Matemática Contemporânea, Vol. 7, 129–179
http://doi.org/10.21711/231766361994/rmc77

GALOIS GROUPS AND QUADRATIC FORMS

Tara L. Smith*

Abstract

These notes represent the material for a five-lecture mini-course, given at the Brazilian Algebra Meeting in Diamantina, Brazil, in August 1992. The lectures explore the connections between the Galois groups arising over a given field and the behavior of quadratic forms over that field. No particular background is assumed beyond that of a good graduate-level understanding of abstract algebra including Galois theory.

1 Algebraic Theory of Quadratic Forms; The Witt Ring of a Field

The algebraic theory of quadratic forms (i.e. homogeneous polynomials of degree 2) over fields of characteristic not 2 originated with the work of E. Witt, in his classical paper of 1937 [Wi:1937]. Instead of considering individual forms over the given field, Witt looked at the entire collection of all forms over a fixed ground field F (of characteristic not 2). From this collection Witt constructed an algebraic object, specifically a commutative ring, the Witt ring of the field F. One is then naturally led to the question of how the structure of the Witt ring reflects the behavior of quadratic forms over F and vice-versa.

In this section we present the basic background material necessary for studying the algebraic theory of quadratic forms. This includes the major theorems of Witt (cancellation, decomposition, and chain equivalence), invariants of forms (dimension, determinant, and Witt index), and the construction of the Witt ring $W(F)$. The presentation of the material in this section and the next borrows heavily from [La:1973].

*Research supported in part by NSF Grant DMS-9196244

Throughout these notes, all fields will be assumed to have characteristic not 2. The algebraic theory of quadratic forms over fields of characteristic $= 2$ has also been developed, but it requires different methods, and it would take us too far afield to consider this case. Then let F be a field of characteristic not 2. An n-ary quadratic form over F is a homogeneous polynomial of degree 2 in n variables over F. It will have the general form

$$f(X) = f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j, \text{ for } a_{ij} \in F.$$

It is customary to render the coefficients symmetric by rewriting f as

$$f(X) = \sum_{i,j} \frac{1}{2}(a_{ij} + a_{ji})x_ix_j = \sum_{i,j} b_{ij}x_ix_j, \text{ where } b_{ij} = \frac{1}{2}(a_{ij} + a_{ji}).$$

Thus f determines a unique $n \times n$ symmetric matrix $M_f = (b_{ij})$, and viewing $X = (x_1, \ldots, x_n)$ as a column vector, we have $f(X) = X^t M_f X$. The number n is the *dimension* of the form f, denoted $dim(f)$.

Definition 1.1 *The determinant $det(f)$ of the quadratic form f is defined to be the determinant of the symmetric matrix M determined by the quadratic form f.*

Two quadratic forms f and g will be called *equivalent* if there exists a nonsingular homogeneous linear change of variable taking g to f, i.e. if there exists $C \in \mathbf{GL}_n(F)$ such that $f(X) = g(CX)$, or such that $M_f = C^t M_g C$ (the corresponding symmetric matrices are congruent). One can easily check that this defines an equivalence relation. Notice that $dim(f)$ is invariant under this equivalence relation, and that $det(f)$, when viewed as an element of the square class group $\dot{F}/\dot{F}^2$, is also an invariant of the equivalence class of f. (Here and in what follows, $\dot{F}$ denotes the multiplicative group of nonzero elements of F.)

Example. Consider the linear change of variable $x_1 \to x_1 + x_2$, $x_2 \to x_1 - x_2$. The corresponding matrix C is given by $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Then if $g(X) = x_1x_2$, we have $f(X) = g(CX) = (x_1 + x_2)(x_1 - x_2) = x_1^2 - x_2^2$. Thus the quadratic form

x_1x_2 is equivalent to the form $x_1^2 - x_2^2$. This particular (equivalence class of) quadratic form is actually quite important, as we shall see.

Definition 1.2 *The (equivalence class of the) quadratic form described in the example above is called the hyperbolic plane, and will be denoted* $\mathbf{H}$. *It has the nice property that it represents every element of* F. *(A form is said to represent* $a \in F$ *if there exists a nonzero vector* $v \in F^n$ *such that* $v^t M_f v = a$, *i.e. if* $f(v) = a$. *Here we may take* $v = \left(\left(\frac{a+1}{2}\right), \left(\frac{a-1}{2}\right)\right) \in F^2$.*) A form with the property that it represents all nonzero elements of* F *is said to be universal.*

To any quadratic form f we associate a "quadratic map" $Q_f : F^n \to F$ by letting $e_1, \ldots, e_n$ be the standard basis of F^n, and for $X = \sum x_i e_i \in F^n$, defining $Q_f(X) = X^t M_f X$. This map has the properties

(1) $$Q_f(ax) = a^2 Q_f(x), \qquad \forall a \in F, x \in F^n$$

(2) $B_f(x,y) := \frac{1}{2}[Q_f(x+y) - Q_f(x) - Q_f(y)]$ is a symmetric bilinear pairing.

We can also take a coordinate-free approach: Let V be a finite-dimensional F-vector space, $B : V \times V \to F$ a symmetric bilinear pairing on V. Associate a quadratic map $q_B : V \to F$ by $q_B(x) = B(x,x) \in F$ for $x \in V$. If we coordinatize V (choose a basis $e_1, \ldots, e_n$) then the "quadratic space"(V, B, q) gives rise to a quadratic form (determined up to equivalence class, depending on choice of basis). If (V, B), (V', B') are quadratic spaces, we say they are *isometric* (denoted $\simeq$) if there exists a linear isomorphism $\sigma : V \to V'$ such that $B'(\sigma(x), \sigma(y)) = B(x,y)$ $\forall x, y \in V$. There exists a one-to-one correspondence between equivalence classes of n-ary qudaratic forms over F and isometry classes of n-dimensional quadratic spaces over F. Specifically we now have three different ways of looking at quadratic forms:

$$\left\{\begin{array}{c}\text{equivalence classes}\\ \text{of homogeneous}\\ \text{polynomials of}\\ \text{degree 2 over F}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{congruence classes}\\ \text{of symmetric}\\ \text{matrices over F}\end{array}\right\} \leftrightarrow \left\{\begin{array}{c}\text{isometry classes}\\ \text{of symmetric}\\ \text{bilinear pairings}\\ \text{on F-vector spaces}\end{array}\right\}$$

Given two quadratic spaces (V_1, B_1) and (V_2, B_2) of dimensions n and m respectively, we can form a new quadratic space (V, B) of dimension $m+n$ where $V = V_1 \oplus V_2$ and $B : V \times V \to F$ is defined by $B((x_1, x_2), (y_1, y_2)) = B_1(x_1, y_1) + B_2(x_2, y_2)$ for $x_i \in V_i, i = 1, 2$. This gives rise to a new quadratic form $q = q_1 \perp q_2$. The associated matrix M_q is the direct sum of the matrices of the forms q_1 and q_2. (We remark here for future reference that the direct sum of hyperbolic planes is called a *hyperbolic space.*) We can also define a binary operation $\otimes$ to get a new quadratic space (V', B') of dimension mn, where $V' = V_1 \otimes_F V_2$, and $B' : V' \times V' \to F$ is defined by $B'(x_1 \otimes x_2, y_1 \otimes y_2) = B_1(x_1, y_1)B_2(x_2, y_2) \in F$. We then have a new form q', which is denoted $q_1 \otimes q_2$, or simply $q_1 q_2$. The matrix $M_{q'}$ is the Kronecker product of the matrices for q_1 and q_2.

We want to focus our attention on so-called "regular" quadratic forms, i.e. those forms f such that M_f is nonsingular, or equivalently such that $\forall x \in V, B(x, y) = 0 \quad \forall y \in V \Rightarrow x = 0$. From now on we will assume all quadratic forms are regular unless otherwise stated. We now state several of the fundamental results in the algebraic theory of quadratic forms, mostly without proof. Proofs can be found in any standard text on algebraic theory of quadratic forms, such as [La:1973] or [Sc:1985].

Theorem 1.3 *(First Representation Theorem) Let $d \in F, d \neq 0$ be represented by q (i.e. $\exists v \in V, v \neq 0$ such that $q(v) = d$). Then there exists another quadratic space (V', q'), together with an isometry $V \simeq dx^2 \perp V'$.*

Corollary 1.4 *Any n-ary quadratic form over a field F of characteristic not 2 is equivalent to some diagonal form $d_1 x_1^2 + \ldots + d_n x_n^2$.*

Remarks. The diagonalizability of a quadratic form (in such a way that any one nonzero represented element can be chosen to appear in the diagonalization) is equivalent to the existence of an orthogonal basis for the quadratic space (V, B) (with a prescribed vector of "nonzero length" as one of the basis vectors). The isometry class of the diagonal form $d_1 x_1^2 + \ldots + d_n x_n^2$ will be abbreviated by $\langle d_1, \ldots, d_n \rangle$. For diagonal forms we have $\langle a_1, \ldots, a_n \rangle \perp \langle b_1, \ldots, b_m \rangle \simeq$

$\langle a_1, \ldots, a_n, b_1, \ldots, b_m \rangle$, and $\langle a_1, \ldots, a_n \rangle \otimes \langle b_1, \ldots, b_m \rangle \simeq \langle a_1 b_1, \ldots, a_n b_1, \ldots, a_1 b_m, \ldots, a_n b_m \rangle$. Notice also that $det(\langle a_1, \ldots, a_n \rangle) = a_1 a_2 \ldots a_n \in \dot{F}/\dot{F}^2$.

Definition 1.5 *The form q is isotropic if $\exists v \in V, v \neq 0$, such that $q(v) = 0$, i.e. if q represents 0. The form q is said to be anisotropic otherwise.*

Proposition 1.6 *For a regular binary (2-dimensional) quadratic form q, the following are equivalent.*

1. *q is isotropic.*

2. *$q \simeq \langle 1, -1 \rangle$, i.e. q is a hyperbolic plane.*

3. *The determinant $det(q)$ of $q = -1 \in \dot{F}/\dot{F}^2$.*

Proof. The equivalence of (2) and (3) follows directly from the Representation Theorem above. That (2) implies (1) is clear. Finally, for (1) implies (3), notice that for a binary form $\langle a, b \rangle$ to represent 0, there must exist nonzero elements x and y in F such that $ax^2 + by^2 = 0$. Then $ax^2 = -by^2$, so $det(q) = ab = -1 \in \dot{F}/\dot{F}^2$. □

Theorem 1.7 *(Witt's Cancellation Theorem) If q, q_1, q_2 are quadratic forms over F, and $q \perp q_1 \simeq q \perp q_2$, then $q_1 \simeq q_2$.*

Proof.(Sketch) It suffices to consider the case $q = \langle a \rangle, a \in \dot{F}$. We may view the isometry as an identification of the respective quadratic spaces, so that we are working in one space $(V, Q), Q \simeq q \perp q_1 \simeq q \perp q_2$. Then since both forms represent a, there are vectors u and v in V such that $Q(u) = a, q_1 = u^{\perp}$ and $Q(v) = a, q_2 = v^{\perp}$. To prove the theorem we need only find an isometry of V taking u to v. Without loss of generality we may assume that the vector $w = u - v$ is anisotropic. Let τ be the "hyperplane reflection with respect to w", i.e. $\tau(x) = x - \frac{2B(x,w)}{q(w)} w$. Then one can check that τ is the desired isometry. □

Theorem 1.8 *(Witt's Decomposition Theorem) Any regular quadratic space (V,q) splits into an orthogonal sum $(V_h, q_h) \perp (V_a, q_a)$, where V_h is a hyperbolic space and V_a is anisotropic. The isometry types of V_h and V_a are uniquely determined. V is isotropic if and only if V_h is nonzero.*

Proof. (Sketch) We prove the last statement first. Clearly if V_h is nonzero then V is isotropic. Then assume V is isotropic, and let x be an isotropic vector, so $q(x) = 0$. Since V is regular, there is a vector y which is not orthogonal to x, and since x is orthogonal to itself, we see that x and y are linearly independent. Let H_1 be the subspace spanned by x and y. It is easy to check that H_1 has determinant $-1 \in \dot{F}/\dot{F}^2$, so by the Proposition above we see $H_1 \simeq \mathbf{H}$. Then V_h is nonzero. Moreover, $V \simeq H_1 \perp H_1^{\perp}$, where $H_1^{\perp}$ is regular, and by Witt's Cancellation Theorem, $H_1^{\perp}$ is uniquely determined up to isometry. One proceeds by induction on $dim(V)$. □

Definition 1.9 *The Witt index of the quadratic space (V,q) is defined to be $\frac{1}{2}dim V_h$. This is an invariant of the equivalence class of q. We may occasionally write q_a and q_h to denote the subforms of q corresponding to the spaces V_a and V_h respectively.*

Definition 1.10 *We denote the set of nonzero elements represented by the form q as $D_F(q)$, i.e.*

$$D_F(q) = \{d \in \dot{F} | there\ exists\ v \in V such\ that\ q(v) = d\}$$

Corollary 1.11 *(Second Representation Theorem) Let q be a regular quadratic form, $d \in \dot{F}$. Then $d \in D(q) \iff q \perp \langle -d \rangle$ is isotropic.*

Proof. The forward implication is clear. For the reverse direction, let $(x_1, \ldots x_{n+1})$ be an isoptropic vector for $q \perp \langle -d \rangle$. Then $a_1x_1^2 + \ldots + a_nx_n^2 - dx_{n+1}^2 = 0$. If $x_{n+1} \neq 0$, then $d = a_1(\frac{x_1}{x_{n+1}})^2 + \ldots + a_n(\frac{x_n}{x_{n+1}})^2 \in D(q)$. If $x_{n+1} = 0$, then $(x_1, \ldots x_n)$ is an isotropic vector for q. Thus q contains a hyperbolic plane, and therefore is universal. Hence q must represent d. □

We are now in a position to define the *Witt ring* $W(F)$ of F. The construction itself is somewhat technical, but we will soon develop a more intuitive understanding of this ring. Let $M(F)$ denote the set of all isometry classes of regular quadratic forms on F. On this set we have defined two binary operations, $\perp$, which acts like addition, and $\otimes$, which acts like commutative multiplication. These operations make $M(F)$ into a commutative semiring, and under $\perp$, $M(F)$ is a "cancellation semigroup"–it would be a group (and in fact a ring) if only every element in $M(F)$ had an additive inverse. There is a canonical construction to remedy this deficiency, the so-called Grothendieck construction.

Let M be any commutative cancellation semigroup. Define an equivalence relation $\sim$ on $M \times M$ by $(x, y) \sim (x', y') \iff x + y' = x' + y$. Define the Grothendieck group of M to be $Groth(M) = (M \times M)/\sim$, with addition induced by $(x, y) + (x', y') = (x + x', y + y')$. Then $Groth(M)$ is a group with (x, y) and (y, x) as additive inverses. Furthermore, M embeds naturally in $Groth(M)$ under the map $i : M \rightarrow Groth(M)$ given by $i(x) = (x, 0)$. Now $(x, y) = i(x) - i(y)$, so $Groth(M)$ is the additive group generated by M. If M has a commutative multiplication making it into a semiring, then defining $(x, y) \cdot (x', y') = (xx' + yy', x'y + xy')$ induces a multiplication on $Groth(M)$ making it into a commutative ring.

Definition 1.12 $\widehat{W}(F) = Groth(M(F))$ *is the Witt-Grothendieck ring of quadratic forms over F. Elements in $\widehat{W}(F)$ are of the form $q_1 - q_2$, where q_1, q_2 are (isometry classes of) nonsingular quadratic forms over F.*

Observe that $\mathbf{ZH}$, consisting of all hyperbolic spaces and their inverses, forms an ideal of $\widehat{W}(F)$. Indeed, for any regular form q, we have $q \otimes \mathbf{H} = n \cdot \mathbf{H}$, where $n = dim(q)$. (For any positive integer n, and any form φ, we have $n \cdot \varphi = \varphi \perp \ldots \perp \varphi$, an orthogonal sum of n copies of φ.)

Definition 1.13 *The quotient ring $W(F) = \widehat{W}(F)/\mathbf{ZH}$ is the Witt ring of F. We have the following facts about the elements in the Witt ring:*

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

2. Two forms q and q' represent the same element in $W(F) \Longleftrightarrow q_a \simeq q'_a$.

3. If $dim(q) = dim(q')$, then the two forms q and q' represent the same element in $W(F) \Longleftrightarrow q \simeq q'$.

