

W-Groups and Values of Binary Forms

Ján Mináč and Tara L. Smith

Abstract: The purpose of this article is to investigate the connections between the values assumed by binary quadratic forms over a field F (of characteristic not 2) and certain 2-groups arising as Galois groups over F . The groups in question will always be quotients of the so-called W -group of F . This group is the Galois group of the compositum over F of all quadratic extensions, cyclic extensions of order 4, and dihedral extensions of order 8. In this paper we show how the W -group and its quotients determine the values assumed by any binary quadratic form. The main result of this paper is to apply these ideas to give a simple characterization via Galois groups of fields with level ≤ 4 .

Contents:

§1. Preliminary Results and Definitions

§2. Main Lemmas

§3. Values of Binary Forms

§4. Determining the Level from the W -Group

§5. Properties and Examples of Level 4 Groups

References

§1 Preliminary Results and Definitions

We begin by recalling the relevant properties of the W -group which were developed in [MSp2] and [Sp]. (Some facts in [Sp] are proved only when F has finitely many square classes. In [MSp2], however, it is shown that these hold in the general setting.) We also recall some facts from quadratic forms and field theory, most of which can be found in standard references on quadratic forms and cohomology, e.g. [L], [Se1], [Se2], [La]. All fields will be assumed to have characteristic other than 2. All subgroups will be assumed to be topologically closed, and all homomorphisms between pro-2-groups will be assumed to be continuous. Every attempt has been made to keep the notations and conventions developed in [Sp]. In particular, we define the following notations.

Let F be a field, $F^* := F \setminus \{0\}$, and a an arbitrary element of F^* . We let $[a]$ denote the square class of a in the square class group F^*/F^{*2} , but we may occasionally write a for $[a]$ when the context is clear. Let $\{[a_i]: i \in I\}$ be a basis for F^*/F^{*2} , where I is some linearly ordered index set. Also let G be a pro-2-group, g and h be arbitrary elements of G , and $\{\sigma_j: j \in J\}$ be a minimal set of (topological) generators for G , where J is some index set. We then define

$F^{(2)} :=$ the compositum of F and all quadratic extensions of F .

- $F^{(3)} :=$ the compositum of $F^{(2)}$ and all quadratic extensions of $F^{(2)}$ which are Galois extensions of F .
- $F^{(2)} :=$ the quadratic closure of F , i.e. the compositum of all Galois extensions of F of degree a power of 2.
- $\cup_I F_i :=$ the smallest subfield containing all F_i , $i \in I$, inside of some given field.
- $G_F :=$ $\text{Gal}(F^{(2)}/F)$.
- $G^{(2)} :=$ $G^2[G, G]$, the Frattini subgroup $\Phi(G)$ of the pro-2-group G .
(Note that $G^{(2)} = G^2 := \langle g^2 \mid g \in G \rangle$ since $[G, G] \subseteq G^2$.)
- $G^{(3)} :=$ $(G^{(2)})^2[G^{(2)}, G]$.
- $G^{[2]} :=$ $G/G^{(2)}$.
- $G^{[3]} :=$ $G/G^{(3)}$. $G^{[3]}$ can be viewed as G with the additional relations
- (i) $g^4 = 1 \ \forall g \in G$,
 - (ii) $[g^2, h] = 1 \ \forall g, h \in G$,
 - (iii) $[[g, h], k] = 1 \ \forall g, h, k \in G$. (This is in fact a consequence of (ii).)
- $Z(G) :=$ the center of G .
- $s(F) :=$ the level of F , i.e. the least integer n such that -1 can be expressed as a sum of n squares in F , or ∞ if no such n exists.
- $G^{\text{ab}} :=$ $G/[G, G]$, the abelianization of G .
- $(a, b) :=$ the F -quaternion algebra generated by two anticommuting elements i and j , with $i^2 = a$ and $j^2 = b$, viewed as an element of the Brauer group $\text{Br}(F)$. (We write this group multiplicatively.)
- $\text{KR} :=$ the Kaplansky radical of $F := \{a \in F : \langle 1, -a \rangle \text{ is universal}\}$.

Proposition 1.1 [V], [MSp2] $F^{(3)}$ is the compositum of $F^{(2)}$ and all cyclic of order 4 and dihedral of order 8 extensions of F .

Proposition 1.2 $\text{Gal}(F^{(2)}/F) \cong G_F^{[2]}$. $\text{Gal}(F^{(3)}/F) \cong G_F^{[3]} =: \mathbb{G}_F$, the W -group of F .

The W -group \mathbb{G}_F of a field F is closely related to the Witt ring $W(F)$ of F . Indeed, it can be shown that $W(F)$ determines \mathbb{G}_F and, in all but a few special cases, \mathbb{G}_F determines $W(F)$. The nature of this correspondence is central to the results in this article, and we undertake a detailed explanation in §2. The precise connection between $W(F)$ and \mathbb{G}_F has been documented in [MSp2] and [Sp], as well as in [Sm] for abstract Witt rings. For any two fields F and K of characteristic not 2, we have the following.

Proposition 1.3 $W(F) \cong W(K) \Rightarrow \mathbb{G}_F \cong \mathbb{G}_K$.

Proposition 1.4 *Suppose that $\mathbb{G}_F \cong \mathbb{G}_K$, and assume also that if $\langle 1, 1 \rangle_F$ is universal, then $s(F) = s(K)$. Then $W(F) \cong W(K)$.*

We have that $\mathbb{G}_F \cong \text{Gal}(F^{(3)}/F)$. By the definition of $F^{(3)}$ we can then see that if a group G in the category \mathcal{C} of groups which are central extensions of an elementary abelian 2-group by an elementary abelian 2-group occurs as a Galois group over F , then G is isomorphic to a quotient group of \mathbb{G}_F . Conversely, any quotient of \mathbb{G}_F is in \mathcal{C} and appears as a Galois group for some field K , $F \subseteq K \subseteq F^{(3)}$. This fact, together with the connection between \mathbb{G}_F and $W(F)$, suggests that the presence or absence of certain groups as quotients of \mathbb{G}_F (i.e. as Galois groups over F) will give information about the behavior of quadratic forms over F . Indeed this is the case. In fact, as we will show in §3, the value group of any binary quadratic form over F can be determined from this approach. The question of the level $s(F)$ can also be tackled in this way. In §4 we develop Galois-theoretic criteria for determining when $s(F) \leq 2$ and when $s(F) \leq 4$. (Recall that if $s(F) < \infty$, then $s(F) = 2^k$ for some integer k . See, e.g., [L].) This gives a new and potentially fruitful way of looking at the "level question", which asks whether, for a field F with finitely many square classes, it is possible to have $s(F)$ take on a value other than 1, 2, 4, or ∞ . (In [MSp1] it is shown that $s(F) = \infty \Leftrightarrow \mathbb{G}_F$ has an element of order 2 which is not in its Frattini subgroup. See also [Sp] and [Sm].)

§2 Main Lemmas

In this section we collect a few simple arguments which we use frequently. Their purpose is to make clear to the reader how one goes about translating field-theoretic information into group theoretic results, and vice-versa. We begin with a definition to make our language less cumbersome.

