QUADRATIC FORMS OVER FIELDS II: STRUCTURE OF THE WITT RING

PETE L. CLARK

Contents

We continue to let K denote a field of characteristic different from 2, which is "fixed" in the sense that it will not be mentioned in statements of the results.

1. The filtration on the Witt ring

At the end of Chapter 1 we defined rings $\widehat{W}(K)$ and $W(K) = \widehat{W}(K)/\langle \mathbb{H} \rangle$ and surjective ring homomorphisms

$$\dim : \widehat{W}(K) \to \mathbb{Z},$$

$$\dim_0 : W(K) \to \mathbb{Z}/2\mathbb{Z}.$$

By definition, the **augmentation ideal** $\hat{I}$ is the kernel of $\dim : \widehat{W}(K) \to \mathbb{Z}$ and similarly the **fundamental ideal** $I = I(K)$ is the kernel of $\dim_0 : W(K) \to \mathbb{Z}/2\mathbb{Z}$. (In particular, since $\mathbb{Z}/2\mathbb{Z}$ is a field, I is a maximal ideal.) Thus elements of I correspond to anisotropic quadratic forms of even dimension.

To a remarkable degree, the modern algebraic theory of quadratic forms is concerned with the filtration given by powers of the fundamental ideal:

$$W(F) \supset I \supset I^2 \supset \ldots \supset I^n \ldots.$$

We cannot resist mentioning the following beautiful result right away: although we are far from having assembled enough machinery to prove it, it is extremely useful in understanding the big picture on the fundamental filtration.

Theorem 1. *(Arason-Pfister Haupsatz, 1971) Let q be a nontrivial anisotropic quadratic form. If $q \in I^n$, then $\dim q \geq 2^n$.*

Corollary 2. *The Witt ring is separated for the I-adic topology: $\bigcap_{n \geq 1} I^n = 0$.*

Proof. Indeed, a nonzero element of the intersection would represent a notnrivial anisotropic form of dimension at least 2^n for all $n \in \mathbb{Z}^+$: absurd. □

In particular, it is of interest to compute the successive quotients $\frac{I^n}{I^{n+1}}$. Note that each I^n/I^{n+1} is a $W(F)/I = \mathbb{Z}/2\mathbb{Z}$-module, i.e., an abelian group in which each nonzero element has order 2.

By Corollary 2, for a nontrivial anisotropic quadratic form q, there exists a unique $n \in \mathbb{N}$ such that $f \in I^n \setminus I^{n+1}$, and thus we may consider the element $\iota_n(f) := f + I^{n+1} \in I^n/I^{n+1}$ as a nontrivial **invariant** of f.

Let us try on this philosophy for size. If $q \in I^0 \setminus I^1$, then q has odd dimension, and $\iota_0(q)$ is simply the unique nontrivial element of $\mathbb{Z}/2\mathbb{Z}$. This is apparently not so interesting, but in fact already this allows us to deduce some useful facts.

Proposition 3. *Let* $\mathfrak{p}$ *be a prime ideal of the* $W(K)$.
a) If the integral domain $W(K)/\mathfrak{p}$ *has characteristic* 0*, then* $W(K)/\mathfrak{p} \cong \mathbb{Z}$ *(so* $\mathfrak{p}$ *is not maximal).*
b If the integral domain $W(K)/\mathfrak{p}$ *has positive characteristic* p*, then* $W(K)/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$ *(so* $\mathfrak{p}$ *is maximal).*

Proof. For any $a \in K^\times$ we have an identity

$$(\langle a \rangle + \langle 1 \rangle)(\langle a \rangle - \langle 1 \rangle) = \langle a \rangle \otimes \langle a \rangle - \langle 1 \rangle = \langle a^2 \rangle - \langle 1 \rangle = \langle 1 \rangle - \langle 1 \rangle \equiv \langle 1, -1 \rangle \equiv 0.$$

Writing $\overline{a}$ for the class of $\langle a \rangle$ in $W(K)/\mathfrak{p}$, since this quotient ring is a domain we have $\overline{a} = \pm 1$. Since $W(K)$ is additively generated by the unary forms $\langle a \rangle$, $W(K)/\mathfrak{p}$ is additively generated by 1, i.e., is a cyclic group, either infinite or of prime order. □

Proposition 4. *The unique prime ideal* $\mathfrak{p}$ *of* $W(K)$ *such that* $W(K)/\mathfrak{p}$ *has characteristic* 2 *is the fundamental ideal* I.

Proof. Let $\mathfrak{p}$ be a prime ideal such that $W(K)/\mathfrak{p}$ has characteristic 2. Then by Proposition 3 we in fact have that for all $a \in K^\times$, $\overline{a} = 1$ in $W(K)/\mathfrak{p}$ (by our assumption that the residue characteristic is 2, the distinction between 1 and -1 disappears!). But then this means that reduction modulo $\mathfrak{p}$ sends a quadratic form q to its dimension mod 2, whence the kernel is none other than I itself. □

Now we press on. Suppose $q \in I$, i.e., q has even dimension. We wish to define a natural "invariant" of f landing in I/I^2. Well, let's cheat: what invariants of quadratic forms taking values in elementary 2-groups do we already know? Exactly one: the discriminant $d(q) \in K^\times/K^{\times 2}$.

A little thought shows that something is slightly awry here: although the discriminant is a well-defined additive homomorphism from $\widehat{W}(K) \to K^\times/K^{\times 2}$, since the hyperbolic plane has discriminant -1, then (unless -1 is a square in K, a hypothesis that we certainly do not wish to impose), the discriminant *does not* factor through $W(K)$.

This is disappointing, but do not lose heart. In the words of Lam, "[T]here exists an ingenious way to remedy this." Namely, for an n-dimensional quadratic form q, we define its **signed determinant**

$$d_\pm(q) = (-1)^{\frac{n(n-1)}{2}} d(q) \in K^\times/K^{\times 2}.$$

In other words, if $\dim q \equiv 0, 1 \pmod 4$, then $d_\pm(q) = d(q)$, whereas if $\dim q \equiv 2, 3 \pmod 4$, $d_\pm(q) = -d(q)$. In particular, $d_\pm(\mathbb{H}) = 1$.

So does $d_\pm$ factor through $W(F)$? No, still not quite. The problem is that $d_\pm$ is now not necessarily a homomorphism. What we have is

$$d_\pm(q \oplus q') = \epsilon d_\pm(q) d_\pm(q'),$$

where $\epsilon \in \{\pm 1\}$ depends only on the dimensions of q and q' mod 4. For instance, if $\dim q \equiv \dim q' \equiv 1 \pmod 4$, then $\epsilon = 1$. However, if $\dim q$ and $\dim q'$ are both even, then one sees easily that $\epsilon = 1$. It follows that $d_\pm : \hat{I} \to K^\times/K^{\times 2}$ is a (clearly surjective) group homomorphism, which factors through a surjective homomorphism $d_\pm : I \to K^\times/K^\times$. Our task is now to show that the kernel of $d_\pm$ is precisely I^2.

For one direction, recall Corollary 1.30, which says that I is additively generated by classes of binary forms $\langle 1, -a\rangle$. So I^2 is generated by classes of quaternary forms

$$\langle 1, -a\rangle \otimes \langle 1, -b\rangle = \langle 1, -a, -b, ab\rangle.$$

The discriminant of such a quaternary form is $1 \cdot -a \cdot -b \cdot ab = a^2b^2 \equiv 1 \pmod K)^{\times 2}$. Thus $I^2 \subset \ker(d_\pm)$. Thus $d_\pm$ factors through a surjective homomorphism $\alpha : I/I^2 \to K^\times/K^\times$. To show that α is an isomorphism we will construct the inverse! Namely, define $\beta : K^\times/K^{\times 2}$ by $\beta : a \mapsto \langle 1, -a\rangle$. Then we have (denoting equivalence in the Witt ring by $\equiv$)

$$\beta(a) + \beta(b) - \beta(ab) \equiv \langle 1, -a, 1, -b, -1, ab\rangle \equiv \langle 1, -a, -b, ab\rangle \in I^2,$$

so β is a homomorphism. It is easy to see that $\alpha \circ \beta = 1$. Moreover, the relation $\beta(\alpha q) = q$ holds for q of the form $\langle 1, -a\rangle$ which is a set of generators for I/I^2, so we must have $\beta \circ \alpha = 1$. Thus α and β are inverse isomorphisms, and we have proved:

Theorem 5. *The signed determinant induces an isomorphism of groups*

$$d_\pm : I/I^2 \xrightarrow{\sim} K^\times/K^{\times 2}.$$

It follows that we have an extension of abelian groups

$$0 \to I/I^2 \to W(K)/I^2 \to W(K)/I \to 0.$$

Thus we have an extension

$$1 \to K^\times/K^{\times 2} \to W(K)/I^2 \to \mathbb{Z}/2\mathbb{Z} \to 0.$$

A splitting of this sequence amounts to the existence of an odd-dimensional anisotropic form q such that $d_\pm(q \oplus q) = 1$. But since q is odd dimensional, $\dim q \oplus q \equiv 2 \pmod 4$, so $d_\pm(q \oplus q) = -1 d(q \oplus q) = -d(q)^2 = -1$, so this happens iff $-1 \in K^{\times^2}$. In the general case, we define an explicit extensoin of $\mathbb{Z}/2\mathbb{Z}$ by $K^\times/K^\times$, called $Q(K)$, by the following twisted group law:

$$(x, y) \star (x', y') = (xx' \cdot (-1)^{y+y'}, y + y').$$

Now a straightforward calculation gives the following important result.