We can then see that the problem of classifying all isometry classes of quadratic forms over the field F is really that of determining the Witt ring $W(F)$. Note also that the 0-element of $W(F)$ is given by any hyperbolic space, that the multiplicative identity of $W(F)$ is the one-dimensional form $\langle 1 \rangle$, and that the additive inverse of any form $\langle a_1, \ldots a_n \rangle \in W(F)$ is $\langle -a_1, \ldots - a_n \rangle$.

We can translate the invariants $dim(q)$ and $det(q)$ so that they are well-defined on elements of the Witt ring. To do this we must modify them in such a way that $\mathbf{H}$ will be in the kernel of each of the maps. Thus we make the following definitions.

Definition 1.14 *The mod 2 dimension $dim_0(q)$ of the quadratic form q is defined to be $dim(q)$ viewed as an element of $\mathbf{Z}/2\mathbf{Z}$. If $q = q' \in W(F)$, then $dim_0(q) = dim_0(q')$. The map $dim_0 : W(F) \to \mathbf{Z}/2\mathbf{Z}$ is a well-defined ring epimorphism. The kernel of this homorphism is denoted IF, and consists precisely of (images of) even-dimensional forms in $W(F)$. IF is called the fundamental ideal of the Witt ring $W(F)$.*

Definition 1.15 *The signed determinant $d_{\pm}(q)$ is given by $d_{\pm}(q) = (-1)^{\frac{n(n-1)}{2}} det(q) \in \dot{F}/\dot{F}^2$. This map is well defined on $W(F)$, and gives a group epimorphism $IF \to \dot{F}/\dot{F}^2$, with kernel $I^2F = (IF)^2$. (This last statement requires proof; see [La:1973].)*

Before concluding this introductory section, we want to specify how one accounts for isometries between (diagonal) quadratic forms. The following theorem of Witt, which we will state without proof (see [La:1973] or [Sc:1985]), says that to understand isometries between diagonal forms in general, it suffices to understand isometries between binary diagonal forms.

Theorem 1.16 *(Witt's Chain Equivalence Theorem) If $\langle a_1, a_2, \ldots, a_n\rangle \simeq \langle b_1, b_2, \ldots, b_n\rangle$, then it is possible to get from the first diagonal form to the second diagonal form by a finite sequence of intermediate isometries involving only two of the diagonal entries of the form, i.e. isometries of the type*

$$\langle c_1, \ldots, c_i, \ldots, c_j, \ldots, c_n\rangle \to \langle c_1, \ldots, c_i', \ldots, c_j', \ldots, c_n\rangle,$$

where $\langle c_i, c_j\rangle \simeq \langle c_i', c_j'\rangle$.

Understanding isometries between binary diagonal forms is in theory quite simple. Two binary forms are isometric if and only if they have the same determinant and represent a common value. This follows immediately from the First Representation Theorem and the fact that the determinant of a form is an invariant of its isometry class.

We conclude this section by actually determining the Witt ring for the fields $\mathbf{C}, \mathbf{R}$, and $\mathbf{F}_q$, the finite field with $q = p^i$ elements.

1. Let $F = \mathbf{C}$. Then $F = F^2$, i.e. every element is a square. The unique nonzero anisotropic form is $\langle 1\rangle$, since $\langle a\rangle = \langle ab^2\rangle \quad \forall a, b \in \dot{F}$. Therefore $W(F) \cong \mathbf{Z}/2\mathbf{Z}$. This generalizes to "quadratically closed fields", i.e. those field with $F = F^2$.

2. Let $F = \mathbf{R}$. Then F has two square classes: $\dot{F}/\dot{F}^2 = \pm 1$. We have
$$\langle a\rangle \cong \begin{cases} \langle 1\rangle & \text{if} \quad a \in \dot{F}^2 \\ \langle -1\rangle & \text{if} \quad a \in -\dot{F}^2 \end{cases}$$
Thus a nonzero anisotropic form is either $r\langle 1\rangle$ (positive definite) or $r\langle -1\rangle$ (negative definite) for some positive integer r, and $W(\mathbf{R}) \cong \mathbf{Z}$. This generalizes to "Euclidean fields" , i.e. fields F with $\dot{F}/\dot{F}^2 = \{1, -1\}$ for which -1 is not a sum of squares.

3. Let $F = \mathbf{F}_q$. There are two cases to consider. First, assume $q \equiv 1(4)$. In this case we have $-1 \in \dot{F}^2$. Fix $s \notin \dot{F}^2$. The four anisotropic forms in

$W(F)$ are given by $0, \langle 1\rangle, \langle s\rangle, \langle 1, s\rangle$, and we have $W(F) \cong \mathbf{Z}/2\mathbf{Z}[\dot{F}/\dot{F}^2] \cong \mathbf{Z}/2\mathbf{Z}[\mathbf{Z}/2\mathbf{Z}]$. In the case $q \equiv 3(4)$, we have $-1 \notin \dot{F}^2$, and the four anisotropic forms are $0, \langle 1\rangle, \langle -1\rangle, \langle 1, 1\rangle$. Then $W(F) \cong \mathbf{Z}/4\mathbf{Z}$, generated by $\langle 1\rangle$.

2 Witt Rings and Quaternion Algebras

In the preceding section we have seen how to construct the Witt ring of a field, and have observed that we have isomorphisms $W(F)/IF \cong \mathbf{Z}/2\mathbf{Z}$ and $IF/I^2F \cong \dot{F}/\dot{F}^2$. In this section we will try to understand the quotient I^2F/I^3F, which will be very important for our study of the connections between Witt rings and Galois groups. This quotient is closely related to the behavior of quaternion algebras over the field F, and we will need to examine the connections between splitting of quaternion algebras and behavior of quadratic forms over F. The splitting of these algebras is in turn related to the Galois-theoretic properties of the field. We embark now, therefore, on an investigation of quaternion algebras and their connections to quadratic forms. We will end this section by finding some simple quadratic form theoretic criteria for the realization of certain small 2-groups as Galois groups over a field. We will give characterizations of Witt rings of fields with more sophisticated quadratic form structures in subsequent sections. These characterizations will often hinge on the study of the splitting of certain products of quaternion algebras over the field in question.

Definition 2.1 *Let F be a field of characteristic not 2, $a, b \in \dot{F}$. Consider the F-algebra with generators i, j and relations $i^2 = a, j^2 = b, ij = -ji$, i.e. i and j are anticommuting generators with squares a and b respectively. This F-algebra is called an F-quaternion algebra, and is denoted $(\frac{a,b}{F})$. When the field F is understood, we may sometimes denote this algebra simply by (a, b).*

The motivation for the definition is the classical case $F = \mathbf{R}, a = b = -1$. This algebra, $(\frac{-1,-1}{\mathbf{R}})$ is the skew field of classical quaternions (Hamiltonians).

Given a quaternion algebra $A = (\frac{a,b}{F})$, define $k = ij$. Among i, j, k, any pair will anticommute. As an F-vector space, $A = F \oplus Fi \oplus Fj \oplus Fk$, so $dim_F A = 4$. This is easily seen by representing A as a matrix algebra, and showing that the four elements $1, i, j, k$ are independent in this representation. For example, let K be any field containing $F(\sqrt{-a}, \sqrt{b})$. Set

$$x = \sqrt{-a}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad y = \sqrt{b}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Then sending $i \rightarrow x, j \rightarrow y$ gives an algebra homomorphism $A \rightarrow \mathrm{M}_2(K)$ in which the images of $1, i, j, k$ are F-linearly independent. Moreover, this construction clearly shows that $(\frac{-1,1}{F}) \cong \mathrm{M}_2(F)$.

Observations 2.2 *We have the following facts about quaternion algebras, which we present without proof. (See [Pi:1982].)*

1. *If K is any extension field of F, then $K \otimes_F (\frac{a,b}{F}) \cong (\frac{a,b}{K})$.*

2. *$A = (\frac{a,b}{F})$ is a central simple F-algebra.*

3. *The algebra $(\frac{a,b}{F})$ is symmetric in a and b; i.e. $(\frac{a,b}{F}) \cong (\frac{b,a}{F})$.*

4. *$(\frac{a,b}{F}) \cong (\frac{ax^2,by^2}{F})$ for any $x, y \neq 0 \in F$.*

5. *Any F-quaternion algebra $(\frac{a,b}{F})$ is either a skew field (division algebra) or is isomorphic to $\mathrm{M}_2(F)$ (split quaternion algebra).*

Definition 2.3 *Observe that any $v \in A = (\frac{a,b}{F})$ can be written as $v = \alpha + \beta i + \gamma j + \delta k$. We define $A_0 = \{\beta i + \gamma j + \delta k\}$ to be the pure quaternions. A_0 forms a three-dimensional subspace of A. For $0 \neq v \in A$, we have $v \in A_0 \iff v^2 \in F$ but $v \notin F$. A_0 is invariant under F-algebra automorphisms of A.*

Definition 2.4 *For any $v = \alpha + \beta i + \gamma j + \delta k \in A$, we define the conjugate $\overline{v}$ of v to be $\overline{v} = \alpha - \beta i - \gamma j - \delta k$. We then have $v = \overline{v} \iff v \in F$, $v = -\overline{v} \iff v \in A_0$. This operation obeys the usual properties of conjugation, namely $\overline{x+y} = \overline{x} + \overline{y}$, $\overline{rx} = r\overline{x}, r \in F$, $\overline{xy} = \overline{y}\,\overline{x}$. Define the trace of $x \in A$*

to be $T(x) = x + \overline{x} \in F$, and the norm of $x \in A$ to be $N(x) = x\overline{x} \in F$. We can associate a symmetric bilinear form to A by defining $B(x,y) = \frac{1}{2}T(x\overline{y}) = \frac{1}{2}(x\overline{y} + y\overline{x}) \in F$ for $x, y \in A$. The associated 4-dimensional quadratic form is just $N(x)$; this is called the norm form of A.

Observations 2.5 *The set $\{1, i, j, k\}$ forms an orthogonal basis for the quadratic space (A, N). The diagonalization of N with respect to this basis is given by $\langle 1, -a, -b, ab\rangle$. We abbreviate this form by $\langle\langle -a, -b\rangle\rangle$. (In general, we may write $\langle\langle a_1, a_2, \ldots a_n\rangle\rangle$ to denote the n-fold tensor product $\langle 1, a_1\rangle \otimes \langle 1, a_2\rangle \otimes \ldots \otimes \langle 1, a_n\rangle$. Such a form is called an n-fold Pfister form.)*

Proposition 2.6 *N is a group form; i.e. $D_F(N)$ forms a multiplicative group.*

Proof. $N(xy) = xy \cdot \overline{xy} = xN(y)\overline{x} = x\overline{x}N(y) = N(x)N(y)$. □

Corollary 2.7 *$x \in A$ is invertible $\iff$ $N(x) \neq 0$ $\iff$ x is anisotropic. Thus A is a division algebra if and only if N is anisotropic.*

Proof. If x has an inverse x^{-1}, then $N(x)N(x^{-1}) = N(1) = 1$ so $N(x) \neq 0$. If $N(x) = \alpha \neq 0$, then $x\overline{x} = \alpha \cdot 1$, so $x^{-1} = \overline{x}\alpha^{-1}$. The final statement is obvious. □

Theorem 2.8 *Let $A = (\frac{a,b}{F}), A' = (\frac{a',b'}{F})$. The following statements are equivalent:*

(i) $A \cong A'$ as F-algebras.

(ii) $A \cong A'$ as quadratic spaces.

(iii) $A_0 \cong A_0'$ as quadratic spaces.

Proof. The equivalence of (ii) and (iii) follows from Witt's Cancellation Theorem. For (i) implies (ii), let $\varphi : A \to A'$ be an algebra isomorphism. Then $\varphi(A_0) = A_0'$. Take $x = \alpha + x_0 \in F \oplus A_0$. Then $\varphi(x) = \alpha + \varphi(x_0) \in F \oplus A_0'$. $\varphi(\overline{x}) = \varphi(\alpha - x_0) = \alpha - \varphi(x_0) = \overline{\varphi(x)}$. (So algebra isomorphisms commute with the conjugation operation.) To confirm that (i) implies (ii), we need only check that φ is an isometry: $N'(\varphi(x)) = \varphi(x)\cdot\varphi(\bar{x}) = \varphi(x\bar{x}) = \varphi(N(x)) = N(x)$, as desired. It remains to show that (iii) implies (i). Let $\sigma : A_0 \to A_0'$ be an isometry. Since i is orthogonal to j, we must have $\sigma(i)$ orthogonal to $\sigma(j)$, and hence $\sigma(i)$ and $\sigma(j)$ anticommute. Furthemore, $-\sigma(i)^2 = \sigma(i)\sigma(\bar{i}) = N(\sigma(i)) = N(i) = -a$, and therefore $\sigma(i)^2 = a$. Similarly, $\sigma(j)^2 = b$, so $A' \cong (\frac{a,b}{F}) = A$. □

Example. The algebras $(\frac{a,a}{F})$ and $(\frac{a,-1}{F})$ are always isomorphic, since their corresponding norm forms are $\langle 1,-a,-a,a^2\rangle$ and $\langle 1,-a,1,-a\rangle$, which are clearly isometric. We will use this fact repeatedly later.

Theorem 2.9 *N is isotropic $\iff$ N is hyperbolic $\iff$ $A \cong \mathbf{M}_2(F)$.*

Proof. A four dimensional isotropic form of determinant 1 (such as N) must be hyperbolic by determinant considerations. Then the algebra $A' = (\frac{-1,1}{F}) \cong \mathbf{M}_2(F)$ has $N' \simeq 2\mathbf{H} \simeq N$, so $A \cong \mathbf{M}_2(F)$. (Note also that (N, A) is hyperbolic $\iff$ (N, A_0) is isotropic, $\iff$ $\langle -a, -b, ab\rangle$ represents 0.) □

Theorem 2.10 *(Splitting Criteria) Let $A = (\frac{a,b}{F})$. The f ollowing are equivalent.*

1) A is split. ($A \cong \mathbf{M}_2(F)$; A is not a division algebra.)

2) $\langle a,b\rangle$ represents 1.

3) a is a norm from $F(\sqrt{b})$.

3') b is a norm from $F(\sqrt{a})$.

Proof. A is split $\iff$ $\langle\langle -a,-b\rangle\rangle \simeq 2\mathbf{H}$, $\iff$ $\langle 1,-a,-b,ab\rangle = 0 \in W(F)$, $\iff$ $\langle a,b\rangle \simeq \langle 1,ab\rangle$, $\iff$ $\langle a,b\rangle$ represents 1. This proves (1) $\iff$ (2). Notice also that $\langle 1,-a,-b,ab\rangle = 0 \in W(F)$ $\iff$ $\langle 1,-b\rangle \simeq \langle a,-ab\rangle$, $\iff$ $\langle 1,-b\rangle$ represents a. If $b = 1$, then all conditions are vacuously true. If $b \neq 1 \in \dot{F}/\dot{F}^2$, then the "norm form" for the (proper) field extension $F(\sqrt{b})$ is $\langle 1,-b\rangle$, so $\langle a,b\rangle$ represents 1 $\iff$ $\langle 1,-b\rangle$ represents a, $\iff$ $a \in N(F(\sqrt{b})/F)$, giving (2) $\iff$ (3). (3') follows by symmetry. □

Examples

1. $(\frac{a,1}{F})$ is split $\forall a \in \dot{F}$.
2. $(\frac{a,-a}{F})$ is split $\forall a \in \dot{F}$.
3. $(\frac{a,1-a}{F})$ is split $\forall a \in \dot{F}, a \neq 1$.
4. Over $\mathbf{F}_q$ (or any field over which binary forms are universal), all quaternion algebras split.

Corollary 2.11 *(Classification of Binary Forms) Given two nonsingular forms* $q = \langle a, b\rangle$ *and* $q' = \langle a', b'\rangle$, *we have* $q \simeq q' \iff d(q) = d(q') \in \dot{F}/\dot{F}^2$ *and* $(\frac{a,b}{F}) \cong (\frac{a',b'}{F})$.