Definition 2.1 *Suppose that $A = \{[a_i] : i \in I\}$ is a basis of F^*/F^{*2} , and that $\Sigma = \{\sigma_i : i \in I\}$ is a minimal system of generators of \mathbb{G}_F . We say that A is orthonormal to Σ if $\sigma_i(\sqrt{a_j}) = (-1)^{\delta(i,j)}(\sqrt{a_j})$ for all $i, j \in I$.*

Let $\{[a_i] : i \in I\}$ be a basis for F^*/F^{*2} , and let S be the free pro-2-group on generators $x_i, i \in I$. We take \mathbb{G}_F to be generated by $\{\sigma_i : i \in I\}$ where each σ_i has the property $\sigma_i(\sqrt{a_j}) = (-1)^{\delta(i,j)}(\sqrt{a_j}) \forall i, j \in I$; here $\delta(i, j)$ is the Kronecker delta. (The existence of such a set of generators follows from Kummer theory. See [AT].) We then

have a continuous surjection $\varphi: S \rightarrow G_F$ given by $x_i \rightarrow \sigma_i$. Let R^* denote the kernel of this map, so R^* is a closed normal subgroup of S . We have the exact sequence

$$1 \rightarrow R^* \rightarrow S \rightarrow G_F \rightarrow 1.$$

Using $G_F = G_F/G_F^{(3)}$, we obtain a new exact sequence

$$1 \rightarrow R \rightarrow S^{[3]} \rightarrow G_F \rightarrow 1$$

for some closed subgroup $R \subseteq \Phi(S^{[3]})$. Now $\Phi(S^{[3]})$ is topologically generated by $\{z_i^2, [z_i, z_j] : i, j \in I\}$, where z_i is the image of x_i in $S^{[3]}$. Note that $\Phi(S^{[3]})$ is a topological product of groups of order 2. Moreover, $\Phi(S^{[3]}) \subseteq Z(S^{[3]})$, and in fact $\Phi(S^{[3]}) = Z(S^{[3]})$ if $|I| \geq 2$. To describe G_F , it suffices to describe R . To do this we define a pairing $\langle, \rangle : \Phi(S^{[3]}) \times P \rightarrow \mathbb{Z}/2\mathbb{Z}$, where P is the set consisting of 0 and homogeneous polynomials of degree 2 in the variables $t_i, i \in I$, with coefficients in $\mathbb{Z}/2\mathbb{Z}$. The pairing \langle, \rangle is defined by letting $\{z_i^2, i \in I, [z_i, z_j], i, j \in I, i < j\} \subseteq \Phi(S^{[3]})$ and $\{t_i^2, i \in I, t_i t_j, i, j \in I, i < j\} \subseteq P$ be dual bases to each other. Let Q denote the group of quaternion algebras over F . We have a group homomorphism $\theta: P \rightarrow Q$ determined by $\theta(t_i^2) = (a_i, a_i)$ and $\theta(t_i t_j) = (a_i, a_j), i < j$. Then $R = (\ker \theta)^\perp := \{s \in \Phi(S^{[3]}) \mid \langle s, q \rangle = 0 \forall q \in \ker \theta\}$. The pairing \langle, \rangle induces a perfect duality $R \times Q \rightarrow \mathbb{Z}/2\mathbb{Z}$. Notice that R is defined relative to the given basis for F^*/F^{*2} . We shall, by abuse of notation, use the symbol \langle, \rangle for four different "pairings":

- (I) $\langle, \rangle : \Phi(S^{[3]}) \times P \longrightarrow \mathbb{Z}/2\mathbb{Z}$, as described above.
- (II) $\langle, \rangle : R \times Q \longrightarrow \mathbb{Z}/2\mathbb{Z}$, induced from I, as above.
- (III) $\langle, \rangle : \Phi(G_F) \times Q \longrightarrow \mathbb{Z}/2\mathbb{Z}$, defined by lifting generators σ_i of G_F to generators z_i of $S^{[3]}$, and (a_i, a_j) to $t_i t_j \in P$, and applying (I). This is well defined if the σ_i, z_i , and t_i are given.
- (IV) $\langle, \rangle : \Phi(S^{[3]}) \times Q \longrightarrow \mathbb{Z}/2\mathbb{Z}$, again defined by using (I) and lifting elements of Q to the corresponding elements of P .

While (I) and (II) are actually "perfect pairings", the maps given in (III) and (IV) are just convenient ways of writing the pairing (I) without explicitly referring to the lifting. We believe that this should cause no confusion in practice.

Now $\Phi(S^{[3]})$ is an elementary abelian (multiplicative) 2-group, so given a basis for the group, we can talk about which basis elements, or "factors", occur in an expression for any element in $\Phi(S^{[3]})$. Dependence relations among elements in Q translate into conditions on factors which must be satisfied by elements in R . For example, if (a_i, a_j) and (a_k, a_m) are two algebras in Q which are independent, then there is an element in R which has $[z_i, z_j]$ as a factor, but not $[z_k, z_m]$. On the other hand, if $\prod (a_i, a_j) = 1 \in Q$, then every element of R must have an even number of the corresponding squares and commutators occurring in its "factorization". As a special case, if $(a_i, a_j) = 1$ (or $(a_k, a_k) =$

1), then $[z_i, z_j]$ (or z_k^2) does not appear as a factor of any element in R . We will prove a couple of specific results along these lines in Lemmas 2.3 and 2.4 below. See [MSp2] and [Sp] for more details. This construction can also be done using the transgression map in group cohomology (see [MSp2]).

Definition 2.2 Suppose that $u \in \Phi(S^{[3]})$, $r \in R$, and that $z_i, i \in I$ is a given set of generators of $S^{[3]}$. Then we say u divides r or u enters r to mean that there exists $w \in \Phi(S^{[3]})$ such that

- i) $r = uw$
- ii) No element z_i^2 or $[z_i, z_j]$, $i, j \in I$, appears in both the decomposition of u and the decomposition of w .

In this case we shall write $u \mid r$.

For example, $z_1^2[z_2, z_3] \mid z_1^2[z_1, z_2][z_2, z_3]$, but $z_1^2[z_2, z_3] \nmid z_1^2 z_2^2$. The next two lemmas illustrate in a detailed way the comments made above on the connections between elements appearing in R and dependence relations in Q . Lemma 2.4 will be of particular importance in §4.

Lemma 2.3 Suppose $\Sigma = \{\sigma, \sigma_i, i \in I\}$ is a minimal system of generators of \mathbb{G}_F , and $A = \{a, a_i, i \in I\}$ is a basis for F^*/F^{*2} , orthonormal to Σ . Let also $\{z, z_i, i \in I\}$ be a system of generators of $S^{[3]}$ corresponding to Σ . Then z^2 does not enter any relation of \mathbb{G}_F if and only if $(a, a) = 1$.

Proof For each relation r of \mathbb{G}_F we have $\langle r, (a, a) \rangle = 0$ if and only if z^2 doesn't enter r . Hence, from the perfect duality between R and Q , we find $(a, a) = 1$ iff for each $r \in R$, the element z^2 does not enter r .

Lemma 2.4 Suppose that $A = \{a, b, c, d_i; i \in I\}$ is a basis for F^*/F^{*2} , and that $\Sigma = \{\sigma_x, \sigma_y, \sigma_z, \sigma_{w(i)}; i \in I\}$ is a minimal system of generators of \mathbb{G}_F orthonormal to A . Let $C = \{x, y, z, w_i; i \in I\}$ be the corresponding minimal set of generators of $S^{[3]}$. Then $(a, a)(b, c) = 1$ if and only if x^2 and $[y, z]$ enter or fail to enter each relation r of \mathbb{G}_F simultaneously.

Proof For each relation $r \in R$ we have $\langle r, (a, a)(b, c) \rangle = 0$ if and only if either both x^2 and $[y, z]$ divide r or neither x^2 nor $[y, z]$ divides r . Again the lemma follows from the perfect pairing between R and Q .

Lemma 2.5 For some linearly ordered index set I and some subset $J \subseteq I$, let $A = \{a_i : i \in I\}$ be a basis for F^*/F^{*2} such that $\{a_j : j \in J\}$ forms a basis for $D(\langle 1, 1 \rangle)$. Let $\Sigma = \{\sigma_i : i \in I\}$ be a minimal set of generators of \mathbb{G}_F orthonormal to A , and let $C = \{z_i : i \in I\}$ be the corresponding generators of $S^{[3]}$. Then for each $i \in I \setminus J$ there exists $s_i \in R$ such that z_i^2 divides s_i , but z_k^2 does not divide s_i for any $k \neq i$.

Proof First observe that the elements (a_i, a_i) , $i \in I \setminus J$, are linearly independent in Q . Indeed, if they are not, then $\prod_{i \in I \setminus J} (a_i, a_i)^{\alpha(i)} = 1$ for some $\alpha(i) \in \{0, 1\}$, where $\alpha(i) = 0$ for all but finitely many (nonzero) values of i . Then

$$1 = \prod_{i \in I \setminus J} (a_i, a_i)^{\alpha(i)} = \prod_{i \in I \setminus J} (-1, a_i)^{\alpha(i)} = (-1, \prod_{i \in I \setminus J} a_i^{\alpha(i)}).$$

This means that $\prod_{i \in I \setminus J} a_i^{\alpha(i)} \in D_F(\langle 1, 1 \rangle)$, contradicting the independence of the a_i 's.