Theorem 6. *(Pfister) The set map*

$$(\dim_0, d_\pm) : M(K) \to Q(K)$$

is a monoid homomorphism, inducing a group isomorphism $W(K)/I^2 \cong Q(K)$.

Exercise: Prove Proposition 6.

An immediate, but important, consequence of this is the following

Corollary 7. *(Pfister) I^2 consists of classes of even dimensional forms q with $d(q) = (-1)^{\frac{n(n-1)}{2}}$.*

In turn, we deduce the following.

Corollary 8. *A nontrivial anisotropic form $q \in I^2$ has dimension at least 4.*

Proof. By virtue of being in I, the dimension of q must be even, so it remains to see that q cannot have dimension 2. But a 2-dimensional form in I^2 has $d(q) = -d_{\pm}(q) = -1$, thus (Exercise 1.XX) $q \cong \mathbb{H}$ and is therefore isotropic. □

Theorem 9. *(No u-invariant 3) If K admits an anisotropic ternary form, it admits an anisotropic quaternary form.*

Proof. Let q be an anisotropic ternary quadratic form, say of discriminant d. Consider the unary quadratic form $q' = \langle -d \rangle$. Then q and q' have the same mod 2 dimension and the same signed discriminant but represent distinct elements of $W(K)$, so by Theorem 8 there exists $q'' := q - q' \in I^2 \setminus 0$. Therefore q is a nontrivial anisotropic form in I^2, so by Corollary 8 it has dimension at least 4. □

Theorem 10. *For a field K, TFAE:*
(i) $\widehat{W}(K)$ is Noetherian.
(ii) $W(K)$ is Noetherian.
(iii) $K^\times / K^{\times 2}$ is finite.

Proof. Quotients of Noetherian rings are Noetherian, so (i) $\Longrightarrow$ (ii). (ii) $\Longrightarrow$ (iii): if $W(K)$ is Noetherian, then the fundamental ideal I is a finitely generated R-module, so $I/I^2 \cong K^\times / K^{\times 2}$ is a finitely generated $R/I = \mathbb{Z}/2\mathbb{Z}$-module, which simply means that it is a finite $\mathbb{Z}/2\mathbb{Z}$-vector space. (iii) $\Longrightarrow$ (i): by diagonalization, $\widehat{W}(K)$ is additively generated by unary forms $\langle a \rangle$ for $a \in K^\times / K^{\times 2}$. Thus if $K^\times / K^{\times 2}$ is finite, then $\widehat{W}(K)$ is finitely generated as a $\mathbb{Z}$-module, hence certainly a Noetherian ring. □

2. Some Witt Ring Computations

It would now be natural to ask for a description of the quotient I^2/I^3. But this turns out to be more intricate than the preceding cases, to the extent that a study of certain other algebraic objects is a prerequisite. It is interesting to pause here and see some applications of the apparently modest machinery we have already developed to the computation of Witt rings.

To begin at the beginning:

Proposition 11. *For a field K, TFAE:*
(i) K admits no quadratic field extensions ("quadratically closed").
(ii) $K^\times = K^{\times 2}$.
(iii) There is a (unique!) ring isomorphism $W(K) = \mathbb{Z}/2\mathbb{Z}$.
(iv) $I = 0$.
(v) $I = I^2$.

Proof. (i) $\iff$ (ii) is basic field theory. Over any field, we have the trivial anisotropic form and the one-dimensional forms, which correspond to $K^\times/K^{\times 2}$. If K is quadratically closed, this gives two anisotropic forms so far. (ii) $\implies$ (iii): if K is quadratically closed, every equation $x^2 = a$ for $a \in K^\times$ has a solution, so every 1-dimensional form is universal and thus every 2-dimensional form is isotropic. It follows that $\#W(K) = 2$ and then that $W(K) = \mathbb{Z}/2\mathbb{Z}$, the unique ring with two elements. (iii) $\implies$ (iv) follows from the fact that $W(K)/I \cong \mathbb{Z}/2\mathbb{Z}$. (iv) $\implies$ (v) is clear. Finally, in general we have $I/I^2 \cong K^\times/K^{\times 2}$, so (v) $\implies$ (ii). □

Let us reexamine the computation of $W(\mathbb{R})$ in light of our recently acqiuired knowledge. It follows from Sylvester's Law of Nullity (Theorem 1.25) that representatives for the nontrivial anisotropic quadratic forms are $n\langle 1\rangle$ for $n \in \mathbb{Z}^+$ and $n\langle -1\rangle$ for $n \in \mathbb{Z}$. In the Witt ring, $\langle -1\rangle \equiv -\langle 1\rangle$, so that as an abelian group $W(\mathbb{R}) \cong \mathbb{Z}$. Since $(m\langle 1\rangle) \otimes (n\langle 1\rangle) = mn\langle 1\rangle$, it follows easily that indeed $W(\mathbb{R}) \cong \mathbb{Z}$ as a ring. Moreover, since $W(\mathbb{R})/I \cong \mathbb{Z}/2\mathbb{Z}$, this means that $I = 2\mathbb{Z}$ and thus $I^n = 2^n\mathbb{Z}$ for all $n \in \mathbb{Z}^+$. It follows that for all n, $I^n/I^{n+1} \cong \mathbb{Z}/2\mathbb{Z}$. For $n = 1$ we can corroborate this as follows:

$$I/I^2 \cong \mathbb{R}^\times/\mathbb{R}^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}.$$

Thus we have an example of a field in which for all $n > 0$, $I^n \neq 0$, however in a very simple way. Soon enough we will generalize this example by showing that any *ordering* on a field gives rise to a surjective ring homomorphism $W(K) \to \mathbb{Z}$.

Our next order of business is to compute the Witt ring of a finite field $\mathbb{F}_q$ (for q odd, of course). As in Exercise X.X, the key classical fact here is that any binary quadratic form over a finite field is universal. This is a very special case of the Chevalley-Warning theorem (CITE), but in this case there is a very agreeably short, elementary proof. Namely, we may assume that $q = ax^2 + by^2$ for $ab \in \mathbb{F}_q^\times$, and let $c \in \mathbb{F}_q^\times$. We are trying to "solve the equation $ax^2 + by^2 = c$ for $x, y \in \mathbb{F}_q$. Solving for x^2 (why not?) gives

$$x^2 = \frac{1}{a}\left(c - by^2\right).$$

Now, as x ranges over all elements of $\mathbb{F}_q$, evidently x^2 takes on exactly $\frac{q-1}{2} + 1 = \frac{q+1}{2}$ distinct values. A moment's thought shows that, similarly, as y ranges over all elements of $\mathbb{F}_q$, $\frac{1}{a}\left(c - by^2\right)$ takes on exactly $\frac{q+1}{2}$ distinct values. If these sets of values were disjoint, then we would have $\frac{q+1}{2} + \frac{q+1}{2} = q + 1$ different elements of $\mathbb{F}_q$ – too many!

Just to give a name to this general property of fields, say that a field K is **quadratically C^1** if every binary form over K is universal (equivalently, every ternary form is anisotropic). Now the key observation:

Proposition 12. *For a quadratically C^1 field K, $I^2 = 0$.*

Proof. Indeed, if not, then by Corollary 8, there is an anisotropic form of dimension at least 4. This is a contradiction, with one dimension to spare! □

So:

Theorem 13. *Let K be a quadratically C^1 field. Then:*
a) $W(K) = Q(K)$ is an extension of $\mathbb{Z}/2\mathbb{Z}$ by $K^\times/K^{\times 2}$, split iff $-1 \in K^\times$.

b) Let q_1 and q_2 be nontrivial anisotropic forms. Then $q_1 \cong q_2$ iff $\dim(q_1) = \dim(q_2)$ and $d(q_1) = d(q_2)$.