We will want to work with quaternion algebras viewed as elements in the Brauer group $Br(F)$ of the field F. Recall that the Brauer group $Br(F)$ consists of equivalence classes of central simple F-algebras, under the equivalence relation $A \sim B \iff \exists r, s$ such that $\mathbf{M}_r(A) \cong \mathbf{M}_s(B)$ as F-algebras. The set of equivalence classes is made into a commutative group under the operation $\otimes_F$. We will be concerned solely with the subgroup of the Brauer group generated by the quaternion algebras. We will use the same notation to denote either a quaternion algebra or its equivalence class in the Brauer group. This should not cause any confusion in practice, as it should always be clear from the context what is intended. We will denote the product of two equivalence classes of quaternion algebras $(a, b), (c, d) \in Br(F)$ by $(a, b)(c, d)$, and the identity element (i.e. the class of F) will be denoted by 1. We will need the following facts about quaternion algebras, or their equivalence classes in the Brauer group, which we state without proof. (See [La:1973] or [Pi:1982].)

Theorem 2.12 *Let* $a, b, c, d \in \dot{F}$. *We have the following results.*

1. $(a, b)(a, c) = (a, bc) \in Br(F)$ *(weak bilinearity).*
2. $(a, b)(a, b) = 1 \in Br(F)$; *and thus* $(a, b) \cong (c, d) \iff (a, b)(c, d) = 1 \in Br(F)$.

3. $(a,b)(c,d) = 1 \in Br(F) \iff \exists x \in \dot{F}$ *such that* $(a,b) \cong (a,x), (c,d) \cong (c,x)$*, and* (ac,x) *is split;* $\iff bN(F(\sqrt{a})/F) \cap dN(F(\sqrt{c})/F) \cap N(F(\sqrt{ac})/F) \neq \emptyset$ *(common slot property, or linkage).*

Next we wish to understand the connections between splitting of (products of) quaternion algebras and structure of the Witt ring. Let $Br_2(F)$ denote the "2-part of the Brauer group", i.e. $Br_2(F) = \{x \in Br(F) : x^2 = 1\}$. Then in fact $Br_2(F)$ is the subgroup of $Br(F)$ generated by the (classes of) quaternion algebras. (This is a celebrated result of Merkurjev, [Me:1981], see also [Wd:1986].) It can then further be shown that $Br_2(F) \cong I^2F/I^3F$. The isomorphism is realized through the so-called Hasse-Witt invariant of a quadratic form.

Definition 2.13 *For a quadratic form* $q \simeq \langle a_1, \ldots a_n \rangle$ *over* F*, define the Hasse invariant of* q *to be* $s(q) = \prod_{i<j} (\frac{a_i a_j}{F}) \in Br_2(F)$ *This is an invariant of the isometry class of* q *(see [La:1973]). Let* $q \in I^2F$*, and set* $dim(q) = n = 2m$*. Then define the Hasse-Witt invariant* $\tilde{s}(q)$ *of* q *by* $\tilde{s}(q) = s(q) \cdot (\frac{-1,-1}{F})^{m(m-1)/2} \in Br_2(F)$*.*

Theorem 2.14 *The Hasse-Witt invariant determines a well-defined isomorphism* $I^2F/I^3F \to Br_2(F)$*.(For a proof, see [Me:1981] and [Wd:1986], and also [La:1973].)*

Note that the Hasse-Witt invariant of the form $\langle\langle -a, -b \rangle\rangle$ is precisely the (Brauer group class of) the quaternion algebra $(\frac{a,b}{F})$, so that quaternion algebras correspond under this isomorphism precisely to their associated norm forms. (I^2F is generated by these 2-fold Pfister forms, so in some sense this completely determines $\tilde{s}$.) Then a sum of 2-fold Pfister forms will be in I^3F precisely when the product of their corresponding quaternion algebras splits.

The close connection between I^2F/I^3F and $Br_2(F)$ is the linchpin of the proof for many of the results in the fourth and fifth sections of these notes, as this is critical to the understanding of the structure of the so-called "W-group"of F, which is a particular 2-Galois group of F. However, before we get to that point, we want to understand the connections among the appearance of small 2-groups as Galois groups over F, the splitting of quaternion algebras over F, and the behavior of quadratic forms over F.

First let us consider the rather trivial case of the realizability of $\mathbf{Z}/2\mathbf{Z}$ as an F-Galois group. Extensions of F with $\mathbf{Z}/2\mathbf{Z}$ as Galois group look like $F(\sqrt{a})$, $a \in \dot{F}, a \notin \dot{F}^2$. Thus $\mathbf{Z}/2\mathbf{Z}$ is not realizable as an F-Galois group precisely when F is quadratically closed, i.e. when $\dot{F}^2 = \dot{F}$. We determined the Witt ring of such a field at the end of the first section. We thus have the following.

Proposition 2.15 *The group $\mathbf{Z}/2\mathbf{Z}$ is not realizable as a Galois group over the field F if and only if $W(F) \cong \mathbf{Z}/2\mathbf{Z}$.*

Recall from Galois theory that if L and K are Galois extensions of F with $Gal(L/F) = G, Gal(K/F) = H$, and $L \cap K = F$, then LK (the compositum of L and K) is Galois over F, and $Gal(LK/F) \cong G \times H$. Thus if there exists an extension L with $Gal(L/F) \cong G$ for a given G, then there will also exist an extension M with $Gal(M/F) \cong G \times \mathbf{Z}/2\mathbf{Z}$ provided that $\dot{F}/\dot{F}^2$ is "big enough", i.e. as long as it is possible to find $a \in \dot{F}/\dot{F}^2$, $\sqrt{a} \notin L$. This is for the most part not too interesting, so from here on we will restrict our attention to the realizability of groups which do not have $\mathbf{Z}/2\mathbf{Z}$ as a direct factor.

We consider next groups of order 4. Of course there is only one that does not have $\mathbf{Z}/2\mathbf{Z}$ as a direct factor, namely $\mathbf{Z}/4\mathbf{Z}$, or C (for "cyclic") as we will denote it from here on. The realizability of this group turns out to be quite interesting. We have the following theorem, whose proof is "folklore".

Theorem 2.16 *Let F be a field of characteristic not 2, and $a \in \dot{F}, a \notin \dot{F}^2$. The following are equivalent.*

(i) $\exists$ an extension L/F with $Gal(L/F) \cong C$, such that $F(\sqrt{a})$ is the (unique) quadratic intermediate field between L and F.

(ii) $(\frac{a,a}{F}) \cong \mathbf{M}_2(F)$.

(iii) a is a sum of two squares in F.

(iv) The quadratic form $\langle a, a\rangle$ represents 1 over F.

Any such extension looks like $F(\sqrt{x + y\sqrt{a}})$, $\quad x, y \in F, x^2 - y^2a = z^2a, \exists z \in \dot{F}$.

Proof. (i) $\Longleftrightarrow$ (iv) is an elementary Galois theory exercise: Let $K = F(\sqrt{a}) \subsetneq L$. Then since L is necessarily a quadratic extension of K, we may write $L = F(\alpha)$, where $\alpha = \sqrt{x + y\sqrt{a}}$ for some $x, y \in F$, $\quad y \neq 0$. Then α satisfies the fourth degree polynomial $t^4 - 2xt^2 + x^2 - y^2a$ over F. It is easy to verify that the other roots of this polynomial are $-\alpha, \tilde{\alpha} = \sqrt{x - y\sqrt{a}}$, and $-\tilde{\alpha}$. Then L/F is Galois $\Longleftrightarrow$ $\tilde{\alpha} \in L$ $\Longleftrightarrow$ $\alpha\tilde{\alpha} = \sqrt{x^2 - y^2a} \in \dot{L}$ $\Longleftrightarrow$ $x^2 - y^2a \in \dot{L}^2$. Moreover, $\dot{L}^2 \cap K = \dot{K}^2 \cup (x + y\sqrt{a})K^2$, and $x^2 - y^2a \in F$. Thus $x^2 - y^2a \in \dot{L}^2$ $\Longleftrightarrow$ $x^2 - y^2a \in \dot{K}^2$ $\Longleftrightarrow$ $x^2 - y^2a \in \dot{F}^2 \cup a\dot{F}^2$. If $x^2 - y^2a \in \dot{F}^2$, then one can show $Gal(L/F) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Thus $Gal(L/F) \cong \mathbf{Z}/4\mathbf{Z} \Longrightarrow L = F(\sqrt{x + y\sqrt{a}})$, where $N_{F(\sqrt{a})/F)}(x + y\sqrt{a}) = az^2 \in a\dot{F}^2$. In other words, $x^2 = ay^2 + az^2$ has a solution over F. Conversely, if $L = F(\alpha)$ is such an extension of F, then it is not hard to see that L/F is Galois of degree 4, with cyclic Galois group generated by σ, where $\sigma(\alpha) = \tilde{\alpha}$. For (ii) $\Longleftrightarrow$ (iv) $\Longleftrightarrow$ (iii), observe that $(a, a) \cong \mathrm{M}_2(F)$ $\Longleftrightarrow$ $ax^2 + ay^2 = 1$ has a solution over F. Multiplying through by a, we see that $a^2x^2 + a^2y^2 = (ax)^2 + (ay)^2 = a$ for some $x, y \in F$, i.e. a is a sum of two squares in F. □

If F does not have C as a Galois group, then any sum of squares in F must in fact already be a square in F, i.e.$\sum F^2 = F$. Such a field is called *pythagorean.* Then either F is quadratically closed, or $-1 \notin \sum \dot{F}^2$, since if $-1 \in \sum \dot{F}^2$, then $\sum \dot{F}^2 = \dot{F}^2 = F$ (any element can always be expressed as a difference of two squares), and F would be quadratically closed. If $-1 \notin \sum \dot{F}^2$, we say F is a *real* field. Pythagorean real fields have some interesting quadratic form theoretic properties.

Corollary 2.17 *Let F be a field of characteristic not 2. The following are equivalent.*

1. *F is pythagorean.*

2. C is not a Galois group over F.

3. $W(F)$ is torsion free or $W(F) \cong \mathbf{Z}/2\mathbf{Z}$.

Proof. The equivalence of (1) and (2) follows directly from the preceding theorem, since if F is not pythagorean, there exists $a \in \dot{F}$ which is a sum of two squares, but which is not itself a square, and hence there exists a C-extension of F containing $F(\sqrt{a})$ as its unique quadratic intermediate field. Conversely, if F has a C-extension, then the unique quadratic intermediate field is $F(\sqrt{a})$ for some $a \in \dot{F}$, and by the theorem a must be a sum of two squares which is not a square. Then F cannot be pythagorean. Next consider (1) $\Longrightarrow$ (3). From the remarks preceding the corollary we may assume F is real. Let $q = \langle a_1, \ldots, a_n \rangle$ be an anisotropic form over F. Then for any positive integer k, $kq = q \perp \ldots \perp q$ is anisotropic. Indeed, $D_F(q) = D_F(kq)$. (Notice that if 0 is a sum of non-zero squares, then -1 is also a sum of squares.) To see (3) $\Longrightarrow$ (1), let $a \in F$ be a sum of two squares but not a square. Then $\langle 1, 1 \rangle \simeq \langle a, a \rangle$, so $2\langle 1, -a \rangle = 0 \in W(F)$, but $det(\langle 1, -a \rangle) \neq -1$, so $\langle 1, -a \rangle \neq 0 \in W(F)$. Thus there exists an element of additive order 2 in $W(F)$, and $W(F)$ is not torsion free. □

Before concluding this section we give the following theorem without proof, which says the realizability of any cyclic 2-group, of order bigger than 2, as a Galois group over F, hinges on the realizability of C. See [KLe:1975] for a proof.

Theorem 2.18 *For a field F of characteristic not 2, the following are equivalent.*

1. F admits a C-extension.

2. F admits a $\mathbf{Z}/2^n\mathbf{Z}$-extension for some $n \geq 2$.

3. F admits a $\mathbf{Z}/2^n\mathbf{Z}$-extension for every n.

Combining this with our result above, we get the following criteria for the "nonrealizability"of cyclic 2-extensions over a field F.

Corollary 2.19 *For a field F of characteristic not 2, the following are equivalent.*

1. *F admits no C-extension.*
2. *F admits no $\mathbf{Z}/2^n\mathbf{Z}$-extension for some $n \geq 2$.*
3. *F admits no $\mathbf{Z}/2^n\mathbf{Z}$-extension for any $n \geq 2$.*
4. *F is pythagorean*

In the next section, we will examine criteria for the realizability of other small 2-groups as Galois groups over F in terms of the behavior of quadratic forms over F. Our study will be aided by a powerful theorem of Fröhlich, which relates the realizability of certain groups as Galois groups to the splitting of products of certain quaternion algebras over F.

3 Galois Groups and Quaternion Algebras

In the preceding section we developed criteria for the realizability of groups of order 4 as Galois groups over F. We begin here with a study of the realizability of groups of order 8. There are exactly five such groups, three of which are abelian, and which have essentially been handled in the preceding section. The remaining two groups are D, the dihedral group of order 8, and Q, the quaternion group of order 8. Let us recall presentations of these two groups in terms of generators and relations:

$$D = \langle x, y | x^2 = y^2 = 1 = [x,y]^2, [x,y] \text{ central}\rangle$$
$$Q = \langle i, j | i^4 = j^4 = 1, i^2 = j^2 = [i,j]\rangle$$

Thus D is generated by two anticommuting reflections x and y, while Q is generated by two anticommuting elements i and j, each of order 4. The following theorem on the realizability of D as a Galois group over F is "folklore"; this result, along with the result on the realizability of C, is fundamental to the understanding of the W-group of F , which will be constructed in section 4 of these notes.

Theorem 3.1 *Let $a, b \in \dot{F}$, independent mod $\dot{F}^2$. There exists a Galois extension L/F with $Gal(L/F) \cong D, F \subsetneq F(\sqrt{a},\sqrt{b}) \subsetneq L$, and with $Gal(L/F(\sqrt{ab})) \cong C$, if and only if the equation $ax^2 + by^2 = z^2$ has a nontrivial solution over F. Any such extension can be written as $F(\sqrt{a},\sqrt{b},\sqrt{z + x\sqrt{a}})$, where $z^2 - ax^2 = by^2, \exists y \in F$. Equivalently, there exists such an extension if and only if $(\frac{a,b}{F})$ is split.*

Proof. Suppose first that L is such an extension. Then there are five intermediate subfields of codimension 2 in L; let K be one of them such that $\sqrt{b} \notin K$. Then $K = F(\sqrt{a},\sqrt{t})$ for some $t \in F(\sqrt{a})$, and it follows that $L = K(\sqrt{b}) = F(\sqrt{a},\sqrt{b},\sqrt{t})$. Since L is a C-extension of $F(\sqrt{ab})$ containing $F(\sqrt{ab},\sqrt{b})$ as its quadratic intermediate field, we see from the result in section 2 that $t = z + y\sqrt{b}$, for some $z, y, \in F(\sqrt{ab})$, where $N_{F(\sqrt{ab},\sqrt{b})/F(\sqrt{ab})}(t) = z^2 - by^2 = bx^2 \in F(\sqrt{ab})$. Since also $t \in F(\sqrt{a})$, we have $N_{F(\sqrt{ab},\sqrt{b})/F(\sqrt{ab})}(t) = N_{F(\sqrt{a})/F}(t)$, so $N_{F(\sqrt{a})/F}(t) \in b \cdot F(\sqrt{ab})^2 \cap \dot{F} = b\dot{F}^2 \cup a\dot{F}^2$. If $N_{F(\sqrt{a})/F}(t) \in a\dot{F}^2$, we would have $F(\sqrt{a},\sqrt{t})$ being a C-extension of F inside L, which is impossible since C is not a quotient of D. Thus we must have $N_{F(\sqrt{a})/F}(t) = b \in \dot{F}/\dot{F}^2$, and thus $b \in N(F(\sqrt{a})/F)$, so $ax^2 + by^2 = z^2$ has a nontrivial solution in F, as desired.