Since R is dual to Q we see that for each $i \in I \setminus J$ there must exist $s_i \in R$ such that $\langle s_i, (a_i, a_j) \rangle = \delta_{ij}$. This in turn means that s_i , written as a product of elements of the form z_j^2 and $[z_k, z_m]$, will be divisible by z_i^2 , but not by any other z_k^2 .

§3 Values of Binary Forms

An examination of the W-group \mathbb{G}_F of F will yield complete information regarding the value set $D_F(\langle a, b \rangle)$ of any binary F-quadratic form $\langle a, b \rangle$, $a, b \in F^*$. (We may write $D(\langle a, b \rangle)$ when the field F is clearly understood.) First observe that it is sufficient to determine the values assumed by the 1-fold Pfister forms $\langle 1, a \rangle$. This is because $D_F(\langle a, b \rangle) = a \cdot D_F(\langle 1, ab \rangle)$. This simplifies our problem since $D_F(\langle 1, a \rangle)$ forms a subgroup of F^*/F^{*2} .

The determination of $D(\langle 1, a \rangle)$ falls into two distinct cases: $a \in F^{*2}$ and $a \notin F^{*2}$. We begin with the former, i.e. $D(\langle 1, 1 \rangle)$, as this is somewhat simpler. In both cases we use repeatedly the lemmas from §2.

Theorem 3.1 For some linearly ordered index set I and some subset $J \subseteq I$, let $\{[a_i] : i \in I\}$ be a basis for F^*/F^{*2} such that $\{[a_j] : j \in J\}$ forms a basis for $D(\langle 1, 1 \rangle)$. Then the maximal abelian quotient $(\mathbb{G}_F)^{ab}$ of \mathbb{G}_F is isomorphic to $\prod_{j \in J} (\mathbb{Z}/4\mathbb{Z}) \times \prod_{i \in I \setminus J} (\mathbb{Z}/2\mathbb{Z})$.

Proof The idea of the proof is to represent $(\mathbb{G}_F)^{ab}$ as a quotient of $S^{[3]}$ by some closed normal subgroup, which can be defined very explicitly. It will then be easy to see that $(\mathbb{G}_F)^{ab}$ has the required form.

Let $\{z_i : i \in I\}$ be a set of generators of $S^{[3]}$ which is orthonormal to the basis $\{[a_i] : i \in I\}$ of F^*/F^{*2} , and let R be defined relative to this basis, as described in §2. Enlarge R to $R^\# := \langle R, [z_k, z_m] : k < m, k, m \in I \rangle$. Then $(\mathbb{G}_F)^{ab} \cong S^{[3]}/R^\#$, and to prove the theorem we must show

$$R^\# = \langle z_i^2 : i \in I \setminus J ; [z_k, z_m] : k < m, k, m \in I \rangle =: U.$$

Now $(a_j, a_j) = 1 \in \text{Br}(F)$ for $j \in J$, so by Lemma 2.3 z_j^2 does not enter any $s \in R$. Thus $R^\# \subseteq U$. The reverse inclusion follows immediately from Lemma 2.5 so $R^\# = U$. It is then easy to see that $S^{[3]}/U$ is isomorphic to $\prod_{j \in J} (\mathbb{Z}/4\mathbb{Z}) \times \prod_{i \in I \setminus J} (\mathbb{Z}/2\mathbb{Z})$.

Theorem 3.2 *Let $\{x_i : i \in I\}$ be a minimal set of (topological) generators of \mathbb{G}_F , and let x_i^* denote the image of x_i in \mathbb{G}_F^{ab} . Suppose that the x_i have been chosen so that $\mathbb{G}_F^{\text{ab}} = \prod_{j \in J} \langle x_j^* \rangle \times \prod_{i \in I \setminus J} \langle x_i^* \rangle \cong (\prod_{j \in J} \mathbb{Z}/4\mathbb{Z}) \times (\prod_{i \in I \setminus J} \mathbb{Z}/2\mathbb{Z})$. Let $\{[a_i] : i \in I\}$ be a basis of F^*/F^{*2} orthonormal to the generators $\{x_i : i \in I\}$. Then $\{[a_j] : j \in J\}$ forms a basis for $D_F(\langle 1, 1 \rangle)$.*

Proof $\mathbb{G}_F^{\text{ab}} = \mathbb{G}_F/[\mathbb{G}_F, \mathbb{G}_F] \cong S^{[3]}/R[S^{[3]}, S^{[3]}]$. Let z_i denote the preimage of x_i in $S^{[3]}$. Then $R[S^{[3]}, S^{[3]}] = \langle (z_i)^2 : i \in I \setminus J ; [z_k, z_m] : k < m, k, m \in I \rangle$. It follows that $(z_j)^2$ does not enter any $s \in R$, so $(a_j, a_j) \equiv 1 \in \text{Br}(F)$ by Lemma 2.3, and hence $a_j \in D_F(\langle 1, 1 \rangle)$. On the other hand, $\{(a_i, a_i) : i \in I \setminus J\}$ must be a linearly independent set in $\text{Br}(F)$, so the span of $\{[a_i] : i \in I \setminus J\}$ intersects $D_F(\langle 1, 1 \rangle)$ trivially. Thus $D_F(\langle 1, 1 \rangle)$ is generated by $\{[a_j] : j \in J\}$.

We can achieve the same result from a more field-theoretic approach. Let F^{ab} denote the maximal abelian extension of F inside $F^{(3)}$. Then $\mathbb{G}_F^{\text{ab}} = \mathbb{G}_F/[\mathbb{G}_F, \mathbb{G}_F] \cong \text{Gal}(F^{\text{ab}}/F)$. Moreover, it is not hard to see that F^{ab} is the compositum of $F^{(2)}$ and all $\mathbb{Z}/4\mathbb{Z}$ -extensions L of F . The $\mathbb{Z}/4\mathbb{Z}$ -extensions of a field are well understood and are known to depend on $D_F(\langle 1, 1 \rangle)$. We have $F^{\text{ab}} = F^{(2)} \cup F(\{\sqrt{x+y\sqrt{b}} : b \in D(\langle 1, 1 \rangle) \text{ and } x^2 - y^2b = b\})$. If also $\sqrt{-1} \in F$, then $F^{\text{ab}} = F(\{\sqrt[4]{b} : b \in F^*\})$.

The group $D_F(\langle 1, 1 \rangle)$ can be determined from \mathbb{G}_F^{ab} as follows: Let H be maximal among subgroups of \mathbb{G}_F^{ab} of the form $\prod(\mathbb{Z}/4\mathbb{Z})$. Since $[\mathbb{G}_F, \mathbb{G}_F] \subseteq \Phi(\mathbb{G}_F)$, there is a natural surjection from \mathbb{G}_F^{ab} onto $\mathbb{G}_F/\Phi(\mathbb{G}_F)$. Let H^* be the image of H under this map. Under the identification of F^*/F^{*2} with the dual of $\mathbb{G}_F/\Phi(\mathbb{G}_F)$, $D_F(\langle 1, 1 \rangle)$ will be the precise dual to H^* .

Next we consider the problem of determining $D_F(\langle 1, a \rangle)$ for $a \notin F^{*2}$. Here we choose a basis $\{[a_i] : i \in I\}$ for F^*/F^{*2} in such a way that $[a] = [a_k]$ for some $k \in I$.

Proposition 3.3 *Let $[a_k] \in A = \{[a_i] : i \in I\}$ where A forms a basis for F^*/F^{*2} . Assume $\{[a_j] : j \in J\}$ forms a basis for $D_F(\langle 1, a_k \rangle)$ for some $J \subseteq I$. Let $\{x_i : i \in I\}$ be a set of generators for \mathbb{G}_F , orthonormal to A . Then \mathbb{G}_F has as a homomorphic image the semidirect product $\langle x_j^* : j \in J, j \neq k \rangle \rtimes \langle x_k^* \rangle \cong (\prod_{j \in J, j \neq k} \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$, with action determined by*

$x_k^* x_j^* (x_k^*)^{-1} = (x_j^*)^{-1}$, where x_j^* is the image of x_j , $j \in J$, and x_i is in the kernel for $i \in I \setminus J$.

