have that $V \simeq \mathbb{H} \perp V' \simeq \langle -1, 1\rangle \perp V'$, for some quadratic space (V', B'). Then: $(1, 1, 0, ..., 0)$ is an isotropic vector of V.
$(\Longrightarrow)$: Let $x \neq 0 \in V$ be an isotropic vector. Let $U = F.x$, a 1-dimensional vector space. Since V is regular, B is non-degenerate on V and there exists $y \in V$ such that $B(x, y) \neq 0$. $y \notin U$ because $B(x, \lambda.x) = \lambda B(x, x) = 0$ for all $\lambda \in F$, as x is isotropic. Therefore, consider the subspace $H = \langle x, y\rangle$, a quadratic space using the restriction of B. It has determinant:

$$d(H) = \det \begin{pmatrix} 0 & B(x, y) \\ B(y, x) & B(y, y) \end{pmatrix} .(F^*)^2 = -1.(F^*)^2.$$

So $H \simeq \mathbb{H}$ by Theorem 2.2, because $\det(M_B) = -B(x, y)^2 \neq 0$ gives its invertibility and so equivalently regularity of H. By Proposition 1.11, and because we know that the hyperbolic plane is regular, we see that V contains the hyperbolic subspace as an orthogonal summand.
$\square$

2.2 Preliminaries on Hyperplane Reflections

Let (V, B, q) be a quadratic space, and let $O(V)$ denote the group of isometries of V onto itself. These are also called the autometries of V in [4], terminology which we adopt. For an anisotropic vector $v \in V$, define the hyperplane reflection τ_v by:

$$\tau_v : \left| \begin{array}{ccc} V & \longrightarrow & V \\ x & \longmapsto & x - \frac{2B(x,v)}{q(v)} v \end{array} \right.$$

To prove Witt's Cancellation Theorem, we need the two following facts: Proposition 2.4 and Proposition 2.5. These can be found in [4, p.18-20]. The proof of Proposition 2.4 is just a straightforward check of the defining properties of an autometry, and so we omit the proof. Note that the fact that τ_v is a bijection is obtained from $\tau_v^2 = \mathrm{id}_V$.

Proposition 2.4 *For every anisotropic vector $v \in V$, τ_v is an autometry of V.*

Proposition 2.5 *Let (V, B, q) be a quadratic space, and let $x, y \in V$ be anisotropic vectors. If $q(x) = q(y)$, then there exists $\tau \in O(V)$ such that $\tau(x) = y$.*

Proof: *(of Proposition 2.5)*: We have: $B(x-y, x-y) = B(x,x) - 2B(x,y) + B(y,y) = 2(q(x) - B(x,y))$. F has characteristic not equal to 2, therefore $2 \in F^*$, and so we have two cases: $q(x) \neq B(x,y)$ or $q(x) = B(x,y)$.

- In Case 1, $q(x) \neq B(x,y)$:

$$\begin{aligned} \tau_{x-y}(x) &= x - \frac{2.B(x, x-y)}{q(x-y)}(x-y) \\ &= x - 2\frac{B(x,x) - B(x,y)}{2(q(x) - B(x,y))}(x-y) \\ &= x - (x-y) \\ &= y. \end{aligned}$$

  This gives our autometry, $\tau_{x-y} \in O(V)$, which well defined in Case 1.

- In Case 2: $q(x) = B(x,y) \Longrightarrow q(x) \neq -B(x,y) = B(-x,y) = B(x,y) - 2B(x,y)$ because F has characteristic not equal to 2 and $q(x) = B(x,y) \neq 0$. We have:

$$\begin{aligned} \tau_{-x-y}(x) &= x - \frac{2.B(x, -x-y)}{q(-x-y)}(-x-y) \\ &= x - 2\frac{-B(x,x) - B(x,y)}{2(q(x) + B(x,y))}(-x-y) \\ &= x - x - y \\ &= -y. \end{aligned}$$

  Therefore, $-\tau_{-x-y}(x) = y$ and $-\tau_{-x-y}$ gives our required autometry.

□

2.3 Witt's Cancellation Theorem

Theorem 2.6 *(Witt's Cancellation Theorem:) Let $(V, q, B), (V_1, q_1, B_1), (V_2, q_2, B_2)$ be quadratic spaces. Then:*

$$V \perp V_1 \simeq V \perp V_2 \Longrightarrow V_1 \simeq V_2.$$

Proof: For the first two steps of this proof we follow [11, p.18].
Step 1: V is totally isotropic, V_1 is regular. It is clear that V_1 and V_2 must have the same dimension, as two isometric spaces must have the same dimension by isomorphism of vector spaces. We also have that $B \equiv 0$ and its associated matrix M is the matrix of zeroes. Let M_1, M_2 be the associated matrices for B_1, B_2 respectively. Therefore the associated matrices of $B \perp B_1$ and $B \perp B_2$ are respectively $\begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix}$. By our assumption and Theorem 1.9, there exists $A = \begin{pmatrix} B & C \\ D & E \end{pmatrix} \in GL_n(F)$ such that:

$$\begin{pmatrix} 0 & 0 \\ 0 & M_1 \end{pmatrix} = A^t \begin{pmatrix} 0 & 0 \\ 0 & M_2 \end{pmatrix} A = \begin{pmatrix} D^t M_2 D & D^t M_2 E \\ E^t M_2 D & E^t M_2 E \end{pmatrix}.$$

In particular this gives $M_1 = E^t M_2 E$, and by multiplicativity of the determinant, since M_1 is non-singular by regularity of V_1, we have that E is non-singular. Therefore M_1 and M_2 are congruent, B_1 and B_2 are equivalent, and V_1 and V_2 are isometric.

Step 2: V is totally isotropic. By Corollary 1.15, we can write V_1 and V_2 respectively as $V_1' \perp r\langle 0 \rangle$ and $V_2' \perp s\langle 0 \rangle$, where V_1', V_2' are diagonal and regular. Suppose without loss of generality that $s \geq r$. Our assumption becomes:

$$V \perp r\langle 0 \rangle \perp V_1' \simeq V \perp r\langle 0 \rangle \perp (s-r)\langle 0 \rangle \perp V_2'.$$

We have that $V \perp r\langle 0 \rangle$ is totally isotropic, and by regularity of V_1' and Step 1, we can conclude that $V_1' \simeq V_2' \perp (s-r)\langle 0 \rangle$, and therefore $V_1 = V_1' \perp r\langle 0 \rangle \simeq V_2' \perp (s-r)\langle 0 \rangle \perp r\langle 0 \rangle = V_2$, as required.

Step 3: General case, in which we follow and slightly modify [5, p.21]. Let $V \simeq \langle d_1, ..., d_n \rangle = \langle d_1 \rangle \perp ... \perp \langle d_n \rangle$. Our assumption is therefore:

$$\langle d_1 \rangle \perp ... \perp \langle d_n \rangle \perp V_1 \simeq \langle d_1 \rangle \perp ... \perp \langle d_n \rangle \perp V_2.$$

If we can show that for all $d \in F$, $\langle d \rangle \perp V_1 \simeq \langle d \rangle \perp V_2 \implies V_1 \simeq V_2$, Step 3 will follow immediately by induction. Let $d \in F$. If $d = 0$, then $\langle d \rangle$ is totally isotropic and this was done in Step 2. Suppose that $d \neq 0$, and that $\langle d \rangle \perp V_1 \simeq \langle d \rangle \perp V_2$. Pick an orthogonal basis for $\langle d \rangle \perp V_1$, with v_1 the basis vector corresponding to $\langle d \rangle$, and similarly for $\langle d \rangle \perp V_2$ with a vector v_2. Let $\phi : \langle d \rangle \perp V_1 \to \langle d \rangle \perp V_2$ denote the isometry of our assumption.
By definition of an isometry, and if q_i' is the quadratic form of the quadratic space $\langle d \rangle \perp V_i$, we have: $q_2'(\phi(v_1)) = q_1'(v_1) = d$. We also have $q_2'(v_2) = d$, so we obtain: $q_2'(\phi(v_1)) = q_2'(v_2) = d$. By Proposition 2.5, there exists $\tau \in O(\langle d \rangle \perp V_2)$ such that: $\tau(\phi(v_1)) = v_2$. We now show easily that $(\tau \circ \phi)(V_1) = V_2$. We know that $V_i = \langle v_i \rangle^{\perp}$, by the definition of an orthogonal sum, for each $i = 1, 2$. Therefore, if $x \in V_1$, $0 = B_1'(v_1, x) = B_2'(\tau(\phi(v_1)), \tau(\phi(x))) = B_2'(v_2, \tau(\phi(x))) = 0$ so $(\tau \circ \phi)(x) \in V_2 = \langle v_2 \rangle^{\perp}$. We show the other direction in exactly the same way. In conclusion, $V_1 \simeq V_2$ via the isometry $\tau \circ \phi$.

□

2.4 Witt's Decomposition Theorem

Let (U, B) be a quadratic space. We denote by $m.U$ the orthogonal sum of m copies of U, that is: $m.U = U\perp ... \perp U$. Witt's Decomposition Theorem, found in [11, p.15], provides a way to characterise the equivalence classes of the Witt Ring in terms of anisotropic quadratic forms.

Theorem 2.7 *(Witt's Decomposition Theorem:) Any quadratic space (V, q) splits into an orthogonal sum, $(V_t, q_t)\perp(V_h, q_h)\perp(V_a, q_a)$, where V_t is totally isotropic, V_h is hyperbolic space (or zero), and V_a is anisotropic. This is called the "Witt Decomposition" of V. Furthermore, V_t, V_h, V_a are all unique up to isometry.*

Proof: Existence: Let (V, B, q) be a quadratic space. Let $V_t = \mathrm{rad}(V)$, a subspace of V which is clearly totally isotropic. By completing a basis of V_t to a basis of V, there exists a subspace $V_0 \subset V$ such that $V_0 \oplus V_t = V$, as usual as quadratic spaces with the restricted quadratic form. Since $B(V_t, V_0) = B(\mathrm{rad}(V), V_0) = 0$, we have $V_t \perp V_0 = V$. If V_0 is anisotropic, then we are done. If V_0 is isotropic, then by Theorem 2.3, there exists $V_1 \subset V$ such that: $V_0 \simeq \mathbb{H}\perp V_1$. If V_1 is anisotropic then we are done, with $V \simeq V_t\perp\mathbb{H}\perp V_1$. If V_1 is isotropic, then there exists V_2 such that $V_1 \simeq \mathbb{H}\perp V_2$, and so on and so forth. For dimension reasons, this process must terminate at some integer $a \geq 0$, so that:

$$V \simeq V_t\perp(\mathbb{H}\perp ... \perp\mathbb{H})\perp V_a.$$

Uniqueness: Suppose that we have: $V = V_t\perp V_h\perp V_a = V_t'\perp V_h'\perp V_a'$, two Witt decompositions of V. Firstly, we have that: $\mathrm{rad}(V) = \mathrm{rad}(V_t\perp V_h\perp V_a) = \mathrm{rad}(V_t)\perp\mathrm{rad}(V_h\perp V_a)$. (It is easily shown that $\mathrm{rad}(V_1\perp V_2) = \mathrm{rad}(V_1)\perp\mathrm{rad}(V_2)$.) Since $V_h\perp V_a$ is regular, $\mathrm{rad}(V_h\perp V_a) = 0$ and $\mathrm{rad}(V) = \mathrm{rad}(V_t) = \mathrm{rad}(V_t') = V_t = V_t'$, because V_t and V_t' are totally isotropic, so $B \equiv 0$ on V_t and V_t'. By Witt's Cancellation theorem, this gives us:

$$V_h\perp V_a \simeq V_h'\perp V_a'.$$

Let $m, m' \in \mathbb{Z}_{\geq 0}$ be such that $V_h \simeq m.\mathbb{H}, V_h' \simeq m'.\mathbb{H}$. Suppose without loss of generality that $m \geq m'$. Then by Witt's Cancellation theorem, we have $(m - m').\mathbb{H}\perp V_a \simeq V_a'$. V_a' is anisotropic, and if $m > m'$, $(m - m').\mathbb{H}\perp V_a$ would be isotropic by Theorem 2.3. Therefore $m = m'$, so $V_h \simeq V_h'$ and by Witt's Cancellation theorem $V_a \simeq V_a'$.

□

2.5 Witt's Chain Equivalence Theorem

We include Witt's Chain Equivalence theorem because it is quite remarkable, and importantly will allow us to show that the signature homomorphism of Chapter 4 is well-defined. The definitions, the statement of the main theorem, and its proof can all be found in [11, p.21]. However, the formulation of Lemma 2.10 is more relevant in [5, p.12], so that is the source we have used.

Definition 2.8 *Let $f = \langle a_1, ..., a_n\rangle, g = \langle b_1, ..., b_n\rangle$. We say that f and g are simply-equivalent if there exists $i, j \in [\![1, n]\!]$ such that:*

$$\begin{cases} \langle a_i, a_j\rangle \simeq \langle b_i, b_j\rangle \text{ for } i \neq j \quad \text{or} \quad \langle a_i\rangle \simeq \langle b_i\rangle \text{ for } i = j \\ a_k = b_k \text{ for all } k \neq i, j. \end{cases}$$

Definition 2.9 *Let f, g be (diagonal) quadratic forms, of dimension $n \in \mathbb{N}$. We say that f and g are chain-equivalent if there exists a sequence of diagonal quadratic forms $f_0, ..., f_m$ such that*

$$\begin{cases} f_i, f_{i+1} \text{ are simply equivalent for all } i \in [\![0, m-1]\!] \\ f_0 = f \\ f_m = g. \end{cases}$$

This is denoted by $f \approx g$.

Lemma 2.10 *Let q, q' be non-singular binary quadratic forms. Then, if q represents $e \in F^*$, $q \simeq \langle e, ed(q)\rangle$. Moreover:*

$$q \simeq q' \iff d(q) = d(q') \text{ and } q, q' \text{ represent a common element } e \in F^*.$$

Proof: By the Representation Criterion, we have $q \simeq \langle e, f\rangle$ for some $f \in F^*$, because q is non-singular. Then $d(q) = ef.(F^*)^2$, so that $ed(q) = e^2f.(F^*)^2 = f.(F^*)^2$, and therefore $\langle ed(q)\rangle \simeq \langle f\rangle$, as required. For the 'only if' direction, we know that the determinant of a quadratic form is invariant under isometry, by Proposition 1.17. It is clear from the definition of isometric quadratic forms that $D(q) = D(q')$. The reverse implication is immediate from the first half of this lemma. □

Theorem 2.11 *(Witt's Chain-Equivalence Theorem:) Let f, g be quadratic forms of the same dimension. Then:*

$$f \simeq g \iff f \approx g.$$

We direct the reader to [11, §1, p.21] for a proof of Witt's Chain-Equivalence Theorem, which uses Lemma 2.10. The proof is quite long, not particularly enlightening for the rest of this project, and is written out in sufficient detail in [11].

3 The Witt Ring

From Chapter 3 onwards, we concern ourselves with non-singular quadratic forms. Since every quadratic form is diagonalizable, non-singularity simply means that there are no zeros in the diagonalization. As a result, the dimension of the underlying quadratic space is given by the number of terms in the diagonalization. This allows to talk about quadratic spaces by directly refering to quadratic forms, because when we work with isometry classes of quadratic forms, the dimension is the only important feature of the underlying vector space. As a result, we will refer mostly to non-singular quadratic forms q, or their isometry classes, rather than explicitly talking about the pair (V, q).

3.1 The Grothendieck-Witt Ring

Definition 3.1 *A semi-ring (resp. abelian semi-group) is a ring (resp. an abelian group) without the requirement of additive inverses. We call a semi-ring S (resp. abelian semi-group) a cancellation semi-ring (resp. an abelian cancellation semi-group) if it satisfies:*

$$\forall x, y, z \in S, x + y = x + z \Longrightarrow y = z.$$

Let F be a field, with characteristic not equal to 2. Let $M(F)$ denote the set of all isometry classes of non-singular quadratic forms over the field F. We saw in Chapter 1 that $M(F)$ was a semi-ring, with the additive law $'\perp'$ and multiplicative law $'\otimes'$. We saw in Chapter 2, thanks to Witt's Cancellation Theorem, that $M(F)$ is a cancellation semi-ring. The following lemma from [4, p.23] will help us define the Grothendieck group of a cancellation semi-group and provide a 'universal property' for semi-group homomorphisms to extend to group homomorphisms of the Grothendieck group. We elaborate on the 'sketch' proof which is provided by Cassels in [4].

Lemma 3.2 *Let S be an abelian semi-group with cancellation. Then there is an abelian group G and a semi-group homomorphism $\alpha : S \to G$ with the following property:*
Let H be any abelian group and $\beta : S \to H$ a semigroup homomorphism. Then there exists a unique group homomorphism $\rho : G \to H$ such that the following diagram commutes:

$$\begin{tikzcd} S \arrow[r, hook, "\alpha"] \arrow[dr, "\beta"'] & G \arrow[d, "\rho"] \\ & H \end{tikzcd}$$

Moreover, the group G is uniquely determined up to isomorphism by this property, and $\alpha : S \hookrightarrow G$ is an injection.

Proof: We need to show existence, that the property holds, and then uniqueness. The existence part of the proof will provide a construction and definition of the Grothendieck group of S.