Conversely, suppose $t \in \dot{F}(\sqrt{a})$ is such that $N_{F(\sqrt{a})/F}(t) = by^2, y \in F$. Let $L = F(\sqrt{a},\sqrt{b},\sqrt{t})$. One can verify that L is indeed Galois over F, that $Gal(L/F(\sqrt{ab})) \cong C$, and letting τ be a generator of $Gal(L/F(\sqrt{ab}))$ and σ the generator of $Gal(L/F(\sqrt{a},\sqrt{t})$, one can check that σ and τ together generate $Gal(L/F)$, and that $\langle \sigma, \tau \rangle \cong D$. □

Observations 3.2 *We can make the following observations concerning the realizability of D as Galois group over the field F.*

1) *If $-1 \notin \dot{F}^2$ and $|\dot{F}/\dot{F}^2| \geq 4$, then D is always realizable as an F-Galois group, since for $a \in \dot{F}, a \notin \dot{F}^2, a$ and $-a$ are independent mod $\dot{F}^2$, and $(a, -a) = 1 \quad \forall a \in \dot{F}$.*

2) *If $-1 \in \dot{F}^2, D$ appears as a Galois group over $F \iff \exists$ an element $a \in \dot{F}, a \notin \dot{F}^2$, such that $\langle 1, a \rangle$ represents some element outside of $\dot{F}^2 \cup a\dot{F}^2$.*

Definition 3.3 *A field F which has the property $x^2 + ay^2 \in \dot{F}^2 \cup a\dot{F}^2 \quad \forall a \notin \pm\dot{F}^2$ is called rigid.*

R. Ware has shown that a field is rigid $\iff$ $W(F) \cong \mathbf{Z}/n\mathbf{Z}[G]$ for some $n \in \mathbf{Z}$ and some group G. (In fact, it is not hard to show that either $n = 2$, and $G \cong \dot{F}/\dot{F}^2$, or $n \in \{0, 4\}$ and G is isomorphic to a subgroup of index 2 in $\dot{F}/\dot{F}^2$ not containing -1.) (See [Wa:1978]) Thus we have the following criterion for the nonrealizability of D as Galois group over F.

Proposition 3.4 *D does not appear as a Galois group over F $\iff$ one of the following three conditions holds:*

1. *$-1 \in \dot{F}^2$ and F is rigid ($\iff$ $W(F) \cong \mathbf{Z}/2\mathbf{Z}[\dot{F}/\dot{F}^2]$).*
2. *$\dot{F}/\dot{F}^2 = \{1, -1\}, -1 \notin \dot{F}^2$, but$-1$ is a sum of two squares in F ($\iff$ $W(F) \cong \mathbf{Z}/4\mathbf{Z}$).*
3. *$\dot{F}/\dot{F}^2 = \{1, -1\}$ and -1 is not a sum of squares in F (i.e. F is Euclidean) ($\iff$ $W(F) \cong \mathbf{Z}$).*

Definition 3.5 *The least positive integer n such that -1 can be written as a sum of n squares in F is called the level of the field F, and is denoted $s(F)$. If F is real (-1 is not a sum of squares in F), then we define $s(F) = \infty$. (Thus from the remarks preceding the proposition above, we see that the level of a rigid field is 1, 2, or ∞. This is quite easy to prove, and is left as an exercise for the reader.)*

The other nonabelian group of order 8 is Q. The study of the realizability of Q as a Galois group began over a century ago. The first example of a field F realizing Q as a Galois group over $\mathbf{Q}$ was constructed by Dedekind [De:1886]. Bucht [Bu:1910] characterized quaternion extensions for fields where -1 is not a sum of two squares, and Witt [Wi:1936] solved the general case. More recently, Jensen and Yui [JeY:1987], R. Ware [Wa:1990] and I. Kiming [Ki:1990] have given treatments of such extensions. The following theorem (given without proof) describes the realization of the quaternion group as a Galois group over a field F.

Theorem 3.6 *Let F be a field of characteristic not 2, and let $a, b \in \dot{F}$, independent mod $\dot{F}^2$. The following conditions are equivalent.*

1. *There exists a Galois extension L of F, with $Gal(L/F) \cong Q$, and such that $F(\sqrt{a},\sqrt{b})$ is the unique biquadratic intermediate field between F and L.*

2. $(\frac{a,b}{F})(\frac{a,a}{F})(\frac{b,b}{F}) = 1 \in Br(F)$.

3. $\langle a, b, ab\rangle \simeq \langle 1, 1, 1\rangle$.

Moreover, if $ax_1^2 + bx_2^2 + \frac{1}{ab}x_3^2 \simeq y_1^2 + y_2^2 + y_3^2$, where the isometry is given by $x_i = \sum_{j=1}^{3} p_{ij}y_j, det(p_{ij}) = 1$, then the quaternion extensions containing $F(\sqrt{a},\sqrt{b})$ are given by $L = F(\sqrt{r(1 + p_{11}\sqrt{a} + p_{22}\sqrt{b} + p_{33}\sqrt{ab})}), r \in \dot{F}$.

Remark. The equivalence of the first and third statements is Witt's criterion for the realizability of Q. To see the equivalence of the second and third statements, notice that in $Br(F)$ we have

$$\begin{aligned}
(a,b)(a,a)(b,b) &= (a,b)(a,-1)(b,-1) = (a,-b)(b,-1)\\
&= (a,-b)(b,-1)(-1,-1)(-1,-1)\\
&= (a,-b)(-b,-1)(-1,-1) = (-a,-b)(-1,-1), \quad \text{and}\\
(-a,-b)(-1,-1) &= 1 \in Br(F) \iff (-a,-b) = (-1,-1), \iff \langle a,b,ab\rangle\\
&\simeq \langle 1,1,1\rangle.
\end{aligned}$$

We can make some additional observations concerning the realizability of Q as an F-Galois group, based on the level $s(F)$ of the field F.

Proposition 3.7 *Let $a, b \in \dot{F}$, independent mod $\dot{F}^2$.*

1. *If $s(F) = 1$, then $F(\sqrt{a},\sqrt{b})$ embeds in a Q-extension of F $\iff$ it embeds in a D-extension of F.*

2. *If $s(F) = 2$, then Q is realizable as a Galois group over F as long as F has at least four square classes (i.e. as long as F has a biquadratic extension).*

3. *If $s(F) \geq 4$, then if Q is realizable, so are D and C. Moreover ([Wa:1990]), Q is realizable $\iff$ sums of 2 squares in F are not all "rigid". (That is, $\exists a \in D(\langle 1,1\rangle), a \neq 1$, such that $D(\langle 1,a\rangle) \supsetneq \dot{F}^2 \cup a\dot{F}^2$.)*

Proof. For (1), notice that when $s(F) = 1$, then $(a,a) = (b,b) = 1 \in Br(F)$ $\forall a,b \in \dot{F}$. Thus the condition for $F(\sqrt{a},\sqrt{b})$ to embed in a Q-extension implies $(a,b) = 1$, and so $F(\sqrt{a},\sqrt{b})$ embeds in a D-extension L with $Gal(L/F(\sqrt{ab})) \cong C$. Conversely, if $F(\sqrt{a},\sqrt{b})$ embeds in a D-extension L of F, then the realizability criterion for D implies that one, and hence all, of $(a,b),(a,ab),(b,ab) = 1 \in Br(F)$, and we see $(a,b)(a,a)(b,b) = 1 \in Br(F)$ as desired.

For (2), let $a \in \dot{F}$ such that -1 and a are independent mod $\dot{F}^2$. We always have $(a,-a) = 1 \in Br(F)$, and if -1 is a sum of two squares then also $(-1,-1) = 1 \in Br(F)$. Then we have $(a,-1)(a,a)(-1,-1) = (a,-a)(-1,-1) = 1$, so Q is realizable as the Galois group of a quadratic extension of $F(\sqrt{a},\sqrt{-1})$.

For (3), we have Q realizable $\Longrightarrow \exists a,b \in \dot{F}$, independent mod $\dot{F}^2$, such that $\langle a,b,ab\rangle \simeq \langle 1,1,1\rangle$. Since $-1 \notin D_F(\langle 1,1\rangle)$, we must have $\{a,b,-1\}$ independent, so $|\dot{F}/\dot{F}^2| \geq 8$. Then by our earlier proposition, D occurs as an F-Galois group. Now a is a sum of three squares, so if a is not a sum of two squares, then sums of two squares cannot all be rigid. If a is a sum of two squares, then $\langle 1,a,a\rangle \simeq \langle 1,1,1\rangle \simeq \langle a,b,ab\rangle$ and by Witt's Cancellation Theorem , we have $\langle b,ab\rangle \simeq \langle 1,a\rangle$ so a is a sum of two squares which is not rigid. Then there exists an element c which is a sum of two squares but not a square, and thus a C-extension of F containing $F(\sqrt{c})$. Conversely, if Q is not realizable, then $a \in D_F(\langle 1,1\rangle)$ must be rigid (which in and of itself implies either $-1 \in \dot{F}^2$ or F is real and $|\dot{F}/\dot{F}^2| \geq 4$), or else we have $\langle b,ab\rangle \simeq \langle 1,a\rangle \Longrightarrow \langle a,b,ab\rangle \simeq \langle 1,a,a\rangle \simeq \langle 1,1,1\rangle$, where a,b are independent mod $\dot{F}^2$, and Q is realizable. □

This completes the analysis of the realizability of groups of order 8 as Galois groups over the field F, in terms of the behavior of quadratic forms over F. Notice that in fact the realizability of the groups C, D, and Q could all be framed in terms of the splitting of quaternion algebras or products of quaternion algebras. These are really just special cases of a much more general result given by Fröhlich, describing the realizability of certain Galois groups over F in terms of the splitting of products of certain quaternion algebras, determined by the presentation of the group [Fr:1985]. We will state a special case of this result here, and make use of it to analyze the realizability of a few more small 2-groups in terms of the behavior of quadratic forms, although the groups we will be considering are sufficiently small that one could give direct proofs of Fröhlich's result on a case-by-case basis.

Theorem 3.8 *(Embedding Criterion) Let* $K = F(\sqrt{a_1}, \ldots, \sqrt{a_r})$, *where* $a_1, \ldots, a_r$ *are independent mod* $\dot{F}^2$. *Let* $G = Gal(K/F) \cong (\mathbf{Z}/2\mathbf{Z})^r$. *Consider a (nonsplit) central extension* $\hat{G}$ *of* $\mathbf{Z}/2\mathbf{Z}$ *by* G*:*

$$1 \to \mathbf{Z}/2\mathbf{Z} \to \hat{G} \to G \to 1$$

Let $\langle \sigma_1, \ldots, \sigma_r \rangle = G$, *where* $\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}\sqrt{a_j}$, *and let* $\tau_1, \ldots, \tau_r$ *be a lifting of* $\sigma_1, \ldots, \sigma_r$ *to* $\hat{G}$. *Let* $c_{ij} \in \{0, 1\}$ *be defined by* $c_{ij} = 0 \iff [\tau_i, \tau_j] = 1, \quad i \neq j$ *and* $c_{ii} = 0 \iff \tau_i^2 = 1$. *There exists a Galois extension* $L/F, L \supseteq K$, *with* $Gal(L/F) \cong \hat{G}$, *and such that* $\hat{G} \to G$ *is the natural surjection of Galois groups,* $\iff \prod_{i \leq j}(a_i, a_j)^{c_{ij}} = 1 \in Br(F)$.

Notice that for $\hat{G} \cong C, D$, or Q, this gives exactly the results we have already obtained, concerning the realizability of these groups in terms of splitting of quaternion algebras. The groups whose realizability can be analyzed through this Embedding Criterion can all be realized as central products of the groups C, D, Q and the Klein 4-group $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, amalgamating the unique nontrivial central involutions in D and Q and an element of order two in C and the Klein 4-group. Since central products with the Klein 4-group are equivalent to direct products with $\mathbf{Z}/2\mathbf{Z}$, from our standpoint such groups are uninteresting. The Embedding Criterion will be most useful in investigating central products of D, Q, and C. These groups have been studied by many people; one rather thorough treatment is given in [LaSm:1989]. Central products of D and

Q are precisely the "extra-special" 2-groups, and as such are quite well-known. Each factor of C, D, or Q will contribute factors of (a_i, a_i), (a_i, a_j) $i \neq j$, or $(a_i, a_j)(a_i, a_i)(a_j, a_j)$, $i \neq j$, respectively, to the product of quaternion algebras. Of course, most 2-groups are not one of these central products, and hence can not be analyzed by our version of the Embedding Theorem. For the remainder of this section, however, we will concentrate on two more of those that can be analyzed in this way, specifically the central products DC of order 16 and DD of order 32. These are all the groups that can be expressed by relations involving no more than two quaternion algebras. It is also possible to analyze groups which require more than two quaternion algebras to express (see, e.g. [Sm:1993a] for a study of the realizability of DQ); however, the non-realizability of larger groups is of course more common, and gives predictably less information about the quadratic form structure of the field.

Groups of order 16 are small enough that it is in fact possible to study each of them in terms of realizability. Five of the fourteen groups of order 16 are abelian, and hence we already know something about their realizability. Of the remaining nine, two are direct products of nonabelian groups of order 8 with $\mathbf{Z}/2\mathbf{Z}$. Among the other seven, only one is covered by the Embedding Criterion given above. Several of the remaining six, however, have been analyzed by other methods, including Fröhlich's more general version of the Embedding Criterion. See, for example [C:1990], [Ki:1990] and [Sch:1989]. The group that is handled by our Embedding Criterion is DC, the central product obtained from the direct product $D \times C$ by identifying the unique central element of order 2 in D with the unique element of order 2 in C. This group has the following presentation.

$$DC = \langle x, y, z | x^2 = y^2 = z^4 = 1, [x, y] = z^2, z \text{ central} \rangle$$

By the Embedding Criterion we see that F has a Galois extension L with $Gal(L/F) \cong DC \iff \exists a, b, c$, independent mod $\dot{F}^2$, such that $(a, b)(c, c) = 1 \in Br(F)$. It turns out that the realizability of DC is related in a particularly nice way to the quadratic form structure of the field. We have the following theorem, combining results in [MiSm:1991] and [Wa:1978].

Theorem 3.9 *Let F be a field with $|\dot{F}/\dot{F}^2| \geq 8$. The following statements are equivalent.*

1. *DC does not appear as a Galois group over F.*
2. *F is a rigid field (i.e. for $a \notin \pm\dot{F}^2, D_F(\langle 1, a\rangle) = \dot{F}^2 \cup a\dot{F}^2$).*
3. *$W(F)$ is isomorphic to a group ring $\mathbf{Z}/n\mathbf{Z}[G]$.*

If F is a rigid field with at least 8 square classes, then $s(F) = 1 \iff D$ is not a Galois group over $F, s(F) = 2 \iff C$ and D are Galois groups over F, and $s(F) = \infty \iff C$ is not a Galois group over F. If $s(F) \neq 2$, then also Q cannot be realized as a Galois group over F when F is a rigid field.

Proof. The proof of (1) $\iff$ (2) can be found in [MiSm:1991], and the proof of (2) $\iff$ (3) in [Wa:1978]. We have already remarked that a rigid field has level 1, 2, or ∞. Moreover, we have observed that D is not an F-Galois group $\iff$ F is rigid and $s(F) = 1$. If $s(F) = 2$, then $(-1,-1) = 1$ and $(a, -a) = 1$ guarantee the realizability of C and D. If, however, $\exists c \in \dot{F}, c \notin \pm\dot{F}^2, (c, c) = 1 \in Br(F)$, then choosing a independent from $c, -1$ in $\dot{F}/\dot{F}^2$ gives $(a, -a)(c, c) = 1 \in Br(F)$, which implies DC can be realized over F. Thus if $s(F) = \infty$ and C is realizable over F, so is DC. Conversely, if C is not realizable, then $s(F) \neq 1, 2$, and so $s(F) = \infty$ by default. If F is rigid and $s(F) = \infty$, then of course all sums of squares in F are rigid, and by the proposition concerning the realizability of Q, we have that Q is also not an F-Galois group. If $s(F) = 1$ and F is rigid, then D is not realizable, and by the same proposition Q is not realizable. □

Let us summarize the connections we have thus far observed concerning the realizability of small 2-groups as Galois groups over F and the quadratic form structure of F.

1. $\mathbf{Z}/2\mathbf{Z}$ is realizable over $F \iff |\dot{F}/\dot{F}^2| \geq 2$.
2. $\mathbf{Z}/4\mathbf{Z}$ is realizable over $F \iff F$ is not pythagorean, $\iff \mathbf{Z}/2^n\mathbf{Z}$ is realizable over F $\forall n$.

3. D is realizable over $F \iff$ either $|\dot{F}/\dot{F}^2| \geq 4$ and $s(F) \geq 2$, or $s(F) = 1$ and F is not rigid.

4. Q is realizable over $F \iff |\dot{F}/\dot{F}^2| \geq 4$ and either $s(F) = 2$ or $s(F) \neq 2$ and sums of squares (other than $\pm\dot{F}^2$) are not all rigid.