Proof. Since $I^2 = 0$, part a) follows immediately from Theorem 6. As for part b), it is certainly always the case that congruent anisotropic forms have equal mod 2 dimension and discriminant. Conversely, assume that their mod 2 dimensions and discriminants agree. Then since K is quadratically C^1, q_1 and q_2 both have dimension 1, in which case having equal discriminants means they are congruent, or both have dimension 2, equal discriminant d and are both universal, so each is congruent to $\langle 1, d\rangle$ (Exercise 1.X). □

Corollary 14. *Let $\mathbb{F}_q$ be a finite field.*
a) If $q \equiv 1 \pmod 4$, then $W(K)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}[t]/(t-1)^2$.
b) If $q \equiv 3 \pmod 4$, then $W(K)$ is isomorphic to the ring $\mathbb{Z}/4\mathbb{Z}$.

Proof. In each case, since $\mathbb{F}_q^\times$ is cyclic of even order, $\mathbb{F}_q^\times/\mathbb{F}_q^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$, so by Theorem 13, $W(K)$ is, as an abelian group an extension of $\mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}/2\mathbb{Z}$. Moreover, the extension is split iff -1 is a square in $\mathbb{F}_q$ iff $q \equiv 1 \pmod 4$.
Case 1: $q \equiv 3 \pmod 4$, then $W(K) \cong \mathbb{Z}/4\mathbb{Z}$ as an abelian group. To show that this is indeed an isomorphism of rings, it suffices to check that the multiplicative identity does indeed have additive order 4, or even that $2 \cdot \langle 1\rangle = x^2 + y^2$. But the sum of two squares form is hyperbolic iff -1 is a square in K, which we have assumed it isn't.
Case 2: $q \equiv 1 \pmod 4$. Then $W(K) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Among commutative unital rings with this underlying abelian group, it is easy to see that there are 2: the direct product $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and the nonreduced local ring $\mathbb{Z}/2\mathbb{Z}[t]/(t-1)^2$. In the former case there would be two maximal ideals of residue characteristic 2, contradicting Proposition 4. Thus it must be the latter case that obtains. □

Other quadratically C^1 fields: a function field in one variable over an algebraically closed field, a Laurent series field over an algebraically closed field, a Henselian valued field with algebraically closed residue field. To pick a simple example:

Corollary 15. *Let C be an algebraically closed field of characteristic different from 2. Then $W(C((t))) \cong \mathbb{Z}/2\mathbb{Z}[t]/(t-1)^2$.*

Proof. Indeed $C((t))$ is a quadratically C^1 field in which -1 is a square, so by Theorem 13a) as additive groups we have $W(C((t)) \cong C((t))^\times/C((t))^{\times 2} \times \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z})^2$. The same argument as in the proof of Corollary 14 allows us to conclude that the ring structure is

$$W(C((t)) \cong \mathbb{Z}/2\mathbb{Z}[t]/(t-1)^2.$$

□

The reader with a very strong algebra background will recognize that every field in the above list of quadratically C^1 fields has vanishing Brauer group. This is a clue that our next invariant I^2/I^3 should have something to do with division algebras over K. Our next major task is to motivate – for all readers! – the connection between quadratic forms and the simplest and best understood class of division algebras, the (nonsplit) **quaternion algebras**.

3. Some Witt Kernel computations

Let L/K be a field extension. If (V, q) is a quadratic space over K, then we may **extend scalars** to get a quadratic space $(V, q)_{/L}$ over L. Namley, we take the underlying vector space to be $V_L = V \otimes_K L$ and we put $q(v \otimes \alpha) := \alpha^2 q(v)$. If $e_1, \ldots, e_N$ is a K-basis for V, then it is also an L-basis for V_L and the Gram matrix M of the associated bilinear form $B_L(x, y) = \frac{1}{2}(q_L(x + y) - q_L(x) - q_L(y))$ is the same as the Gram matrix of (V, q). In particular, $(V, q)_{/L}$ is nonsingular iff (V, q) is nonsingular.

In the language of quadratic polynomials, scalar extension is yet more straighforward: we have a natural inclusion of polynomial rings $K[x] \hookrightarrow L[x]$ by which we may view any homogeneous quadratic polynomial with K-coefficients as a homogeneous quadratic polynomial with L-coefficients.

This scalar extension process $q \mapsto q_L$, since it preserves nonsingularity, induces a map on Witt-Grothendieck rings $\widehat{W}(K) \to \widehat{W}(L)$. It is easy to see that this is in fact a homomorphism of rings. Moreover, certainly $\mathbb{H}_L = \mathbb{H}$ – i.e., this homomorphism carries the hyperbolic plane to itself. Therefore it induces a homomorphism on Witt rings

$$\Phi_K^L : W(K) \to W(L).$$

The functorial perspective on Witt rings is as follows: not only do we want to understand the Witt ring of any given field K, but we wish to understand the homomorphisms $W(K) \to W(L)$ induced by all field extensions L. Especially, we wish to compute the **Witt kernel** $\ker \Phi_K^L$. This consists of quadratic forms over K which become hyperbolic over L. On the other hand, especially from an arithmetic geometric perspective, it is just as interesting if not more so to determine which anisotropic quadratic forms over K become isotropic over L. In general the latter is a more delicate question.

There is, however, one situation in which we can speak of anisotropy directly and then formally deduce the Witt kernel. Namely, say a field extension L/K is **anisotropic** if for every anisotropic quadratic form q over K, the extension $q_{/L}$ to L remains anisotropic.

Lemma 16. *If L/K is an anistropic extension, then the Witt kernel is trivial.*

Proof. Suppose on the contrary that there exists a nonhyperbolic quadratic form q over K such that $q_L \cong \mathbb{H}^n$. As for any nondegenerate quadratic form, we may write q as the direct sum of an anistropic form q' (the anistropic core) and some number of hyerbolic planes. By our assumption, q' is nontrivial. Then $[q] = [q']$ in the Witt ring, so $[q']$ is a nontrivial element of the Witt kernel. □

Proposition 17. *For any field K, let $K(t)$ be the univariate rational function field over K. Then $K(t)/K$ is an anistropic extension.*

Proof. Step 1: Let K be any field, and let $(f_1, \ldots, f_n) \in K(t)^n$ be an n-tuple of rational functions, not all zero. Then there exists a nonzero rational function f such that $(ff_1, \ldots, ff_n)$ is a **primitive vector** in $K[t]$, i.e., each $ff_i \in K[t]$ and $\gcd(ff_1, \ldots, ff_n) = 1$. Indeed this holds with $K[t]$ and $K(t)$ replaced by any UFD (even GCD-domain) and its fraction field.

Step 2: Let $q = a_1 x_1^2 + \ldots + a_n x_n^2$ be a nonsingular quadratic form over K such that $q_{K(t)}$ is isotropic: that is, there exist rational functions $f_1, \ldots, f_n$, not all zero, such that

$$a_1 f_1^2 + \ldots + a_n f_n^2 = 0.$$

Let $f \in K(t)^\times$ be the rational function as in Step 1; then multiplying through by f^2 we get a primitive polynomial solution, i.e., there exist polynomials $p_1(t), \ldots, p_n(t) \in K[t]$ with $\gcd(p_1(t), \ldots, p_n(t)) = 1$ and

$$a_1 p_1(t)^2 + \ldots + a_n p_n(t)^2 = 0.$$

Now we substitute $t = 0$ (or any value of K): we cannot have $p_1(0) = \ldots = p_n(0) = 0$, because then all of the p_i's would be divisible by t, contradicting primitivity. Therefore $q(p_1(0), \ldots, p_n(0)) = 0$ shows that q is isotropic over K. □

Corollary 18. *A purely transcendental extension L/K is an anisotropic extension.*

Exercise X.X: Prove Corollary 18.