Existence: $S\times S$ is a semi-group with the additive law: $(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2)$. From the fact that S is a semi-group with cancellation, we see immediately that $S\times S$ also has cancellation, because, for $(x_1,y_1),(x_2,y_2)\in S\times S$:

$$\begin{aligned}(x,y)+(x_1,y_1)=(x,y)+(x_2,y_2) &\Longleftrightarrow (x+x_1,y+y_1)=(x+x_2,y+y_2)\\ &\Longrightarrow x_1=x_2 \text{ and } y_1=y_2 \Longleftrightarrow (x_1,y_1)=(x_2,y_2).\end{aligned}$$

Now consider the relation: $(x_1,y_1)\sim(x_2,y_2)\Longleftrightarrow x_1+y_2=x_2+y_1$. It is clearly reflexive and symmetric and can easily be shown to be transitive using cancellation in S. Therefore $\sim$ is an equivalence relation on $S\times S$. It respects addition in $S\times S$, because if:

$$\begin{cases}(x_1,y_1)\sim(x_2,y_2)\\ (x_1',y_1')\sim(x_2',y_2')\end{cases}$$

then: $x_1+x_1'+y_2+y_2'=x_2+x_2'+y_1+y_1'$ by adding the two corresponding equations, which corresponds to $(x_1+x_1',y_1+y_1')\sim(x_2+x_2',y_2+y_2')$, as required. Hence, $G=S\times S/\sim$ (the equivalence classes of $S\times S$) form a well-defined semi-group. The identity is the equivalence class $\{(s,s),s\in S\}$ as $(x,y)+(s,s)=(s,s)+(x,y)=(x+s,y+s)\equiv(x,y)$ in G, by cancellation of s in S. Furthermore, let $(x,y)\in G$. Then: $(y,x)+(x,y)=(y+x,x+y)=(x+y,x+y)=0_G$. So G is in fact an abelian group, where $-(x,y)=(y,x)$. Define the homomorphism:

$$\alpha:\left|\begin{array}{ccc} S & \longrightarrow & G\\ x & \longmapsto & (x,0)\end{array}\right..$$

It is clear from the above that α is an injection.

The property holds: Let $\beta:S\to H$ be any semi-group homomorphism, for an abelian group H. Consider the image of S in G via α. We have that, for $(x,y)\in G$, $(x,y)=(x,0)+(0,y)=(x,0)-(y,0)$ in G. Therefore, it is easy to check that β extends to G via the homomorphism:

$$\rho:\left|\begin{array}{ccc} G & \longrightarrow & H\\ (x,y) & \longmapsto & \beta(x)-\beta(y)\end{array}\right..$$

We now show uniqueness of this extension. Let $(x,y)\in G$, let $\rho':G\to H$ be such that the diagram commutes. Then, as required, we obtain:

$$\rho(x,y)-\rho'(x,y)=\rho(\alpha(x))-\rho(\alpha(y))-\rho'(\alpha(x))+\rho'(\alpha(y))=\beta(x)-\beta(y)-\beta(x)+\beta(y)=0.$$

Uniqueness of G: Suppose we have $\alpha_i:S\to G_i$ for $i=1,2$, satisfying the property. For $i=1$, take $H=G_2$. Then let $\rho_1:G_1\to G_2$ be the unique homomorphism such that:

$$\begin{tikzcd} S \arrow[r, hook, "\alpha_1"] \arrow[dr, "\alpha_2"'] & G_1 \arrow[d, "\rho_1"] \\ & G_2 \end{tikzcd}$$

commutes. For $i = 2$, take $H = G_1$. Then let $\rho_2 : G_2 \to G_1$ be the unique homomorphism such that:

$$\begin{tikzcd} S \arrow[r, hook, "\alpha_2"] \arrow[dr, "\alpha_1"'] & G_2 \arrow[d, "\rho_2"] \\ & G_1 \end{tikzcd}$$

commutes. By the uniqueness condition in the property and taking $H = G_i$, we know that id_{G_i} is the only homomorphism $h : G_i \to G_i$ which satisfies $h \circ \alpha = \alpha$. Therefore, from the fact that $\alpha_1 = \rho_2 \circ \alpha_2$, and $\alpha_2 = \rho_1 \circ \alpha_1$, we obtain:

$$\begin{cases} \alpha_1 = \rho_2 \circ \rho_1 \circ \alpha_1 \\ \alpha_2 = \rho_1 \circ \rho_2 \circ \alpha_2 \end{cases}$$

By the above, this shows that ρ_1, ρ_2 are inverses of each other, showing that $G_1 \cong G_2$.

□

Definition 3.3 *Let S be a semi-group with cancellation. The Grothendieck group of S is the group $Grot(S) = G = S \times S/\sim$, as defined in the above lemma. In the case of quadratic forms, the Grothendieck group of the semi-group of the isometry classes of the non-singular quadratic forms over a field F is defined and denoted by $\hat{W}(F) = Grot(M(F)) = M(F) \times M(F)/\sim$.*

Remark We saw from the proof of the lemma that we can write any $(q_1, q_2) \in \hat{W}(F)$ as:

$$(q_1, q_2) = (q_1, 0) - (q_2, 0) = \alpha(q_1) - \alpha(q_2).$$

We can therefore drop the notation using pairs of quadratic forms, in favour of a difference of quadratic forms, thanks to the image of $M(F)$ in $\hat{W}(F)$ via the injection α and identifying $\alpha(q)$ with q. The group $\hat{W}(F)$ can in fact be considered as a ring, with the following multiplication law:

$$(q_1, q_2).(s_1, s_2) = (q_1 \otimes s_1 \perp q_2 \otimes s_2, q_2 \otimes s_1 \perp q_1 \otimes s_2).$$

We see immediately that this coincides with the way traditional multiplication would act on differences of quadratic forms, and so our above notation which uses differences is coherent and can be used to consider $\hat{W}(F)$ as a ring, which we call the Grothendieck-Witt ring of F. Under this notation, we will sometimes write '+' instead of '$\perp$' when it is clear that we are working in the ring $\hat{W}(F)$ or $W(F)$.

3.2 The Witt Ring

To define the Witt ring of a field F from the ring $\hat{W}(F)$ defined above, we first need to consider $\mathbb{Z}.\mathbb{H} = \{n.\mathbb{H} \mid n \in \mathbb{Z}\} \subset \hat{W}(F)$, the set consisting of quadratic spaces and their inverses in $\hat{W}(F)$. The following lemma can be found in [11, p.24] and will allow us to define the Witt ring.

Lemma 3.4 *Let q be a non-singular quadratic form, over the field F. Then: $q \otimes \mathbb{H} = \dim(q).\mathbb{H}$.*

Proof: Let $q = \langle d_1, ..., d_n \rangle$ be a diagonalization of q. Since q is non-singular, $d_i \in F^*$ for $i \in [\![1, ..., n]\!]$. If we can show that $\langle a \rangle \otimes \mathbb{H} \simeq \mathbb{H}$ for $a \in F^*$, then the lemma will follow easily by induction, by distributivity. $\mathbb{H} \simeq \langle 1, -1 \rangle$, by Theorem 2.2, and $\langle a \rangle \otimes \mathbb{H} \simeq \langle a \rangle \otimes \langle 1, -1 \rangle \simeq \langle a, -a \rangle$ by Proposition 1.22. $\langle a, -a \rangle$ has determinant -1 and is regular as $a \in F^*$, so by Theorem 2.2, $\langle a, -a \rangle \simeq \mathbb{H}$. $\square$

Corollary 3.5 *$\mathbb{Z}.\mathbb{H}$ is an ideal of $\hat{W}(F)$.* $\square$

Definition 3.6 *The quotient ring $W(F) = \hat{W}(F)/\mathbb{Z}.\mathbb{H}$ is called the Witt ring of the field F.*

The following proposition, taken from [11, §2, p.36], will be very useful when it comes to performing calculations in the Witt ring $W(F)$, as it allows us to work more straightforwardly with anisotropic representatives of the elements of $W(F)$.

Proposition 3.7 *The elements $W(F)$ are in one-to-one correspondence with the isometry classes of all anisotropic forms.*

Proof: Consider an element $q_1 - q_2 + \mathbb{Z}.\mathbb{H} \in W(F)$. Let $q_1 = \langle a_1, ..., a_n \rangle$ and $q_2 = \langle b_1, ..., b_n \rangle$. We know that the quadratic space/form $\mathbb{H} \simeq \langle a, -a \rangle$ for any $a \in F^*$, and it represents the 0-element in $W(F) = \hat{W}(F)/\mathbb{Z}.\mathbb{H}$. Therefore for any $a \in F^*$, $\langle a \rangle + \langle -a \rangle = 0 \Longrightarrow -\langle a \rangle = \langle -a \rangle$. So:

$$q_1 - q_2 + \mathbb{Z}.\mathbb{H} = \langle a_1, ..., a_n \rangle - \langle b_1, ..., b_n \rangle + \mathbb{Z}.\mathbb{H} = \langle a_1, ..., a_n \rangle + \langle -b_1, ..., -b_n \rangle + \mathbb{Z}.\mathbb{H}.$$

We conclude from the above that every element of $W(F)$ can be represented by a quadratic form q. Every quadratic form q, by Witt's Decomposition Theorem, can be written as $q \simeq q_a \perp q_h \perp q_t$ where q_a is anisotropic, q_h is hyperbolic, q_t is totally isotropic. Consider an element of $W(F)$, represented by an element q. We know that q is non-singular by definition of $W(F) = \mathrm{Grot}(M(F))/\mathbb{Z}.\mathbb{H}$. So $q_t = 0$, and $q = q_a \perp q_h$. However, $q_h \in \mathbb{Z}.\mathbb{H}$ and therefore $q = q_a$ in $W(F)$: every element of $W(F)$ is represented by an anisotropic form. For one-to-one correspondence, if two anisotropic forms represent the same element in $W(F)$, they are equivalent, because they cannot differ by a hyperbolic plane - we could find an isotropic vector in one of them otherwise by Theorem 2.3. $\square$

3.3 The Fundamental Ideal of $W(F)$

Consider the function

$$\dim : \left| \begin{array}{ccc} M(F) & \longrightarrow & \mathbb{Z} \\ q & \longmapsto & \dim(q) \end{array} \right. .$$

$M(F)$ is an abelian semi-group and $\mathbb{Z}$ is an abelian group. We have seen that $\dim(q_1 \perp q_2) = \dim(q_1) + \dim(q_2)$, ie: dim is a semi-group homomorphism into the abelian group $\mathbb{Z}$. Therefore, by the universal property of the Grothendieck group, dim extends to a group homomorphism on the Grothendieck group $\dim : \hat{W}(F) \to \mathbb{Z}$, giving $\dim(q_1 - q_2) = \dim(q_1) - \dim(q_2)$. In fact, we can check easily that $\dim : \hat{W}(F) \to \mathbb{Z}$ is a ring homomorphism, as it respects the multiplicative law '$\otimes$' of $\hat{W}(F)$.

Definition 3.8 *Consider the ring homomorphism* $\dim : \hat{W}(F) \to \mathbb{Z}$. *The ideal* $\hat{I}(F) = \ker(\dim)$ *is called the* *fundamental ideal of the Grothendieck-Witt ring* $\hat{W}(F)$. *Let* $I(F)$ *denote the image of* $\hat{I}(F)$ *under the canonical surjection* $\hat{W}(F) \to \hat{W}(F)/\mathbb{Z}.\mathbb{H} = W(F)$. *Then* $I(F)$ *is called the* *fundamental ideal of the Witt ring* $W(F)$, *and* $\hat{I}(F) \cong I(F)$ *because* $\hat{I}(F) \cap \mathbb{Z}.\mathbb{H} = \{0\}$.

The following two propositions, which can be found in [11, p.34-36], are standard, well-known results about these fundamental ideals. Proposition 3.9 will prove to be somewhat analogous to Theorem 5.13 which will appear later in Chapter 5. It is therefore interesting to include now, particularly as it helps prove the maximality of the fundamental ideal $I(F) \subset W(F)$ via Corollary 3.11, a small fact which we will use in proving Lorenz and Leicht's Theorem 5.18 in Chapter 5.

Proposition 3.9 $\hat{I}(F)$ *is additively generated by quadratic forms of the form* $\langle a \rangle - \langle 1 \rangle$, *for* $a \in F^*$.

Proof: Let $s \in \hat{I}(F) \subset \hat{W}(F)$. Then, we know that the elements of $\hat{W}(F)$ are of the form $q_1 - q_2$. There exists $q_1, q_2 \in M(F)$ such that $s = q_1 - q_2$, and since $s \in \hat{I}(F)$, $\dim(s) = \dim(q_1 - q_2) = \dim(q_1) - \dim(q_2) = 0$. So we have diagonalisations (of same dimension) of q_1 and q_2: $q_1 = \langle a_1, ..., a_n \rangle$ and $q_2 = \langle b_1, ..., b_n \rangle$, where $a_i, b_i \in F^*$ for each $i = 1, ..., n$.. Since $\hat{W}(F)$ is an abelian group:

$$s = \sum_{i=1}^{n}(\langle a_i \rangle) - \sum_{i=1}^{n}(\langle b_i \rangle) = \sum_{i=1}^{n}(\langle a_i \rangle) - \sum_{i=1}^{n}(\langle b_i \rangle) + n.\langle 1 \rangle - n.\langle 1 \rangle = \sum_{i=1}^{n}(\langle a_i \rangle - \langle 1 \rangle) - \sum_{i=1}^{n}(\langle b_i \rangle - \langle 1 \rangle).$$

□

Proposition 3.10 *Consider* $I(F) \subset W(F)$. *Let* $q \in M(F)$. *Then:*

$$q \textit{ is a representative of an element in } I(F) \iff \dim(q) \textit{ is even.}$$

Proof: $(\Longrightarrow)$: We have that $q + (\mathbb{Z}.\mathbb{H}) \in I(F)$, so by our isomorphism $\hat{I}(F) \cong I(F)$, $q \in \hat{I}(F)$. Therefore writing $q = q_1 - q_2$ in $\hat{W}(F)$, we must have $\dim(q_1) - \dim(q_2) = 0$. Picking a representative of $q + \mathbb{Z}.\mathbb{H}$, say $q + n.\mathbb{H}$ for some $n \in \mathbb{Z}$, we get that $\dim(q + .\mathbb{H}) = 2n$.
$(\Longleftarrow)$: Let $q \in M(F)$ be an even-dimensional non-singular quadratic form. Let $n \in \mathbb{Z}$ such that $\dim(q) = 2n$. Consider $q + \mathbb{Z}.\mathbb{H} \in W(F)$. Then: $\dim(q - (n-1)\mathbb{H}) = 2n - 2(n-1) = 2$, and $q' = q - (n-1)\mathbb{H}$ is a representative of $q + \mathbb{Z}.\mathbb{H}$. We can therefore assume that q has dimension equal to 2, ie: $q = \langle a, b \rangle$, for some $a, b \in F^*$. In $\hat{W}(F)$, we can write $q = \langle a \rangle - \langle -b \rangle$, giving $q \in \hat{I}(F)$. The image of $q \in \hat{I}(F)$ under the canonical projection $\hat{W}(F) \to W(F)$ - and therefore the coset it represents - is in $I(F)$, by definition of $I(F)$.

□

Corollary 3.11 *We have the following isomorphism:*

$$W(F)/I(F) \cong \mathbb{Z}/2\mathbb{Z}.$$

The proof follows immediately from the fact that $\dim : W(F) \to \mathbb{Z}/2\mathbb{Z}$ is a surjective homomorphism, is well-defined because each equivalence class of $W(F)$ has a representative of dimension 0 or 1, the homomorphism has $I(F)$ as its kernel by Proposition 3.10.

Remark This shows that $I(F)$ is a maximal ideal of $W(F)$, as $\mathbb{Z}/2\mathbb{Z}$ is the finite field containing 2 elements.

Example Suppose that F is quadratically closed, $F = \mathbb{C}$ for example. Then for every $a \in F^*$, there exists $b \in F^*$ such that $a = b^2$, and $\langle a \rangle \simeq \langle b^2 \rangle \simeq \langle 1 \rangle$. Therefore, any n-dimensional non-singular quadratic form over F is isometric to $n.\langle 1 \rangle$, and any element $n.\langle 1 \rangle - m.\langle 1 \rangle$ of $\hat{W}(F)$ is in the kernel of $\dim : \hat{W}(F) \to \mathbb{Z}$ if and only if $n = m$. However, $n.\langle 1 \rangle - n.\langle 1 \rangle = (n\langle 1 \rangle, n\langle 1 \rangle) = 0$ in $\hat{W}(F)$, and therefore $\hat{I}(F) = 0$. From $I(F) \cong \hat{I}(F) = 0$ and Corollary 3.11, we conclude that $W(F) \cong \mathbb{Z}/2\mathbb{Z}$.

4 Ordered Fields

An important characterization of Pfister's Local Global Principle will rely on the 'signature homomorphism' on quadratic forms in the Witt ring of a field of characteristic not equal to 2. This characterization, along with an understanding of the Harrison topology on the set of orders on fields, will be key to elaborating on Scheiderer's paper [18] on 'the u-invariant of one-dimensional function fields over real power series fields'.