Proof As in Theorem 3.1, the idea is to represent the given quotient of \mathbb{G}_F as a quotient of $S^{[3]}$, given explicitly in terms of generators and relations, in such a way that it will be easy to see that the group is precisely the semidirect product described in the statement of the theorem. Let $\mathbb{G}_F = \langle z_i : i \in I \rangle / R$, where $\langle z_i : i \in I \rangle \cong S^{[3]}$ and the image of z_i in \mathbb{G}_F is x_i . To prove the proposition we need only show that the map $S^{[3]} \rightarrow S^{[3]}/R'$ factors through \mathbb{G}_F , where $R' := \langle z_j^2 [z_k, z_j] : j \in J; [z_m, z_n] : m, n \in J, m, n \neq k; z_i : i \in I \setminus J \rangle$. In other words, we must show $R \subseteq R'$. If we can do this we are done, for it is clear that $S^{[3]}/R'$ is isomorphic to the semidirect product described above. Now $R \subseteq R'$ if, for all $j \in J, j \neq k$, we have z_j^2 entering $r \in R$ exactly when $[z_k, z_j]$ does. From Lemma 2.4 we see $R \subseteq R'$ if $(a_j, a_j) = (a_k, a_j)$, or equivalently if $a_j \in D_F(\langle 1, a_k \rangle)$. By our choice of J this is always true, so $R \subseteq R'$.

To read off the value group of a binary form (of determinant $\neq 1$), given \mathbb{G}_F , let $x \in \mathbb{G}_F \setminus \Phi(\mathbb{G}_F)$, and extend to a basis for a set of coset representatives for $\mathbb{G}_F / \Phi(\mathbb{G}_F)$, say $\{x_i : i \in I\}$, where $x = x_k$ for some k in the index set I . Consider a surjective map $\theta : \mathbb{G}_F \rightarrow (\prod_{j \in J} \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$ (with action as described in the preceding proposition) where the $\mathbb{Z}/2\mathbb{Z}$ -factor is generated by the image of x , and the $(\prod_{j \in J} \mathbb{Z}/4\mathbb{Z})$ -factor is generated by the image of $\langle x_i : i \in I, i \neq k \rangle \Phi(\mathbb{G}_F)$. Let $\{y_j : j \in J\}$ be a minimal set of elements in \mathbb{G}_F whose images generate $\prod_{j \in J} \mathbb{Z}/4\mathbb{Z}$. Then $\{y_j : j \in J, x_k\}$ can be extended to a set of generators for \mathbb{G}_F , say $\{y_i : i \in I', x_k\}$, such that each y_i lies in $\langle x_i : i \in I, i \neq k \rangle \Phi(\mathbb{G}_F)$ and such that $\{y_i : i \in I' \setminus J\} \subseteq \ker(\theta)$. Let $\{b_i : i \in I', a_k\}$ be the corresponding orthonormal basis for F^*/F^{*2} .

Proposition 3.4 *In the situation described above, $\{b_j : j \in J; a_k\} \subseteq D_F(\langle 1, a_k \rangle)$.*

Proof This is essentially a reverse of the preceding proof. If we have such a surjection θ , then (letting y_i^*, x_k^* denote the preimages of y_i and x_k in $S^{[3]}$) we see that the induced map

$$\theta^* : S^{[3]} \rightarrow S^{[3]}/R' = \langle y_j^\# : j \in J \rangle \rtimes \langle x_k^\# \rangle \cong (\prod_{j \in J} \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$$

must factor through $\mathbb{G}_F \cong S^{[3]}/R$. In other words, $R \subseteq R'$. Here $R' = \langle (y_j^*)^2 [x_k^*, y_j^*] : j \in J; [y_m^*, y_n^*] : m, n \in I'; y_i^* : i \in I' \setminus J, x_k^{*2} \rangle$. If $R \subseteq R'$, then necessarily y_j^{*2} appears as a factor in $s \in R$ if and only if $[x_k^*, y_j^*]$ appears. This in turn implies $(b_j, b_j)(a_k, b_j) = 1 \in \text{Br}(F)$, and so $b_j \in D_F(\langle 1, a_k \rangle)$.

As in the case $D_F(\langle 1, 1 \rangle)$, we could also have taken a field-theoretic approach to the determination of $D_F(\langle 1, a \rangle)$, $a \notin F^{*2}$. Specifically, if $\theta: \mathbb{G}_F \rightarrow (\prod \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$ is the projection corresponding to the determination of $D_F(\langle 1, a \rangle)$ as described above, then $F(\sqrt{b}: b \in D_F(\langle 1, a \rangle))$ is the fixed field of the subgroup $(\ker \theta)(\Phi(\mathbb{G}_F))$ of \mathbb{G}_F . Partial diagrams of the lattices of fields and groups are given in Figures 3.5 and 3.6. Here, $(D_F(\langle 1, a \rangle))^\perp$ denotes a subgroup of F^*/F^{*2} such that $F^*/F^{*2} = D_F(\langle 1, a \rangle) \oplus (D_F(\langle 1, a \rangle))^\perp$. For $b, c \in F^*/F^{*2}$, linearly independent mod F^{*2} , we define a $\mathbf{D}^{b,c}$ -extension of F to be a field L such that $\text{Gal}(L/F) \cong \mathbf{D}$, the dihedral group of order 8, and $\text{Gal}(L/F(\sqrt{bc})) \cong \mathbb{Z}/4\mathbb{Z}$. Such L exists iff $(b, c) = 1 \in \text{Br}(F)$, iff $b \in D_F(\langle 1, bc \rangle)$ [F]. We have

$$\text{Gal}(\cup_{b \in D(\langle 1, a \rangle)} \mathbf{D}^{b, ab}\text{-ext'ns}/F) \cong (\prod_{j \in J, j \neq k} \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z} \times (\prod_{i \in I \setminus J} \mathbb{Z}/2\mathbb{Z}).$$

Figure 3.5

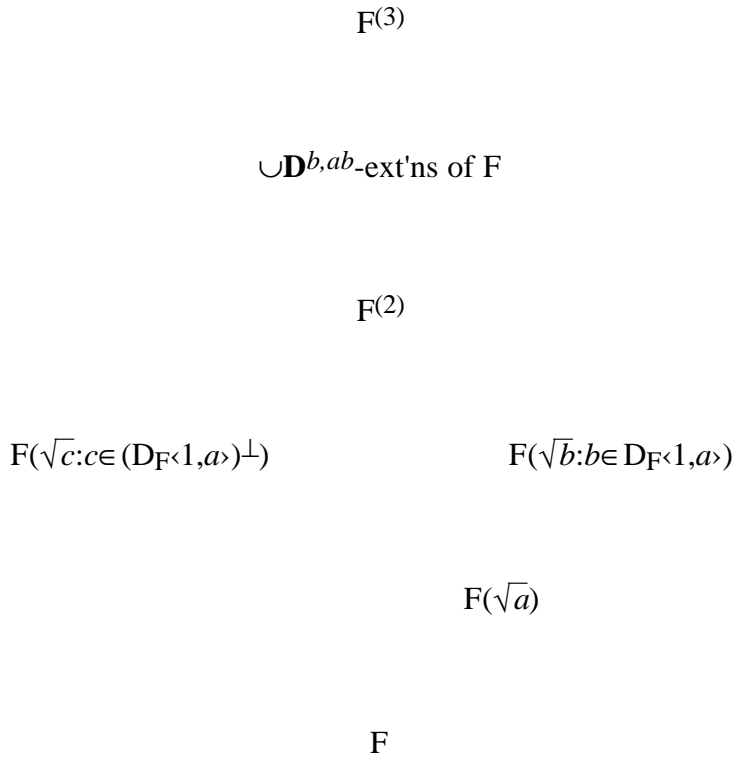
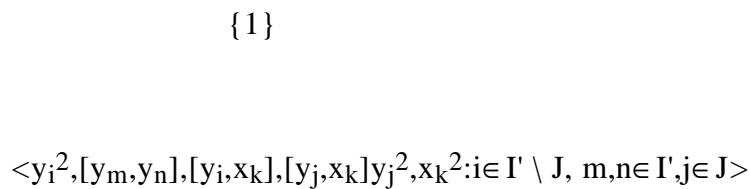


Figure 3.6



$$\Phi(\mathbb{G}_F)$$

$$\Phi\langle y_j: j \in J; x_k \rangle$$

$$\Phi\langle y_i: i \in I' \setminus J \rangle (= \Phi \ker \theta)$$

$$\Phi\langle y_i: i \in I' \rangle$$

$$\mathbb{G}_F$$

We can use the techniques developed above to determine the Kaplansky radical KR or $-\text{KR} := \{a \in F^*/F^{*2}: \langle 1, a \rangle \text{ is universal}\}$.