Remark: The proof of Proposition X.X used only that q was a form – i.e., a homogeneous polynomial – not that it was a *quadratic* form. Indeed any system of homogeneous polynomials would work as well, so the argument really shows: if $V_{/K}$ is a projective variety which has a $K(t)$-rational point, then it has a K-rational point.[1]

Theorem 19. *(Springer) Let L/K be a field extension of finite* odd *degree d. Then L/K is anisotropic.*

Proof. We go by induction on the degree, the case $d = 1$ being trivial. Suppose the result holds for all field extensions of odd degree less than d, and L/K be an extension of odd degree d. If L/K had any proper subextension, then we would be done by a dévissage argument. So we may assume in particular that L is monogenic over K: $L = K[x]$. Let $p(t) \in K[t]$ be the minimal polynomial of x. Let q be an anisotropic quadratic form over K which becomes isotropic over L: i.e., there exists an equation

$$q(g_1(t), \ldots, g_n(t)) = h(t)p(t) \tag{1}$$

with polynomials $g_i, h \in K[t]$, not all $g_i = 0$, and $M := \max \deg g_i \leq d-1$. As in the proof of Proposition 17, we may also assume that $(g_1, \ldots, g_n)$ is a primitive vector in $K[t]$. Since q is anisotropic, the left hand side of (1) has degree $2M \leq 2d-2$, so $\deg h$ is *odd* and at most $d-2$. In particular, h has an irreducible factor $\tilde{h}$ of odd degree at most $d-2$; let y be a root of $\tilde{h}$ in $\overline{K}$. Taking $t = y$ in (1), we see that $q(g_1(y), \ldots, g_n(y)) = 0$. Note that since $K[t]$ is a PID, the condition $\gcd(g_1, \ldots, g_n) = 1$ is equivalent to the fact that $1 \in \langle g_1, \ldots, g_n \rangle$, which implies that the polynomials $g_1, \ldots, g_n$ remain setwise coprime as elements of $K[y][t]$. In particular, not all $g_i(y)$ are equal to 0, so that $q_{K[y]}$ is isotropic. By induction, this implies that q was isotropic, contradiction! □

[1] The same conclusion can be shown for arbitrary varieties over any infinite field, or for complete varieties over a finite field. I don't know whether it is true for arbitrary varieties over a finite field.

Remark: Recall from [FT, §11] that a field is formally real if for all $n \in \mathbb{Z}^+$, the sum of n squares form $[n]\langle 1\rangle$ is anisotropic. Thus as a special case of Springer's Theorem, an odd degree extension of a formally real field remains formally real. This was proved as [FT, Prop. 95] and indeed we have essentially reproduced the argument given there.

Let us now turn things around and ask what properties are implied by an anisotropic extension of fields L/K. Note that an element of the Witt Kernel must be even-dimensional, so let's look at the simplest case: which binary forms lie in $\ker \Phi_K^L$? By Exercise X.X, a binary form is isometric to the hyperbolic plane iff it has discriminant -1. Therefore the form $\langle a, b\rangle$ lies in $\ker \Phi_K^L$ iff $-ab \in L^{\times 2}$ and represents a nontrivial element if $-ab \in K^\times \setminus K^{\times 2}$. In other words, the polynomial t^2+ab is irreducible over K but has a root over L: this happens iff $L \supset K(\sqrt{-ab})$. In particular, there are no anisotropic binary forms in the Witt kernel if K is algebraically closed in L or if L/K has odd degree (the latter being consistent with Springer's theorem).

On the other hand, suppose that $L = K(\sqrt{a})$ *is* a quadratic extension. Then a nontrivial element of the Witt kernel is given by the binary form $\alpha = \langle 1, -a\rangle$. Since the Witt kernel is an ideal, it follows that the entire principal ideal $\alpha W(K)$ lies in the Witt kernel. Remarkably, we have equality:

Theorem 20. *For $a \in K^\times \setminus K^{\times 2}$, the kernel of the canonical map $W(K) \to W(K(\sqrt{a}))$ is the principal ideal $\alpha W(K)$.*

We will need the following result in the proof.

Lemma 21. *Let K be a field and $L = K(\sqrt{a})$. Let q be an anisotropic form over K. Then q becomes isotropic over L iff q contains a binary subform isometric to $\langle b\rangle \cdot \alpha$ for some $b \in K^\times$.*

Proof. Certainly $\langle b\rangle \cdot \alpha$ becomes hyperbolic over L, so if q contains such a subform it becomes isotropic over L. Conversely, write $q = \langle b_1, \ldots, b_n\rangle$ and suppose that q_L is isotropic, so there exists an equation

$$\sum_{i=1}^n b_i (x_i + y_i\sqrt{a})^2 = 0$$

with $x_i, y_i \in K$ and not all zero. Equating the rational and irrational parts, we get

$$\sum_{i=1}^n b_i x_i^2 + a \sum_{i=1}^n b_i y_i^2 = 0 \tag{2}$$

and

$$\sum_{i=1}^n b_i x_i y_i = 0. \tag{3}$$

Now (3) expresses the orthogonality of the vectors $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in the quadratic space (K^n, q), whereas (2) implies $q(x) = -aq(y)$. Since q is anisotropic, we get $x = 0 \iff q(x) = 0 \iff q(y) = 0 \iff y = 0$, but by assumption x and y cannot both be zero, hence neither of them are zero. Therefore q contains the binary form

$$\langle q(x), q(y)\rangle = \langle -aq(y), q(y)\rangle \equiv q(y) \cdot \alpha.$$

□

Now we give the *proof* of Theorem 20. We claim that for any anisotropic form q in the Witt kernel, we have $q \cong \alpha \otimes q'$ for some quadratic form q': this certainly suffices to prove the theorem. Recall that $\dim q$ is necessarily even. We prove the result by induction on $m = \frac{\dim q}{2}$, the case $m = 0$ being trivial. By Lemma 22, there is a quadratic form r and an isometry $q \cong \langle b \rangle \cdot \alpha \oplus r$. By Witt Cancellation, r becomes hyperbolic over $L = K(\sqrt{a})$. By induction, this gives us r' such that $r \cong r' \otimes \alpha$ and thus

$$q \cong \langle b \rangle \cdot \alpha \oplus (r' \otimes \alpha) \cong (\langle b \rangle \oplus r') \otimes \alpha.$$

□

Corollary 22. *Let q be a quadratic form over K of dimension $2m$ that becomes hyperbolic over $L = K(\sqrt{a})$. Then:*
a) $-a \cdot q \cong q$.
b) If q is anistropic, then $d(q) = (-a)^m$ and $d_{\pm}(q) = a^m$.
c) If q also becomes hyperbolic over $K(\sqrt{-a})$, then $2q = 0 \in W(K)$.

Proof. a) By Theorem 20, we may write $q = [r]\mathbb{H} \oplus (q' \otimes \alpha)$ for some q'. But $-a \cdot \mathbb{H} \cong \mathbb{H}$ and $-a \cdot \alpha = \langle -a, 1 \rangle \cong \alpha$, we have $-a \cdot q \cong q$.

b) If q is anisotropic, $r = 0$ and $q \cong q' \otimes \alpha$. A computation gives

$$d(q) = (-a)^m, d_{\pm}(q) = (-1)^m d(q) = a^m.$$

c) Suppose that q is also hyperbolic over $K(\sqrt{-a})$. If $\sqrt{-a} \in K$, then q is hyperbolic over K, i.e., $q = 0 \in W(K)$. If $K(\sqrt{-a}) \supsetneq K$, then applying part a) with $L = K(\sqrt{-a})$, we get $a \cdot q \cong q$, so $2q \cong q + q \cong (a \cdot q) + (-a \cdot q) = \langle a, -a \rangle \cdot q = \mathbb{H} \cdot q = 0 \in W(K)$. □

In fact Corollary 22c) is the result that we really want – it will be used later on in the proof of Pfister's Local-Global Principle, the biggest single theorem in this chapter. Thus, although there is certainly much more to be said about Witt kernels – e.g., finite extensions of degree $2m > 2$, nonrational function fields – we press on to the next topic.

4. Orderings and quadratic forms

In looking over the simple Witt ring computations of the previous section, one sees that sometimes the Witt ring is (as an additive group) torsion and sometimes it is not. In particular, over the real numbers, for any $n \in \mathbb{Z}^+$, the sum of n squares form $n\langle 1 \rangle$ is anistropic, since indeed a sum of real squares cannot be zero unless every element is zero.

This argument extends to all formally real fields. A field K is **formally real** if it satisfies either of the following equivalent conditions:

(FR1) There does not exist $n \in \mathbb{Z}^+$ and $x_1, \ldots, x_n \in K$ such that $-1 = x_1^2 + \ldots + x_n^2$.
(FR2) For all n, if $x_1^2 + \ldots + x_n^2 = 0$, then $x_1 = \ldots = x_n = 0$.