4.1 Orders and Quadratic Preorderings

Definition 4.1 *Let F be a field. Let $\leq$ be an order relation on the set F. We say that F is an ordered field, and that $\leq$ is a field order on F if:*

1. *$\leq$ is a total order on F.*

2. *$\forall a, b, c \in F, a \leq b \Longrightarrow a + c \leq b + c$.*

3. *$\forall a, b, c \in F, a \leq b$ and $0 \leq c \Longrightarrow ac \leq bc$.*

Definition 4.2 *Let F be a field. Let $P \subset F$ be a subset of F. We say that P is an order on F if:*

A. *$P \cup -P = F$*

B. *$P \cap -P = \{0\}$*

C. *$P + P \subset P$ and $PP \subset P$.*

We call the elements of P the positive elements of F with respect to this order.

Inspiration for the following lemma comes from [14, p.1,2], and explains why P is given the term 'order'! We will use orders $P \subset F$ in this project, until Chapter 6, where the notation '$\leq$' will become more relevant.

Lemma 4.3 *Let F be a field. There is a one-to-one correspondence between field orders $\leq$ and orders P on F. This correspondence is given by:*

$$\begin{array}{rcl} \leq & \longrightarrow & P = \{a \in F \mid 0 \leq a\} \\ [a \leq b \Longleftrightarrow b - a \in P] & \longleftarrow & P \end{array}$$

Proof: Let F be a field. Suppose that $\leq$ is a field order on F, so that it satisfies $(1), (2), (3)$. Then we want to show that $P = \{a \in F \mid 0 \leq a\}$ satisfies $(A), (B), (C)$. We have that $0 \leq -a \Longleftrightarrow a \leq 0$ by (2), so $-P = \{a \in F \mid a \leq 0\}$. We immediately have $(1) \implies (A)$. If $a \in P \cap -P$, then $a \leq 0$ and $0 \leq a$ and by antisymmetry of $\leq$, $a = 0$. This proves (B). Let $a, b \in P$. Then: $0 \leq a$ and $a \leq a + b$ by (2), so by transitivity $0 \leq a + b$, and $a + b \in P$. We also have $0 \leq b \implies 0.a = 0 \leq ab$, so $ab \in P$.

Conversely, let P be an order on F. Let $a, b, c \in F$. Suppose that $a \leq b$, ie: $b - a \in P$. Then: $b + c - (a + c) = b - a \in P$, proving (2). Suppose now that $0 \leq c$, ie: $c - 0 = c \in P$. Then $(b - a)c = bc - ac \in P$, showing (3). We have $b - a \in F$, and (A) gives $b - a \in P$ or $a - b \in P$, ie: $a \leq b$ or $b \leq a$, proving (1). (B) easily gives antisymmetry and reflexivity since $0 \in P$. Transitivity is given by (C). Suppose that $b - a \in P$ and $c - b \in P$, then $c - b + b - a = c - a \in P$ by (C) as required.

To show these are inverse constructions of each other, consider:

$$\leq \longrightarrow P = \{a \in F \mid 0 \leq a\} \longrightarrow \tilde{\leq} = [a \tilde{\leq} b \iff b - a \in P].$$

Then $a \tilde{\leq} b \iff b - a \in$P $\iff 0 \leq b - a \iff a \leq b$, as required. Consider now:

$$P \longrightarrow \leq = [a \leq b \iff b - a \in P] \longrightarrow \tilde{P} = \{a \in F \mid 0 \leq a\}.$$

Then $a \in \tilde{P} \iff 0 \leq a \iff a - 0 = a \in P$, as required, so that $\tilde{P} = P$. $\square$

4.2 Formally Real Fields

Definition 4.4 *A subset T of a field F is called a quadratic preordering on F if:*

1. *$T + T \subset T$ and $TT \subset T$*
2. *$F^2 \subset T$.*

We say that $T \subset F$ is a proper quadratic preordering if, additionally : $-1 \notin T$.

Remark From this definition, it is clear that $0, 1 \in T$. Also note that if $P \subset F$ is an order of F, then P is a proper quadratic preordering of F, because if $a \in F$, then $a \in P \implies a^2 \in P$, and $-a \in P \implies (-a)(-a) = a^2 \in P$.

Example An easy and important example of a quadratic preordering is the set of all sums of squares in F, ie:

$$\sum F^2 = \{\sum_{i=1}^{n} a_i^2 \mid n \in \mathbb{N}, a_i \in F\}.$$

In fact, for a field F, $\sum F^2$ is the unique minimal (with respect to inclusion) quadratic preordering of F. This is clear, because it is contained in any quadratic preordering T of F. For any $n \in \mathbb{N}$, for any $i \in [\![1, n]\!]$, for any $a_i \in F$, we have: $a_i^2 \in T$ by (2), $\sum_{i=1}^{n} a_i^2 \in T$ by (1). So $\sum F^2 \subset T$, and by the above remark $\sum F^2 \subset P$ for any order P of F as well.

Definition 4.5 *Let F be a field. As above, we denote by $\sum F^2 = \{\sum_{i=1}^{n} a_i^2 \mid n \in \mathbb{N}, a_i \in F\}$ the set of all sums of squares in F. We call F a formally real field if $-1 \notin \sum F^2$.*

Proposition 4.6 *If F is an ordered field, then it is a formally real field.*

Proof: If $-1 \in \sum F^2$, then $-1 \in P$ for any order P of F by the example above. Since $1 \in P$ for any order P of F, this proves the contrapositive. $\square$

In what follows, we use notation which stays in line with [1], and look to elucidate a number of the important facts which are mentioned in passing in [1, p.2,3]. In particular, the method used to prove the Artin-Schreier theorem below, via Lemma 4.9, can be found in [14, §1].

Definition 4.7 *Let $\chi(F)$ denote the set of all orders of F. For any proper quadratic preordering T of F, we denote as follows the set of all orders of F containing the quadratic preordering T: $\chi_T(F) = \{P \in \chi(F) \mid T \subset P\}$.*

Theorem 4.8 *(Artin-Schreier:) Let T be a **proper** quadratic preordering of F. Then there exists an order P of F containing T. Moreover, T is equal to the intersection of all orders of F which contain it. That is:*

$$T = \bigcap \chi_T(F) = \bigcap_{T \subset P, P \text{ order of } F} P.$$

We will need the two following lemmas in order to prove the above theorem. Lemma 4.9 can be found in [14, §1], and Zorn's Lemma is of course a well known set theory result.

Lemma 4.9 *Let $T \subset F$ be a proper quadratic preordering. Let $a \in F$ such that $a \notin -T$. Then:*

$T + aT$ is a proper quadratic preordering containing both a and T.

Proof: Let $S = T + aT$. It is clear that $SS \subset S, S + S \subset S$, and we have that $F^2 \subset T \subset S$, as $0 \in T$. We also have $1 \in T$, so $a \in S$. We just need to show that $-1 \notin S$. Suppose by contradiction that there exists $b, c \in T$ such that $-1 = c + ab$. We know that $-1 \notin T$, so $b \neq 0$, and $-a = \frac{1}{b}(1 + c) = \frac{1}{b^2}(1 + c)b \in T$, by Definition 4.4. Therefore, $a \in -T$, a contradiction. $\square$

Lemma 4.10 *(Zorn's lemma:) Let Σ be a partially ordered set, such that every chain in Σ has an upper bound in Σ. Then the set Σ contains at least one maximal element.*

Proof: *(Proof of Theorem 4.8.)*

We follow the proof outlined in [14]. Denote by Σ the set of proper quadratic preorderings of F which contain T, ordered by inclusion. We want to use Zorn's Lemma to show that there exists a maximal proper quadratic preordering containing T, say P, and then show that P is in fact an order of F. We then prove the second half of the theorem using Lemma 4.9. Consider an increasing chain $\{T_i\}_{i \in I}$ of proper quadratic preorderings. We want to show that $\bigcup_{i \in I} T_i$ is an upper bound in Σ for the chain, ie: that it is a proper quadratic preordering.

- Clearly $-1 \notin \bigcup_{i \in I} T_i$.

- Let $a, b \in \bigcup_{i\in I} T_i$. Then there exists, wlog, $i \leq j \in I$ such that $a \in T_i, b \in T_j$. Then:

$$a + b \in T_j \subset \bigcup_{i\in I} T_i, \qquad ab \in T_j \subset \bigcup_{i\in I} T_i.$$

- $\forall a \in F, \forall i \in I, a^2 \in T_i$, so $\forall a \in F, \bigcup_{i\in I} T_i$, as required.

By Zorn's Lemma, there exists a maximal proper quadratic preordering P containing T. We have that $-1 \notin P \implies P \cap -P = \{0\}$, because, showing the contrapositive, if $a \neq 0 \in P \cap -P$, then $a, -a \in P$, $-a^2 \in P$. By (2) of Definition 4.4, we have $a^{-2} \in P$, and therefore $-1 \in P$. We just need to show that $P \cup -P = F$. Let $a \in F$, such that $a \notin -P$. By Lemma 4.9, $P + aP$ is a proper quadratic preordering, strictly larger than P unless $a \in P$, so by maximality of P, $a \in P$. So $F = P \cup -P$ and in conclusion P is an order of F.

We now prove the second half of the theorem. Clearly $T \subset \bigcap_{T\subset P, P \text{ order of } F} P$. We want to show that $b \in \bigcap_{T\subset P, P \text{ order of } F} P \implies b \in T$. Let $b \in F$ and suppose that $b \notin T$. This shows that $b \neq 0$ as $0 \in T$. We need to show that there exists an order P of F, containing T, such that $b \notin P$. We know that $-b \in -T$. Let $S = T - bT$. This is a proper quadratic preordering of F by Lemma 4.9. By the first half of this theorem, there exists an order P of F containing S, and therefore containing $-b$. So $b \notin P$, by (B) of Definition 4.2 and the fact that $b \neq 0$, and this concludes our proof.

$\square$

Corollary 4.11 *(Artin-Schreier:) Let F be a field. Then:*

$$F \text{ is formally real} \iff F \text{ is an ordered field.}$$

Proof: The set of sums of squares $\sum F^2$ is a proper quadratic ordering of F because F is formally real, and therefore there exists an order of F by Theorem 4.8. Proposition 4.6 is the reverse implication. $\square$

The above corollary of the Artin-Schreier theorem provides a characterization of the fields we will work over in the context of Pfister's Local-Global Principle.

4.3 The Signature Homomorphism

Let F be a formally real field, of characteristic not equal to 2, so that F is an ordered field. Lam's conference notes [12, §1] provide a short reference and flavour for signatures with respect to field orders, and are useful insofar as they are discussed in the same context as our Chapter 5. However, we do not use them for anything other than definitions in this section.

Definition 4.12 *Let P be an order of F. We define as follows the sign map of the order P:*

$$sgn_P : \left| \begin{array}{ccc} F^* & \longrightarrow & \mathbb{Z} \\ a & \longmapsto & \begin{cases} -1 \text{ if } a \in -P \\ 1 \text{ if } a \in P \end{cases} \end{array} \right.$$

Definition 4.13 *Let P be an order of F. We define as follows the* <u>*signature at P*</u>*:*

$$sgn_P : \left| \begin{array}{rcl} M(F) & \longrightarrow & \mathbb{Z} \\ q = \langle d_1, ..., d_n \rangle & \longmapsto & \sum_{i=1}^n sgn_P(d_i). \end{array} \right.$$

Remark For the homomorphism to be well-defined on $M(F)$, we need to show that the signature of a quadratic form is invariant under isometry. This why we introduced chain-equivalence and Witt's Chain Equivalence theorem in Chapter 2. Let P be an order on F, and consider two isometric non-singular quadratic forms and their diagonalizations:

$$q_1 = \langle a_1, ..., a_n \rangle \simeq \langle b_1, ..., b_n \rangle = q_2.$$

By Witt's Chain Equivalence Theorem, these quadratic forms are chain-equivalent. It is enough to show that two simply-equivalent quadratic forms have the same signature, as the result will follow immediately by induction. Suppose, without loss of generality in the ordering, that $\langle a_1, a_2 \rangle \simeq \langle b_1, b_2 \rangle$ and $\forall i \in [\![3, n]\!], a_i = b_i$. We just need to check that: $\text{sgn}_P(a_1) + \text{sgn}_P(a_2) = \text{sgn}_P(b_1) + \text{sgn}_P(b_2)$. By Lemma 2.10, we know that $a_1 a_2.(F^*)^2 = b_1 b_2.(F^*)^2$ and that there exists $x_1, x_2, y_1, y_2 \in F, e \in F^*$, such that $a_1 x_1^2 + a_2 x_2^2 = b_1 y_1^2 + b_2 y_2^2 = e$. F is formally real, implying that $-1 \notin (F^*)^2$, and so $a_1 a_2$ and $b_1 b_2$ have the same sign. After this consideration, the only remaining case where $sgn(\langle a_1, a_2 \rangle) \neq \text{sgn}(\langle b_1, b_2 \rangle)$, without loss of generality, is: $a \in P, b \in P$ and $c \in -P, d \in -P$. Since $F^2 \subset P, P + P \subset P$, and $PP \subset P$, we obtain $e \in P \cap -P$, so $e = 0$, contradicting Lemma 2.10. Therefore, $\text{sgn}_P(q_1) = \text{sgn}(q_2)$, and we have shown that the signature of a non-singular quadratic form is invariant under isometry.

Remark Using the universal property of the Grothendieck group of a semi-group, the signature homomorphism extends naturally from $M(F)$ to $\hat{W}(F) : \text{sgn}_P(q_1 - q_2) = \text{sgn}_P(q_1) - \text{sgn}_P(q_2)$. In fact, sgn_P is actually a ring homomorphism. This follows by induction after noting that $\text{sgn}_P(ab) = \text{sgn}_P(a)\text{sgn}_P(b)$ for $a, b \in F^*$. Moreover, $\text{sgn}_P(n.\langle 1, -1 \rangle) = n.(1 - 1) = 0$ for all $n \in \mathbb{Z}$. From this, we can conclude that sgn_P descends to a well-defined ring homomorphism on the Witt ring of any ordered field: $\text{sgn}_P : W(F) \to \mathbb{Z}$.

Example Consider the field $F = \mathbb{R}$. We know that $\langle ab^2 \rangle \simeq \langle a \rangle$ for all $a \in F, b \in F^*$, and since every positive element of $\mathbb{R}$ is a square in $\mathbb{R}$, $\langle b \rangle \simeq \langle \pm 1 \rangle$ for all $b \in \mathbb{R}^*$. We easily obtain the following result, called Sylvester's Law - as stated in [11, §2, p.42] - because the dimension $n = n_+ + n_-$ determines the number of terms in the orthognal sum of a diagonalization $n_+.\langle 1 \rangle \perp n_-.\langle -1 \rangle$, and the signature determines n_+ and n_- subsequently.

Proposition 4.14 *(<u>Sylvester's Law:</u>) Two non-singular quadratic forms over $\mathbb{R}$ are equivalent if and only if they have the same dimension and the same signature.*

An immediate corollary of the above discussion is that $\hat{W}(\mathbb{R})$ is generated by $\langle -1 \rangle$ and $\langle 1 \rangle$ as an free abelian group/free $\mathbb{Z}$-module, and since $-\langle 1 \rangle = \langle -1 \rangle$ in $W(F)$, we easily conclude that $W(\mathbb{R}) \cong \mathbb{Z}$ by sending $\langle 1 \rangle$ in $W(\mathbb{R})$ to 1 in $\mathbb{Z}$.

Definition 4.15 *Let T be a proper quadratic preordering. We define the following ring homomorphism:*

$$sgn_T : \left| \begin{array}{rcl} W(F) & \longrightarrow & \mathbb{Z}^{\chi_T(F)} \\ q & \longmapsto & (sgn_P(q))_{P \in \chi_T(F)} \end{array} \right.$$

5 Pfister's Local-Global Principle for Formally Real Fields

Let F be a formally real field, of characteristic not equal to 2. In this chapter, we follow very closely the third chapter of K.J. Becher's article 'Local-global principles over real fields' [1]. The aim is to prove Pfister's Local-Global Principle by completing and elaborating on Becher's approach, so that the proof becomes accessible to a less involved reader. Becher's paper employs the structure of Lewis polynomials on $W(F)$ and the machinery of Pfister forms to obtain a more direct proof of the principle, and is similar to [12, §1] insofar as it revolves around the use of T-hyperbolic forms. Other proofs, found in standard textbooks such as [11] or [17] for example, often rely on more extensive notions such as Pythageorean fields, field extensions, extensions of orderings, and Scharlau's transfer lemma.

5.1 Definitions and Lewis' Theorem

Definition 5.1 *Let T be a quadratic preordering of F. A quadratic form ν over F is <u>T-positive</u> if $D(\nu) \subset T$, ie: all elements represented by ν are elements of T. Let q be a quadratic form over F. We say that q is <u>T-isotropic</u> if there exists a (non-trivial) T-positive quadratic form ν over F such that $\nu \otimes q$ is an isotropic quadratic form. We say that q is <u>T-hyperbolic</u> if there exists a (non-trivial) T-positive quadratic form ν over F such that $\nu \otimes q$ is a hyperbolic quadratic form.*

The following theorem is stated in [1], and can also be found in [13]. We proceed by induction, as suggested by Becher, as opposed to following a commutative algebra argument which interested readers can find in [13].

Theorem 5.2 *(<u>Lewis' Theorem</u>:) We define as follows the <u>n-th Lewis Polynomial</u> in $\mathbb{Z}[X]$:*

$$P_n(X) = \prod_{i=0}^{n} (X - n + 2i).$$

Let $n \in \mathbb{N}$ and let q be a regular quadratic form of dimension n over F. Then:

$$P_n(q) = 0 \text{ in } W(F).$$

(Note that, here, n and $2i$ denote the elements of $W(F)$ with respective representatives $n\langle 1\rangle$ and $2i\langle 1\rangle$, as $W(F)$ is a ring with multiplicative identity $\langle 1\rangle$.)