Corollary 3.7 *Let $\{[a_i]: i \in I\}$ be a basis for F^*/F^{*2} . For $k \in I$, $a_k \in -\text{KR}$ if and only if there is a projection θ of \mathbb{G}_F onto $(\prod_{i \in I, i \neq k} \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$ (with actions as described above) such that $\theta^{-1}(\prod \mathbb{Z}/4\mathbb{Z})$ is contained in the subgroup of \mathbb{G}_F which fixes $\sqrt{a_k}$.*

We make one final observation here. Let $\theta: \mathbb{G}_F \rightarrow \langle x_j: j \in J, j \neq k \rangle \times \langle x_k \rangle \cong (\prod_{j \in J, j \neq k} \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z}$ be a projection determining $D_F(\langle 1, a \rangle)$. Then there exists a projection $\theta': \mathbb{G}_F \rightarrow \langle x_j: j \in J, j \neq k \rangle \times \langle x_k \rangle \cong (\prod_{j \in J, j \neq k} \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z}$, such that θ factors through θ' , if and only if $(a_k, a_k) = 1 \in \text{Br}(F)$. For if $(a_k, a_k) = 1$, then letting $R'' = \langle (z_j)^2 [z_k, z_j]: j \in J, j \neq k; [z_m, z_n]: m, n \in I, m, n \neq k; z_i: i \in I \setminus J \rangle$, we see $R \subseteq R'' \subseteq R'$. Thus we have $\theta': \mathbb{G}_F \cong S^{[3]}/R \rightarrow (\prod_{j \in J, j \neq k} \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z} \cong S^{[3]}/R''$, and $\pi: (\prod_{j \in J, j \neq k} \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z} \cong S^{[3]}/R'' \rightarrow (\prod_{j \in J, j \neq k} \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/2\mathbb{Z} \cong S^{[3]}/R'$, with $\theta = \pi\theta'$. Conversely, if $(a_k, a_k) \neq 1$, then z_k^2 necessarily enters some relation $r \in R$, and so $z_k^2 \in \langle R, (z_j)^2 [z_k, z_j]: j \in J, j \neq k; [z_m, z_n]: m, n \in I, m, n \neq k; z_i: i \in I \setminus J \rangle$, and no such θ' can exist.

Corollary 3.8 *If there exists a projection θ' of \mathbb{G}_F onto $(\prod_{i \in I, i \neq k} \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z}$ as above, then $s(F) \leq 2$. If $s(F) = 2$, then there exists such a projection.*

Proof If θ' exists, let $\{y_i: i \in I, i \neq k; x_k\}$ be the corresponding generators of \mathbb{G}_F and $\{b_i: i \in I, i \neq k; a_k\}$ be a basis of F^*/F^{*2} orthonormal to the given generators. Then $a_k \in -KR$ and $(a_k, a_k) = 1$. However, it is known, when $s(F) \geq 2$, that for any element $a \in -KR$, we have $a \in D_F(\langle 1, 1 \rangle)$ if and only if $-1 \in D_F(\langle 1, 1 \rangle)$ [B]. We have $a_k \in D_F(\langle 1, 1 \rangle)$, and so $s(F) \leq 2$. Conversely, if $s(F) = 2$, then $(-1, -1) = 1 \in \text{Br}(F)$, $-1 \neq 1$, and $-1 \in -KR$. Thus there exists such a map θ' in which the left hand factor $(\prod \mathbb{Z}/4\mathbb{Z})$ has a preimage lying in the subgroup of \mathbb{G}_F which fixes $\sqrt{-1}$.

§4 Determining the Level from the W-Group

We have seen in §3 how to determine when $s(F) \leq 2$, and Mináč and Spira have given a W-group criterion for $s(F) = \infty$ [MSp1]. In this section we provide a Galois-theoretic description of those fields F for which $s(F) = 4$.

The crucial group for handling the level 4 case is the W-group \mathbf{G}_2 of the 2-adic field \mathbb{Q}_2 . This group has order 256 and can be described in the following ways ([Sp:ex.4.3], [MSp2]):

- 1) $\mathbf{G}_2 \cong \langle \rho, \sigma, \tau \mid \rho^4 = \sigma^4 = \tau^4 = 1; \rho^2 = [\tau, \sigma]; [\rho, \sigma]^2 = [\rho, \tau]^2 = 1; [\rho, \sigma], [\rho, \tau], [\sigma, \tau], \sigma^2, \tau^2 \text{ central} \rangle$
- 2) $\mathbf{G}_2 \cong [(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})] \rtimes \mathbb{Z}/4\mathbb{Z}$.
Here, reading from left to right, $\mathbb{Z}/2\mathbb{Z} = \langle [\rho, \sigma] \rangle$, $\mathbb{Z}/4\mathbb{Z} = \langle \sigma \rangle$, $\mathbb{Z}/2\mathbb{Z} = \langle [\rho, \tau] \rangle$, $\mathbb{Z}/4\mathbb{Z} = \langle \rho \rangle$, $\mathbb{Z}/4\mathbb{Z} = \langle \tau \rangle$. The action under the semidirect products can be read off from the presentation given in (1).
- 3) Let \mathbf{S} be the free 2-group on 2 generators σ, τ in the category \mathbf{C} of central extensions of elementary 2-groups by elementary 2-groups. (One can easily check that $|\mathbf{S}| = 32$, and that $\langle [\sigma, \tau] \rangle \cong \mathbb{Z}/2\mathbb{Z}$.) Then \mathbf{G}_2 can be viewed as the free product in \mathbf{C} of \mathbf{S} with $\langle \rho \rangle \cong \mathbb{Z}/4\mathbb{Z}$, amalgamating $\langle [\sigma, \tau] \rangle$ with the unique subgroup $\langle \rho^2 \rangle$ of order 2 in $\langle \rho \rangle$.

We can now give a necessary condition for $s(F) = 4$.

Proposition 4.1 *If $s(F) = 4$, then \mathbf{G}_2 is a quotient of \mathbb{G}_F .*

Proof If $s(F) = 4$, then we can find $b, c \in D_F(\langle 1, 1 \rangle) \setminus F^{*2}$ such that $-1 = b + c$, and such that $-1, b, c$ are independent mod F^{*2} . Indeed, if $-b, -c$, or $-bc \in F^{*2}$, then $-1 \in D_F(\langle 1, 1 \rangle)$, while if $bc \in F^{*2}$, then $c = bf^2$ for some $f \in F^*$, and $-1 = b + bf^2 = b(1 + f^2) \in D_F(\langle 1, 1 \rangle)$. In either case, $s(F) \leq 2$. We can thus fix a basis $\mathbf{B} = \{-1, b, c, d_i: i \in I\}$ for F^*/F^{*2} . Let $\{x, y, z, w_i: i \in I\}$ be a set of generators of \mathbf{S} [3]

which form an "orthonormal basis" with respect to \mathbf{B} . Let N be the normal subgroup of $S^{[3]}$ generated by $\{R; w_i; i \in I\}$. (Here, as before, R denotes the group of relations of \mathbb{G}_F in $S^{[3]}$.) We claim $S^{[3]}/N \cong \mathbf{G}_2$.