Formally real fields play an important role in general field theory: indeed, see

[FT, Ch. 11] for an introduction.[2]

Hand in hand with the notion of formal reality is that of ordered fields. An **ordering** on a field K is a total ordering $<$ on the underlying set of K which is compatible with the field axioms in the sense that it satisfies the following properties:

(OF1) $\forall x_1, x_2, y_1, y_2 \in K$, $x_1 \leq x_2$, $y_1 \leq y_2 \implies x_1 + y_1 \leq x_2 + y_2$.
(OF2) $\forall x, y \in K$, $x, y \geq 0 \implies xy \geq 0$.

For an ordering $<$ on a field K, we may consider the associated **positive cone**

$$P = P_< = \{x \in K \mid x > 0\}.$$

The positive cone of any ordering satisfies the following properties:

(PC1) $P + P \subset P$,
(PC2) $P \cdot P \subset P$,
(PC3) $P \cup (-P) = K^\times$,
(PC4) $P \cap (-P) = \emptyset$,

and conversely, any subset $P \subset K$ satisfying these four axioms is the positive cone of a unique ordering on K. Thus there is no mathematical loss in identifying an ordering with its positive cone, and at times it is convenient to do so.

For a field K, we define the set of sums of squares of elements of K:

$$\Sigma_\square = \{x_1^2 + \ldots + x_n^2 \mid x_1, \ldots, x_n \in K\}$$

and also

$$\Sigma_\square^\bullet = \Sigma_\square \setminus \{0\},$$

the set of nonzero sums of squares. It is easy to see that $\Sigma_\square^\bullet$ lies in the positive cone of any ordering on K. On the other hand, $-1 < 0$, so in any ordered field -1 is not a sum of squares. That is, ordered fields are formally real. This is all quite straightforward to prove. The converse, that any formally real field admits at least one ordering, is a celebrated theorem of Artin-Schreier [FT, Thm. 92].

Let $q = a_1x_1^2 + \ldots + a_nx_n^2$ be a nonsingular diagonal quadratic form. Suppose that K admits an ordering $<$ such that $a_i > 0$ for all i. Then, again, q represents a nontorsion element of $W(K)$, i.e., every positive integer multiple $[n]q$ is anisotropic, since for all $x = (x_1, \ldots, x_n) \in K^n$, $q(x) = a_1x_1^2 + \ldots + a_nx_n^2 \geq 0$, with equality iff $x = 0$. (Of course, the same holds if all of the coefficients of q are negative with respect to the ordering: in fancy language, anisotropy of forms is a similarity invariant.)

If $(K, <)$ is an ordered field and F is a subfield of K, then $<$ restricts to an ordering of F. So, for instance, the sum of n squares form is also anisotropic over $\mathbb{Q}$, or any number field which admits a real embedding.

[2] As a general rule, we will recall definitions and statements of results here, but for proofs the reader is referred to *loc. cit.*.

Example: Let $K = \mathbb{Q}(\sqrt{2})$, and consider the binary quadratic form $q(x,y) = (1+\sqrt{2})x^2 + y^2$. This form is a nontorsion element of the Witt group of K becase in the ordering $<_1$ on K in which $\sqrt{2} > 0$, all its coefficients are positive. Note though that there is another ordering $<_2$ on K– in which $\sqrt{2} < 0$ – with respect to which the form is "indefinite": i.e., it has both positive and negative coefficients.

Exercise: Let K be a number field with $r > 0$ real embeddings $\iota_1, \ldots, \iota_r : K \hookrightarrow \mathbb{R}$(recall that these correspond to real roots of any minimal polynomial $P(t)$ for K). Define the **total signature** $\Sigma(q)$ of q to be the vector $(\sigma(\iota_1(q)), \ldots, \sigma(\iota_r(q)),$ where $\sigma(f)$ denotes the signature of a real quadratic form. Show that for any $s \in \mathbb{Z}^r$, there exists a quadratic form q over K with total signature $\Sigma(q) = s$. (Hint: Artin-Whaples approximation.)

The following result will be useful for us.

Theorem 23. *a) For a nonzero element x of K, TFAE:*
(i) x is positive with respect to every ordering on K.
(ii) $x \in \Sigma_\square$, i.e., x is a sum of squares.
b) It follows that if K is not formally real, $\Sigma_\square = K^\times$.

Proof. This is [FT, Cor. 94]. □

The following is an immediate consequence.

Corollary 24. *For a field K, the following are equivalent:*
(i) K admits a unique *ordering.*
(ii) The set $\Sigma_\square^\bullet$ of nonzero sums of squares satisfies axioms (PC3) and (PC4).

A formally real field is **real-closed** if it is formally real and admits no proper formally real algebraic extensions. Here is a spectacular result [FT, Thm. 98].

Theorem 25. *(Grand Artin-Schreier Theorem) The following are equivalent:*
(i) K is formally real and admits no proper formally real algebraic extension.
(ii) K is formally real, every odd degree polynomial over K has a root in K, and for each $x \in K^\times$, exactly one of $x, -x$ is a square.
(iii) K is formally real and $K(\sqrt{-1})$ is algebraically closed.
(iv) The absolute Galois group of K is finite and nontrivial.

The implication (i) $\implies$ (iii) shows that in a real-closed field, $\Sigma_\square^\bullet$ forms a positive cone. It follows, by Corollary 24, that a real-closed field has a unique ordering, in which the positive elements are precisely the squares.

In particular, $\mathbb{R}$ is a real closed field, and every real-closed field R possesses more than a passing resemblance to $\mathbb{R}$. (In fact, in the sense of model theory, any real-closed field is *elementarily equivalent* to the real numbers. This is one of the fundamental facts underpinning non-standard analysis.)

Proposition 26. *Sylvester's law of nullity holds over any real-closed field R. That is, if R is real closed, and q is any nonsingular quadratic form over R, then there exist uniquely determined non-negative integers r and s such that $q \cong [r]\langle 1\rangle \oplus [s]\langle -1\rangle$. It follows that $W(R) \cong \mathbb{Z}$.*

Exercise: Prove Proposition 26.

A **real-closure** of a formally real field K is an algebraic extension R of K which is real-closed. Every formally real field admits a real-closure [FT, Prop. 101]. **Warning**: unlike in the case of algebraic closure, two real-closures R_1 and R_2 of a formally real field K need not be isomorphic as K-algebras (or even as abstract fields). However, the uniqueness can be recovered by working in the category of ordered fields: suppose $(K, <)$ is an ordered field. Then a real-closure of $(K, <)$ (i.e., as an ordered field) is a real-closed field R and a field embedding $K \hookrightarrow R$ such that the unique ordering on R restricts to the given ordering $<$ on K. We speak of R as being a real-closure of K *relative to the ordering* $<$. We may also suppress the $<$ and speak of "the ordered field K".

Theorem 27. *(Existence and uniqueness of real-closures of ordered fields)*
a) Every ordered field possesses a real-closure relative to the given ordering.
b) Let K_1 and K_2 be two ordered fields, and let R_1 and R_2 be real-closures of K_1 and K_2 relative to their given orderings. Let $f : K_1 \to K_2$ be an isomorphism of ordered fields. Then f extends uniquely to an order isomorphism $F : R_1 \to R_2$.

Proof. This is [FT, Thm. TOBEADDED!]. □

Combining the previous two results, for any ordered field K we may define a signature map $\sigma : W(K) \to \mathbb{Z}$. Indeed, letting R be "the" real-closure of the ordered field K, there is a natural ring homomorphism $W(K) \to W(R)$ and a canonical isomorphism $W(R) \to \mathbb{Z}$, and we define σ to be the composite of these two maps. Again, if $\sigma(q) \neq 0$, then q is a nontorsion element of the Witt group of K.

Now let us take things one step further and bundle together the signatures over all possible orderings into a single invariant. Namely, let $X(K)$ be the set of all orderings of K. For $q \in W(K)$, we define the **total signature** $\Sigma(q) = (\sigma_P(q))_{P \in X(K)}$, where σ_P is the signature with respect to the ordering P. That is, Σ is a homomorphism of groups

$$\Sigma : W(K) \to \prod_{P \in X(K)} \mathbb{Z}.$$

(Note: really the direct product, not the direct sum: consider for instance the total signature of the unit quadratic form $\langle 1 \rangle$.)
Now we are ready to state a fantastic result.

Theorem 28. *(Pfister) a) We have $W(K)[\mathrm{tors}] = W(K)[2^\infty]$.*
b) (Local-global principle) We have an exact sequence of abelian groups

$$0 \to W(K)[\mathrm{tors}] \to W(K) \overset{\Sigma}{\to} \prod_{P \in X(F)} \mathbb{Z}.$$

In other words, part a) asserts that the only torsion in the Witt ring is 2-primary torsion. Part b) asserts that a quadratic form has a hyperbolic multiple iff its total signature is zero. In particular, $W(K)$ is a torsion group iff K is not formally real.