Proof: First of all, it is easy to show via two inductions - or by simply matching the right terms in the product - that:

$$\begin{cases} P_n(X) = X(X^2 - 2^2)(X^2 - 4^2)...(X^2 - n^2) \text{ if } n \text{ is even.} \\ P_n(X) = (X^2 - 1^2)(X^2 - 3^2)...(X^2 - n^2) \text{ if } n \text{ is odd.} \end{cases}$$

These expressions can be found in [13]. This shows that $P_n(X)$ is an odd polynomial when n is even, and an even polynomial when n is odd. Secondly, note that for all $n \in \mathbb{N}$,

$$\begin{aligned} P_n(X) &= \prod_{i=0}^{n}(X - n + 2i) \\ &= \prod_{i=0}^{n}((X-1) - (n-1) + 2i) \\ &= (X - n + 2n)\prod_{i=0}^{n-1}((X-1) - (n-1) + 2i) \\ &= (X+n)P_{n-1}(X-1). \end{aligned}$$

Thirdly, let q be a regular quadratic form of dimension n. Note that, for all $a \in F^*$, in $W(F)$,

$$(\langle a \rangle \otimes q)^2 = (\langle a \rangle \otimes q) \otimes (\langle a \rangle \otimes q) = \langle a^2 \rangle \otimes q^2 = \langle 1 \rangle \otimes q^2 = q^2.$$

From our first point, the equality $P_n(q) = 0$ actually depends on q^2, and we therefore have that: $\forall a \in F^*, P_n(\langle a \rangle \otimes q) = 0 \iff P_n(q) = 0$. This means that for all $a \in F^*$, we can scale q by a, allowing us to assume without loss of generality that q represents 1. By the Representation Criterion, $q \simeq \langle 1 \rangle \perp \phi$ for ϕ an $n-1$-dimensional regular quadratic form. By induction on n, we have $P_{n-1}(\phi)$ and using our second point:

$$P_n(q) = (q + n.1).P_{n-1}(q-1) = (q+n.1).P_{n-1}(1+\phi-1) = (q+n.1).P_{n-1}(\phi) = 0 \text{ in } W(F).$$

The base case, $n = 1$ is trivial because $P_1(X) = X^2 - 1$ and all regular 1-dimensional quadratic forms are of the form $\langle a \rangle$ for some $a \in F^*$. Since $\langle a \rangle \otimes \langle a \rangle = \langle a^2 \rangle \simeq \langle 1 \rangle$, $P_1(\langle a \rangle) = 0$. □

As in [1], we denote by $I_T(F)$ the set of all T-hyperbolic quadratic forms over F. Unlike [1] however, we will not prove that $I_T(F)$ is a radical ideal of $W(F)$ straightaway, as this fact is not used until much later in the chapter, and is much easier to understand once we have proved Pfister's Theorem 5.13.

Proposition 5.3 *The set $I_T(F)$ is an ideal of $W(F)$.*

Proof: Let $\phi, \phi' \in I_T(F)$, let q be an anisotropic quadratic forms representing an element of $W(F)$. There exists ν, ν' T-positive quadratic forms over F such that $\nu \otimes \phi, \nu \otimes \phi'$ are hyperbolic. Note that $\nu \otimes \nu'$ is T-positive by the fact that $TT \subset T$. Then $(\nu \otimes \nu')(\phi - \phi')$ is a difference of hyperbolic spaces by Lemma 3.4, and $\nu \otimes q \otimes \phi$ is hyperbolic by the same lemma. So $I_T(F)$ is an ideal of $W(F)$. □

In order to prove that $I_T(F)$ is a radical ideal in $W(F)$, we will need the following commutative algebra lemma, which is easy to prove and used freely in [1, p.4].

Lemma 5.4 *Let R be a commutative ring, let $I \subset R$ be an ideal of R. Then:*

$$I \text{ is a radical ideal of } R \iff [\forall x \in R, x^2 \in I \implies x \in I].$$

Proof: The 'only if' direction is immediate from the definition of a radical ideal, that is, an ideal which is equal to its own radical. Suppose by contradiction that there exists $x \in R$ such that $x^n \in I$ but $x \notin I$. Take $n \in \mathbb{N}$ to be minimal such that $x^n \in I$. Then $n \geq 3$, as $n = 2$ gives $x \in I$ by our assumption. However, this means that there exists $k \in [\![1, n-1]\!]$ such that $x^{2k} \in I$, as $2(n-1) \geq n$ for $n \geq 3$. Our assumption gives $x^k \in I$, but this contradicts the minimality of n. □

5.2 Pfister Forms and the Multiplicative Property

Definition 5.5 *Let $n \in \mathbb{N}$, let $a_1, ..., a_n \in F^*$. We denote by $\langle\langle a_1, ..., a_n\rangle\rangle$ the 2^n-dimensional form*

$$\langle\langle a_1, ..., a_n\rangle\rangle = \bigotimes_{i=1}^{n} \langle 1, a_i\rangle = \langle 1, a_1\rangle \otimes ... \otimes \langle 1, a_n\rangle$$

and we call this an n-fold Pfister form.

It is clear from the above definition that an n-fold Pfister form is a 2^n-dimensional quadratic form which represents 1. This motivates the following notation.

Definition 5.6 *If q is a Pfister form, then there exists a quadratic form q' such that $q \simeq \langle 1\rangle \perp q'$. We call q' the pure subform of q, uniquely determined up to isometry by Witt's Cancellation Theorem, and we use the above notation for any such Pfister form.*

Remark If $a_i = -1$ in the above definition for some $i \in [\![1, n]\!]$, then $\langle\langle a_1, ..., a_n\rangle\rangle$ is hyperbolic. This is because $\langle 1, a_i\rangle \otimes \langle 1, a_j\rangle \simeq \mathbb{H} \otimes \langle 1, a_j\rangle \simeq \dim(\langle 1, a_j\rangle).\mathbb{H} \simeq 2.\mathbb{H}$, by Lemma 3.4, so $\langle\langle a_1, ..., a_n\rangle\rangle \simeq 2^{n-1}\mathbb{H}$, by induction.

We define first what it means, according to Scharlau [17, p.69], what it means for a quadratic form to be multiplicative. Our chosen definition of multiplicativity also corresponds to Becher's use of the notion, which we can deduce from his paper on 'Supreme Pfsiter Forms' [2]. Recall that for a quadratic space (V, q), $D(q) = \{d \in F^* \mid \exists v \in V, q(v) = d\}$. We define, for a quadratic form q, the following set $G(q) = \{a \in F^* \mid \langle a\rangle \otimes q \simeq q\}$.

Definition 5.7 *An anisotropic form q is called multiplicative if $D(q) = G(q)$. An isotropic form q is called multiplicative if it is hyperbolic.*

The following equivalence relation on Pfister forms, somewhat analogous to Witt's Chain Equivalence for diagonal quadratic forms in Chapter 2, will be a useful tool for proving that Pfister forms are multiplicative. To this end, we adopt the approach taken by Scharlau in [17, §4, p.142], which is well-suited to presenting the rest of [1, §3]. Very similar definitions and proofs can be found in [7], which serves as useful complimentary reading.

Definition 5.8 *Two n-fold Pfister forms $\langle\langle a_1, ..., a_n\rangle\rangle$ and $\langle\langle b_1, ..., b_n\rangle\rangle$ are simply-p-equivalent if there exists $i, j \in [\![1, n]\!]$ such that $\langle\langle a_i, a_j\rangle\rangle \simeq \langle\langle b_i, b_j\rangle\rangle$ and for all $k \neq i, j, a_k = b_k$. Two*

n-fold Pfister forms ϕ and ψ are <u>*chain-p-equivalent*</u> *if there exists $\phi_0, ..., \phi_m$, n-fold Pfister forms such that:*

$$\begin{cases} \phi_0 = \phi \\ \phi_m = \psi \\ \psi_i \text{ and } \psi_{i+1} \text{ are simply-p-equivalent for all } i \in [\![0, n-1]\!]. \end{cases}$$

In the latter case, we write $\phi \approx \psi$, and chain-p-equivalence is clearly an equivalence relation.

Remark Although this follows trivially from the definition of chain-p-equivalence, it is important to note for the following proofs that the chain-p-equivalence of two Pfister forms implies that they are isometric.

Theorem 5.9 *Let ϕ be an n-fold Pfister form. Then:*

$$b \in D(\phi') \iff \exists b_2, ..., b_n \in F^*, \langle\langle b, b_2, ..., b_n\rangle\rangle \simeq \phi.$$

To prove the theorem above, we first need to prove the following lemma. Both of these results can be found, along with their proofs, in [17, §4, p.143,144]. The multiplicativity of Pfister forms follows as a corollary of these results, which we prove following Scharlau's text [17] once more.

Lemma 5.10

- *If $c \in F^*$ is represented by $\langle 1, a\rangle$, then $\langle\langle a, b\rangle\rangle \simeq \langle\langle a, bc\rangle\rangle$.*
- *If $c \in F^*$ is represented by $\langle a, b\rangle$, then $\langle\langle a, b\rangle\rangle \simeq \langle\langle c, ab\rangle\rangle$.*

Proof:

- We have: $\langle\langle a, b\rangle\rangle = \langle 1, a, b, ab\rangle$ and $\langle\langle a, bc\rangle\rangle = \langle 1, a, bc, abc\rangle\rangle$. We know that c is represented by $\langle 1, a\rangle$, and therefore bc is represented by $\langle b, ab\rangle$, as well as by $\langle bc, abc\rangle$. Since $b.ab.(F^*)^2 = bc.abc.(F^*)^2$, Lemma 2.10 gives $\langle b, ab\rangle \simeq \langle bc, abc\rangle$, which shows - thanks to the first line of this proof - that $\langle\langle a, b\rangle\rangle \simeq \langle\langle a, bc\rangle\rangle$.
- Similarly: $\langle\langle c, ab\rangle\rangle = \langle 1, c, ab, abc\rangle$. We know that c is represented by both $\langle a, b\rangle$ and $\langle c, abc\rangle$, which both have the same determinant. So $\langle 1, c, ab, abc\rangle \simeq \langle 1, a, ab, b\rangle \simeq \langle\langle a, b\rangle\rangle$.

□

Proof: (*of Theorem 5.9*:) The 'if' statement of the theorem is trivial, since $\langle\langle b, b_2, ..., b_n\rangle\rangle = \langle 1, b\rangle \otimes \langle 1, b_2\rangle \otimes ... \otimes \langle 1, b_n\rangle$ and taking the term of the resulting orthogonal sum given by: $\langle b\rangle \otimes \langle 1\rangle \otimes ... \otimes \langle 1\rangle = \langle b\rangle$.
The 'only if' direction is proved by induction on n. If $n = 1$, let $q = \langle 1, a\rangle$, then $b \in D(q') = D(\langle a\rangle) \implies a.(F^*)^2 = b.(F^*)^2 \implies \langle a\rangle \simeq \langle b\rangle \implies q = \langle\langle b\rangle\rangle$. Let $n \in \mathbb{N}$. Let $q = \langle\langle a_1, ..., a_{n-1}\rangle\rangle$, let $a_n \in F^*$, and let $\phi = \langle\langle a_1, ..., a_n\rangle\rangle = q \otimes \langle 1, a_n\rangle = q \perp \langle a_n\rangle \otimes q$. In

particular, $\phi' = q'\perp\langle a_n\rangle \otimes q$, by cancelling $\langle 1\rangle$ using Witt's Cancellation Theorem. Let $b \in D(\phi')$. By the above, $b = x + a_n y$ for some $x \in D(q') \cup \{0\}, y \in D(q) \cup \{0\}$. Write: $y = t^2 + z$, where $t \in F$ and $z \in D(q') \cup \{0\}$. The induction hypothesis gives us:

$$\exists c_2, ..., c_{n-1} \in F, q \approx \langle\langle x, c_2, ..., c_{n-1}\rangle\rangle \text{ if } x \neq 0$$

$$\exists d_2, ..., d_{n-1} \in F, q \approx \langle\langle z, d_2, ..., d_{n-1}\rangle\rangle \text{ if } z \neq 0.$$

<u>Case 1</u> : $y = 0$. Then $x = b$, so $q \approx \langle\langle b, c_2, ..., c_{n-1}\rangle\rangle$ and $\phi = q\otimes\langle 1, a_n\rangle \approx \langle\langle b, c_2, ..., c_{n-1}, a_n\rangle\rangle$ as required.

<u>Case 2</u> : $y \neq 0$ and first suppose that $z \neq 0$. y is represented by $\langle 1, z\rangle$ by definition, so by the first point of Lemma 5.12 gives us that $\langle\langle z, a_n\rangle\rangle \simeq \langle\langle z, a_n y\rangle\rangle$. Therefore:

$$\begin{aligned}\phi &\approx \langle\langle z, d_2, ..., d_{n-1}, a_n\rangle\rangle\\ &\approx \langle\langle z, d_2, ..., d_{n-1}, a_n y\rangle\rangle\\ &\approx \langle\langle a_1, ..., a_{n-1}, a_n y\rangle\rangle.\end{aligned}$$

Now suppose that $z = 0$. Then $y = t^2 \neq 0$ is a square in F^*. So $\langle a_n\rangle \simeq \langle a_n y\rangle$ trivially, and we again obtain $\phi \approx \langle\langle a_1, ..., a_{n-1}, a_n y\rangle\rangle$.

<u>Case 2.1</u> : If $x = 0$, then $b = a_n y$ and we get $\phi \approx \langle\langle a_1, ..., a_{n-1}, a_n y\rangle\rangle \approx \langle\langle b, a_1, ..., a_{n-1}\rangle\rangle$ as required.

<u>Case 2.2</u> : If $x \neq 0$, remember that $q \approx \langle\langle x, c_2, ..., c_{n-1}\rangle\rangle \approx \langle\langle a_1, ..., a_{n-1}\rangle\rangle$. We also know that $b = x + a_n y$ is clearly represented by $\langle x, a_n y\rangle$, and therefore by the second point of Lemma 5.10, $\langle\langle x, a_n y\rangle\rangle \simeq \langle\langle b, x a_n y\rangle\rangle$. Therefore:

$$\begin{aligned}\phi &\approx \langle\langle a_1, ..., a_{n-1}, a_n y\rangle\rangle\\ &\approx \langle\langle x, c_2, ..., c_{n-1}, a_n y\rangle\rangle\\ &\approx \langle\langle b, c_2, ..., c_{n-1}, x a_n y\rangle\rangle.\end{aligned}$$

□

Corollary 5.11 *Pfister forms are multiplicative quadratic forms.*

Proof: We again use [17] as inspiration for this proof. Let ϕ be an anisotropic n-fold Pfister form. The inclusion $G(\phi) \subset D(\phi)$ is trivial because every Pfister form represents 1, and therefore, if $a \in G(\phi)$, then $\langle a\rangle \otimes \phi$ represents a, and by the isometry $\phi \simeq \langle a\rangle \otimes \phi$ we get that $a \in D(\phi)$. For the reverse inclusion, let $a \in D(\phi)$, considering the pure subform of ϕ, there exists $t \in F$, $b \in D(\phi')$ such that: $t^2 + b = a$. By Theorem 5.10, there exists $b_2, ..., b_{n-1} \in F$ such that $\phi \approx \langle\langle b, b_2, ..., b_n\rangle\rangle$. We know that $a \in D(\langle 1, b\rangle) \cap D(\langle a, ab\rangle)$ and considering determinants with Lemma 2.10, $\langle 1, b\rangle \simeq \langle a, ab\rangle = \langle a\rangle \otimes \langle 1, b\rangle$. So: $a\phi \simeq a\langle 1, b\rangle \otimes \langle\langle b_2, ..., b_n\rangle\rangle \simeq \langle 1, b\rangle \otimes \langle\langle b_2, ..., b_n\rangle\rangle \simeq \phi$, so $a \in G(\phi)$ as required.

Suppose now that ϕ is an isotropic n-fold Pfister form. Then by Theorem 2.3, ϕ contains a hyperbolic plane as an orthogonal summand, and since $-1 \notin D(\langle 1\rangle)$ because F is formally real, $-1 \in D(\phi')$. By Theorem 5.10, there exists $b_2, ..., b_n \in F^*$ such that $\phi \simeq \langle\langle -1, b_2, ..., b_n\rangle\rangle = \langle 1, -1\rangle \otimes \langle\langle b_2, ..., b_n\rangle\rangle \simeq 2^{n-1}.\mathbb{H}$, by Lemma 3.4. So ϕ is hyperbolic, as required. □

5.3 The ideal $I_T(F)$

In this section of Chapter 5, we develop our understanding of the ideal $I_T(F)$, following Becher's approach in [1]. The most important results in this section are Theorem 5.13, attributed to Pfister, and Proposition 5.14 which we finally prove using the annihilating Lewis polynomials discussed in Section 5.1. We start by proving a proposition which is posed as an exercise by Becher in [1, p.5].