5. DC is realizable over $F \iff |\dot{F}/\dot{F}^2| \geq 8$ and F is not rigid, $\iff W(F)$ is not a group ring $\mathbf{Z}/n\mathbf{Z}[G]$.

We conclude this study of small 2-groups and quadratic forms by examining the group $D \times D$, of order 64, and its quotient DD, which has the presentation

$$\langle x, y, z, w | x^2 = y^2 = z^2 = w^2 = [x,y]^2 = [z,w]^2 = 1, [x,y] = [z,w] = \epsilon, \\ \epsilon \text{ central}, \epsilon^2 = 1, [x,z] = [x,w] = [y,z] = [y,w] = 1\rangle.$$

Thus by the Embedding Criterion, DD is a Galois group over $F \iff \exists a,b,c,d \in \dot{F}$, independent mod $\dot{F}^2$, such that $(a,b)(c,d) = 1 \in Br(F)$. To study the realizability of this group, we will make use of the "common slot", or "linkage"property of quaternion algebras: $(a,b)(c,d) = 1 \iff \exists x \in \dot{F}$ such that $(a,b) = (a,x), (c,d) = (c,x)$, and $(ac,x) = 1 \in Br(F)$. (See [Sm:1993a,b] for details of the following results.)

Theorem 3.10 *DD is a Galois group over $F \iff D \times D$ is a Galois group over F. If DD is realizable, then so is DC. If $s(F) \geq 4$ and $|\dot{F}/\dot{F}^2| \geq 16$, then the realizability of Q as a Galois group over F implies the realizability of $D \times D$.*

Proof. (Sketch) In order to show the realizability of $D \times D$, it suffices to show the existence of two "independent"D-extensions, i.e. we must find two split quaternion algebras (r,s) and (t,u), with r,s,t,u independent mod $\dot{F}^2$. If DD is realizable, we have a,b,c,d, independent mod $\dot{F}^2$, with $(a,b)(c,d) = 1$. If $(a,b) = (c,d) = 1$, we are done. If not, choose x such that $(a,bx) = (c,dx) = (ac,x) = 1$. Clearly $x \neq 1$. By analyzing various possible dependence relations among the elements a, bx, c, dx, ac, x, it is possible to show that at least one of the three sets $\{a, bx, c, dx\}, \{a, bx, ac, x\}, \{c, dx, ac, x\}$ is a linearly independent set mod $\dot{F}^2$, and thus $D \times D$ is realizable. The reverse implication is trivial, since DD is a quotient of $D \times D$. If two independent D-extensions exist, then at least one must correspond to the splitting of a quaternion algebra (r, s) with $r, s, -1$ all independent mod $\dot{F}^2$. Then $\langle 1, -r, -s, rs\rangle = 0 \in W(F)$, so $rs \notin \pm\dot{F}^2, \langle 1, rs\rangle$ represents $r \notin \dot{F}^2 \cup rs\dot{F}^2$, and F cannot be rigid. Thus F has DC as Galois group. Finally, if Q is realizable and $s(F) \geq 4$, then sums of two squares are not rigid, so $\exists a \in D_F(\langle 1,1\rangle), b \in D_F(\langle 1,a\rangle)$, with $b \notin \dot{F}^2 \cup a\dot{F}^2$, so $(-a, b) = 1 \in Br(F)$, and $a, b, -1$ are independent mod $\dot{F}^2$. Since $|\dot{F}/\dot{F}^2| \geq 16, \exists c$ such that $a, b, -1, c$ are all independent mod $\dot{F}^2$, and thus $(c, -c)$ and $(-a, b)$ give two independent split quaternion algebras realizing $D \times D$. This result is interesting in that the realizability of a group of order 8 (Q) turns out to force the existence of groups of order 16 (DC), 32 (DD), and 64 ($D \times D$). □

We conclude this section by providing (without proof) the Witt ring criteria for realizability of $D \times D$. This result illustrates again how closely the Galois structure of F and Witt ring structure of F are connected.

Theorem 3.11 *Assume $|\dot{F}/\dot{F}^2| \geq 16$ and F is not rigid. If $s(F) \geq 2$, then DD (and hence also $D \times D$) is not a Galois group over $F \iff$ either $W(F) \cong (\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}[\Delta])[\Delta']$ (and $s(F) = \infty$) or $W(F) \cong (\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}[\Delta])[\Delta']$ (and $s(F) = 2$), where $\Delta \cong D_F(\langle 1,1\rangle)$ if $s(F) = \infty$, $\Delta \cong D_F(\langle 1,1\rangle)/\pm\dot{F}^2$ if $s(F) = 2$, and $\Delta' \cong \dot{F}/\pm D_F(\langle 1,1\rangle)$. If $s(F) = 1$, then DD is not a Galois group over $F \iff$ either $W(F) \cong (\mathbf{Z}/2\mathbf{Z}[\mathbf{Z}/2\mathbf{Z}] \times \mathbf{Z}/2\mathbf{Z}[\Delta])[\Delta']$ or $W(F) \cong (\mathbf{Z}/2\mathbf{Z}[\mathbf{Z}/2\mathbf{Z}] \times \mathbf{Z}/2\mathbf{Z}[\mathbf{Z}/2\mathbf{Z}] \times \mathbf{Z}/2\mathbf{Z}[\mathbf{Z}/2\mathbf{Z}])[\Delta']$, where $\Delta' \cong \dot{F}/B_F, B_F = \{a \in \dot{F} | a$ or $-a$ is not rigid$\}$.*

4 Absolute 2-Galois Groups, W-Groups, and Witt Rings

In this section we will examine connections between larger 2-Galois groups of F and the structure of $W(F)$. In particular we will study Galois groups from which it is possible to recover (almost) all information about $W(F)$. The two groups we will consider are the absolute 2-Galois group of F (i.e. the Galois group of the maximal 2-extension of the field F), and the so-called W-group of F, which is the Galois group of a generally much smaller 2-extension of F. We begin by defining each of these groups and describing to what extent each group determines and is determined by the Witt ring of F. We then study in more detail how various group-theoretic properties of these groups determine ring-theoretic properties of $W(F)$, and vice versa.The results concerning the absolute 2-Galois group which are presented here come primarily from the work of B. Jacob and R. Ware ([Wa:1979], [JWa:1989], [JWa:pre]), though many others have contributed to this study. The results on the W-group come primarily from work of Mináč and Spira, as well as the author ([Sp:1987], [MiSp:1990], [Sm:1988], [MiSp:1992], [MiSm1993a,b]). In many instances the results for the absolute 2-galois group and for the W-group are quite similar; the differences reflect the fact that the W-group is a quotient of the absolute 2-Galois group. Nonetheless, the somewhat surprising fact is that no information on the structure of the Witt ring is lost by considering this quotient rather than the larger group.

The purpose of the final two sections of these notes is primarily to demonstrate how closely the Witt ring of a field and the 2-Galois groups of that field are interrelated. The proofs of the results given here are in general considerably more technical than those of the results in the preceding sections, and for the most part will be omitted. The interested reader is encouraged to refer to the cited references for full proofs.

Definition 4.1 *Let $F(2)$ denote the maximal 2-extension (i.e. the quadratic closure) of the field F, and $G_F(2)$ the Galois group $Gal(F(2)/F)$ of this extension. Let $F^{(2)}$ denote the compositum of all quadratic extensions of F, and $F^{(3)}$ denote the compositum of all quadratic extensions K of $F^{(2)}$ such that K/F is Galois. Define the W-group $\mathbf{G}_F$ of F to be $Gal(F^{(3)}/F)$. Then both $G_F(2)$ and $\mathbf{G}_F$ are pro-2-groups, and $\mathbf{G}_F$ is a quotient of $G_F(2)$. The smaller group has the useful properties that it is of exponent 4, and that squares and commutators are central. Letting Φ_F denote the subgroup of $\mathbf{G}_F$ topologically generated by the squares of elements in $\mathbf{G}_F$, we have that $\Phi_F = Gal(F^{(3)}/F^{(2)})$*

and $\mathbf{G}_F/\Phi_F \cong Gal(F^{(2)}/F)$. Notice that $\mathbf{G}_F/\Phi_F \cong \prod_{i\in I} \mathbf{Z}/2\mathbf{Z}$ if and only if $\dot{F}/\dot{F}^2 \cong \bigoplus_{i\in I} \mathbf{Z}/2\mathbf{Z}$. This is immediate from the fact that $F^{(2)}$ is the compositum of quadratic extensions $F(\sqrt{a})$, where the a's range over a basis of $\dot{F}/\dot{F}^2$. It can also be shown that $F^{(3)}$ is the compositum over F of all quadratic, cyclic of order 4, and dihedral of order 8 extensions of F.

We have already seen that the splitting of the quaternion algebra $(\frac{a,b}{F})$ corresponds to the existence of either a dihedral of order 8 extension of F or (if $a = b \in \dot{F}/\dot{F}^2$) a cyclic of order 4 extension of F. Thus in some sense the W-group is the smallest Galois group over F carrying complete information about the splitting of quaternion algebras over F. On the other hand, knowing about the splitting of all quaternion algebras over F is equivalent to understanding the equivalence classes of all binary quadratic forms over F, and since equivalence of any two forms can be realized as a chain of equivalences of binary forms (by Witt's Chain Equivalence Theorem), it is thus not surprising that it is indeed possible to recover the structure of the Witt ring from the W-group. What is perhaps somewhat more surprising, however, is that this smaller Galois group, the W-group, in some ways does a better job of capturing the Witt ring structure than does the larger absolute 2-Galois group.

Theorem 4.2 *([Wa:1979]) Let F, L be fields with $G_F(2) \cong G_L(2)$. Then $W(F) \cong W(L)$, unless the level of one of the fields is 1 and of the other is 2.*

Remark. Once cannot hope to get rid of the condition on the levels of the fields in the theorem above. For example, the absolute 2-Galois group for $\mathbf{F}_3$ is $\mathbf{Z}_2$, as is the absolute 2-Galois group for $\mathbf{F}_5$. However, their Witt rings are not isomorphic, as we saw in 1. Moreover, the converse of the theorem is not true. For example, the fields $F_1 = \mathbf{C}((t_1))((t_2))$ and $F_2 = \mathbf{Q}_5$ each have Witt ring isomorphic to $\mathbf{Z}/2\mathbf{Z}[\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}]$, but $G_{F_1}(2)$ is abelian, while $G_{F_2}(2)$ is nonabelian. Other examples are given in [Wa:1979]. For the W-group, the situation is slightly better, as the following theorem indicates.

Theorem 4.3 *([Sp:1987]) Let F, L be fields with $\mathbf{G}_F \cong \mathbf{G}_L$. Then $W(F) \cong W(L)$ unless $\langle 1,1\rangle$ is universal over F, and $s(F) \neq s(L)$. If $W(F) \cong W(L)$, then $\mathbf{G}_F \cong \mathbf{G}_L$.*

Thus the Witt ring determines the W-group completely, and except in a relatively small number of cases, the W-group determines the Witt ring. The W-group has one further advantage over the absolute 2-Galois group in certain instances: when the square class group $\dot{F}/\dot{F}^2$ is finite, so is the W-group.

To gain some sense of the manner in which the W-group reflects the Witt ring, let us briefly sketch the construction of $\mathbf{G}_F$ from $W(F)$. Let $B = \{[a_i] : i \in I\}$ be a basis for $\dot{F}/\dot{F}^2$, where I is some (linearly ordered) index set. Let S be the free pro-2-group on $\{x_1 : i \in I\}$. Set $\bar{S} = S/\Phi(S)^2[\Phi(S), S]$ where Φ is the Frattini subgroup of S, and let z_i be the image of x_i in $\bar{S}$. Then $\mathbf{G}_F$ is $\bar{S}/R$, where $R \subseteq \Phi(\bar{S})$ and R is dual to $I^2F/I^3F \cong Br_2(F)$. More specifically, let $G_F(2)$ be (topologically) generated by $\{\sigma_i : i \in I\}$, where each σ_i has the property $\sigma_i(\sqrt{a_j}) = (-1)^{\delta_{ij}}(\sqrt{a_j})$, where δ_{ij} is the Kronecker delta. (The existence of such a set of generators follows from Kummer theory.) Then $G_F(2)$ can be viewed as an image of S under the map $x_i \to \sigma_i$. Now $\mathbf{G}_F = G_F(2)/\Phi(G_F(2))^2[\Phi(G_F(2)), G_F(2)] \cong \bar{S}/R$. To describe $\mathbf{G}_F$ it suffices to describe R. Note that $\Phi(\bar{S})$ is (topologically) generated by $\{z_i^2, [z_j, z_k] : i,j,k \in I, j < k\}$, and each of these generators is central and of order 2. Let Q be the abelian 2-group with basis $\{([a_i],[a_i]), ([a_j],[a_k]) : i,j,k \in I, j < k\}$, and define a pairing $\langle , \rangle : \Phi(\bar{S}) \times Q \to \mathbf{Z}/2\mathbf{Z}$ by letting these two sets serve as dual bases to each other. We have a group homomorphism $\theta : Q \to Br_2(F)$ determined by $([a_i],[a_j]) \to (\frac{a_i,a_j}{F})$ for all $i \leq j$. Then $R = (ker\theta^{\perp}) = \{s \in \Phi(\bar{S}) | \langle s, q\rangle = 0 \ \ \forall q \in ker\theta\}$. Moreover, the image of z_i in $\mathbf{G}_F$ is the image of σ_i in $\mathbf{G}_F$, i.e the following diagram commutes (where the maps are the obvious projections).

$$\begin{tikzcd}
S \arrow[r, "x_i \to \sigma_i"] \arrow[d, "x_i \to x_i"'] & G_F(2) \arrow[d, "\sigma_i \to r_i"] \\
\bar{S} \arrow[r, "x_i \to r_i"] & \mathbf{G}_F
\end{tikzcd}$$

Since $\Phi(\bar{S})$ is an elementary abelian 2-group, given a basis for the group, we can talk about which basis elements, or "factors", occur in an expression for any element in $\Phi(\bar{S})$ (or R). Dependence relations among quaternion algebras translate into conditions on factors which must be satisfied by elements in R. For example, if $(a_i, a_j), i \neq j$ and $(a_k, a_l), k \neq l$ are two algebras which are independent in $Br_2(F)$, then there is an element in R which has $[z_i, z_j]$ as a factor but not $[z_k, z_l]$. On the other hand, if $\prod(a_i, a_j) = 1 \in Br(F)$, then every element of R must have an even number of the corresponding squares and commutators occuring in its "factorization". As a special case, if $(a_i, a_j) = 1, i \neq j$ (respectively if $(a_k, a_k) = 1$), then $[z_i, z_j]$ (respectively z_k^2) does not appear as a factor of any element of R. The subgroup R of $\bar{S}$ can be described alternatively as

$$R = \langle \prod z_i^{2\beta_{ii}} \prod_{i<j} [z_i, z_j]^{\beta_{ij}} \mid \exists f \in H^1(I^2F/I^3F, 2) \text{ with } f(\langle\langle -a_i, -a_j \rangle\rangle) = \beta_{ij} \rangle.$$

As constructed, it is of course not at all clear that the isomorphism type of $\mathbf{G}_F$ does not depend on the choice of basis for $\dot{F}/\dot{F}^2$, but this is in fact the case. For many applications it is most convenient to start with a fortuitous choice of basis for $\dot{F}/\dot{F}^2$, and proceed from there. For example, one often wants to specify that -1 corresponds to a particular basis element a_i, since the relation $(\frac{a,a}{F}) \cong (\frac{a,-1}{F})$ holds for every $a \in \dot{F}$.

It is important to note that $\mathbf{G}_F$ is an extension of an elementary abelian 2-group by an elementary abelian 2-group, and that commutators and squares are central and of order 2. Moreover, any such group which appears as a Galois group over F must in fact be a quotient of $\mathbf{G}_F$. The construction of $F^{(3)}$ implies it is a maximal extension of F having such a Galois group; on the other hand, for any two Galois extensions K and L of F, whose Galois groups are extensions of elementary 2-groups by elementary 2-groups, their compositum will also have this property. Thus much can be said about what groups appear as Galois groups over F by just looking at the possible quotients of $\mathbf{G}_F$, and at the same time $\mathbf{G}_F$ determines and is determined by $W(F)$. These observations will be the underlying theme of the results presented in section 5 of these notes.