Following [**?**], we prove these results by factoring them through the theory of Pythagorean and Euclidean fields. Some of the results obtained along the way are of independent interest.

4.1. **Euclidean and Pythagorean fields.**

A field K is **Euclidean** if it is formally real and $\# K^\times/K^{\times 2} = 2$.

Thus a real-closed field is Euclidean. A good way to think of a Euclidean field is a field which behaves like a real-closed field as far as quadratic extensions are concerned. (Indeed, since the name "Euclidean" is not especially meaningful to me here, I contemplated replacing it with "quadratically real-closed". But even ignoring the risks of introducing nonstandard terminology, the phrase "quadratically real-closed" is a mouthful.)

A field K is **Pythagorean** if the sum of two squares is always a square. Equivalently, $\Sigma_\square^\bullet = K^{\times 2}$.

Example: Quadratically closed fields and real-closed fields are Pythagorean. The field of constructible real numbers is Pythagorean. A finite field is not Pythagorean. $\mathbb{Q}$ is not Pythagorean.

We now have a string of easy facts about Euclidean and Pythagorean fields.

Proposition 29. *In a Euclidean field, the two square classes are* ± 1.

Proof. Indeed, in any formally real field ± 1 represent distinct square clases. □

Proposition 30. *Let K be a Euclidean field.*
a) K is Pythagorean with a unique ordering.
b) The signature map $\sigma : W(K) \to \mathbb{Z}$ is an isomorphism.

Proof. Part a): if K is Euclidean, then it is formally real, so the sum of two squares is always non-negative, and in a Euclidean field any non-negative element is a square. That the ordering is unique follows from [FT, Lemma 90]. b) Once again the proof of Sylvester's Law of Nullity given in the case of $K = \mathbb{R}$, goes through verbatim for any Euclidean field, as we ask the reader to check. □

Lemma 31. *Let K be a field of characteristic different from 2, $a \in K^\times \setminus K^{\times 2}$, and $L = K(\sqrt{a})$. Then we have an exact sequence*

$$1 \to \{K^{\times 2}, aK^{\times 2}\} \to K^\times/K^{\times 2} \overset{\iota}{\to} L^\times/L^{\times 2} \overset{N}{\to} K^\times/K^{\times 2},$$

where ι is induced by the inclusion map $K \hookrightarrow L$ and N is induced by the norm map from L to K: explicitly, $x + ay \mapsto x^2 - ay^2$.

Proof. This is nothing else than the first three terms of inflation-restriction sequence associated to the normal subgroup Gal_L of Gal_K and the Gal_K-module μ_2 (i.e., $\mathbb{Z}/2\mathbb{Z}$ with trivial action):

$$0 \to H^1(\mathrm{Gal}(L/K), \mu_2) \overset{\mathrm{inf}}{\to} H^1(\mathrm{Gal}_K, \mu_2) \overset{\mathrm{res}}{\to} H^1(\mathrm{Gal}_L, \mu_2)^{\mathrm{Gal}(L/K)}.$$

For a proof which avoids use of Galois cohomology at the expense of a more detailed study of quadratic forms under quadratic field extensions, see [Lam05, Thm. VII.3.8]. □

Here is an analogue of the Grand Artin-Schreier Theorem for Euclidean fields.

Theorem 32. *For a field K (of any characteristic), TFAE:*
(i) K is Euclidean.
(ii) K is formally real and admits no formally real quadratic extension.
(iii) $\sqrt{-1} \notin K$ and $K(\sqrt{-1})$ is quadratically closed.
(iv) K has characteristic different from 2 admits a quadratic extension which is quadratically closed.

Proof. (ii) $\implies$ (i): Let $a \in K^\times \setminus K^{\times 2}$. By hypothesis, $K(\sqrt{a})$ is not formally real. By [FT, Prop. 96] a is negative with respect to every ordering on K, so $-a$ is positive with respect to every ordering on K hence by [FT, Cor. 94] there exist $x_1, \ldots, x_n \in K$ such that

$$-a = x_1^2 + \ldots + x_n^2.$$

Out of all representations of $-a$ as a sum of squares, we may take one with n minimal: in particular $x_i \neq 0$ for all i. Suppose $n \geq 2$. If $x_1^2 + x_2^2$ were not a square in K, then as above we would have

$$-(x_1^2 + x_2^2) = y_1^2 + \ldots + y_m^2,$$

contradicting the formal reality of K. Therefore $n = 1$, i.e., $a = -x_1^2 \in -K^\times$.
(i) $\implies$ (iii): By definition of Euclidean, $\sqrt{-1} \notin K$. Now put $L = K(\sqrt{-1})$. Then, since K is Pythagorean, the norm map from L to K – concretely $x + \sqrt{-1}y \in L \mapsto x^2 + y^2 \in K$ – induces the trivial homomorphism $L^\times/L^{\times 2} \rightarrow K^{times}/K^{\times 2}$. It follows from Lemma 31 that $L^\times/L^{\times 2} \cong K^\times/\pm K^{\times 2}$, i.e., is trivial. [There should be a proof of this independent of Lam's result.]
(iii) $\implies$ (iv) is immediate.
(iv) $\implies$ (ii): Write $L = K(\sqrt{a})$. The norm map $L^\times/L^{\times 2} \rightarrow K^\times/K^{\times 2}$ has image $\{x^2 - ay^2 \mid x, y \in K, x^2 - ay^2 \neq 0\}/K^{\times 2}$. Since $L^\times = L^{\times 2}$, we conclude that $K^{\times 2} = \{x^2 - ay^2 \mid x, y \in K, x^2 - ay^2 \neq 0\}$. In particular, $-a \in K^{\times 2}$. Thus $L = K(\sqrt{-1})$ and the equality $\{x^2 - ay^2 \mid x, y \in K, x^2 - ay^2 \neq 0\}/K^{\times 2}$ asserts the Pythagoreanness of K. Since K is Pythagorean, if it were not formally real then -1 would be a square in K, contradiction. Also the exact sequence of Lemma 31 implies that $K^\times/K^{\times 2} = \{\pm 1\}$, so L/K is the only quadratic extension of K. □

Proposition 33. *A field K is Pythagorean iff for all $x \in K$, $1 + x^2 \in K$.*

Exercise X.X: Prove Proposition 33.

Proposition 34. *For a field K, TFAE:*
(i) K is quadratically closed.
(ii) K is Pythagorean and is not *formally real.*

Proof. That (i) $\implies$ (ii) is immediate from the definitions. Conversely, if K is Pythagorean then $\Sigma_\square = K^\times$, whereas if K is not formally real, then by Theorem 23b) $\Sigma_\square = K^\times$. □

A class $\mathcal{C}$ of fields is **closable** if it satisfies the following two properties:

(CC1) For every field extension K, there exists an algebraic extension L/K such that $L \in \mathcal{C}$.
(CC2) Let $\{L_i\}$ be a family of subfields of a field C. Suppose that for all i, $L_i \in \mathcal{C}$. Then $K = \bigcap_i L_i \in \mathcal{C}$.

Let $\mathcal{C}$ be a closable class of fields. Then, inside any algebraic closure $\overline{K}$ of K,

K admits a $\mathcal{C}$-**closure**: that is a subextension $K_{\mathcal{C}}$ of $\overline{K}/K$ which lies in $\mathcal{C}$ and is the unique minimal subextension with this property: namely the intersection of all subextensions L/K which lie in $\mathcal{C}$. The $\mathcal{C}$-closure $K_{\mathcal{C}}$ is well-defined up to K-algebra isomorphism indepedent of the choice of algebraic closure $\overline{K}$.