Proposition 5.12 *Let $T \subset F$ is a proper quadratic preordering, let $a_1, ..., a_n \in F^*$. Then:*

$$\langle a_1, ..., a_n\rangle \text{ is } T\text{-isotropic} \iff \exists t_1, ..., t_n \in T^\times, \langle a_1t_1, ..., a_nt_n\rangle \text{ is isotropic.}$$

Proof: ($\Longrightarrow$): There exists $t_1, ..., t_m \in T^\times$ such that $\langle t_1, ..., t_m\rangle \otimes \langle a_1, ..., a_n\rangle$ is isotropic. Therefore, there exists $\{x_{ij}\}$, where $x_{ij} \in F$ for $i \in [\![1, m]\!], j \in [\![1, n]\!]$, such that:

$$0 = \sum_{i=1}^{m}\sum_{j=1}^{n} t_i a_j x_{ij}^2 = \sum_{j=1}^{n} a_j(\sum_{i=1}^{m} t_i x_{ij}^2).$$

Setting $t'_j = \sum_{i=1}^m t_i x_{ij}^2$, and because $F^2 \subset T, T+T \subset T, TT \subset T$, we get $a_1t'_1+...+a_nt'_n = 0$, and therefore $\langle a_1t'_1, ..., a_nt'_n\rangle$ is isotropic via the non-zero vector (1,1,...,1).
($\Longleftarrow$) : Suppose there exists $t_1, ..., t_n \in T^\times$ such that $\langle a_1t_1, ..., a_nt_n\rangle$ is isotropic. There exists $x_1, ..., x_n \in F$, not all zero, such that: $a_1t_1x_1^2 + ... + a_nt_nx_n^2 = 0$. Consider

$$\langle t_1, ..., t_n\rangle \otimes \langle a_1, ..., a_n\rangle = \langle t_1a_1\rangle \perp \langle t_1a_2\rangle \perp ... \perp \langle t_na_n\rangle.$$

Setting $x_{ij} = 0$ if $i \neq j$ and $x_{ii} = x_i$ for all $i, j \in [\![1, n]\!]$, we get that: $\sum_{i=1}^n \sum_{j=1}^n t_ia_jx_{ij}^2 = 0$, so that $\langle t_1, ..., t_n\rangle \otimes \langle a_1, ..., a_n\rangle$ is isotropic, as required.

□

We can now follow Becher's proof [1, p.5], and prove one of Pfister's theorems, making the ideal $I_T(F)$ easier to understand and allowing us to better understand torsion in $W(F)$.

Theorem 5.13 *(Pfister:) The ideal $I_T(F)$ is generated by the binary quadratic forms $\langle 1, -t\rangle$ where $t \in T^\times$.*

Proof: Let T be a proper quadratic preordering of F. Let $t \in T^\times$. We have that $\langle 1, t\rangle \otimes \langle 1, -t\rangle = \langle 1, t, -t, -t^2\rangle \simeq \langle -1, 1\rangle \perp \langle -t, t\rangle \simeq \mathbb{H} \perp \mathbb{H}$. Therefore $\langle 1, -t\rangle$ is T-hyperbolic, so $\langle 1, -t\rangle \in I_T(F)$ for all $t \in T^\times$. Consider the ideal $A \subset W(F)$ generated by the binary forms $\langle 1, -t\rangle$, for $t \in T^\times$. Then $A \subset I_T(F)$ by the above. We want to show that $A = I_T(F)$. To this end, suppose by contradiction that there exists ϕ representing a class of quadratic forms in $I_T(F)$, such that $\phi \notin A$. We can choose ϕ to have minimal such (strictly positive) dimension. We write $\phi = \langle a_1, ..., a_n\rangle$. Since ϕ is T-hyperbolic, it is therefore clearly T-isotropic. By Proposition 5.12, there exists $t_1, ...t_n \in T^\times$ such that $\langle a_1t_1, ..., a_nt_n\rangle$ is isotropic. We denote by $\phi' = \langle a_1t_1, ..., a_nt_n\rangle$ this isotropic quadratic form. We know that $\langle 1, -t_i\rangle \in A$, and therefore $\langle a_i\rangle \otimes \langle 1, -t_i\rangle = \langle a_i, -a_it_i\rangle \in A$.

In $W(F)$, we have that $\phi - \phi' = \langle a_1, -a_1t_1\rangle + ... + \langle a_n, -a_nt_n\rangle \in A$ by the above. So $\phi \equiv \phi' \mod A$. We know that ϕ' is isotropic, and has dimension n. Therefore ϕ' contains a hyperbolic plane by Theorem 2.3, and is Witt equivalent (remembering that $W(F) = \hat{W}(F)/\mathbb{Z}.\mathbb{H}$) to some quadratic form ψ of dimension $n-2$. Because $\psi = \phi'$ in W(F) by definition of ψ, and by minimality of the choice of n, the dimension of ϕ, this implies that $\psi \in A$. However, this gives us: $\phi \equiv \phi' \equiv \psi \equiv 0 \mod A$, so that $\phi \in A$, a contradiction. $\square$

Remark One should immediately note that, by Proposition 3.9, we have the inclusion $I_T(F) \subset I(F)$, as by the above theorem the generators of $I_T(F)$ form a subset of the generators of $I(F)$, thanks to the isomorphism $\hat{I}(F) \cong I(F)$. This remark is seen just as easily by using Proposition 3.10, and noting that the generators of $I_T(F)$ all have even dimension. By using the above theorem to prove Proposition 5.14, which we find again in [1], we avoid the case where q is a quadratic form of odd dimension, simplifying the proof given in [1].

Proposition 5.14 *The set $I_T(F)$ is a radical ideal of the Witt Ring $W(F)$.*

Proof: Let q be an anisotropic quadratic form of dimension n representing an element of $W(F)$. By Lemma 5.4, it suffices to show that $q^2 \in I_T(F) \implies q \in I_T(F)$. We have that $I_T(F) \subset I(F)$, by Proposition 3.10 and Theorem 5.13, so q^2 has even dimension. This implies that n is even because dim is a ring homomorphism into $\mathbb{Z}$ and therefore that $P_n(X)$ is an odd polynomial. Therefore $P_n(X) = bX + X^2f(X)$ for some $b \in \mathbb{Z}, f(X) \in \mathbb{Z}[X]$, and by the form of $P_n(X)$ given in the proof of Theorem 5.2, X^2 does not divide P_n, showing that $b \neq 0$. We have $P_n(q) = bq + q^2f(q) = 0$ and $q^2 \in I_T(F) \implies q^2f(q) \in I_T(F) \implies bq = -q^2f(q) \in I_T(F)$. There exists ν a T-positive quadratic form such that $\nu \otimes bq$ is hyperbolic, ie: $b\nu \otimes q$ is hyperbolic. This also means that $-b\nu \otimes q \in W(F)$ is hyperbolic. If $b > 0$ then $b\nu$ is a T-positive quadratic form, and if $b < 0$ then $-b\nu$ is T-positive, so we are done.

$\square$

Corollary 5.15 *A quadratic form q over F is T-hyperbolic if and only if there exists a T-positive Pfister form $\tau = \langle 1, t_1\rangle \otimes ... \otimes \langle 1, t_n\rangle$ with $t_1, ..., t_n \in T^\times$ such that $\tau \otimes q$ is hyperbolic. - [1, p.5]*

Proof: The 'if' statement is trivial. For the 'only if' statement, let $\phi \in I_T(F)$. By Theorem 5.13, there exists $a_1, ..., a_n \in F$, $t_1, ..., t_n \in T^\times$ such that $\phi = \langle a_1\rangle \otimes \langle 1, -t_1\rangle \perp ... \perp \langle a_n\rangle \otimes \langle 1, -t_n\rangle$. We have $\phi = \langle a_1, -a_1t_1\rangle \perp ... \perp \langle a_n, -a_nt_n\rangle$. Considering each term of the orthogonal sum given by expanding $\bigotimes_{i=1}^n \langle 1, t_i\rangle \otimes \phi$, we have, for all $j \in [\![1, n]\!]$:

$$\begin{aligned}
\bigotimes_{i=1}^{n} \langle 1, t_i\rangle \otimes \langle a_j, -t_ja_j\rangle &= \bigotimes_{i\neq j} \langle 1, t_i\rangle \otimes \langle 1, t_j\rangle \otimes \langle 1, -t_j\rangle \otimes \langle a_j\rangle \\
&\simeq \bigotimes_{i\neq j} \langle 1, t_i\rangle \otimes (\langle 1, -1\rangle \perp \langle 1, -1\rangle) \otimes \langle a_j\rangle \\
&\simeq \bigotimes_{i\neq j} \langle 1, t_i\rangle \otimes \langle 1, t_j\rangle \otimes 2\mathbb{H} \otimes \langle a_j\rangle \in \mathbb{Z}_{>0}.\mathbb{H}
\end{aligned}$$

thanks to Lemma 3.4. We conclude therefore that $\bigotimes_{i=1}^{n}\langle 1, t_i\rangle \otimes \phi$ is hyperbolic, as required. $\square$

Remark We can now make a very important remark, which is only made in passing in [1, p.4]. The torsion subgroup of $W(F)$, denoted by $W(F)_{tors}$ is equal to $I_{\sum F^2}(F)$. Theorem 5.13 shows that $I_{\sum F^2}(F)$ is generated by binary forms $\langle 1, -w\rangle$ where $w \in (\sum F^2)^\times$. Then w is a sum of 2^n squares for some $n \in \mathbb{N}$ large enough, and:

$$2^n.\langle 1, -w\rangle = 2^n\langle 1\rangle \otimes \langle 1, -w\rangle = \langle 1, ..., 1, -w, ..., -w\rangle.$$

Since w is a sum of 2^n squares, $2^n\langle 1, -w\rangle$ is isotropic. However, note that $2^n\langle 1\rangle = \langle\langle 1, ..., 1\rangle\rangle$, an n-fold Pfister form, and therefore $2^n\langle 1\rangle \otimes \langle 1, -w\rangle = \langle\langle 1, ..., 1, -w\rangle\rangle$ is an $(n+1)$-Pfister form. We have shown that Pfister forms are multiplicative, so that an isotropic Pfister form is hyperbolic. Therefore: $2^n\langle 1\rangle \otimes \langle 1, -w\rangle = 0$ in $W(F) = \hat{W}(F)/\mathbb{Z}.\mathbb{H}$. Conversely, suppose ϕ is an anisotropic form representing an element of $W(F)$ and there exists $n \in \mathbb{N}$ such that $n\langle 1\rangle \otimes \phi = 0$ in $W(F)$. Then $n\langle 1\rangle \otimes \phi$ is hyperbolic, and $\phi \in I_{\sum F^2}(F)$, as $n\langle 1\rangle$ is trivially $\sum F^2$-positive. This important remark motivates the following theorem of Scharlau, which is included and proved in Becher's paper [1, p.5,6], and will also be used in our proof of Pfister's Local-Global Principle.

Theorem 5.16 *(Scharlau:) The order of any torsion element of $W(F)$ is a power of 2.*

Proof: Let ϕ be a torsion element of $W(F)$, ie: $\phi \in I_{\sum F^2}(F)$ by the above remark. By Corollary 5.15, there exists $t_1, ..., t_n \in \sum F^2$ such that $\langle 1, t_1\rangle \otimes ... \otimes \langle 1, t_n\rangle \otimes \phi$ is hyperbolic. t_i is as sum of n_i squares in F. Let $m = \max\{n_i, 1 \le i \le n\}$. Therefore, $t_i \in D(2^m.\langle 1\rangle)$. We know that $2^m.\langle 1\rangle$ is a Pfister form, and is multiplicative by Corollary 5.11. Therefore:

$$\langle 1, t_i\rangle \otimes 2^m\langle 1\rangle \simeq 2^m\langle 1\rangle \perp \langle t_i\rangle \otimes 2^m\langle 1\rangle \simeq 2^m\langle 1\rangle \perp 2^m\langle 1\rangle \simeq 2^{m+1}\langle 1\rangle.$$

We therefore get by induction that $2^m.\langle 1, t_1\rangle \otimes ... \otimes \langle 1, t_n\rangle \simeq 2^{m+n}\langle 1\rangle$. As a result, $2^{m+n}\langle 1\rangle.\phi = 2^{m+n}\phi$ is hyperbolic, ie: $2^{m+n}\phi = 0$ in $W(F)$. Therefore, the order of ϕ in $W(F)$ must divide 2^{m+n}, which allows us to conclude that it must be a power of 2.

$\square$

5.4 Pfister's Local-Global Principle

We prove the following proposition, which is stated outright as a remark by Becher in [1, p.6], and is the first result to underline the relevance of the work we did in Chapter 4 on signatures. This proposition, along with Theorem 5.18 - attributed to Lorenz and Leicht and found in [1] - is required to prove that $I_F(T)$ is the kernel of sgn_T, which is defined at the end of Chapter 4.

Proposition 5.17 *Let P be an order of F. Then:*

$$I_P(F) = \ker(sgn_P),$$

that is the ideal $I_P(F)$ is the kernel of the signature at P homomorphism $sgn_P : W(F) \to \mathbb{Z}$.

Proof: We know that $I_P(F)$ is generated by the binary forms $\langle 1, -a\rangle, a \in P^\times$. Since $1 \in P$, for all $a \in P^\times, \mathrm{sgn}_P(\langle 1, -a\rangle) = 1 - 1 = 0$, so $I_P(F) \subset \ker(\mathrm{sgn}_P)$. For the reverse inclusion, suppose that $\langle a_1, ..., a_n\rangle \in \ker(\mathrm{sgn}_P)$ be an anisotropic form representing an element of $W(F)$. Then for each $i \in [\![1, n]\!]$, $a_i \neq 0$ and $\mathrm{sgn}_P(\langle a_1, ..., a_n\rangle) = \mathrm{sgn}_P(a_1) + ... + \mathrm{sgn}(a_n) = 0 \implies a_1, ..., a_{n/2} \in P$ and $a_{n/2+1}, ..., a_n \in -P$ without loss of generality in the order of the a_i's. In $W(F)$, we can simultaneously add and subtract $\frac{n}{2}$ $\langle 1\rangle$'s to $\langle a_1, ..., a_n\rangle$, to obtain:

$$\begin{aligned}&\langle -1, a_1\rangle \perp ... \perp \langle -1, a_{n/2}\rangle \perp \langle 1, a_{n/2}\rangle \perp ... \perp \langle 1, a_n\rangle \\ &\qquad = -\langle 1, -a_1\rangle \perp ... \perp -\langle 1, -a_{n/2}\rangle \perp \langle 1, -(-a_{n/2})\rangle \perp ... \perp \langle 1, -(-a_n)\rangle.\end{aligned}$$

Because $-a_i \in P^\times$ for each $\frac{n}{2} + 1 \leq i \leq n$, and because $I_P(F)$ is generated by the binary forms $\langle 1, -a\rangle, a \in P^\times$, we have that $\ker(\mathrm{sgn}_P) \subset I_P(F)$. □

Theorem 5.18 *(Lorenz-Leicht:) Let $\mathfrak{p} \subset W(F)$ be a prime ideal of $W(F)$ different from $I(F)$. Let $P \subset F$ be the set:*

$$P = \{a \in F \mid a = 0 \text{ or } \langle 1, -a\rangle \in \mathfrak{p}\}.$$

Then P is an order of F such that $I_P(F) \subset \mathfrak{p}$. Moreover, if $I_T(F) \subset \mathfrak{p}$ for some proper quadratic preordering T, then $T \subset P$ and $I_T(F) \subset I_P(F) \subset \mathfrak{p}$.

Proof: Let $\mathfrak{p} \subset W(F)$ be a prime ideal of $W(F)$, not equal to $I(F)$. We need to show that P, as defined in the statement of the theorem, is an order of F, that is:

1. $P \cup -P = F$
2. $P \cap -P = \{0\}$
3. $PP \subset P$ and $P + P \subset P$.

1. Let $a \in F$. If $a = 0$, then $a \in P$ by definition of P. If $a \neq 0$, then consider:

$$\langle 1, -a\rangle \otimes \langle 1, a\rangle = \langle 1, a, -a, -a^2\rangle = 2\langle 1, -1\rangle = 0 \in \mathfrak{p} \text{ in } W(F).$$

   Since $\mathfrak{p}$ is a prime ideal of $W(F)$, we have that $\langle 1, -a\rangle$ or $\langle 1, a\rangle \in \mathfrak{p}$, and by definition of P, $a \in P \cup -P$, as required.

2. Suppose by contradiction that there exists $a \in F^*$ such that $a \in P \cap -P$. Then: $a, -a \in P \implies -a^2 \in P \implies \langle 1, a^2\rangle \in \mathfrak{p} \implies \langle 1, 1\rangle \implies -1 \in P$. We know that $I(F)$ is a maximal ideal of $W(F)$, and that $\mathfrak{p}$ is not equal to $I(F)$. We cannot have $I(F) \subset \mathfrak{p}$ - otherwise they would be equal by maximality of $I(F)$ - and as a result there exists $b \in F^*$ such that $\langle 1, -b\rangle \notin \mathfrak{p}$ by Proposition 3.9. Therefore, because $\mathfrak{p}$ is a prime ideal of $W(F)$, $\langle 1, -b\rangle \otimes \langle 1, -b\rangle \notin \mathfrak{p}$. Note that $\langle 1, 1\rangle \otimes \langle 1, -b\rangle = \langle 1, -b\rangle \otimes \langle 1, -b\rangle$. Therefore: $\langle 1, 1\rangle \notin \mathfrak{p}$ which shows that $-1 \notin P$, contradicting the above discussion. We conclude that $P \cap -P = \{0\}$.