Let $U = \langle x, y, z \rangle \subseteq S^{[3]}$. Then $S^{[3]} = U \cdot N$, so $S^{[3]}/N \cong U/(U \cap N)$. Hence to prove \mathbb{G}_F has \mathbf{G}_2 as a quotient, we need only show $U \cap N = \langle x^2[y, z] \rangle$, for then clearly $U/(U \cap N) \cong \mathbf{G}_2$. First observe that $U \cap N \subseteq \Phi(U)$. To prove this, consider a homomorphism $\varphi: S^{[3]} \rightarrow U/\Phi(U)$ such that $\varphi(w_i) = 1$ and $\varphi(x)$, $\varphi(y)$, and $\varphi(z)$ are their images in the quotient group $U/\Phi(U)$. Then the kernel of φ contains N . Thus there is a surjective map $S^{[3]}/N \cong U/U \cap N \rightarrow U/\Phi(U)$, and hence $U \cap N \subseteq \Phi(U)$. Let $T := \langle [x, w_i], [y, w_i], [z, w_i], w_i^2, [w_i, w_j]; i, j \in I, i < j \rangle$. Then the group $U \cap N = \Phi(U) \cap N$ can be characterized as follows:

$$\Phi(U) \cap N = \{u \in \Phi(U): \exists t \in T \text{ s.t. } t \cdot u = r \text{ for some } r \in R\}$$

Indeed, suppose $t \cdot u = r$, and hence $u = t^{-1}r$. Since $R, T \subseteq N$, we have $u \in N$ as well, so $u \in \Phi(U) \cap N$. Conversely, let $u \in \Phi(U) \cap N$. We have $\Phi(U) \cap N \subseteq \Phi(S^{[3]}) \cap N$. We claim also that $\Phi(S^{[3]}) \cap N = TR$. Since both $\Phi(S^{[3]})$ and N contain both T and R , we have $TR \subseteq \Phi(S^{[3]}) \cap N$. To prove the converse consider the subgroup H of $S^{[3]}$ generated by TR and $\{w_i; i \in I\}$. It is easy to check that each element h of H can be uniquely written as $h = (\prod_{i \in I} w_i^{e(i)})g$, $e(i) \in \{0, 1\}$, $g \in TR$. An element h will be in $\Phi(S^{[3]})$ if and only if $e(i) = 0$ for all i . Thus we see that $H = N$ and $\Phi(S^{[3]}) \cap N = TR$. Thus given $u \in \Phi(U) \cap N \subseteq TR$, $\exists t \in T, r \in R$ such that $u = t \cdot r$, and hence $u = t^{-1}r$.

To conclude the proof, it is enough to show that R does not contain any element r which has a factor from $\{x^2, y^2, z^2, [x, y], [x, z], [y, z]\}$ or any of their combinations except $x^2[y, z]$. For then any element $r \in R$ which has any factors in $U \cap N$ must be of the form $r = x^2[y, z]t$, for some $t \in T$, and we will have $U \cap N = \langle x^2[y, z] \rangle$ as desired. We do this by considering which of their "corresponding" (products of) quaternion algebras split. First, since $(-1, -1) \neq 1 \in \text{Br}(F)$, there exists some element $r \in R$ which has x^2 as a factor. However, since we know $-1 \in D_F(\langle b, c \rangle)$, we have $\langle -1, -bc \rangle \cong \langle b, c \rangle$, and hence $\langle -b, -c \rangle \cong \langle 1, bc \rangle$. Working in $\text{Br}(F)$, we have $1 = (-b, -c) = (-1, -1)(-1, b)(-1, c)(b, c) = (-1, -1)(b, c)$, since $(-1, b) = (-1, c) = 1$. From this we see (by Lemma 2.4) that x^2 divides some element in R if and only if $[y, z]$ also divides that same element. Thus $x^2[y, z] \in U \cap N$. All that remains to show is that $[x, y]$, $[x, z]$, y^2 , and z^2 do not divide any element of R . This is immediate (from Lemma 2.3), since $(-1, b) = (-1, c) = (b, b) = (c, c) = 1 \in \text{Br}(F)$. From these observations it is now clear that $S^{[3]}/N \cong \mathbf{G}_2$ as claimed.

Proposition 4.2 *Suppose $\{x^*, y^*, z^*, w_i^* : i \in I\}$ is a minimal system of generators for \mathbb{G}_F , with $\{a, b, c, d_i : i \in I\}$ a corresponding orthonormal basis for F^*/F^{*2} , such that there*

exists a surjection $\varphi: \mathbb{G}_F \rightarrow \mathbf{G}_2$ with $\varphi(x^*) = \rho$, $\varphi(y^*) = \sigma$, $\varphi(z^*) = \tau$, and $\varphi(w_i^*) = 1 \ \forall i \in I$ (notation for \mathbf{G}_2 as above). If $a \in -KR$, then $s(F) \leq 4$.

Proof Let $\{x, y, z, w_i\}$ be the preimages in $S^{[3]}$ for the given generators of \mathbb{G}_F , and suppose φ is as given above. We will show that $(b,b) = 1 \in \text{Br}(F)$. An analogous argument shows $(c,c) = 1$. To see $(b,b) = 1$, it suffices to show that y^2 does not enter any relation $r \in R \subseteq S^{[3]}$ (Lemma 2.3). If y^2 did enter some r , then considering the composite map $S^{[3]} \rightarrow \mathbb{G}_F \rightarrow \mathbf{G}_2$, we see we would have some relation among $\rho^2, \sigma^2, \tau^2, [\rho, \sigma], [\rho, \tau], [\sigma, \tau]$ in \mathbf{G}_2 involving σ^2 (which is the image in \mathbf{G}_2 of y^2). Since no such relation exists, we must have $(b,b) = 1$. The same argument is used to show $(c,c) = 1$, by replacing σ with τ . To complete the proof we show $a \in D(\langle b, c \rangle)$. Then by the result of Berman [B] mentioned earlier (Cor 3.8), we have $s(F) \leq 4$. Now $a \in D(\langle b, c \rangle) \Leftrightarrow 1 \in D(\langle ab, ac \rangle) \Leftrightarrow (ab, ac) = 1 \in \text{Br}(F)$. Observe that for any $r \in R$, either x^2 and $[y, z]$ both divide r or neither does. (This is because their images ρ^2 and $[\sigma, \tau]$ in \mathbf{G}_2 satisfy this condition.) Thus by Lemma 2.4, we see $(a, a) = (b, c)$ and thus $(a, a)(b, c) = 1$. Also $(-1, b) = (b, b) = 1$ and $(-1, c) = (c, c) = 1$. Finally, since $a \in -KR$, we have $bc \in D(\langle 1, a \rangle)$, and thus $(-a, bc) = 1$. Combining all this we see

$$\begin{aligned} 1 &= (-a, bc)(-1, b)(-1, c)(a, a)(b, c) = (-a, bc)(-1, bc)(a, a)(b, c) \\ &= (a, bc)(a, a)(b, c) = (a, b)(a, c)(a, a)(b, c) \\ &= (a, ab)(c, ab) = (ac, ab). \end{aligned}$$

This was the desired result.

Remark 4.3 It is certainly possible to have \mathbf{G}_2 as a homomorphic image of \mathbb{G}_F even when $s(F) \neq 4$. For example, we can consider any field F for which $\text{Gal}(F(2)/F)$, the Galois group of the maximal 2-extension of F , is free. If F has at least 8 square classes, then \mathbf{G}_2 will appear as a Galois group over F , but the level of F need not be 4. As an explicit example of such a field, one can take $F = \mathbb{C}(t)$, where \mathbb{C} is the field of complex numbers and t is an indeterminate. (See [L:Ch.2,p.45] and [R:Ch.1.8].) Alternatively, using techniques of Marshall and Kula [K], one can construct a field F of infinite level whose Witt ring $W(F)$ is the direct product of \mathbb{Z} with the Witt ring of \mathbb{Q}_2 . The W-group of such a field will have \mathbf{G}_2 as a quotient. See [MSm]. Our next theorem and the material in §5 will develop necessary and sufficient criteria for F to be of level 4.

Theorem 4.4 For a field F with $F^*/F^{*2} \cong (\prod_{i \in I} \mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})^3$, we have $s(F) = 4 \Leftrightarrow$ there exists a surjection π of \mathbb{G}_F onto $\mathbf{G}^* := \langle w_i^*: i \in I \rangle \rtimes \langle x^*, y^*, z^* \rangle \cong (\prod_{i \in I} \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbf{G}_2$, where $[y^*, w_i^*] = [z^*, w_i^*] = 1$, $[x^*, w_i^*] = (w_i^*)^2$, and x^*, y^*, z^*

satisfy the same relations as ρ, σ, τ above, but there do not exist surjections of \mathbb{G}_F onto $[(\prod_{i \in I} \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}] \rtimes \mathbb{Z}/4\mathbb{Z}$, with relations as in (2.13), or onto $(\prod_{i \in I} \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})^3$.