Next we will look at how the larger structure of the Witt ring in general corresponds to the group-theoretic structure of the absolute 2-Galois group and of the W-group. First we will examine the notion of a "basic indecomposable Witt ring", and how Witt rings in general can be constructed from such components, and then see what the corresponding constructions are for the Galois groups we are considering.

Definition 4.4 *An element $a \in \dot{F}/\dot{F}^2$ is rigid if $b \in D_F(\langle 1, a\rangle) \Longrightarrow b = 1$ or $b = a$. If $\dot{F}/\dot{F}^2 \neq \{1, -1\}$, we say $a \in \dot{F}/\dot{F}^2$ is basic if either a or $-a$ is not rigid, and let B_F denote the set of basic elements. (If $\dot{F}/\dot{F}^2 = \{1, -1\}$, we take 1 and -1 both to be basic.) We say the Witt ring $W(F)$ (or the field F) is basic if $\dot{F}/\dot{F}^2 = B_F$. By a result of Berman ([Be:1978]) we have that B_F is always a subgroup of $\dot{F}/\dot{F}^2$, containing -1. Let $\Delta \cong (\dot{F}/\dot{F}^2)/B_F$. Then in fact, $W(F) \cong R[\Delta]$ for some Witt ring R [Ma:1980].*

Definition 4.5 *A Witt ring is called indecomposable if it is not a nontrivial direct product of two other Witt rings in the category of Witt rings. Given two Witt rings W_1 and W_2, generated (as Witt rings) by square class groups G_1 and G_2 of the fields F_1 and F_2 respectively, then their direct product $W_1 \times W_2$ is generated by $G_1 \times G_2$ and has the property that the "quaternion algebra" (a, b) associated with the form $\langle\langle -a, -b\rangle\rangle$ is split if and only if $(\frac{a_1,b_1}{F_1})$ and $(\frac{a_2,b_2}{F_2})$ are split, where $a = (a_1, a_2)$ and $b = (b_1, b_2)$ in $G_1 \times G_2$. In other words, the ideal quotient I^2/I^3 in the direct product is precisely the direct product of the corresponding ideal quotients for the factors. For details see [Ma:1980].*

Definition 4.6 *A Witt ring is called basic indecomposable if it is both basic and indeomposable. A Witt ring is said to be of elementary type if it is built up from the indecomposable Witt rings of finite, real closed, and local fields, using the two operations of direct product (in the category of Witt rings) and group ring formation.*

The basic indecomposable Witt rings generating all elementary type Witt rings are $\mathbf{Z}, \mathbf{Z}/4\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}$, and $\mathbf{L}_{2k,0} = W(L), [L : \mathbf{Q}_2] = 2k-2, \sqrt{-1} \in L$, $\mathbf{L}_{2k,1} = W(L), [L : \mathbf{Q}_2] = 2k-2, \sqrt{-1} \notin L$, and $\mathbf{L}_{2k-1} = W(L), [L : \mathbf{Q}_2] = 2k-3$. (See [Ma:1980] for a more detailed explanation.)

The article [JWa:1989] by B. Jacob and R. Ware determines all possible absolute 2-Galois groups corresponding to finite, real closed, and local fields, and also determines how direct product in the category of Witt rings and group ring formation are manifested in the absolute Galois group. However, as mentioned earlier, the Witt ring does not completely determine the absolute 2-Galois group, as it does the W-group. Thus in [JWa:1989], Jacob and Ware were not able to determine whether certain "possible"pro-2-Galois groups are in fact realizable. This was partially resolved in [JWa:pre], but the description is rather complex. The problem lies in the fact that in order to say something about the absolute 2-Galois groups of a field, one must know quite a bit about the extensions of the field. For example, to be able to describe the Galois group of a field with Witt ring $R_1 \times R_2$, one needs to find field extensions having Witt rings R_1 and R_2. More importantly, one must keep track of how the Galois group acts on the $2^n th$ roots of unity. The following theorem, which is presented without proof, is a watered-down version of the results of [J:1981] and [JWa:1989]. It describes the correspondence between constructions of Witt rings via direct products and group ring formation, and the corresponding absolute 2-Galois groups.

Theorem 4.7 *([J:1981], [JWa:1989])*

1. *Let L_1 and L_2 be two field extensions of F inside $F(2)$, and suppose that field restriction induces an isomorphism $W(F) \cong W(L_1) \times W(L_2)$. Then $G_F(2) \cong G_{L_1}(2) *_2 G_{L_2}(2)$, where $*_2$ denotes the free product in the category of pro-2-groups. Conversely, if the inclusion maps $G_{L_i}(2) \to G_F(2)$ induce an isomorphism $G_F(2) \cong G_{L_1}(2) *_2 G_{L_2}(2)$, then $W(F) \cong W(L_1) \times W(L_2)$.*

2. *Let $W(F) \cong R[\Delta]$, where Δ is an elementary abelian 2-group, and $R \neq \mathbf{Z}/2\mathbf{Z}$. Then there exists a field K with $W(K) \cong R$, and a split short exact sequence*

$$1 \to A \to G_F(2) \to G_K(2) \to 1$$

where $A \cong (\mathbf{Z}_2)^I$, where $\mathbf{Z}_2$ denotes the 2-adic integers, with $|I| = dim_{\mathbf{Z}/2\mathbf{Z}}\Delta$ (i.e. A is the free abelian pro-2-group on $|I|$ generators). In particular, $G_F(2)$ is isomorphic to a semidirect product of A and $G_K(2)$. Conversely, let F be a field such that there is a split short exact sequence

$$1 \to A \to G_F(2) \to \bar{G} \to 1$$

where A is an abelian pro-2-group and $\bar{G} \neq 1$. Let $\Delta = Hom(A, \mathbf{Z}/2\mathbf{Z})$. Then there is a field $\bar{F}$ such that $G_{\bar{F}}(2) \cong \bar{G}$, and $W(F) \cong W(\bar{F})[\Delta]$.

When working with W-groups, one does not actually have to worry about finding appropriate field extensions with the right Witt rings in order to be able to say something about how the structure of the Galois group corresponds to group ring and direct product formation. This is essentially because the W-group can be constructed from the Witt ring itself, without any reference to the underlying field. This is of course not the case with the absolute 2-Galois group of a field. The downside is that in many instances the W-group carries significantly less information about the nature of all 2-extensions of F than does $G_F(2)$. Nonetheless, it is significant to note that in the cases when the Witt ring determines $G_F(2)$, then indeed the W-group determines $G_F(2)$ (except in the case mentioned above where the W-group fails to determine $W(F)$), and so this relatively small 2-extension completely specifies all Galois 2-extensions the field may possess.

The W-group analogue to the above theorem could be proved simply by the observation that $\mathbf{G}_F = G_F(2)/\Phi(G_F(2))^2[\Phi(G_F(2)), G_F(2)]$, but it is perhaps more enlightening to view the result in terms of the significance of group ring and direct product formation on I^2F/I^3F (or $Br_2(F)$), and the corresponding relations that determine $\mathbf{G}_F$. In any case it should be no surprise that group ring formation again corresponds to a semidirect product (and here we will describe the conjugation action of the semidirect product explicitly), and that direct products of Witt rings correspond to free products of W-groups, in an appropriately restricted category.

Let $W = W_1 \times W_2$ be a direct product of Witt rings. The "square class group" of the underlying field is in one-one correspondence with the one-dimenional forms of W. Denote this by G, and the square class groups for W_1 and W_2 by G_1 and G_2 respectively. Let also the W-group of W_i be denoted $\mathbf{G}_i, i = 1, 2$, and the W-group of W by $\mathbf{G}$. Finally, let $\tilde{*}$ denote the free-product in the category C of pro-2-groups whose squares and commutators are central and of order 2. In other words, for $H_1, H_2 \in C$, $H_1 \tilde{*} H_2 := H = [H_1 \times (H_1/\Phi(H_1) \otimes_{\mathbf{Z}/2\mathbf{Z}} H_2/\Phi(H_2))] \rtimes H_2$, where $H_1/\Phi(H_1) \otimes_{\mathbf{Z}/2\mathbf{Z}} H_2/\Phi(H_2)$ lies in the center of H, and for $h_i \in H_i, h_1h_2 = h_2h_1 \cdot (\bar{h}_1 \otimes \bar{h}_2)$, where $\bar{h}_i$ denotes the image of h_i in $H_i/\Phi(H_i)$.

Proposition 4.8 *([Sm:1988], [MiSm:1993b]) Keep the notation above. Then* $\mathbf{G} \cong \mathbf{G}_1 \tilde{*} \mathbf{G}_2$. *Conversely, if* $\mathbf{G} \cong \mathbf{G}_1 \tilde{*} \mathbf{G}_2$, *where* $\mathbf{G}_i$ *corresponds to the W-group associated to the Witt ring* W_i, *then* $\mathbf{G}$ *corresponds to the W-group associated to the Witt ring* $W_1 \times W_2$.

Sketch of Proof. Let $\mathbf{G}_i \cong \bar{S}_i/R_i$, and let $\bar{S} = \bar{S}_1 \tilde{*} \bar{S}_2$. Then $\mathbf{G} = \bar{S}/R$ for some R. Moreover, since any relation among quaternion algebras in W_i continues to hold in W, we have that R_i is a subgroup of $R, i = 1, 2$. We need to show that these are the "only" relations in R, i.e. that $R \cong R_1 \times R_2$. But we know that $I^2/I^3 \cong (I_1^2/I_1^3 \times I_2^2/I_2^3)$. Then $R = (I^2/I^3)^* \cong (I_1^2/I_1^3 \times I_2^2/I_2^3)^* \cong (I_1^2/I_1^3)^* \times (I_2^2/I_2^3)^* = R_1 \times R_2$, as desired. (Here * denotes the "dual".)

Conversely, if the W-groups $\mathbf{G}_i$ are as given, then it is indeed possible to construct a Witt ring W with W-group $\mathbf{G}$ (although the proof is outside the scope of these notes), and the corresponding Witt ring will have the properties $G \cong G_1 \times G_2$ and $I^2/I^3 \cong (I_1^2/I_1^3 \times I_2^2/I_2^3)$. This is precisely what is needed to guarantee that $W \cong W_1 \times W_2$. □

Now let us look at group ring formation. Assume that the Witt ring W is a group ring over some other Witt ring $\widetilde{W}$, i.e. $W \cong \widetilde{W}[\Delta]$ for some elementary 2-group Δ. Let G denote the square class group of W, and H the square class group of $\widetilde{W}$. Then $\Delta \cong G/H$, and the elements of $G \backslash H$ are all rigid in W. Let $\mathbf{G}$ be the W-group of W, and let $\widetilde{\mathbf{G}}$ be the W-group corresponding to $\widetilde{W}$, and let $\Delta \cong \sum_{i \in I} \mathbf{Z}/2\mathbf{Z}$. We have the following.

Proposition 4.9 *([Sm:1988], [MiSm:1993b]) Keep the notation above. Then* $\mathbf{G} \cong (\mathbf{Z}/4\mathbf{Z})^I \times \widetilde{\mathbf{G}}$ *if* $-1 = 1 \in \widetilde{W}$, *while* $\mathbf{G} \cong (\mathbf{Z}/4\mathbf{Z})^I \rtimes \widetilde{\mathbf{G}}$ *if* $-1 \neq 1 \in \widetilde{W}$. *In other words, there is a split short exact sequence*

$$1 \to (\mathbf{Z}/4\mathbf{Z})^I \to \mathbf{G} \to \widetilde{\mathbf{G}} \to 1.$$

(The precise action of the semi-direct product determined by this split exact sequence will be explained below.) Conversely, given $\mathbf{G} \cong (\mathbf{Z}/4\mathbf{Z})^I \rtimes \widetilde{\mathbf{G}}$, *with appropriate action, then in fact* $W \cong \widetilde{W}[\Delta]$ *where* $\Delta \cong \sum_{i \in I} \mathbf{Z}/2\mathbf{Z}$.

Sketch of Proof. Since $\widetilde{W}[\Delta_1 \oplus \Delta_2] \cong \widetilde{W}[\Delta_1][\Delta_2]$, we will make the simplifying assumption that $\Delta = \{1, b\} \cong \mathbf{Z}/2\mathbf{Z}$. Then $G = H \cup bH$, and everything in bH is rigid. Let $\widetilde{\mathbf{G}} \cong S/\widetilde{R}$, where $\{x_i : i \in I\}$ is a set of generators of S dual to a given basis $B = \{a_i : i \in I\}$ for H. Then choosing $B \cup \{b\}$ as a basis for G, we may take $\mathbf{G}$ to be generated by $\{x_i : i \in I\} \cup \{y\}$, subject to relations $R \supseteq \widetilde{R}$, where the given generators of $\mathbf{G}$ are taken to be dual to the given basis for G.

Assume first that $-1 = 1 \in \widetilde{W}$. To see that $\mathbf{G} \cong \mathbf{Z}/4\mathbf{Z} \times \widetilde{\mathbf{G}}$, we need only see that $R = \langle \widetilde{R}, [x_i, y] \rangle$, or equivalently that the only relations among the quaternion algebras $\{(a_i, a_j); (a_i, b); (b, b)\}$ are those that already exist among the quaternion algebras $\{(a_i, a_j)\}$, as well as $(b, b) = 1$. But since b is rigid, this is indeed the case.

If $-1 \neq 1 \in \widetilde{W}$, let the basis B be chosen so that $-1 = a_1$. Then $\mathbf{G} \cong \mathbf{Z}/4\mathbf{Z} \rtimes \widetilde{\mathbf{G}}$ where the action of the semi-direct product is induced by $x_1 y x_1^{-1} = y^{-1}$, y commutes with all other $x_i, i \in I$. The reason for this is that the only new relations among the quaternion algebras are again just those that are required to exist because of the rules governing quaternion algebras, namely $(b, b) = (-1, b) \neq 1$. Thus $R = \langle \tilde{R}; \quad [x_i, y] \ : \ i \in I, i \neq 1; \quad y^2[x_1, y] \rangle$.

Conversely, if $\mathbf{G}$ is a semi-direct product of $\widetilde{\mathbf{G}}$ with $\mathbf{Z}/4\mathbf{Z}$ as described, then the element b of $\dot{F}/\dot{F}^2$ which is "dual" to the generator of the $\mathbf{Z}/4\mathbf{Z}$-factor is rigid, and W is a group ring over $\Delta = \{1, b\}$. (See [Ma:1980], [Sm:1988], and [MiSm:1993b] for details.) □

Because of the direct correspondence between the W-group and the Witt ring, the structures of these two algebraic objects are related in many ways. We will examine a few more of these connections in the next and final section of these notes. We conclude this section with the following chart, giving the Witt rings and W-groups associated to real closed, finite, and p-adic fields. Here $\mathbf{Z}_n$ is used to denote $\mathbf{Z}/n\mathbf{Z}$.

Field	**Witt Ring**	**W-Group**
$\mathbf{R}$	$\mathbf{Z}$	$\mathbf{Z}_2$
$\mathbf{F}_q$	$\mathbf{Z}_2[\mathbf{Z}_2]$ or $\mathbf{Z}_4$	$\mathbf{Z}_4$
$\mathbf{Q}_p, p \equiv 3(4)$	$\mathbf{Z}_4[\mathbf{Z}_2]$	$\mathbf{Z}_4 \rtimes \mathbf{Z}_4$
$\mathbf{Q}_p, p \equiv 1(4)$	$\mathbf{Z}_2[\mathbf{Z}_2 \oplus \mathbf{Z}_2]$	$\mathbf{Z}_4 \times \mathbf{Z}_4$
$\mathbf{Q}_2$	$\mathbf{Z}_8 \oplus \mathbf{Z}_2(1-x) \oplus \mathbf{Z}_2(1-y)$	$[(\mathbf{Z}_2 \times \mathbf{Z}_4) \rtimes (\mathbf{Z}_2 \times \mathbf{Z}_4)] \rtimes \mathbf{Z}_4$

5 W-Groups and Quadratic Forms

In this final section we will study further connections between the behavior of the W-group $\mathbf{G}_F$ and the behavior of quadratic forms over F. In particular we will show how the W-group reflects orderings on the field F, how the W-group determines the level of the field, and how the quadratic form theoretic properties of a field being pythagorean or rigid are reflected in the W-group. Principle references for this section are [MiSp:1990], [MiSm:1993a] and [MiSm:1993b].

The connection between orderings on F and the W-group can be made through the one-to-one correspondence between orderings on F and "signatures" on the Witt ring $W(F)$.