3. Let $a, b \in P$. If one of a or b is 0 then it is clear that $ab, a+b \in P$. Suppose that $a, b \neq 0$. Then: $-\langle 1, -a\rangle \otimes \langle 1, -b\rangle = -\langle 1, -a, -b, ab\rangle = \langle -1, a, b, -ab\rangle \in \mathfrak{p}$. Therefore, since $\langle 1, -a\rangle, \langle 1, -b\rangle \in \mathfrak{p}$, we have:

$$\langle -1, a, b, -ab\rangle + \langle 1, -a\rangle + \langle 1, -b\rangle = \langle 1, -ab\rangle \in \mathfrak{p} \text{ in W(F)}.$$

This shows us that $ab \in P$, as required. Now suppose by contradiction that $a + b \notin P$, ie: $a + b \in -P$ by (1). There exists $c \in P$ such that $a + b = -c$, and we see easily that $c \neq 0$. Therefore, $c^{-1} \in P$ and there exists $s = ac^{-1}, t = bc^{-1} \in P$ such that $s + t = -1$. Therefore $\langle s, t\rangle$ represents -1, and has the same determinant as $\langle -1, -st\rangle$. Lemma 2.10 gives $\langle s, t\rangle = \langle -1, -st\rangle$ in $W(F)$. We have:

$$\langle 1, s\rangle \otimes \langle 1, t\rangle = \langle 1, s, t, st\rangle = \langle 1, -1, -st, st\rangle = 0 \in \mathfrak{p} \text{ in } W(F),$$

and because $\mathfrak{p}$ is prime ideal, this gives us that $-s \in P$ or $-t \in P$, a contradiction. So $a + b \in P$.

We know that $I_P(F)$ is the ideal generated by the binary forms $\langle 1, -a\rangle$ for $a \in P^\times$. The prime ideal $\mathfrak{p}$, by defintion of P, contains all of these generators. Therefore $I_P(F) \subset \mathfrak{p}$. Let T be a proper quadratic preordering of F, such that $I_T(F) \subset \mathfrak{p}$. Then, given that $I_T(F)$ is generated by the binary forms $\langle 1, -t\rangle, t \in T^\times$, we have $\langle 1, -t\rangle \in \mathfrak{p}$ for all $t \in T^\times$, so $t \in P$ for all $t \in T^\times$, ie: $T \subset P$. This gives $I_T(F) \subset I_P(F)$ by considering their generators.

□

The final two theorems are due to Pfister, with Theorem 5.20 being Pfister's celebrated Local-Global Principle and the main result of this project, and can be found in [1, p.6,7], along with sligthly less detailed proofs. We have chosen this final formulation of the principle as it is best suited to the applications we will look to explore in Chapter 6. Succinctly, as stated in [1, §1, p.1], "Pfister's Local-Global Principle says that a non-singular quadratic form over a formally real field represents a torsion element in the Witt ring if and only if its signature at each ordering of the field is zero."

Theorem 5.19 *(Pfister:) Let T be a proper quadratic preordering. The ideal $I_T(F)$ is equal to the kernel of the homomorphism $sgn_T : W(F) \to \mathbb{Z}^{\chi_T(F)}$.*

Proof: By the definition of sgn_T, it is clear that

$$\ker(\mathrm{sgn}_T) = \bigcap_{P \in \chi_T(F)} \ker(sgn_P) = \bigcap_{P \in \chi_T(F)} I_P(F),$$

the last equality using Proposition 5.17. We want to show that $I_T(F) = \ker(\mathrm{sgn}_T)$, that is:

$$I_T(F) = \bigcap_{P \in \chi_T(F)} I_P(F).$$

From the fact that $\chi_T(F) = \{P \in \chi(F) \mid T \subset P\}$, this gives us the trivial inclusion:

$$I_T(F) \subset \bigcap_{P \in \chi_T(F)} I_P(F)$$

as $I_T(F) \subset I_P(F)$ for all $P \in \chi_T(F)$. We showed in Proposition 5.14 that $I_T(F)$ is a radical ideal of $W(F)$. Therefore,

$$I_T(F) = r(I_T(F)) = \bigcap_{I_T(F) \subset \mathfrak{p}, \mathfrak{p} \text{ prime ideal of } W(F)} \mathfrak{p},$$

a standard commutative algebra result. For readers unfamiliar with this result, a standard reference is for example [16, §1, p.30]. Let $\mathfrak{p}$ be a prime ideal of $W(F)$ containing $I_T(F)$. By Lorenz-Leicht, there exists an order $P_\mathfrak{p}$ of F for the prime ideal $\mathfrak{p}$, such that $I_{P_\mathfrak{p}}(F) \subset \mathfrak{p}$, as well as $T \subset P$ because $I_T(F) \subset \mathfrak{p}$. Firstly, this gives us:

$$\{P_\mathfrak{p} \mid I_T(F) \subset \mathfrak{p}, \mathfrak{p} \text{ prime ideal of } W(F)\} \subset \chi_T(F),$$

giving us the first inclusion of (1) below. Secondly, $I_{P_\mathfrak{p}}(F) \subset \mathfrak{p}$ gives us the second inclusion of (1).

$$\bigcap_{P \in \chi_T(F)} I_P(F) \subset \bigcap_{I_T(F) \subset \mathfrak{p}, \mathfrak{p} \text{ prime ideal of } W(F)} I_{P_\mathfrak{p}(F)} \subset \bigcap_{I_T(F) \subset \mathfrak{p}, \mathfrak{p} \text{ prime ideal of } W(F)} \mathfrak{p} = I_T(F). \tag{1}$$

□

Theorem 5.20 *(Pfister's Local-Global Principle:) Let F be a formally real field, let ϕ be a non-singular quadratic form over F. The following are equivalent:*

1. *$sgn_P(\phi) = 0$ for every ordering P of F.*
2. *ϕ represents a torsion element in $W(F)$.*
3. *There exists $a_1, ..., a_n \in F^*$ and $t_1, ..., t_n \in \sum(F^*)^2$ such that ϕ is Witt equivalent to the form $\langle a_1, -t_1a_1\rangle \perp ... \perp \langle a_n, -t_na_n\rangle$.*
4. *ϕ represents a nilpotent element of $W(F)$.*

Proof: Let T be the proper quadratic preordering $T = \sum F^2$. Let ϕ be a (non-singular) quadratic form over F. We have that $\chi_T(F) = \chi(F)$ because $\sum F^2 \subset P$ for any order P of F. We also now know that $\ker(\mathrm{sgn}_T) = I_{\sum F^2}(F) = W(F)_{tors}$. We therefore have the following equivalences:

$$\begin{aligned}
&\mathrm{sgn}_P(\phi) = 0 \text{ for all orders } P \text{ of } F \\
&\qquad \iff \mathrm{sgn}_{\sum F^2}(\phi) = 0 \\
&\qquad \iff \phi \in \ker(sgn_{\sum F^2}) \\
&\qquad \iff \phi \in I_{\sum F^2}(F) = W(F)_{tors} \\
&\qquad \iff \phi \text{ is of the form } a_1\langle 1, -t_1\rangle \perp ... \perp a_n\langle 1, -t_n\rangle \text{ for some } a_i \in F, t_i \in \sum F^2.
\end{aligned}$$

as $I_{\sum F^2}(F)$ is generated by the binary forms $\langle 1, -t\rangle, t \in \sum F^2$. This proves (1) $\iff$ (2) $\iff$ (3).

(1) $\implies$ (4) : For every prime ideal $\mathfrak{p} \subset W(F)$, we have $\mathfrak{p} \subset I_{P_\mathfrak{p}}(F)$ and $\phi \in I_{P_\mathfrak{p}}(F)$ for

every prime ideal $\mathfrak{p} \subset W(F)$ by assuming (1). Therefore ϕ is in every prime ideal of $W(F)$, so $\phi \in \bigcap_{\mathfrak{p} \text{ prime ideal of } W(F)} \mathfrak{p} = N(W(F))$, the nilradical of $W(F)$, which shows that ϕ is nilpotent. This standard commutative algebra result can, again, be found in [16, §1, p.28].
(4) $\implies$ (2) : There exists $n \in \mathbb{N}$ such that $\phi^n = 0 \in I_{\sum F^2}(F)$, in $W(F)$. Since $I_{\sum F^2}(F)$ is a radical ideal, we obtain $\phi \in I_{\sum F^2}(F) = W(F)_{tors}$, as required. $\square$

6 The u-invariant of Formally Real Fields

6.1 The u-invariant

We introduce the u-invariant of a field F - sometimes called the 'universal invariant' - as defined in [11, §11, p.315] or in [17, §2, p.102].

Definition 6.1 *Let F be a field of characteristic not equal to 2. We define the* <u>*u-invariant*</u> *of F as the maximum dimension of any anisotropic quadratic form over F, that is:*

$$u(F) = \sup\{\dim(q), q \text{ anisotropic form over } F\}.$$

If no such maximum dimension exists, we write $u(F) = \infty$.

By the above definition, for a field F (of characteristic not equal to 2) and q is a quadratic form over F, then $\dim(q) > u(F) \implies q$ is isotropic.

Remark Consider the quadratic form $n\langle 1\rangle = \langle 1, ..., 1\rangle$, for some $n \in \mathbb{N}$. Suppose that $n\langle 1\rangle$ is isotropic and that there exists $x_1, ..., x_n \in F$, with $x_i \neq 0$, such that $x_1^2 + ... + x_n^2 = 0$. Then $-1 = \sum_{j\neq i}(\frac{x_j}{x_i})^2 \in \sum F^2$. Therefore F is non-formally real. We can conclude that $u(F) = \infty$ when F is formally real, because $n\langle 1\rangle$ is anisotropic over F for all $n \in \mathbb{N}$.

In view of the above remark, we discuss a few examples and interesting facts about the u-invariant of non-formally real fields. We explain the following example which is stated in [11, §11, p.316]. We then discuss the u-invariant of finite fields, showing that $u(\mathbb{F}_q) = 2$ when q is odd, a fact found in [11] for example.

Example Let F be a quadratically closed field of characteristic not equal to 2, as in one of the final examples of Chapter 3. Then $\langle 1\rangle$ is clealy anisotropic, but if $a, b \in F^*$, then $\langle a, b\rangle \simeq \langle 1, 1\rangle$ is isotropic via the vector $(1, \sqrt{-1})$. Therefore $u(F) = 1$. Conversely, if $u(F) = 1$, let $a \in F$ and consider the quadratic form $\langle a, -1\rangle$. There exists $x, y \in F$ not both zero, $ax^2 - y^2 = 0$. If $a \neq 0$, then $x \neq 0$ - because otherwise $x = y = 0$ - and $a = (\frac{y}{x})^2$. In conclusion, F is quadratically closed $\iff u(F) = 1$. For example, $u(\mathbb{C}) = 1$.

Example Suppose that $F = \mathbb{F}_q$ is the finite field containing q elements, where q is a prime power, and that $\mathrm{char}(F) \neq 2$ so q is odd. F^* has $q - 1$ elements, and consider the surjective homomorphism

$$f : \left| \begin{array}{ccc} F^* & \longrightarrow & (F^*)^2 \\ x & \longmapsto & x^2 \end{array} \right.$$

which is surjective. Clearly $\ker(f) = \{\pm 1\}$, and therefore $|(F^*)^2| = |F^*/\ker(f)| = \frac{q-1}{2}$. We can conclude that the group of squares classes $F^*/(F^*)^2$ contains two elements: $F^*/(F^*)^2 = \{1, s\}$ for some $s \in F^*$. We want to show that s is a sum of two squares in F.

What follows can be attributed to [11, §2, p.44]. If -1 is a square, then $\mathbb{H} \simeq \langle 1, 1\rangle$ and since $\mathbb{H}$ represents every element of F^* by the proof of Theorem 2.2, it represents s. If -1 is not a square, consider $(F^*)^2$ and $1 + (F^*)^2$, subsets which have the same cardinality, and

$1 \notin 1 + (F^*)^2$. Therefore, there must exist $t \in F^*$ such that $s = 1 + t^2 \notin (F^*)^2$. In both cases, s is a sum of squares.

Up to isometry there are 3 different binary forms: $\langle 1, 1\rangle, \langle 1, s\rangle, \langle s, s\rangle$. We showed in Chapter 2 that, for a quadratic form q and any $a, b \in F^*$, $a \in D(q) \iff ab^2 \in D(q)$, so it is enough to show that $1, s \in D(q)$ to show that a quadratic form over $F = \mathbb{F}_q$ represents every element of F^*. If q represents every element of F^*, then for any $d \in F$, $q \perp \langle d\rangle$ is isotropic because q represents $-d$. Since s is a sum of squares, we have that $\langle 1, 1\rangle, \langle 1, s\rangle$ both represent 1 and s, and $\langle s, s\rangle = \langle s\rangle \otimes \langle 1, 1\rangle \simeq \langle s^{-1}\rangle \otimes \langle 1, 1\rangle$ allows us to conclude that $\langle s, s\rangle$ also represents 1 and s. We conclude that any 3-dimensional form is isotropic. It is easy to check that $\langle 1, 1\rangle$ is anisotropic when -1 is not a square, $\langle 1, s\rangle$ is anisotropic when -1 is a square. This shows that: $u(F) = 2$.

We present a final proposition, from [11, §11, p.317], before adapting the definition of the u-invariant to suit formally real-fields. This second definition is due to Elman and Lam, given in [8, §6, p.375]. It provides a more general version of the u-invariant, which can be finite for formally real fields and coincides with Definition 6.1 for non-formally real fields.

Proposition 6.2 *Let F be a field of characteristic not equal to 2, and suppose that $u(F) < \infty$. Then $I(F)$ is a nilpotent ideal.*

Proof: Let $n \in \mathbb{N}$. We know from Proposition 3.9 that $IF \subset W(F)$ is the ideal generated by the binary forms $\langle 1, -a\rangle, a \in F^*$. Therefore $I(F)^n$ is the ideal generated by the forms $\langle 1, -a_1\rangle \otimes ... \otimes \langle 1, -a_n\rangle = \langle\langle -a_1, ..., -a_n\rangle\rangle$, ie: $I(F)^n$ is generated by the n-fold Pfister forms of $W(F)$. Let $n \in \mathbb{N}$ be such that $2^n > u(F)$. Then every n-fold Pfister form (therefore of dimension 2^n) is isotropic, and by the multiplicativity of Pfister forms, they are all hyperbolic, ie: equal to zero in the Witt ring $W(F)$. So $I(F)^n = 0$. □

Definition 6.3 *Let F be a field of characteristic not equal to 2. We define the general u-invariant of F as the maximum dimension among anisotropic quadratic forms which represent torsion elements in the Witt ring. That is:*

$$u'(F) = \sup\{\dim(q), q \text{ anisotropic form in } W(F)_{tors}\}.$$

Proposition 6.4 *Let F be a non-formally real field of characteristic not equal to 2. Then: $u'(F) = u(F)$.*

Proof: We want to show that $W(F) = W(F)_{tors}$. Firstly, start by considering Lorenz-Leicht's result stated in Theorem 5.18, and importantly its proof. At no point in the proof that P is an order of F did we use the fact that F was formally real. Let F be non-formally real, of characteristic not equal to 2. Then the first part of the theorem shows that $I(F)$ (being maximal) is the only prime ideal of $W(F)$, otherwise F has an order P and by Artin-Schreier in Corollary 4.11, F would be formally real. Therefore, $I(F) = N(W(F))$, using $N(W(F)) = \bigcap_{P \subset W(F) \text{ prime ideal}} P$ from [16, §1, p.28]. We know that $\langle 1, 1\rangle \in I(F)$, having even dimension. There exists $n \in \mathbb{N}$ such that $(\langle 1,1\rangle)^n = 2^n\langle 1\rangle = 0$ in $W(F)$. Therefore, for any anisotropic form f representing an element of $W(F)$, $2^n\langle 1\rangle \otimes f = 2^n.f = 0$. $\square$

Example Let $F = \mathbb{R}$. We know from Pfister Local-Global Principle that torsion forms over $\mathbb{R}$ are precisely the quadratic forms with signature equal to 0. We also know that for all $a \in \mathbb{R}^*$, $\langle a\rangle \simeq \langle \pm 1\rangle$. A torsion form over $\mathbb{R}$ is therefore a quadratic form for which $n_+ = n_-$, using the notation introduced in the discussion of Sylvester's Law. Given that $\langle 1, -1\rangle$ is isotropic, any form of dimension greater than 2 is isotropic and since $\langle -1\rangle$, $\langle 1\rangle$ are not torsion, we conclude that $u'(\mathbb{R}) = 0$.

Remark The general u-invariant of a formally real field is always even, as Pfister's Local Global principle requires the signature of a torsion form to be equal to 0. This can also be seen by remembering that $I_{\sum F^2}(F) = W(F)_{tors}$ is generated by the binary forms $\langle 1, -a\rangle, a \in (\sum F^2)^\times$.