Proposition 35. *The classes of quadratically closed fields and Pythagorean fields are each closable. Therefore, inside a fixed algebraic closure $\overline{K}$, K admits a unique quadratic closure K_{QC} and a Pythagorean closure K_P. We have $K_P \subset K_{QC}$.*

Proof. Since an algebraically closed field is both quadratically closed and Pythagorean, both classes satisfy (C1). Now let $\{L_i\}$ be a family of subfields of a field C, and put $K = \bigcap_i L_i$. Let $x \in K$. Then $\pm\sqrt{x}$ lie in L_i for all i, so $\pm\sqrt{x} \in K$. Thus K is quadratically closed. Moreover, $1 + x^2 \in L_i$ for all i, so $1 + x^2 \in K$. Thus K is Pythagorean. □

Warning: Nothwithstanding the name, the real-closed fields are not a closable class. They do not satisfy (C1) since a subfield of a real-closed field is formally real. Moreover, they do not satisfy (C2): indeed, any algebraically closed field of characteristic 0 admits infinitely many index 2 subfields, each of which is real-closed by Artin-Schreier, but the intersection of any two of them has index 4 so is not real-closed. The problem can be traced back to the condition that for all x in a real-closed field, *either* x or $-x$ is a square. If R_1 and R_2 are two real-closed subfields of an algebraically closed field C and $x \in R_1 \cap R_2$, then it may happen that x (but not $-x$) is a square in R_1 and that $-x$ (but not x is a square in R_2, and thus neither x nor $-x$ is a square in $R_1 \cap R_2$. For very similar reasons, the class of Euclidean fields is not closable.

The following important result characterizes fields with torsionfree Witt ring.

Theorem 36. *a) A field K is Pythagorean and not formally real iff $W(K) = \mathbb{Z}/2\mathbb{Z}$.*
b) A field K is Pythagorean and formally real iff $W(K)[\text{tors}] = 0$ iff $W(K)[2] = 0$.

Proof. a) By Proposition 34, a field is Pythagorean and not formally real iff it is quadratically closed, whereas by Proposition 11, a field is quadratically closed iff its Witt ring is $\mathbb{Z}/2\mathbb{Z}$.

Turning, to part b): Suppose first that K is Pythagorean and formally real. Let q be an anistropic quadratic form over K. We must show that for all $n \in \mathbb{Z}^+$, $[n]q$ is also anisotropic. Indeed, write

$$q = a_1 t_1^2 + \ldots + a_d t_d^2,$$

so

$$[n]q = a_1(t_{11}^2 + \ldots + t_{1n}^2) + \ldots + a_d(t_{d1}^2 + \ldots + t_{dn}^2).$$

Thus, if $x = (x_{11}, \ldots, x_{dn})$ is such that $[n]q(x) = 0$, we have

$$a_1(x_{11}^2 + \ldots + x_{1n}^2) + \ldots + a_d(x_{d1}^2 + \ldots + x_{dn}^2) = 0.$$

Since K is Pythagorean, there exist $y_1, \ldots, y_d$ such that for all $1 \leq i \leq d$,

$$x_{i1}^2 + \ldots + x_{in}^2 = y_i^2,$$

and then

$$q(y) = a_1 y_1^2 + \ldots + a_d y_d^2 = 0.$$

Since q is anisotropic, $y_1 = \ldots = y_d = 0$, and since K is formally real that forces $x_{ij} = 0$ for all i, j.

Obviously $W(K)[\text{tors}] = 0 \implies W(K)[2] = 0$.

Finally, assume that $W(K)[2] = 0$. For $y \in K$, put $d = 1 + y^2$. Then the two binary quadratic forms $\langle 1, 1\rangle$ and $\langle d, d\rangle$ both represent d and have discriminant 1 so are isometric, i.e., $[2]\langle 1\rangle = [2]\langle d\rangle$ in $W(K)$. But we are assuming there is no 2-torsion, so $\langle 1\rangle = \langle d\rangle$, i.e., d is a square. Thus K is Pythagorean. Applying part a), K must be formally real. □

4.2. **Proof of Pfister's Local-Global Principle.**

We will need the following Lemma, which provides a link between prime ideals of $W(K)$ and orderings on K.

Lemma 37. *Let $\mathfrak{p}$ be a prime ideal of $W(K)$ which is* not *the fundamental ideal I. Then*

$$P := \{a \in K \mid \langle a\rangle \equiv 1 \pmod{\mathfrak{p}}\}$$

is (the positive cone of) an ordering on K.

Proof. From the proof of Proposition 3 we have for all $a \in K^\times$, $\langle a\rangle \equiv \pm 1 \pmod{\mathfrak{p}}$. Moreover, by Proposition 4, since $\mathfrak{p} \neq I$, $2 \notin \mathfrak{p}$, so for all $a \in K^\times$, $\langle a\rangle$ is congruent modulo $\mathfrak{p}$ to exactly one of ± 1.
(PC2): Clearly if $\langle a\rangle \equiv 1 \pmod{\mathfrak{p}}$ and $\langle b\rangle \equiv 1 \pmod{\mathfrak{p}}$, then $\langle ab\rangle \equiv 1 \pmod{\mathfrak{p}}$, so $P \cdot P \subset P$.
(PC1): Let $a, b \in K^\times$ and put $c = a + b$. Then $\langle c\rangle \equiv 2 \pmod{\mathfrak{p}}$, so $\langle c\rangle \notin \mathfrak{p}$: in particular, $c \neq 0$. Now consider the two nonsingular binary quadratic forms $q_1 = \langle a, b\rangle$ and $q_2 = \langle c\rangle\langle 1, ab\rangle$. Both q_1 and q_2 have discriminant ab and represent the element $c = a + b$, so by X.X $q_1 \cong q_2$. In particular they are equal elements of $W(K)$. Reducing this equality modulo $\mathfrak{p}$ gives $2 \equiv 2\langle c\rangle \pmod{\mathfrak{p}}$. Since $2 \neq 0$ in the domain $W(K)/\mathfrak{p}$, we may cancel to get $\langle c\rangle \equiv 1 \pmod{\mathfrak{p}}$, i.e., $c \in P$.
(PC3) This follows from the remark that for every $a \in K^\times$, either $a \equiv 1 \pmod{\mathfrak{p}}$ or $-a \equiv 1 \pmod{\mathfrak{p}}$.
(PC4) Since $2 \notin \mathfrak{p}$, $-1 \notin P$. But indeed, in the presence of (PC2) and (PC3), this implies that $P \cap (-P) = \varnothing$. Indeed, if $x \in P \cap (-P)$, then $-1 = x \cdot (-x) \cdot (\frac{1}{x})^2 \in P$, contradiction. □

Now we give the proof of Pfister's Theorem (Theorem 28). We follow [Lam05, §$VIII$.3], the basic idea being to reduce to the Euclidean case.

Step 1: Suppose that K is Euclidean. In this case there is a unique ordering and, by Proposition 30, the signature map $\Sigma : W(K) \to \mathbb{Z}$ is an isomorphism.

Step 2: Suppose that K is not formally real. Then we must show that $W(K) = W(K)[2^\infty]$. By Proposition 4 and Lemma 37, the only prime ideal of $W(K)$ is the fundamental ideal I. In other words, I is the intersection of all prime ideals of $W(K)$, which is the **nilradical** of $W(K)$, i.e., the set of all nilpotent elements. In particular, the element $2 \in I$ is nilpotent, so there exists $r \in \mathbb{Z}^+$ such that $2^r = 0$ in $W(K)$. Thus every element of $W(K)$ is 2-torsion.

Step 3: Now let K be an arbirary field of characteristic different from 2. Since $\prod_{P \in X(K)} \mathbb{Z}$ is torsionfree, to prove Pfister's theorem it is enough to show that if $q \in W(K)$ is *not* a 2-primary torsion element, then there exists an ordering P on K

such that the P-signature of q is nonzero. An easy Zorn's Lemma argument shows that, among all algebraic extensions L of K such that $q \in W(L) \setminus W(L)[2^\infty]$, there exists a *maximal* such extension. We claim that such an L is Euclidean. By Step 2 L is formally real. Suppose that there exists aL such that neither a nor $-a$ lies in $L^{\times 2}$. By the maximality of L, q becomes 2-primary torsion in $L(\sqrt{a})$ and $L(\sqrt{-a})$, so that for sufficiently large N, $2^N q$ is hyperbolic over both $L(\sqrt{a})$ and $L(\sqrt{-a})$. Then by Corollary 22, $2 \cdot 2^N q = 0 \in W(L)$, contradiction. Thus L is Euclidean and the hypothesis that q is not 2-primary torsion in L means that it has nonzero signature with respect to the unique ordering of L; this restricts to an ordering P of K on which the signature is nonzero, qed.

5. Steinberg Symbols I

We follow [S, §2.12].

Let K be a field and B a 2-torsion abelian group, written multiplicatively. A **Steinberg symbol with values in B** is a map $\sigma : K^\times \times K^\times \to B$ satisfying:

(SS1) For all $x, y, z \in K^\times$, $\sigma(xy, z) = \sigma(x, z)\sigma(y, z)$ and $\sigma(x, yz) = \sigma(x, y)\sigma(x, z)$;
(SS2) For all $x \in K \setminus \{0, 1\}$, $\sigma(x, 1 - x) = 1$.