Definition 5.1 *A signature on a Witt ring* $W(F)$ *is a map* $\sigma : \dot{F}/\dot{F}^2 \to \{1, -1\}$ *satisfying*

1. $\sigma(-1) = -1$ *and*

2. $\forall a, b \in \dot{F}/\dot{F}^2, \langle\langle -a, -b\rangle\rangle = 0 \in W(F) \Longrightarrow$ *either* $\sigma(a) = 1$ *or* $\sigma(b) = 1$, *or equivalently*

2'. $\sigma(a) = -1$ *and* $b \in D_F(\langle 1, -a\rangle) \Longrightarrow \sigma(b) = 1$.

We will write X_F *to denote the set of signatures on* $W(F)$.

Proposition 5.2 *([Ma:1980])* X_F *is in canonical one-to-one correspondence with the set of orderings on* F.

Theorem 5.3 *([Sp:1987], [Sm:1988], [MiSp:1990])* F *has an ordering (equivalently,* F *is formally real) if and only if* $\mathbf{G}_F$ *contains an element* x *of order 2,* $x \notin \Phi(\mathbf{G}_F)$. *Such an* x *will be called a "(nontrivial) involution" of* $\mathbf{G}_F$. *There is a one-to-one correspondence between the set of orderings on* F *and the cosets* $x\Phi(\mathbf{G}_F)$, *where* x *is a nontrivial involution of* $\mathbf{G}_F$.

Sketch of Proof. We have observed that $\dot{F}/\dot{F}^2$ is "dual" to $\mathbf{G}_F/\Phi(\mathbf{G}_F)$. Moreover, we can view X_F as a subset of the group $H^1(\dot{F}/\dot{F}^2, 2) \cong \mathbf{G}_F/\Phi(\mathbf{G}_F)$ of characters on $\dot{F}/\dot{F}^2$. Let $x \in \mathbf{G}$ be a nontrivial involution, and let $\hat{x}$ be the corresponding character in $H^1(\dot{F}/\dot{F}^2, 2)$. Then a somewhat technical argument with generators and relations for $\mathbf{G}_F$ shows that $\hat{x}$ satisfies conditions (1) and (2') of the definition above, and hence that $\hat{x}$ must be a signature. (This is the approach used in [Sm:1988].) Alternatively, one can explicitly show that the set $P := \{p \in \dot{F} \mid \sqrt{p}^x = \sqrt{p}\}$ is an ordering on F. (This is the method employed in [MiSp:1990].)

Conversely, suppose σ is a signature on $W(F)$. Then σ can be viewed as an element of $\mathbf{G}_F/\Phi(\mathbf{G}_F)$, and thus can be lifted to an element $x \in \mathbf{G}_F$. Notice that any two elements in the same (nonidentity) coset of $\Phi(\mathbf{G}_F)$ in $\mathbf{G}_F$ have the same order, so the result will not depend on the choice of lifting of σ. Choose a basis $\{-1, a_i : i \in I\}$ for $\dot{F}/\dot{F}^2$, such that $\sigma(a_i) = 1 \quad \forall i \in I$. Then we can find dual generators $\{x, x_i : i \in I\}$ for $\mathbf{G}_F$, and showing $x^2 = 1 \in \mathbf{G}_F$ is equivalent to showing the existence of an $f \in H^1(I^2/I^3, 2)$ such that $f(\langle\langle 1,1\rangle\rangle) = 1$ and $f(\langle\langle -a_i, -a_j\rangle\rangle) = f(\langle\langle 1, -a_k\rangle\rangle) = 0 \quad \forall i,j,k \in I$. Setting $f = \frac{1}{4}\sigma$ achieves this.

For any involution x, let σ_x denote the signature induced by x. Then $\sigma_x = \sigma_y \iff x \equiv y \pmod{\Phi(\mathbf{G}_F)}$. Thus the number of distinct signatures on $W(F)$ is exactly the number of $\Phi(\mathbf{G}_F)$-cosets of $\mathbf{G}_F$, excluding $\Phi(\mathbf{G}_F)$, which contain an involution. □

Thus the W-group of a field F contains a nontrivial involution if and only if F has at least one ordering. Recall that a field can be ordered if and only if it is formally real, i.e. if and only if -1 is not a sum of squares in F, or equivalently, $s(F) = \infty$. The level of a field is reflected in the characteristic of $W(F)$, since if $s(F) = n$, we have $n\langle 1\rangle = n\langle -1\rangle$, and so $2n\langle 1\rangle = 0 \in W(F)$, but $(2n-1)\langle 1\rangle \neq 0$. Thus we see that $\mathbf{G}_F$ contains a nontrivial involution $\iff s(F) = \infty \iff$ the characteristic of $W(F) = 0$. It turns out also to be interesting to study when the W-group can be entirely generated by involutions.

Theorem 5.4 *([Sp:1987], [MiSp:1990]) The following conditions are equivalent:*

1. *F is pythagorean.*
2. *$\mathbf{G}_F$ is generated by involutions.*
3. *$\Phi(\mathbf{G}_F) = [\mathbf{G}_F, \mathbf{G}_F]$.*

Sketch of Proof. First suppose F is not formally real. Then F is pythagorean $\iff$ F is quadratically closed $\iff$ $\mathbf{G}_F = \{1\}$ and the theorem is vacuously true. Thus we may assume F is formally real. To see (1) $\implies$ (3), assume F is pythagorean and consider $\mathbf{G}_F/[\mathbf{G}_F, \mathbf{G}_F]$. This is an abelian 2-group, and it must thus be elementary or else F would have $\mathbf{Z}/4\mathbf{Z}$ as a Galois group (since it would be a quotient of $\mathbf{G}_F$), contradicting the fact that F is pythagorean. Thus $[\mathbf{G}_F, \mathbf{G}_F] \subseteq \Phi(\mathbf{G}_F) \subseteq [\mathbf{G}_F, \mathbf{G}_F]$, and (3) is proved. That (3) $\Longrightarrow$ (2) follows because $[\mathbf{G}_F, \mathbf{G}_F] \subseteq \Phi(\mathbf{G}_F)$ implies that the generators of $\mathbf{G}_F/[\mathbf{G}_F, \mathbf{G}_F]$ lift to generators of $\mathbf{G}_F$, and the order of the generators in $\mathbf{G}_F$ may be taken to be the same as their order in $\mathbf{G}_F/[\mathbf{G}_F, \mathbf{G}_F]$. For (2) $\Longrightarrow$ (1), notice that if F is not pythagorean, then $\mathbf{G}_F$ must have $\mathbf{Z}/4\mathbf{Z}$ as a quotient, and thus cannot be generated by involutions. □

Remark. As was shown in section 2, a field F is real pythagorean if and only if $W(F)$ is torsion free. Summarizing what we have shown about pythagorean fields, we have the following list of equivalent conditions.

1. F is pythagorean.

2. $\mathbf{G}_F$ is generated by involutions.

3. $\mathbf{Z}/4\mathbf{Z}$ does not appear as a Galois group over F.

4. $W(F) \cong \mathbf{Z}/2\mathbf{Z}$ or $W(F)$ is torsion free.

The W-group, as we have mentioned, does indeed carry essentially all the information necessary to determine equality between forms in the Witt ring, and in particular the W-group contains complete information about the set of elements represented by any binary quadratic form. Notice that $D_F(\langle b\rangle q) = bD_F(q)$ for any $b \in \dot{F}$, so it is sufficient to determine $D_F(\langle 1, a\rangle)$. The complete description and proofs of how this information is carried in the W-group is rather technical; the reader is referred to [MiSm:1993a] for full details. We present the following two theorems here without proof to give the flavor of the result.

Theorem 5.5 *For some linearly ordered index set I and some subset $J \subseteq I$, let $A = \{a_i : i \in I\}$ be a basis for $\dot{F}/\dot{F}^2$ such that $\{a_j : j \in J\}$ forms a basis for $D_F(\langle 1, 1\rangle)$. Then the maximal abelian quotient $(\mathbf{G}_F)^{ab}$ of $\mathbf{G}_F$ is isomorphic to*

$\prod_{j\in J}(\mathbf{Z}/4\mathbf{Z}) \times \prod_{i\in I\setminus J}(\mathbf{Z}/2\mathbf{Z})$. Moreover, $(\mathbf{G}_F)^{ab} \cong Gal(F^{ab}/F)$, where F^{ab} is the maximal abelian extension of F inside $F^{(3)}$, which in turn is the compositum of all quadratic and cyclic of order 4 extensions of F.

Theorem 5.6 *Let $a \in \dot{F}, a \notin \dot{F}^2$. Then $D_F(\langle 1, a\rangle)$ can be identified from $\mathbf{G}_F$ by the following sequence of steps.*

1. *Let $a = a_k \in A = \{a_i : i \in I\}$ where A is a basis for $\dot{F}/\dot{F}^2$, and let $\{x_i : i \in I\}$ be a set of "dual" generators for $\mathbf{G}_F$.*
2. *Consider projections θ of $\mathbf{G}_F$ onto groups $\langle \bar{y}_j : j \in J\rangle >\!\!\lhd \langle \bar{x}_k\rangle \cong (\prod_{j\in J}\mathbf{Z}/4\mathbf{Z}) >\!\!\lhd \mathbf{Z}/2\mathbf{Z}$, where $\bar{x}_k\bar{y}_j\bar{x}_k^{-1} = \bar{y}_j^{-1}$, $\bar{x}_k$ is the image of x_k, and the preimages y_j of the $\bar{y}_j$ are in $\langle x_i : i \neq k\rangle\Phi(\mathbf{G}_F)$.*
3. *Choose one such map θ with J maximal. Then $\{x_k, y_j : j \in J\}$ forms a partial set of generators for $\mathbf{G}_F$. Extend to a complete set $\{x_k, y_i : i \in I'\}, J \subseteq I'$, such that $\{y_i : i \in I'\} \subseteq \langle x_i : i \neq k\rangle\Phi(\mathbf{G}_F)$ and $\{y_i : i \in I' \setminus J\} \subseteq ker(\theta)$.*
4. *Let $\{a_k, b_i : i \in I'\}$ be a corresponding "dual" basis for $\dot{F}/\dot{F}^2$. Then $\{a_k, b_j : j \in J\}$ forms a basis for $D_F(\langle 1, a_k\rangle)$.*

From a field-theoretic standpoint, this quotient of $\mathbf{G}_F$ arises as the Galois group $Gal(L/F)$ where L is the compositum of all extensions K of F such that $F \subsetneq F(\sqrt{a}) \subsetneq K, Gal(K/F) \cong D$, and $Gal(K/F(\sqrt{a})) \cong \mathbf{Z}/4\mathbf{Z}$.

Remark. If $\theta : \mathbf{G}_F \to \langle \bar{y}_j : j \in J\rangle >\!\!\lhd \langle \bar{x}_k\rangle \cong (\prod_{j\in J}\mathbf{Z}/4\mathbf{Z}) >\!\!\lhd \mathbf{Z}/2\mathbf{Z}$ is a projection determining $D_F(\langle 1, a_k\rangle)$, then there exists a projection $\tilde{\theta} : \mathbf{G}_F \to \langle \tilde{y}_j : j \in J\rangle >\!\!\lhd \langle \tilde{x}_k\rangle \cong (\prod_{j\in J}\mathbf{Z}/4\mathbf{Z}) >\!\!\lhd \mathbf{Z}/4\mathbf{Z}$, such that θ factors through $\tilde{\theta}$, if and only if $(a_k, a_k) = 1 \in Br(F)$. This is essentially because if $(a_k, a_k) = 1$, then x_k^2 does not appear in any of the relations determining $\mathbf{G}_F$, where as if $(a_k, a_k) \neq 1$, then necessarily x_k^2 enters in some relation, and $\mathbf{G}_F$ cannot have such a quotient.

The fields which have the "smallest" W-groups (relative to the size of their square class group) will be those with the fewest relations among their quaternion algebras, i.e. those fields for which $Br_2(F) \cong I^2F/I^3F$ is "large". These are precisely the so-called rigid fields. Recall that a field is *rigid* if $D_F(\langle 1, a\rangle) = \dot{F}^2 \cup a\dot{F}^2$ whenever $a \notin \pm\dot{F}^2$. A result of Ware ([Wa:1979]) proved that F is rigid if and only if $W(F)$ is a group ring $\mathbf{Z}/n\mathbf{Z}[G]$. We have already obtained a Galois theoretic description of such fields in 3 –they are those fields which do not have DC as a Galois group. Now, however, we would like to describe the W-groups of rigid fields. If F is rigid, it is not hard to see that $s(F) = 1, 2$, or ∞. First assume $-1 \in \dot{F}^2$, and let $\{a_i : i \in I\}$ be a basis for $\dot{F}/\dot{F}^2$. Then if F is rigid, the quaternion algebras $(\frac{a_i,a_j}{F}), i < j$ are all independent, while $(\frac{a_i,a_i}{F}) = 1$ since $s(F) = 1$. Next suppose that $s(F) \geq 2$, and let $\{-1, a_i : i \in I\}$ be a basis for $\dot{F}/\dot{F}^2$. If $s(F) = 2$, the only relations among quaternion algebras on the generators arise from $(\frac{a_i,a_i}{F})(\frac{a_i,-1}{F}) = 1$ and $(\frac{-1,-1}{F}) = 1$. If $s(F) = \infty$, then the only relations among the quaternion algebras arise from $(\frac{a_i,a_i}{F})(\frac{a_i,-1}{F}) = 1$. Since the relations on the quaternion algebras are what determine the W-group, we can then "read off" the W-group from the information above. We have the following theorem, which essentially says that for a rigid field, the W-group corresponds to the group "determining" $D_F(\langle 1, -1\rangle)$.

Theorem 5.7 *([Sp:1987], [Sm:1988], [MiSp:1990]) Let* $|\dot{F}/\dot{F}^2| \geq 4$, *and write* $\dot{F}/\dot{F}^2 \cong (\otimes_{i\in I}\mathbf{Z}/2\mathbf{Z}) \otimes \mathbf{Z}/2\mathbf{Z}$, *where I is a nonempty index set. Then*

1. $\mathbf{G}_F \cong (\prod_{i\in I}\mathbf{Z}/4\mathbf{Z}) \times \mathbf{Z}/4\mathbf{Z} \iff$ *F is rigid and* $s(F) = 1$.

2. $\mathbf{G}_F \cong (\prod_{i\in I}\mathbf{Z}/4\mathbf{Z}) >\!\!\lhd \mathbf{Z}/4\mathbf{Z}$, *where the action of a generator σ of the outer $\mathbf{Z}/4\mathbf{Z}$ on $\tau \in \prod_{i\in I}\mathbf{Z}/4\mathbf{Z}$ is given by* $\sigma^{-1}\tau\sigma = \tau^3$, $\iff$ *F is rigid and* $s(F) = 2$.

3. $\mathbf{G}_F \cong (\prod_{i\in I}\mathbf{Z}/4\mathbf{Z}) >\!\!\lhd \mathbf{Z}/2\mathbf{Z}$, *where the action of a generator $\sigma \in \mathbf{Z}/2\mathbf{Z}$ on $\tau \in \prod_{i\in I}\mathbf{Z}/4\mathbf{Z}$ is given by* $\sigma^{-1}\tau\sigma = \tau^3$, $\iff$ *F is rigid and* $s(F) = \infty$.

Remark. The first situation above, where F is rigid and $s(F) = 1$, is almost the only situation in which $\mathbf{G}_F$ is an abelian group. In fact, if $|\dot{F}/\dot{F}^2| \geq 4$ and

$\mathbf{G}_F$ is abelian, then indeed $s(F) = 1$ and F is rigid. If $|\dot{F}/\dot{F}^2| \leq 2$, then $\mathbf{G}_F$ is always abelian (and cyclic). We have $\mathbf{G}_F \cong \mathbf{Z}/2\mathbf{Z} \iff F$ is real (and hence Euclidean), $\iff W(F) \cong \mathbf{Z}$; $\mathbf{G}_F \cong \mathbf{Z}/4\mathbf{Z} \iff |\dot{F}/\dot{F}^2| = 2$ and F is not formally real, $\iff s(F) = 1$ or 2 and $W(F) \cong \mathbf{Z}/2\mathbf{Z}[\mathbf{Z}/2\mathbf{Z}]$ or $W(F) \cong \mathbf{Z}/4\mathbf{Z}$ respectively; and $\mathbf{G}_F = \{1\} \iff F$ is quadratically closed, $\iff W(F) \cong \mathbf{Z}/2\mathbf{Z}$.