6.2 The Harrison Topology

Let F be a formally real field, and therefore an ordered field. We can define a topology on the set $\chi(F)$, which is non-empty because F is formally real, called the Harrison Topology. We first note that an ordering P of F can be regarded as a group epimorphism $\theta : F^* \to (\{\pm 1\}, \times)$, via:

$$\begin{cases} \theta(x) = 1 \text{ if } x \in P^\times \\ \theta(x) = -1 \text{ if } x \notin P^\times. \end{cases}$$

Denote this association $\psi : \chi(F) \longrightarrow \{\pm 1\}^{F^*} = \mathrm{Hom}_{\mathbb{Z}}(F^*, \{\pm 1\})$, where $\psi(P) = \theta$. This has left-inverse

$$\rho : \left| \begin{array}{ccc} \mathrm{Hom}_{\mathbb{Z}}(F^*, \{\pm 1\}) & \longrightarrow & \chi(F) \\ \theta & \longmapsto & \theta^{-1}(1) \cup \{0\} \end{array} \right.$$

which shows that ψ is an injection. Therefore, $\chi(F)$ embeds into the set $\{\pm 1\}^{F^*}$ via ψ, and will therefore inherit the induced topology from $\{\pm 1\}^{F^*}$, which we define in what follows. We consider $\chi(F)$ as a subset of $\{\pm 1\}^{F^*}$ via this embedding. As usual, $\{\pm 1\}^{F^*}$ can be seen as $\prod_{a \in F^*}\{\pm 1\}$, putting the image of a via the homomorphism θ in the a-th position. Consider the discrete topology on $\{\pm 1\}$ and the definition of a product topology on $\prod_{a \in F^*}\{\pm 1\}$ found in [15, §2, p.114]. Define the following sets:

$$\pi_a^{-1}(\epsilon) = H(a, \epsilon) = \{\theta \in \{\pm 1\}^{F^*} \mid \theta(a) = \epsilon\},$$

where $a \in F^*$, $\epsilon = \pm 1$, and π_a is the canonical projection map $\pi_a : \prod_{a \in F^*}\{\pm 1\} \twoheadrightarrow \{\pm 1\}$. The definition of the product topology tells us that this family of sets (for all $\epsilon = \pm 1, a \in F^*$) is a subbasis for the product topology on $\prod_{a \in F^*}\{\pm 1\}$. Remember that a <u>subasis</u> S of a topology on X is a collection of subsets of X whose union equals X. The <u>topology generated by S</u> is defined to be the collection of all unions of finite intersections of elements of S, [15]. We clearly have that $H(a, \epsilon) \cup H(a, -\epsilon) = \prod_{a \in F^*}\{\pm 1\}$ is a disjoint union, as in [17, p.125], and this shows that $H(a, \epsilon)$ is closed for all $a \in F^*$, $\epsilon = \pm 1$, as $H(a, \epsilon)$ is also open, being the pre-image of an open set via the (continuous) canonical projection.

The subbasis $\{H(a, \epsilon), a \in F^*, \epsilon = \pm 1\}$ defined above generates the topology on $\prod_{a \in F^*} \{\pm 1\}$. Therefore $\{H(a, \epsilon) \cap \chi(F), a \in F^*, \epsilon = \pm 1\}$ is a subbasis of $\chi(F)$. The topology it generates on $\chi(F)$ is called the Harrison topology and the sets

$$H(a) = H(a, 1) \cap \chi(F) = \{P \in \chi(F) \mid a \in P\},$$

for $a \in F^*$, are called the Harrison sets. Note that $H(a, -1) \cap \chi(F) = H(-a)$, and therefore the Harrison sets are precisely the elements of this subbasis of $\chi(F)$.

In Section 6.4, we will need the fact that $\chi(F)$ is a compact space. We use Theorem 37.3 from [15, §5, p.234], Tychonoff's Theorem to show that $\prod_{a \in F^*} \{\pm 1\}$ is compact; we use Theorem 26.2 from [15, §3, p.165] which states that a closed subspace of a compact space is compact.

Proposition 6.5 *$\chi(F)$ is a closed subset of $\prod_{a \in F^*} \{\pm 1\}$.*

Proof: We follow the proof given in [17, §3, p.125]. We need to show that the complement of $\chi(F)$ in $\prod_{a \in F^*} \{\pm 1\}$ is open. Let $s \in \prod_{a \in F^*} \{\pm 1\}$, seen as a homomorphism $s : F^* \to \{\pm 1\}$, and suppose it is not defined by an order P of F. Looking at Definition 4.2, this means that (B) or (C) must fail. Property (A) cannot fail by definition of s. This means:

1. $s(a) = s(b) = 1$ but $s(a + b) = -1$ for some $a, b \in F^*$.
2. $s(a) = s(b) = 1$ but $s(ab) = -1$ for some $a, b \in F^*$.
3. $s(a) = s(-a) = \epsilon$ for some $a \in F^*$, some $\epsilon \in \{\pm 1\}$.

We need to find an open neighbourhood of s contained in the complement of $\chi(F)$ in each case. Consider case (1). It is clear that $s \in H(a, 1) \cap H(b, 1)$ by definition of these sets, as well as $s \in H(a + b, -1)$. Let $f \in H(a, 1) \cap H(b, 1) \cap H(a + b, -1)$. If there exists an order P of F such that $\psi(P) = f$, then $a, b \in P^\times$, and $a + b \notin -P^\times$ by definition of ψ and f, a contradiction. Therefore, $f \notin \chi(F)$ which shows that $H(a, 1) \cap H(b, 1) \cap H(a + b, -1)$ is an open neighbourhood of the complement of $\chi(F)$ which contains s. We argue similarly for cases (2) and (3), using the neighbourhoods $H(a, 1) \cap H(b, 1) \cap H(ab, -1)$ and $H(a, \epsilon) \cap H(-a, \epsilon)$ respectively. $\square$

6.3 Discrete Valuation Rings and the Baer-Krull Theorem

We need the Baer-Krull Representation Theorem, which we will find in [9, §2], for Section 6.4. To this end, we introduce the definitions and context required to understand this theorem and its proof. We will not spell out the proof, as it is long and can be found in its entirety in [9, §2, p.37], and it would not be particularly enlightening for the rest of this project. The following of definitions and remarks are inspired by [12] and [9].

Definition 6.6 *A subring A of F is said to be* <u>$\leq$*-convex*</u> *(P-convex if using the associated order P of F) if, for all $x, z \in A, y \in F$, $x < y < z \implies y \in A$.*

Definition 6.7 *A* <u>*valuation*</u> *$v : F^* \to \Gamma$ on a field F, is a surjective homomorphism onto a totally ordered abelian group Γ with ordering $\leq$, such that:*

1. $\forall x, y \in F^*, v(xy) = v(x) + v(y)$.
2. $\forall x, y \in F^*, x + y \neq 0 \implies v(x + y) \geq \min\{v(x), v(y)\}$.

Remark For a valuation v as above, we can define the associated objects, and retain the standard notation provided below:

- $A = \{x \in F \mid x = 0 \text{ or } v(x) \geq 0\}$ is the valuation ring of v.
- $\mathfrak{m} = \{x \in F \mid x = 0 \text{ or } v(x) > 0\}$ is the (unique) maximal ideal of v.
- $U = A \setminus \mathfrak{m}$ is the set of (valuation) units of A.
- $\bar{F} = A/\mathfrak{m}$ is the residue class field of v.

Definition 6.8 *Following the notation provided above, A is a called a* <u>*discrete valuation ring*</u> *if $\Gamma \cong \mathbb{Z}$ and F is the fraction field of A.*

Suppose that A is a discrete valuation ring. We know from commutative algebra ([16, §8, p.113,114]) that A has a unique maximal ideal $\mathfrak{m} = \{x \in F \mid v(x) > 0\}$, as stated above, generated by an irreducible element $t \in \mathfrak{m}$ which is unique up to multiplication by a unit, and any element generating $\mathfrak{m}$ is called a <u>uniformizer</u> of A. Thanks to (i) in the proposition found in [16, §8, p.114], every element $x \neq 0 \in A$ can be written uniquely as $x = ut^n$ for some $u \in U$. For all $x \in A$, denote by $\bar{x}$ the image of x under the canonical surjection $A \longrightarrow A/\mathfrak{m} = \bar{F}$. The following theorem is obtained by combining [9, 2.2.4, p.36] and [12, p.17], and will help us define the notion of compatibility between orderings and valuations in formally real fields.

Theorem 6.9 *Let P be an order of F. Let v be a valuation of F, for which we use the notation defined in the above remark. The following are equivalent:*

1. *$\forall a, b \in F, 0 < a \leq b$ with respect to $P \implies v(a) \geq v(b) \in \Gamma$;*
2. *A is P-convex;*
3. *$\mathfrak{m}$ is P-convex;*
4. *$1 + \mathfrak{m} \subset P$.*
5. *$\bar{P} = \{\bar{x} \in \bar{F} \mid x \in P \cap A\} = \{x + \mathfrak{m} \in A/m \mid x \in P \cap A\}$ is an ordering of the residue class field of v.*

Proof: We follow the proofs of [12] and [9] to prove the above equivalences.

(1) $\implies$ (2) : The defining property of convexity can be restated as: $\forall b \in A, \forall a \in F, 0 < a < b \implies a \in A$, via translation by $-x$ using the notation of Definition 6.6. Let $b \in A$, let $a \in F$, such that $0 < a < b$. By (1), we know that $v(a) \geq v(b)$ in Γ, and since $b \in A$, $0 \leq v(b) \leq v(a)$ by definition of A, and therefore $a \in A$.

(2) $\implies$ (3) : Suppose that $b \in \mathfrak{m}, a \in F$, such that $0 < a < b$. Then $0 < b^{-1} < a^{-1}$, with $b \in \mathfrak{m} \implies b$ not a unit in $A \implies b^{-1} \notin A$. Therefore, by convexity of A, we have $a^{-1} \notin A \implies a$ not a unit in $A \implies a \in \mathfrak{m}$.

(3) $\implies$ (4) : Let $m \in \mathfrak{m}$, suppose $1 + m \notin P$, ie: $1 + m < 0 \implies 1 < -m$ and $0 < 1$ because $1 \in P$, so: $0 < 1 < -m \implies 1 \in \mathfrak{m}$, a contradiction.

(4) $\implies$ (1) : Suppose by contradiction that there exists $a, b \in F$ such that $0 < a < b$ and $v(a) < v(b)$. Then $v(ba^{-1}) = v(b) - v(a) > 0 \implies ba^{-1} \in \mathfrak{m}$. Therefore $-ba^{-1} \in \mathfrak{m}$ and (4) gives $1 - ba^{-1} \in P \implies 1 - ba^{-1} > 0 \implies a > b$.

(3) $\implies$ (5) : Looking at Definition 4.2, properties (A) and (C) are immediately clear by definition of $\bar{P}$. We showed in at the bottom of Page 23, in Chapter 4, that if (B) does not hold for a quadratic preordering T, then $-1 \in T$. Suppose that $-1 \in \bar{P}$, that is: $-1 + \mathfrak{m} \in \bar{P}$, so that there exists $m \in \mathfrak{m}, p \in P \cap A$ such that $-1 + m = p$, ie: $p + 1 = m \in \mathfrak{m}$. But: $0 < 1 < 1 + p$, by convexity of $\mathfrak{m}$, implies that $1 \in \mathfrak{m}$, a contradiction.

(5) $\implies$ (4): Suppose by contradiction that there exists $m \in \mathfrak{m}$ such that $1 + m \notin P$. Then: $-(1 + x) \in P$ and $\overline{-1 - x} = -1 + \mathfrak{m} \in \bar{P}$, contradicting (5). $\square$

Definition 6.10 *Let P be an order of F, let v be a valuation of F. If any (and therefore all) of the conditions of Theorem 6.10 hold for P and v, then we say that v is* <u>*compatible with*</u> *P (or vice versa).*

Remark The definition used in [18, p.3] is: "An ordering P of F is said to be compatible with A (ie: with v) if $1 + at >_P 0$ for every $a \in A$." We see that this corresponds to our above definition, via condition (4) as $\mathfrak{m} = (t)$ where t a uniformizer of A.

We need one more definition from [9, p.36] before stating the Baer-Krull Theorem. Let F be a field, $v : F \to \Gamma$ a valuation on F. Then 2Γ is a (normal) subgroup of Γ, and the quotient group $\bar{\Gamma} = \Gamma/2\Gamma$ is easily seen to be an $\mathbb{F}_2$-vector space. We know that v is surjective, as is the canonical projection $\Gamma \to \Gamma/2\Gamma$, which means choosing an $\mathbb{F}_2$-basis for $\bar{\Gamma}$ gives a family of basis elements $\{v(\pi_i) + 2\Gamma, i \in I\}$ for some index set I and $\pi_i \in F^*$.

Definition 6.11 *The family of elements of F described above, ie: $\{\pi_i, i \in I\}$, is called a* <u>*quadratic*</u> <u>*system of representatives*</u> *of F with respect to v.*

Theorem 6.12 *(<u>Baer-Krull Theorem</u>:) Let F be a field, let v be a valuation on F, $\bar{F}$ the residue class field of v and fix a quadratic system of representatives $\{\pi_i, i \in I\}$ of F. There is a bijective correspondence:*

$$\{P \in \chi(F) \mid A \textit{ is } P\textit{-convex}\} \longleftrightarrow \{-1, 1\}^I \times \chi(\bar{F}), \textit{ie:}$$

$$\{P \in \chi(F) \mid P \text{ is compatible with } v\} \longleftrightarrow \{-1,1\}^I \times \chi(\bar{F}) = \{f \mid f : I \to \{-1,1\}\} \times \chi(\bar{F}).$$

This bijection is given by: $P \mapsto (sgn_{P|\{\pi_i, i\in I\}}, \bar{P})$, where $sgn_{P|\{\pi_i, i\in I\}}$ is the restriction of the sign map of P - as defined at the end of Chapter 4 - to the set $\{\pi_i, i \in I\}$.

We direct the reader to [9, §2, p.37] for a proof of this theorem. The important takeaway - insofar as Section 6.4 is concerned - is that, when A is a discrete valuation ring, there exists exactly two orderings of F which are compatible with v for every ordering of the residue class field $\bar{F}$. This is because, when $\Gamma \cong \mathbb{Z}$, we have $\Gamma/2\Gamma \cong \mathbb{Z}/2\mathbb{Z}$, an $\mathbb{F}_2$-vector space with one basis element. Therefore $|I| = 1$, so that each ordering of $\bar{F}$ corresponds to exactly two orderings of F which are compatible with v (ie: with A) by the above bijection. Finally, we need to define what it means for a discrete valuation ring A to be henselian. This simply means that Hensel's lemma holds in the ring A, and we choose a formulation of the lemma which will be most relevant to our work in Section 6.4.

Definition 6.13 *Let F be the field of fractions of a discrete valuation ring A. We say that A is henselian if the following property holds in A:*
Let $f(X) \in A[X]$, and let $f'(X)$ be the derivative of $f(X)$. Suppose there exists $a_0 \in A$ such that $f(a_0) \equiv 0 \mod \mathfrak{m}$ and $f'(a_0) \not\equiv 0 \mod \mathfrak{m}$. Then there exists $a \in A$ such that $f(a) = 0$ and $a \equiv a_0 \mod \mathfrak{m}$.

6.4 The u-invariant of a Formally Real Residue Class Field.

Let A be a discrete valuation ring with field of fractions F and residue class field $\bar{F}$, with $\text{char}(\bar{F}) \neq 2$. We end the project by exploring the first section of [18] as an interesting application of Pfister's Local-Global Principle, using the preparatory work already done in this chapter. The rest of Scheiderer's paper shows that $u_s(F) = 2u_s(\bar{F})$ for the case where $\bar{F}$ is formally real, F is not necessarily complete, and A is excellent and henselian. Here u_s denotes the strong u-invariant, defined in [18]. This extends a theorem of Harbater, Hartmann and Krashen found in [10], which proves the same result but in the case where $\bar{F}$ has no orderings. In our case, we are simply interested in establishing Proposition 5 from [18], which we state as Theorem 6.14:

Theorem 6.14 *Let A be a discrete valuation ring with field of fractions F and residue class field $\bar{F}$, assumed to be formally real. Suppose that char$(\bar{F}) \neq 2$. Then:*

(a) $u'(F) \geq 2u'(\bar{F})$;

(b) If A is henselian, then equality holds: $u'(F) = 2u'(\bar{F})$.

This result is very similar to the main theorem of [6], which can also be found in [11, §6, p.142-148]. However, these rely on the completeness of the field F. The proof contained in [11, p.145] uses Springer's theorem to recover the structure of $W(F)$ in terms of $W(\bar{F})$, to then show that $u(F) = 2u(\bar{F})$. Theorem 6.14 in [18] relies on Pfister's Local-Global Principle and the Harrison topology, and instead of completeness requires that $\bar{F}$ be formally real. This therefore makes [18] an interesting application of Chapter 5.

First, let F be the formally real fraction field of a valuation ring A, and let t be a uniformizer of A. Note that the Baer-Krull theorem shows that F is formally real if and only if $\bar{F}$ is formally real. Since, for all $a \in A$, $a = ut^n$ for some unique $u \in U, n \in \mathbb{N} \cup \{0\}$, we have that, for all $x \in F^*$, $x = wt^m$ for some unique $w \in U, m \in \mathbb{Z}$. As a result, note that any 1-dimensional form $\langle b \rangle, b \in F$ can be written in the form $\langle u \rangle$ or $\langle ut \rangle$, where $u \in U$, using $b = ut^n$ and removing squares from t^n. This means that we can write any isometry class of non-singular quadratic forms over F in the form $q = q_1 \perp \langle t \rangle \otimes q_2$ where q_1, q_2 have entries in U. For $q = \langle a_1, ..., a_n \rangle$, we denote by $\bar{q} = \langle \bar{a}_1, ..., \bar{a}_n \rangle$ its reduction modulo $\mathfrak{m}$.