Key Example: If K is a nondyadic CDVR or $\mathbb{Q}_2$, then the Hilbert symbol is a Steinberg symbol.

Lemma 38. *Let $\sigma : K^\times \to K^\times \to B$ be a Steinberg symbol. For all $x, y, z, w \in K^\times$, we have:*
a) $\sigma(xy^2, zw^2) = \sigma(x, z)$.
b) $\sigma(1, x) = \sigma(x, -x) = 1$.
c) $\sigma(x, x) = \sigma(x, -1)$.
d) $\sigma(x, y) = \sigma(y, x)$.

Proof. a) This follows from the fact that B is 2-torsion. b) Bimultiplicativity gives $\sigma(1, x) = \sigma(1, x)\sigma(1, x)$, hence $\sigma(1, x) = 1$. In particular $\sigma(1, -1) = 1$. If $x \neq 1$, then $-x = (1 - x)(1 - x^{-1})^{-1}$, so

$$\sigma(x, -x) = \sigma(x, 1-x)\sigma(x, (1-x^{-1})^{-1}) = \sigma(1, 1-x)\sigma(x, 1-x^{-1}) = \sigma(x^{-1}, 1-x^{-1}) = 1.$$

c) $1 = \sigma(x, -x) = \sigma(x, x)\sigma(x, -1)$, so $\sigma(x, x) = \sigma(x, -1)$.
d) We have

$$1 = \sigma(xy, -xy) = \sigma(x, -xy)\sigma(y, -xy) = \sigma(x, -x)\sigma(x, y)\sigma(y, -y)\sigma(y, x) = \sigma(x, y)\sigma(y, x).$$

□

Lemma 39. *Let σ be a Steinberg symbol, and let $x, y \in K^\times$. Then:*
a) If $\langle x, y\rangle$ is isotropic, $\sigma(x, y) = 1$.
b) The value $\sigma(x, y)$ depends only on the isometry class of the binary form $\langle x, y\rangle$.

Proof. a) If $\langle x, y\rangle$ is isotropic, then there is $z \in K^\times$ such that $y = -xz^2$, so $\sigma(x, y) = \sigma(x, -xz^2) = \sigma(x, -x)\sigma(x, z^2) = 1$.
b) If $\langle x, y\rangle \cong \langle z, w\rangle$, then there are $\alpha, \beta \in K$ such that $x\alpha^2 + y\beta^2 = z$. If $\beta = 0$, then $x \equiv z \pmod{K^{\times 2}}$ and thus (e.g. by Witt Cancellation) $y \equiv w \pmod{K^{\times 2}}$, so $\sigma(x, y) = \sigma(z, w)$. Similarly if $\alpha = 0$. If α and β are both nonzero, then

$$x\alpha^2 z^{-1} + y\beta^2 z^{-1} = 1$$

with both terms nonzero, so by (SS2),

$$1 = \sigma(x\alpha^{-1}z^{-1}, y\beta^2 z^{-1}) = \sigma(xz, yz) = \sigma(x,y)\sigma(z, xyz)$$
$$= \sigma(x,y)\sigma(z, zwz) = \sigma(x,y)\sigma(z,w).$$

□

Definition: Let $\langle a_1, \ldots, a_n\rangle$ be a diagonal quadratic form over K, and let σ be a Steinberg symbol on K. We define the **Hasse invariant**

$$H_\sigma(a_1, \ldots, a_n) = \prod_{i<j} \sigma(a_i, a_j).$$

Lemma 40. *Let f and g be diagonal quadratic forms over K, and let σ be a Steinberg symbol on K. Then*

$$H_\sigma(f \oplus g) = H_\sigma(f)H_\sigma(g)\sigma(\det f, \det g). \tag{4}$$

Proof. ... □

Proposition 41. *(Isometry Invariance of H_σ) Let $a_1, \ldots, a_n, b_1, \ldots, b_n \in K^\times$, and suppose that $\langle a_1, \ldots, a_n\rangle = \langle b_1, \ldots, b_n\rangle$. Then for any Steinberg symbol σ, we have $H_\sigma(a_1, \ldots, a_n) = H_\sigma(b_1, \ldots, b_n)$.*

Proof. By Witt's Chain Equivalence Theorem [**?**, Thm. 28], we may assume that $\langle a_1, \ldots, a_n\rangle$ and $\langle b_1, \ldots, b_n\rangle$ are simply equivalent. In fact, from the symmetry of σ and the definition of H_σ we see that $H_\sigma(a_1, \ldots, a_n)$ is invariant under permutations of $a_1, \ldots, a_n$. Thus it suffices to assume that $\langle a_3, \ldots, a_n\rangle = \langle b_3, \ldots, b_n\rangle$ and $\langle a_1, a_2\rangle \cong \langle b_1, b_2\rangle$; in particular $a_1 a_2 \equiv b_1 b_2 \pmod{K^{\times 2}}$. By Lemmas 39 and 40,

$$H_\sigma(a_1, \ldots, a_n) = H_\sigma(a_1, a_2)H_\sigma(a_3, \ldots, a_n)\sigma(a_1 a_2, a_3 \cdots a_n)$$
$$= H_\sigma(b_1, b_2)H_\sigma(b_3, \ldots, b_n)\sigma(b_1, b_2, b_3 \cdots b_n) = H_\sigma(b_1, \ldots, b_n).$$

□

For many purposes, the following modification of the Hasse invariant H_σ proves slightly more natural: for a Steinberg symbol σ and an n-ary quadratic form q, we define the **Witt invariant** $c_\sigma(q)$ as follows:

$$H_\sigma(q),\ n \equiv 1, 2 \pmod 8,$$
$$H_\sigma(q)\sigma(-1, -\det q),\ n \equiv 3, 4 \pmod 8,$$
$$H_\sigma(q)\sigma(-1, -1),\ n \equiv 5, 6 \pmod 8,$$
$$H_\sigma(q)\sigma(-1, \det q),\ n \equiv 7, 8 \pmod 8.$$

Example: Let $q = \bigoplus_{i=1}^n \mathbb{H}$. Then $c_\sigma(q) = 1$.

Proposition 42. *The Witt invariant of a quadratic form depends only on its similarity class.*

Proof. By direct computation... □

Let $\sigma : K^\times \times K^\times \to B$ be a Steinberg symbol. We define $H_\sigma(K)$ as the set

$$\mathbb{Z}/2\mathbb{Z} \times K^\times / K^{\times 2} \times B$$

endowed with the following group law:

$$(0, x, c)(0, x', c') = (0, xx', cc'\sigma(x, x')).$$
$$(0, x, c)(1, x', c') = (1, xx', cc'\sigma(x, -x')).$$

$$(1,x,c)(0,x',c') = (1,xx',cc'\sigma(-x,x')).$$
$$(1,x,c)(1,x',c') = (0,xx',cc'\sigma(x,x')).$$

Theorem 43. *a) $H_\sigma(K)$ is a commutative group, with identity element $(0,1,1)$ and inverses as follows:*

$$(0,x,c)^{-1} = (0,x,c\sigma(x,x)),\ (1,x,c)^{-1} = (1,-x,c).$$

b) The map $B \to H_\sigma(K)$ given by $c \mapsto (0,1,c)$ is an injective group homomorphism. The quotient $H_\sigma(K)/B$ is isomorphic to the extended square class group $Q(K)$.
c) The map $\hat{W}(K) \to H_\sigma(K)$ obtained by sending a quadratic form to $(\dim(q) \pmod 2, d_\pm(q), c_\sigma(q))$ is a homomorphism of groups which factors through $W(K)$.

Theorem 44. *(Milnor) The map $K^\times \times K^\times \to I^2/I^3$ given by*

$$(x,y) \mapsto \langle 1,-x,-y,xy\rangle + I^3$$

is a universal Steinberg symbol.

References

[Cas] J.W.S. Cassels, *Rational quadratic forms.* London Mathematical Society Monographs, 13. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.

[FT] P.L. Clark, *Field Theory*, `http://math.uga.edu/∼pete/FieldTheory.pdf`

[Lam73] T.-Y. Lam, *Algebraic Theory of Quadratic Forms*, 1973.

[Lam05] T.Y. Lam, *Introduction to quadratic forms over fields.* Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.

[OM] T.O. O'Meara, *Introduction to quadratic forms.* Reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000.

[S] W. Scharlau, *Quadratic and Hermitian forms.* Grundlehren der Mathematischen Wissenschaften 270. Springer-Verlag, Berlin, 1985.