Proof Suppose $s(F) = 4$. Then there exists $b, c \in F$ such that $-1, b, c$ are independent mod F^{*2} , $(b, b) = (c, c) = 1$, and $(-1, -1) = (b, c) \neq 1$. Further, $(d, -d) = 1 \quad \forall d \in F^*/F^{*2}$. Let $\{-1, b, c, d_i : i \in I\}$ form a basis for F^*/F^{*2} , and let $\{x, y, z, w_i : i \in I\}$ be a corresponding orthonormal set of generators for $S^{[3]}$, where $\mathbb{G}_F \cong S^{[3]}/R$. For $r \in R$ we have w_i^2 appearing in the expression for $r \Leftrightarrow [x, w_i]$ appears, x^2 appearing $\Leftrightarrow [y, z]$ appears, and $y^2, z^2, [x, y]$, and $[x, z]$ not appearing at all. Let N be the normal subgroup of $S^{[3]}$ generated by $\{[w_i, w_j] : i, j \in I; [w_i, y], [w_i, z], w_i^2[x, w_i] : i \in I; x^2[y, z]\}$. Then $R \subseteq N$, and $S^{[3]}/N$ is isomorphic to the semidirect product of $\prod_{i \in I} \mathbb{Z}/4\mathbb{Z}$ with \mathbf{G}_2 , exactly as described in the statement of the theorem. Also we have seen (Cor 3.8) that $[(\prod_{i \in I} \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}] \rtimes \mathbb{Z}/4\mathbb{Z}$ being a quotient of \mathbb{G}_F implies $s(F) \leq 2$, and that $(\prod_{i \in I} \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})^3$ being a quotient of \mathbb{G}_F implies $\langle 1, 1 \rangle$ is universal (Theorem 3.2), and hence that $s(F) \leq 2$. Thus if $s(F) = 4$, neither of these two groups can be a quotient of \mathbb{G}_F . Conversely, suppose $s(F) \neq 4$. If $s(F) > 4$, then \mathbf{G}^* cannot be a quotient of \mathbb{G}_F by Proposition 4.2. For if it were, then the preimage of x^* would be dual to some $a \in -KR$ by Cor 3.7, and \mathbb{G}_F would have $\mathbf{G}_2 \cong \langle x^*, y^*, z^* \rangle$ as a quotient. If $s(F) = 2$, then again Cor 3.8 shows that $[(\prod_{i \in I} \mathbb{Z}/4\mathbb{Z}) \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}] \rtimes \mathbb{Z}/4\mathbb{Z}$ is a quotient of \mathbb{G}_F , while if $s(F) = 1$, then $\langle 1, 1 \rangle$ is isotropic, hence universal, so $(\prod_{i \in I} \mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})^3$ is a quotient of \mathbb{G}_F .

To conclude this section, we give the following characterization of the maximal level 4 extension of a field F inside $F(2)$.

Theorem 4.5 *Suppose $s(F) = 4$, and $F \subseteq K \subseteq F(2)$ is an extension of fields. The following two conditions on K are equivalent.*

- (1) K is maximal in $F(2)$ with respect to the property $s(K) = 4$.
- (2) $s(K) = 4$ and $D_K(\langle 1, 1, 1 \rangle) \cup -K^2 = K$.

Proof First suppose that K is an extension of F inside $F(2)$. If $D_K(\langle 1, 1, 1 \rangle) \cup -K^2 \neq K$, then (since $K = -K$) $\exists a \in K \setminus -D_K(\langle 1, 1, 1 \rangle) \cup K^2$. Then $M := K(\sqrt{a})$ is a quadratic extension of K inside $F(2)$. We claim $s(M) = 4$. For $\langle 1, 1, 1 \rangle$ is anisotropic over K , and since $-a \notin -D_K(\langle 1, 1, 1 \rangle)$, $\langle 1, 1, 1 \rangle$ is not isometric over K to a form $\langle -a, -x, -ax \rangle$. In particular, it does not contain a subform isometric to $x\langle 1, -a \rangle$ for any $x \in K^*$, and so cannot become isotropic over M [L:Ch.7]. This gives $s(M) = 4$, establishing (1) \Rightarrow (2).

To show (2) \Rightarrow (1), suppose K is an extension of F in $F(2)$, satisfying (2), and consider any extension L of K in $F(2)$. We claim $s(L) \leq 2$. By the usual argument, any such extension L must contain a quadratic extension $M = K(\sqrt{a})$ of K , so it suffices to show $s(M) \leq 2$ for any quadratic extension M of K . Now $K = -K = K^2 \cup -D_K(\langle 1,1,1 \rangle)$, and $a \in K^* \setminus K^{*2}$, so we have $a \in -D_K(\langle 1,1,1 \rangle)$. Thus $-a \in D_K(\langle 1,1,1 \rangle)$, which means $\langle 1,1,1 \rangle \cong \langle -a,-x,ax \rangle$ for some $x \in K^*$. Then clearly $\langle 1,1,1 \rangle$ becomes isotropic over M , and so $s(M) \leq 2$.

§5 Properties and Examples of Level 4 Groups

Theorem 4.4 provides a Galois-theoretic criterion for determining when a field has level 4. However, the description of the group as given is not very conceptually appealing. For that reason we introduce the following notions leading to a group-theoretic description of "level 4 groups", which will describe those groups which appear as W-groups of fields of level 4. We then conclude by considering examples of such groups and studying some of their properties. Recall that we defined C to be the category of groups which are central extensions of elementary 2-groups by elementary 2-groups.

Definition 5.1 A group $H \in C$ will be called an S-product if it is the semidirect product $N \rtimes S$ of some normal subgroup $N \subseteq G$ with S , the free group on 2 generators in C , and if $H^{ab} = H/[H,H] \cong \prod_I \mathbb{Z}/4\mathbb{Z}$, where I is some index set. For example, S is itself an S-product ($N = \{1\}$).

Definition 5.2 A group $G \in C$ will be called a level 4 group if \exists a subgroup H of G and an element $x \in G \setminus H$ such that H is an S-product, $G = \langle x, H \rangle$, and the following two conditions hold.

$$(1) \quad G/[H,H] \cong [\prod_J \mathbb{Z}/2\mathbb{Z} \times (\prod_J \mathbb{Z}/4\mathbb{Z} \times \prod_K \mathbb{Z}/4\mathbb{Z})] \rtimes \mathbb{Z}/2\mathbb{Z},$$

where the last factor $\mathbb{Z}/2\mathbb{Z}$ corresponds to the group generated by the image x' of x , and the factor $(\prod_J \mathbb{Z}/4\mathbb{Z} \times \prod_K \mathbb{Z}/4\mathbb{Z})$ corresponds to the image of H . The image of $S = \langle y, z \rangle \subseteq H$ is in $\prod_J \mathbb{Z}/4\mathbb{Z}$. The first factor $\prod_J \mathbb{Z}/2\mathbb{Z}$ consists of commutators $[x', g]$, $g \in \prod_J \mathbb{Z}/4\mathbb{Z}$. The action of the semidirect product is given by

$$\begin{aligned} x'gx'^{-1} &= g[x',g] \quad \forall g \in \prod_J \mathbb{Z}/4\mathbb{Z}, \\ x'gx'^{-1} &= g^{-1} \quad \forall g \in \prod_K \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

(2) Let $\Theta: H = N \rtimes S \rightarrow G_2$ be the homomorphism which has kernel N , and which sends y, z in $S \subseteq H$ to $\sigma, \tau \in G_2$ (as in the third description of G_2 given at the

beginning of this section). Then there exists a unique surjection $\eta: G \rightarrow \mathbf{G}_2$ which is Θ on H and which takes $x \in G$ to $\rho \in \mathbf{G}_2$.

Now we are ready to give our alternative characterization of W -groups of fields of level 4. The proof requires checking facts about generators and relations, in the manner of the proofs of (4.1) and (4.4); the details are left to the reader.