Lemma 6.15 *Let A be a discrete valuation ring with formally real fraction field F, uniformizer $t \in A$, and residue class field $\bar{F} = A/tA$ of characteristic not equal to 2. Let q_0, q_1 be diagonal quadratic forms, with entries in $U = A^*$ and consider the quadratic form $q = q_0 \perp \langle t \rangle \otimes q_1$ over F. Then:*

$\bar{q}_0$ and $\bar{q}_1$ are torsion forms over $\bar{F}$ $\iff$ $sgn_P(q) = 0$ for every ordering P compatible with A.

Proof: We follow closely the proof from [18] and 'flesh out' most of the arguments. We may assume, without loss of generality, that the discrete valuation $v : F^* \twoheadrightarrow \Gamma$ is 'normed' in the sense of [3, p.392], that is, $\Gamma = \mathbb{Z}$ and therefore normalizers of A are precisely the elements of A which have valuation equal to 1. We have $\Gamma/2\Gamma = \mathbb{Z}/2\mathbb{Z}$, so if e_0 is the single basis element of $\Gamma/2\Gamma$, then 1 is a pre-image of e_0 via the canonical surjection $\Gamma \to 2\Gamma$ as $\Gamma/2\Gamma = \mathbb{Z}/2\mathbb{Z}$. Let t be a preimage of 1 via the surjective valuation, so that $v(t) = 1$ and t is therefore a uniformizer of A. By Definition 6.11, $\{t\}$ is the quadratic system of representatives of F with respect to v. Every order Q of $\bar{F}$, by the Baer-Krull Theorem, is in bijective association with exactly two orders P_0 and P_1 of F which are compatible with A, and satisfying (without loss of generality):

$$\begin{cases} \mathrm{sgn}_{P_0}(t) = 1, \mathrm{sgn}_{P_1}(t) = -1 \\ \bar{P}_0 = \bar{P}_1 = Q. \end{cases}$$

Let $i \in \{0, 1\}$. We have that $Q = \bar{P}_i = \{p + \mathfrak{m} \mid p \in A \cap P_i\}$. Therefore, for all $a \in A^\times$, $\mathrm{sgn}_Q(\bar{a}) = \mathrm{sgn}_Q(a + \mathfrak{m}) = 1 \iff a \in P_i \iff \mathrm{sgn}_{P_i}(a) =$, similarly $\mathrm{sgn}_Q(\bar{a}) = -1 \iff \mathrm{sgn}_{P_i}(a) = -1$. Since q_0, q_1 have entries in $U = A^*$, we have shown that $\mathrm{sgn}_Q(\bar{q}_0) = \mathrm{sgn}_{P_i}(q_0)$ and $\mathrm{sgn}_Q(\bar{q}_1) = \mathrm{sgn}_{P_i}(q_1)$. Finaly, note that, for $j = 0, 1$,

$$\mathrm{sgn}_{P_j}(q) = \mathrm{sgn}_{P_j}(q_0) + \mathrm{sgn}_{P_j}(t)\mathrm{sgn}_{P_j}(q_1) = \mathrm{sgn}_Q(\bar{q}_0) + (-1)^j \mathrm{sgn}_Q(\bar{q}_1).$$

This proves that: $\mathrm{sgn}_{P_0}(q) = \mathrm{sgn}_{P_1}(q) = 0 \iff 2\mathrm{sgn}_Q(\bar{q}_0) = 2\mathrm{sgn}_Q(\bar{q}_1) = 0 \iff \mathrm{sgn}_Q(\bar{q}_0) = \mathrm{sgn}_Q(\bar{q}_1) = 0$, as F has characteristic not equal to 2. As a result, for any quadratic form $q \simeq q_0 \perp \langle t \rangle \otimes q_1$, where q_0, q_1 have entries in A^*, we have:

$\bar{q}_0$ and $\bar{q}_1$ are torson forms over $\bar{F}$
$\iff$ $\mathrm{sgn}_Q(\bar{q}_0) = \mathrm{sgn}_Q(\bar{q}_1) = 0$ for all orders Q of $\bar{F}$ (by Theorem 5.20)
$\iff$ for all orders Q of $\bar{F}$, for all associated orders P_0, P_1 of $F, \mathrm{sgn}_{P_0}(q) = \mathrm{sgn}_{P_1}(q) = 0$
$\iff$ for all orders P of F compatible with $A, \mathrm{sgn}_P(q) = 0$.

□

We continue following and elaborating on the approach provided in [18] for Lemma 6.16 and its proof below.

Lemma 6.16 *Let Z be a closed subset of $\chi(F)$ which does not contain any orderings of F compatible with A. Then there exists a uniformizer t of A with $t > 0$ on Z.*

Proof: For every order $P \in Z$, we know from Theorem 6.9 that $1 + \mathfrak{m} \not\subset P$, ie: there exists $c_P \in \mathfrak{m}$ such that $1 + c_P \notin P$, ie: $-c_P >_P 1$. Let $b_P = -c_P \in \mathfrak{m}$ for each $P \in Z$. Let s_P denote the image of P under the inclusion map $\chi(F) \hookrightarrow \{\pm 1\}^{F^*}$, for a bit of clarity in what follows. We know that Z is a closed subset of $\chi(F)$, which is compact by Section 6.2, and therefore Z is compact, again using the fact that a closed subset of a compact space is compact, [15, §3, p.165]. We want to find an open cover of Z, and extract a finite subcover of Z. Let $P \in Z$. Since $b_P >_P 1$, $b_P - 1 \in P$ and $s_P(b_P - 1) = 1$, giving $s_P \in H(b_P - 1, 1) \cap \chi(F) = H(b_P - 1)$; ie: $P \in H(b_P - 1)$. Therefore: $Z \subset \bigcup_{P \in Z} H(b_P - 1)$, and because the Harrison sets are open sets, this is an open cover of Z. There exists $P_1, ..., P_n \in Z$ such that $Z \subset \bigcup_{i=1}^{n} H(b_{P_i} - 1)$. We conclude that for all $P \in Z$, there exists $i \in [\![1, n]\!]$ such that $s_P \in H(b_{P_i} - 1)$, ie: $s_P(b_{P_i} - 1) = 1$, ie: $b_{P_i} >_P 1$.
Let π be an arbitrary uniformizer of A. We know that $b_{P_i} \in \mathfrak{m} = \pi A$ for each $i \in [\![1, n]\!]$. Define:

$$t = \pi + (1 + \pi^2) \sum_{i=1}^{n} b_{P_i}^2 \in A,$$

as in [18]. Remembering that every element of A is of the form $u\pi^n, u \in A^*, n \in \mathbb{N} \cup \{0\}$, if we show that π only divides t once, then we can conclude that t is an associate of π in A and that $(t) = (\pi) = \mathfrak{m}$ as required. Note that A is a unique factorization domain by [16, §8, p.115], with π the only irreducible element of A, which is why we can talk about π diviving t only once. We have $\pi^2 \mid b_{P_i}^2, \pi^2 \mid (1 + \pi^2) \sum b_{P_i}^2$, and $\pi^2 \nmid \pi$. So $\pi^2 \nmid t$ and $\pi \mid t$, so t is a uniformizer of A. Let $P \in Z$. There exists $i \in [\![1, n]\!]$ such that $b_{P_i}^2 \geq_P b_{P_i} >_P 1$, and since $b_{P_j}^2 \geq_P 0$ for all $j \in [\![1, n]\!]$, we have that:

$$\sum_{i=1}^{n} b_{P_i}^2 >_P 1 \implies (1 + \pi^2) \sum_{i=1}^{n} b_{P_i}^2 >_P 1 + \pi^2,$$

as $1 + \pi^2 >_P 0$. By considering the three cases $\pi \geq_P 0, -1 <_P \pi <_P 0$, and $\pi \leq_P -1$, we easily check that $\pi + 1 + \pi^2 >_P 0$, and conclude that $t >_P 0$ for all $P \in Z$, as required. □

Proof: *(Proof of Theorem 6.14)*

(a) The first part of this proof is inspired from [6]. Let t be a uniformizer of A. We first need to show that, for $q \simeq q_0 \perp \langle t \rangle \otimes q_1$, with q_0, q_1 having entries in A^*, we have: $\bar{q}_0, \bar{q}_1$ anisotropic over $\bar{F} \implies q$ anisotropic over F. Suppose by contradiction that q is isotropic, for a vector $(x_1, ..., x_n, y_1, ..., y_m)$ of elements of F. Rescaling this vector by powers of t, we can assume that $x_1, ..., x_n, y_1, ..., y_m \in A$ and at least one of these elements is in A^*, remembering that elements of F are of the form $ut^k, u \in A^*, k \in \mathbb{Z}$, or equal to 0. Suppose there exists $i \in [\![1, n]\!]$ such that $x_i \in A^*$. Then $x_i \not\equiv 0 \mod \mathfrak{m}$ and $0 = \overline{q(x_1, ..., x_n, y_1, ..., y_m)} = \overline{q_0(x_1, ...,_n) + tq_1(y_1, ..., y_m)} = \bar{q}_0(\bar{x}_1, ..., \bar{x}_n)$, so $(\bar{x}_1, ..., \bar{x}_n)$ is an anisotropic vector of $\bar{q}_0$, a contradiction. Suppose now that $x_i \equiv 0 \mod \mathfrak{m}$ for all $i \in [\![1, n]\!]$, and that there exists $j \in [\![1, m]\!]$ such that $y_j \in A^*$. Therefore, t^2 divides $q_0(x_1, ..., x_n)$, and we conclude that t divides $q_1(y_1, ..., y_m)$, as $q_0(x_1, ..., x_n) + t.q_1(y_1, ..., y_m) = 0$. This yields $\bar{q}_1(\bar{y}_1, ..., \bar{y}_m) \equiv 0 \mod \mathfrak{m}$, and $(\bar{y}_1, ..., \bar{y}_m)$ is an isotropic vector of $\bar{q}_1$, a contradiction.

We now return to the proof in [18], filling out a number of details. We want to show that $u'(F) \geq 2u'(\bar{F})$. Let $q = \langle a_1, ..., a_n \rangle$ be a diagonal quadratic form over F such that $\bar{q}$ is an anisotropic torsion form over $\bar{F}$. Let $Z = \{P \in \chi(F) \mid \mathrm{sgn}_P(q) \neq 0\}$. We want to show that Z is closed, so consider $Z^c = \{P \in \chi(F) \mid \mathrm{sgn}_P(q) = 0\}$, its complement in $\chi(F)$. We can see that an order $P \in Z^c$ if and only if P is contained in an intersection of the form:

$$H(a_1, \epsilon_1) \cap ... \cap H(a_n, \epsilon_n) \cap \chi(F), \text{ where } \sum_{i=1}^{n} \epsilon_i = 0, \epsilon_i = \pm 1.$$

There are $n(n-1)...(\frac{n}{2}+1)$ such intersections, and the union of all of these intersections is equal to Z^c. This shows that Z^c is a finite union and finite intersection of open sets in $\chi(F)$, showing that Z^c is open, and that Z is closed. Given that $\bar{q}$ is torsion, Lemma 6.18 shows that Z cannot contain an order $P \in \chi(F)$ which is compatible with A, as $\mathrm{sgn}_P(q) = 0$ for such an order. Lemma 6.19 gives the existence of a uniformizer π of A such that $\pi > 0$ on Z. Consider the quadratic form $\langle 1, -\pi \rangle \otimes q = q \perp \langle -\pi \rangle \otimes q$. By the first part of this proof, knowing that $\bar{q}$ is anisotropic, we obtain that $q \perp \langle -\pi \rangle \otimes q$ is anisotropic. We want to show that $q \perp \langle -\pi \rangle \otimes q$ is torsion, and use Pfister's Local Global Principle to this end. Suppose that $P \in Z^c$. Then: $\mathrm{sgn}_P(q) = 0$ so $\mathrm{sgn}_P(q \perp \langle -\pi \rangle \otimes q) = 0$. If $P \in Z$, then $\mathrm{sgn}_P(q \perp \langle -\pi \rangle \otimes q) = \mathrm{sgn}_P(q) = \mathrm{sgn}_P(-\pi).\mathrm{sgn}_P(q) = \mathrm{sgn}_P(q) - \mathrm{sgn}_P(q) = 0$ by definition of π. Therefore, every anisotropic torsion form $\bar{q}$ over $\bar{F}$ yields an anisotropic torsion form $\langle 1, -\pi \rangle \otimes q$ over F with twice its dimension, proving that $u'(F) \geq 2u'(\bar{F})$.

(b) Let t be a uniformizer of A, let A be henselian, and recall that every (non-singular) quadratic form q is isometric to $q_0 \perp \langle t \rangle \otimes q_1$, for some q_0, q_1 having entries in A^*. Note that q is torsion $\iff \mathrm{sgn}_P(q) = 0$ for all $P \in \chi(F) \implies \mathrm{sgn}_P(q) = 0$ for all P compatible with $A \implies \bar{q}_0, \bar{q}_1$ are torsion over $\bar{F}$, using Pfister's Local-Global Principle and Lemma 6.18. If we can show that:

$$\bar{q}_0 \text{ or } \bar{q}_1 \text{ isotropic over } \bar{F} \implies q \text{ isotropic over } F,$$

then q being anisotropic and torsion requires both $\bar{q}_0$ and $\bar{q}_1$ to be anisotropic and torsion, ie: they must have dimension lower or equal to $u'(\bar{F})$ and be torsion, proving that $u'(F) \leq u'(\bar{F}) + u'(\bar{F}) = 2u'(\bar{F})$.

Suppose that $\bar{q}_0 = \langle \bar{a}_1, ..., \bar{a}_n \rangle$ is isotropic, with $a_1, ..., a_n \in A^*$. There exists $x_1, ..., x_n \in A$, (so that $\bar{x}_1, ..., \bar{x}_n \in A/\mathfrak{m}$) with $\bar{x}_i \not\equiv 0 \mod \mathfrak{m}$, such that $\bar{a}_1\bar{x}_1^2 + ... + \bar{a}_n\bar{x}_n^2 \equiv 0 \mod \mathfrak{m}$. Define $f(X) = a_1x_1^2 + ... + a_{i-1}x_{i-1}^2 + a_iX^2 + a_{i+1}x_{i-1}^2 + ... + a_nx_n^2$. Then clearly $f(x_i) \equiv 0 \mod \mathfrak{m}$ and $f'(x_i) = 2a_ix_i \not\equiv 0 \mod \mathfrak{m}$ by $a_i \in A^* = A \setminus \mathfrak{m}$, $\mathrm{char}(\bar{F}) \neq 2$, and $\bar{x}_i \not\equiv 0 \mod \mathfrak{m}$. As A is henselian, there exists $\tilde{x}_i \in A$ such that $f(\tilde{x}_i) = 0$, and therefore $(x_1, ..., x_{i-1}, \tilde{x}_i, x_{i+1}, ..., x_n)$ is an isotropic vector for q_0. This shows that q is isotropic, as required. We argue in exactly the same way if we suppose instead that q_1 is isotropic.

$\square$

References

[1] Karim Johannes Becher, *Local-global Principles over Real Fields*, University of Ghent, Gent, Belgium, 2004

[2] Karim Johannes Becher, *Supreme Pfister Forms*, University of Konstanz, 2003.

[3] Nicolas Bourbaki, *Commutative Algebra: Chapters 1-7*, Elements of Mathematics, Springer-Verlag, 2nd printing, 1989.

[4] J.W.S. Cassels, *Rational Quadratic Forms*, Academic Press, Cambridge, UK, 1978.

[5] Pete L. Clark, *Quadratic Forms: Witt's Theory*, University of Georgia, Athens, Georgia

[6] Pete L. Clark, *Quadratic Forms over Discrete Valuation Fields*, University of Georgia, Athens, Georgia

[7] Richard Elman, Tsit-Yuen Lam, *Pfister Forms and K-Theory of Fields*, Journal of Algebra, 181-213 (1972), University of California, Berkeley, California, USA, 1972.

[8] Richard Elman, Tsit-Yuen Lam, *Pfister Forms and their Applications*, Journal of Number Theory 5, 367-378 (1973), University of California, Berkeley, California, USA, 1973.

[9] Antonio J. Engler, Alexander Prestel, *Valued Fields*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2005.

[10] D. Harbater, J. Hartmann, D. Krashen, *Applications of patching to quadratic forms and central simple algebras*, Preprint.

[11] Tsit-Yuen Lam, *Algebraic Theory of Quadratic Forms*, W.A.Benjamin Inc., Massachusetts, USA, 1973.

[12] Tsit-Yuen Lam, *Orderings, Valuations and Quadratic Forms*, CBMS Regional Conference Series in Mathematics, N.52, published by AMS, 1983.

[13] D.W. Lewis, *Witt Rings as Integral Rings*, Inventiones Mathematicae Springer-Verlag, University College Dublin, Ireland, 631-633, 1987.

[14] Falko Lorenz, *Algebra Volume II: Fields with Structure, Algebras and Advanced Topics*, Springer Universitext, 2008.

[15] James R. Munkres, *Topology*, 2nd Edition, Upper Saddle River, NJ: Prentice Hall, 2000.

[16] Miles Reid, *Undergraduate Commutative Algebra*, Cambridge, New York: Cambridge UP, London Mathematical Society Students Texts, 1995.

[17] Winfried Scharlau, *Quadratic and Hermitian forms*, Springer-Verlag, Berlin, Germany, 1985.

[18] Claus Scheiderer, *The u-invariant of One-Dimensional Function Fields over Real Power Series Fields*, University of Konstanz, Konstanz, Germany, 2000.