R. Ware ([Wa:1979]) has also provided a very nice description of the absolute 2-Galois group of a rigid field. A profinite group G is called *metabelian* if there is an exact sequence $1 \to H \to G \to G/H \to 1$ where H is a closed normal abelian subgroup of G and G/H is abelian.

Theorem 5.8 *Let F be a field. The following statements are equivalent.*

1. *F is rigid.*
2. *$G_F(2)$ is metabelian.*
3. *If K is a finite Galois extension of F with $Gal(K/F)$ a 2-group, then $Gal(K/F)$ is metabelian.*
4. *If L is the field obtained from F by adjoining all 2^nth roots of 1 for all $n \geq 1$, then $Gal(F(2)/L)$ is abelian.*
5. *D does not occur as a Galois group over $F(\sqrt{-1})$.*

If F is rigid, then $G_F(2)$ is isomorphic to either

(a) $(\mathbf{Z}_2)^I$ for some set I (in which case $|I| = dim_{\mathbf{Z}/2\mathbf{Z}}\dot{F}/\dot{F}^2$ and if $|I| \geq 1$, then F contains all 2^nth roots of 1, for all $n \geq 1$), or

(b) an extension of $(\mathbf{Z}_2)^I$ by $\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}_2$, or $\mathbf{Z}_2 \times \mathbf{Z}/2\mathbf{Z}$, for some set I.

The results on determining the elements represented by a given binary form can also be used to determine the Kaplansky radical KR (or more precisely, $-KR$) of the field F. This in turn can be used to develop criteria for determining the level of a field from the Galois groups over it.

Definition 5.9 *The Kaplansky radical of the field F is the set of all elements $a \in \dot{F}/\dot{F}^2$ for which the binary form $\langle 1, -a\rangle$ is universal. In particular, $1 \in KR$ for every field F. We define $-KR = \{a \in \dot{F}/\dot{F}^2 | \langle 1, a\rangle$ is universal$\}$.*

Corollary 5.10 *Let $a_k \in A = \{a_i : i \in I\}$, where A is a basis for $\dot{F}/\dot{F}^2$. Then $a_k \in -KR \iff \exists$ a projection $\theta : \mathbf{G}_F \to (\prod_{i\in I, i\neq k} \mathbf{Z}/4\mathbf{Z}) >\!\!\lhd \mathbf{Z}/2\mathbf{Z}$ (with action as described for determining $D_F(\langle 1, a_k\rangle)$) such that $\theta^{-1}(\prod_{i\in I, i\neq k} \mathbf{Z}/4\mathbf{Z})$ is contained in the subgroup of $\mathbf{G}_F$ fixing $\sqrt{a_k}$.*

Remarks. When $s(F) \geq 2$, for any element $a \in -KR$, we have $a \in D_F(n\langle 1\rangle)$ $\iff$ $-1 \in D_F(n\langle 1\rangle)$ ([Be:1978]). Notice also that if $KR \supsetneq \{1\}$, then everything in $\dot{F}$ is basic, in other words, for any $b \in \dot{F}$, either b is not rigid or $-b$ is not rigid. For if $a \in KR, a \neq 1$, then $\langle 1, -a\rangle$ represents b, and so $\langle 1, b\rangle$ represents a, for all $b \in \dot{F}$. If b is rigid, then necessarily $b = a$, and so $b \in KR$. Then $\langle 1, -b\rangle$ is universal, and so $-b$ is not rigid, and b is basic as claimed.

We can now give explicit Galois-theoretic criteria for the level of a field to be $1, 2, 4$, or ∞. It is known that the level of a field must be either ∞ or a power of 2, and that all powers of 2 can occur. However, it is still not known whether there exist fields with only finitely many square classes, which have finite level bigger than 4. (This is related to the so-called "elementary type" question, which asks whether all Witt rings with finite square class groups are of elementary type. If this is indeed the case, then the level of any such field is necessarily either infinite or no bigger than 4.) Since the W-group is finite for fields with finitely many square classes, it may indeed be possible to develop a description of a W-group for a field of level 8, and then determine whether any finite W-groups can satisfy that description. We should observe that the level of a field is in fact quite easy to read off from the Witt ring – it is determined by the characteristic. Reading it off from the W-group proves to be considerably more technical.

We have in fact already seen the necessary and sufficient condition for a field to have level ∞. We know $s(F) = \infty \iff F$ is formally real, $\iff F$ can be ordered, $\iff \mathbf{G}_F$ contains a nontrivial involution. Also $s(F) \leq 2 \iff -1 \in$

$D_F(\langle 1,1\rangle)$, and $s(F) \leq 4 \iff \exists \quad b,c \in D_F(\langle 1,1\rangle)$ such that $-1 \in D_F(\langle b,c\rangle)$. In terms of the W-group $\mathbf{G}_F$, we have the following criterion for $s(F) \leq 2$. (See [MiSm:1993a] for proof.)

Proposition 5.11 *Assume $\dot{F}/\dot{F}^2 \cong (\oplus_{i\in I}\mathbf{Z}/2\mathbf{Z})\oplus\mathbf{Z}/2\mathbf{Z}$, where I is some (possibly empty) index set. If there exists a projection $\tilde{\theta} : \mathbf{G}_F \to (\prod_{i\in I}\mathbf{Z}/4\mathbf{Z}) >\!\!\lhd \mathbf{Z}/4\mathbf{Z}$, where the action of a generator σ of the outer $\mathbf{Z}/4\mathbf{Z}$-factor on $\tau \in \prod_{i\in I}\mathbf{Z}/4\mathbf{Z}$ is given by $\sigma^{-1}\tau\sigma = \tau^3$, then $s(F) \leq 2$. If $s(F) = 2$, then there exists such a projection. If $\langle 1,1\rangle$ is universal, then there exists a projection $\mathbf{G}_F \to (\prod_{i\in I}\mathbf{Z}/4\mathbf{Z}) \times \mathbf{Z}/4\mathbf{Z}$. This is always the case if $s(F) = 1$, and never the case if $s(F) \geq 4$.*

Notice that the one case where we cannot completely determine whether the level is 1 or 2 is precisely the case mentioned earlier, where the W-group does not completely determine the Witt ring, namely the situation where $\langle 1,1\rangle$ is universal, and $s(F) = 1$ or 2, but it cannot be determined from $\mathbf{G}_F$ which of the two cases one is in.

Next we give the Galois-theoretic description of fields of level 4. Such a field must have at least 8 square classes, since a field is of level 4 if and only if $-1 \notin D_F(\langle 1,1\rangle)$, but $-1 \in D_F(\langle b,c\rangle)$ for some $b,c \in D_F(\langle 1,1\rangle)$. Necessarily then, b, c, and -1 are independent mod $\dot{F}^2$. The crucial group for understanding fields of level 4 is the W-group $\mathbf{G}_2$ of the 2-adic field $\mathbf{Q}_2$, which has 8 square classes and is of level 4. This group can be described as follows:

$$\mathbf{G}_2 = \langle x_1,x_2,x_3 | x_i^4 = 1; x_1^2 = [x_2,x_3]; [x_1,x_2]^2 = [x_1,x_3]^2 = 1; [x_i,x_j], x_i^2 \text{ central}\rangle$$

We can then give the following criterion for a field to have level ≤ 4. Fields of level 4 will be those which meet the criterion to have level ≤ 4, but which fail the criteria given above for a field to have level 1 or 2.

Theorem 5.12 *Let F be a field with $\dot{F}/\dot{F}^2 \cong (\prod_{i\in I}\mathbf{Z}/2\mathbf{Z}) \times (\mathbf{Z}/2\mathbf{Z})^3$. Suppose there exists a projection $\pi : \mathbf{G}_F \to \tilde{G} : \langle y_i : i \in I\rangle >\!\!\lhd \langle x_1,x_2,x_3\rangle \cong (\prod_{i\in I}\mathbf{Z}/4\mathbf{Z}) >\!\!\lhd \mathbf{G}_2$, where $[x_2,y_i] = [x_3,y_i] = 1; [x_1,y_i] = y_i^2$, and x_1,x_2,x_3*

satisfy the same relations as their counterparts in the presentation of $\mathbf{G}_2$ *given above. Then* $s(F) \leq 4$. *Conversely, if* $s(F) = 4$, *then there exists such a projection.*

Sketch of Proof. Assume that $s(F) = 4$, and let b, c be such that $b, c \in D_F(\langle 1, 1\rangle)$ and $-1 \in D_F(\langle b, c\rangle)$. Then $(\frac{b,b}{F}) = (\frac{c,c}{F}) = 1 \in Br(F)$, and $(\frac{-1,-1}{F}) = (\frac{b,c}{F}) \neq 1 \in Br(F)$. Also $(\frac{d,d}{F}) = (\frac{-1,d}{F})$ $\forall d \in \dot{F}$. Let $\{-1, b, c, d_i : i \in I\}$ be a basis for $\dot{F}/\dot{F}^2$, and let $\{\tilde{x}_1, \tilde{x}_2, \tilde{x}_3, \tilde{y}_i : i \in I\}$ be a corresponding dual set of generators for $\mathbf{G}_F$. Then the relations above will enable $\mathbf{G}_F$ to project onto the group $\tilde{G}$ as described in the statement of the theorem. Conversely, if $\mathbf{G}_F$ admits such a projection, then let a, b, c be the elements corresponding to x_1, x_2, x_3 respectively. Results we have given earlier show $a \in -KR$, $\quad b, c \in D_F(\langle 1, 1\rangle)$, and so $s(F) \leq 4$. □

The connections between the 2-groups arising as Galois groups over a field F, and the behavior of quadratic forms over that field are many and deep. As we have seen, the fundamental link between the two is the splitting of quaternion algebras and their products over the given field. The absence of certain small 2-groups as Galois groups over a field gives very strong conditions on how quadratic forms over that field must behave. This is not surprising, since to say that a small group cannot be realized is indeed a big restriction. The W-group is the smallest group that actually carries complete information about the Witt ring, since it is the smallest group that determines the splitting of all quaternion algebras. The absolute 2-Galois group in fact carries even more information, so that it is possible for two fields with the same Witt ring to have different absolute 2-Galois groups.

There are a number of questions of interest in quadratic form theory which may be able to be answered by consideration of Galois groups. As mentioned above, one would like to know what the possible values are for the level of a field with finitely many square classes. The related question of whether all such fields have Witt rings of elementary type has not been able to be resolved, either. It would also be of interest to know how the "u-invariant" of a field is determined by the W-group. This invariant, which is equal to the largest integer n such that F has an anisotropic form of dimension n, has proved to be very mysterious, and again nobody knows completely what values it may assume. It would likewise be very interesting to gain more understanding of quadratic forms under field extensions. How is the Witt ring $W(K)$ of an even-degree extension K of F related to the Witt ring $W(F)$? Similarly, what are the connections between $\mathbf{G}_K$ and $\mathbf{G}_F$? The answers to these and many other questions can shed new light on the theory of quadratic forms, and it is possible that the answers lie buried in the 2-Galois groups of the field.

References

[Be:1978] L. Berman, *The Kaplansky Radical and Values of Binary Quadratic Forms over Fields*, Ph.D. Thesis, University of California , Berkeley, California, 1978.

[Bu:1910] G. Bucht, *Über einige algebraische Körper achten Grades*, Arkiv för Matematik, Astronomi och Fysik **2**, 1910, no. 30, 1-36

[C:1990] T. Crespo, *Explicit solutions to embedding problems associated to orthogonal Galois representations*, J. Reine Angew. Math. **409**, 1990, 180-189.

[De:1886] R. Dedekind, *Konstruktion von Quaternionkörpern*, Gesammelte mathematische Werke, Bd. 2, Vieweg Braunschweig, 1931, 376-384.

[Fr:1985] A. Fröhlich, *Orthogonal representations of Galois groups, Stiefel-Whitney classes, and Hasse-Witt invariants*, J. Reine Angew. Math. **360**, 1985, 84-123.

[J:1981] B. Jacob, *On the structure of Pythagorean fields*, J. Algebra **68**, 1981, 247-267.

[JWa:1989] B. Jacob and R. Ware, *A recursive description of the maximal pro-2-Galois group via Witt rings*, Math. Zeit. **200**, 1989, 379-396.

[JWa:pre] ——, *Realizing dyadic factors of elementary type Witt rings and pro-2-Galois groups*, preprint.

[JeY:1987] C. U. Jensen and N. Yui, *Quaternion extensions*, Algebraic Geometry and Commutative Algebra in Honor of Masayoshi Nagata, Kinokuniya, Tokyo, 1987, 155-182.

[Ki:1990] I. Kiming, *Explicit classifications of some 2-extensions of a field of characteristic different from 2*, Canad. J. Math **42**, 1990, 825-855.

[KLe:1975] W. Kuyk and H. W. Lenstra, Jr., *Abelian extensions of arbitrary fields*, Math. Ann. **216**, 1975, 99-104.

[La:1973] T.Y. Lam, *The Algebraic Theory of Quadratic Forms*, W. A. Benjamin, Reading, Massachusetts, 1973, Second printing with revisions, 1980.

[LaSm:1989] T.Y. Lam and T. L. Smith, *On the Clifford-Littlewood-Eckmann groups: A new look at periodicity mod 8*, Rocky Mtn. J. Math. **19**, 1989, 749-786.

[Ma:1980] M. Marshall, *Abstract Witt Rings*, Queen's Papers Pure Appl. Math. vol. 57, Queen's University, Kingston, Ontario, Canada, 1980.

[Me:1981] A. S. Merkurjev, *On the norm residue symbol of degree 2*, Dokl. Akad. Nauk. SSSr **261**, 1981, 542-547; English transl. in Soviet Math. Dokl. **24**, 1981, 546-551.

[MiSm:1991] J. Mináč and T. L. Smith, *A characterization of C-fields via Galois groups*, J. Algebra **137**, 1991, 1-11.

[MiSm:1993a] ———, *W-groups and values of binary forms*, J. Pure Appl. Alg. **87**, 1993, 61-78.

[MiSm:1993b] ———, *Decomposition of Witt rings and Galois groups*, preprint.

[MiSp:1990] J. Mináč and M. Spira, *Formally real fields, pythagorean fields, C-fields, and W-groups*, Math. Zeit. **205**, 1990, 519-530.

[MiSp:1992] ———, *Witt rings and Galois groups*, preprint.

[Pi:1982] R. Pierce, *Associative Algebras*, Grad. Texts in Math. vol 88, Springer-Verlag, New York, 1982.

[Sc:1985] W. Scharlau, *Quadratic and Hermitian Forms*, Grundlehren mat. Wiss. vol 270, Springer-Verlag, Berlin, 1985.

[Sch:1989] L. Schneps, *$\widetilde{D}_4$ et $\widehat{D}_4$ comme groupes de Galois*, C. R. Acad. Sci. Paris, Série **I 308**, 1989, 33-36.

[Sm:1988] T. L. Smith, *Some 2-Groups Arising in Quadratic Form Theory and Their Generalizations*, Ph.D. Thesis, University of California, Berkeley, California, 1988.

[Sm:1993a] ———, *Extra-special 2-groups of order 32 as Galois groups* Canad. J. Math. (to appear)

[Sm:1993b] ———, *Witt rings and realizability of small 2-Galois groups*, preprint.

[Sp:1987] M. Spira, *Witt Rings and Galois Groups*, Ph.D. Thesis, University of California, Berkeley, California, 1987.

[Wd:1986] A. Wadsworth, *Merkurjev's elementary proof of Merkurjev's theorem*, Contemp. Math. **55**, 1986, 741-776.

[Wa:1978] R. Ware, *When are Witt rings group rings?* **II**, Pac. J. Math. **76**, 1978, 51-564.

[Wa:1979] ——, *Quadratic forms and pro-finite 2-groups*, J. Algebra **58**, 1979, 227-237.

[Wa:1990] ——, *A note on the quaternion group as Galois group* Proc. Amer. Math. Soc. **108**, 1990, 621-625.

[Wi:1936] E. Witt, *Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der ordnung* p^f, J. Reine Angew. Math. **174**,1936, 237-245.

[Wi:1937] ——, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. **176**, 1937, 31-44.

Department of Mathematical Sciences
University of Cincinnati
Cincinnati, Ohio 45221-0025 U.S.A.