Theorem 5.3 $s(F) = 4 \Leftrightarrow \mathbb{G}_F$ is a level 4 group.

The simplest examples of fields of level 4 are finite odd-degree extensions of the 2-adic rational numbers \mathbb{Q}_2 . The Witt rings of these fields are well known and are described explicitly in [Ma]. If $[F:\mathbb{Q}_2] = 2k - 3$, $k \geq 2$, then $W(F)$ is completely determined by k .

Following Marshall [Ma], we denote $W(F)$ as \mathbb{L}_{2k-1} . Then we may write [Ma : Prop.5.6]

$$\mathbb{L}_{2k-1} = \mathbb{Z}/8\mathbb{Z} \cdot 1 \oplus \sum_{i=2}^k (\mathbb{Z}/2\mathbb{Z}(1-x_i) \oplus \mathbb{Z}/2\mathbb{Z}(1-y_i)),$$

with multiplication defined by $(1-x_i)(1-y_j) = 4\delta_{ij}$, δ_{ij} denoting the Kronecker delta. We can also explicitly write down the associated W -group $\mathbb{G}_F := \mathbb{G}_{2k-1}$: Define $S^{[3]}$ as in §1, using generators $z_1, z_2, t_2, z_3, t_3, \dots, z_k, t_k$. (The number of generators is necessarily $\log_2 F^*/F^{*2}$, and $|F^*/F^{*2}| = 2^{2k-1}$. See [Ma:Thm.3.18].) Then $\mathbb{G}_{2k-1} \cong S^{[3]}/R$, where $R = \langle (\prod_{i=2}^k [z_i, t_i]) z_1^2 \rangle$. This can easily be seen by using the results of §2 together with [Ma : §5.2-5.3].

It is of course possible to check directly that \mathbb{G}_{2k-1} is a level 4 group. Let σ_i and τ_j be the images of z_i and t_j respectively in \mathbb{G}_{2k-1} . Let $H = \langle \sigma_i, \tau_i : 2 \leq i \leq k \rangle$. Then clearly $\mathbb{G}_{2k-1} = \langle \sigma_1, H \rangle$. Moreover we see that $H = N \rtimes S$, where $S = \langle \sigma_2, \tau_2 \rangle$ and N is the normal closure of $\langle \sigma_3, \tau_3, \dots, \sigma_k, \tau_k \rangle$. Because $H/[H, H] \cong \prod_{i=2}^k \mathbb{Z}/4\mathbb{Z}$, we see that H is an S -product. Now $\mathbb{G}_{2k-1}/[H, H] \cong (\prod_{i=2}^k \mathbb{Z}/2\mathbb{Z} \times \prod_{i=2}^k \mathbb{Z}/4\mathbb{Z}) \rtimes \mathbb{Z}/2\mathbb{Z}$, where the last factor $\mathbb{Z}/2\mathbb{Z}$ corresponds to the group generated by the image σ_1^* of σ_1 , and the second factor $\prod_{i=2}^k \mathbb{Z}/4\mathbb{Z}$ corresponds to the image of H . The first factor $\prod_{i=2}^k \mathbb{Z}/2\mathbb{Z}$ consists of commutators $[\sigma_1^*, g]$, $g \in \prod_{i=2}^k \mathbb{Z}/4\mathbb{Z}$. This checks the first condition of Definition 5.2. To check the second condition, set $\Theta: N \rtimes S \rightarrow \mathbf{G}_2$ to be the homomorphism having kernel N and sending σ_2, τ_2 in S to σ, τ in \mathbf{G}_2 (as in the third description of \mathbf{G}_2 given at the beginning of §4). We want to show that there is a unique surjection $\eta: G \rightarrow \mathbf{G}_2$ which is Θ on H and which takes σ_1^* to $\rho \in \mathbf{G}_2$. Since H and σ_1^* generate G it is clear that there exists at most one such homomorphism η . However, there exists at least one such since the homomorphism $\eta^*: S^{[3]} \rightarrow \mathbf{G}_2$, defined by sending z_1 to ρ , z_2 to σ , t_2 to τ , and all other generators z_i, t_i to 1, factors through \mathbb{G}_{2k-1} . This is because the only nontrivial

relation of $\mathbb{G}_{2^{k-1}}$ is $(\prod_{i=2}^k [z_i, t_i])z_1^2$. Clearly this factor of η^* is the desired homomorphism η . Thus all groups $\mathbb{G}_{2^{k-1}}$ are level 4 groups.

For a level 4 group G , let $r(G)$ denote the $\mathbb{Z}/2\mathbb{Z}$ -rank of the quotient group $G/\Phi(G)$. Since \mathbf{G}_2 is a homomorphic image of every level 4 group, we see that $r(G) \geq 3$.

Proposition 5.4 *The group \mathbf{G}_2 is the only level 4 group for which $r(G) = 3$.*

Proof Let \mathbf{S}_3 be the free group on three generators $\{x, y, z\}$ in C . Since $\mathbf{G}_2 \cong \mathbf{S}_3/\langle x^2[y, z] \rangle$, and since if G is any level 4 group with $r(G) = 3$ we must have a composition of surjective homomorphisms $\mathbf{S}_3 \rightarrow G \rightarrow \mathbf{G}_2$, we see that $G \cong \mathbf{S}_3$ or $G \cong \mathbf{G}_2$. However, \mathbf{S}_3 is not a level 4 group, as is easily checked by observing, for $H = \langle y, z \rangle$, that the image of x in $\mathbf{S}_3/[H, H]$ has order 4, not 2. This contradicts the definition given in 5.2. Thus $G \cong \mathbf{G}_2$ as claimed.

Ultimately, one would like to characterize the W-groups of fields of level 2^k for $k \geq 3$, as well. Unfortunately, our work in this direction has not so far led to such nice results as those for level ≤ 4 . Nonetheless, it is hoped that the detailed description of the "level 4 groups" given above will help in the eventual understanding of these higher level groups.

References

- [AT] E. ARTIN AND J. TATE, "Class Field Theory", W. A. Benjamin, New York, 1967.
- [B] L. BERMAN, "The Kaplansky Radical and Values of Binary Quadratic Forms over Fields," Ph.D. Thesis, University of California, Berkeley, 1978.
- [F] A. FRÖHLICH, Orthogonal representations of Galois groups, Stiefel-Whitney classes, and Hasse-Witt invariants, J. Reine Angew. Math. **360** (1985), 84-123.
- [K] M. KULA, Fields with prescribed quadratic form schemes, Math. Zeit. **167** (1979), 201-212.
- [La] J. LABUTE, Classification of Demushkin groups, Canad. Math. J. **19** (1966), 106-132.

- [L] T. Y. LAM, "The Algebraic Theory of Quadratic Forms," Benjamin, Addison Wesley, 1973. (Revised Printing: 1980.)
- [Ma] M. MARSHALL, "Abstract Witt Rings," Queen's Papers in Pure and Applied Math. 57, Queen's University, Kingston, Ontario, 1980.
- [MSm] J. MINAC AND T. SMITH, Decomposition of Witt rings and Galois Groups, in preparation.
- [MSp1] J. MINAC AND M. SPIRA, Formally real fields, Pythagorean fields, C-fields, and W-groups, Math. Zeit. **205** (1990), 519-530.
- [MSp2] J. MINAC AND M. SPIRA, Witt rings and Galois groups, in preparation.
- [R] L. RIBES, "Introduction to Profinite Groups and Galois Cohomology," Queen's Papers in Pure and Applied Math. 24, Queen's University, Kingston, Ontario, 1970.
- [Se1] J.-P. SERRE, "Cohomologie Galoisienne," Lecture Notes in Mathematics, No. 5, Springer-Verlag, Berlin, 1965.
- [Se2] J.-P. SERRE, "Local Fields," Graduate Texts in Mathematics, No. 67, Springer-Verlag, New York, 1979.
- [Sm] T. SMITH, "Some 2-Groups Arising in Quadratic Form Theory and Their Generalizations," Ph.D. Thesis, University of California, Berkeley, 1988.
- [Sp] M. SPIRA, "Witt Rings and Galois Groups," Ph.D. Thesis, University of California, Berkeley, 1987.
- [V] F. R. VILLEGAS, Relations between quadratic forms and certain Galois extensions, unpublished manuscript.