Can. J. Math. Vol. **46** (4), 1994 pp. 886–896

EXTRA-SPECIAL GROUPS OF ORDER 32 AS GALOIS GROUPS

TARA L. SMITH

ABSTRACT. In this article we examine conditions for the appearance or nonappearance of the two extra-special 2-groups of order 32 as Galois groups over a field F of characteristic not 2. The groups in question are the central products DD of two dihedral groups of order 8, and DQ of a dihedral group with the quaternion group, obtained by identifying the central elements of order 2 in each factor group. It is shown that the realizability of each of these groups as Galois groups over F implies the realizability of other 2-groups (which are not their quotient groups), and in turn that realizability of certain other 2-groups implies the realizability of DD and DQ. We conclude by providing an explicit construction of field extensions with Galois group DD.

1. **Introduction.** The question of the realizability of given groups as Galois groups has been of interest for more than a century. One question of interest is that of "automatic realizability", *i.e.* when does the realizability of one group G as a Galois group over a field F automatically imply the realizability of another group H? Of course, if H is a quotient of G this will always be the case, so the interesting situation is when the realizability is "nontrivial", that is, when H is not a quotient of G. This question has been answered in some depth for groups of order 8 and 16, as well as certain higher-order 2-groups, in papers by a number of authors. See [Je:1989a,b], [JeY:1987], [Ki:1990], [KLe:1975], [MiSm:1991], [Wa:1990], and [Wh:1957], among others. In this article, we consider automatic realizability criteria concerning the two extra-special 2-groups of order 32; we will always work in the case where the characteristic of $F \neq 2$. Recall that a group G of order p^k, p a prime, is called an *extra-special p-group* if the center and the commutator subgroup of G coincide and have order p. Any nonabelian group of order p^3 is extra-special, and any extra-special p-group is a central product of n nonabelian subgroups of order p^3, and has order p^{2n+1}. There are precisely 2 isomorphism types of extra-special p-groups of order p^{2n+1}. See [Ro:1982, pp.140-141]. The 2 groups of order 32 are DD, which has the presentation

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

and DQ, which has the presentation

$$\langle x, y, z, w \mid x^2 = y^2 = z^4 = w^4 = [x, y]^2 = [z, w]^2 = 1, z^2 = w^2 = [x, y] = [z, w] = \epsilon, \\ \epsilon \text{ central}, \epsilon^2 = 1, [x, z] = [x, w] = [y, z] = [y, w] = 1\rangle.$$

Research supported in part by NSF Grant DMS-9196244.
Received by the editors February 24, 1993.
AMS subject classification: 12F.

It has long been known that realizability of certain groups of order a power of 2 over a given field is closely linked to the quadratic structure of that field and the splitting of certain (products of) quaternion algebras. It is this fact which we will exploit to achieve our automatic realizability results. We will write $(\frac{a,b}{F})$ to denote the quaternion algebra generated over F by two anti-commuting elements i and j, such that $i^2 = a, j^2 = b$. We may write just (a, b) when this causes no confusion. Let N_x denote the norm map from $F(\sqrt{x})$ to F, for $x \in \dot{F} \setminus \dot{F}^2$. By abuse of notation, we will also use this to denote $\{y \in \dot{F} : y = N_x(z), \exists z \in F(\sqrt{x})\}$. We will make extensive use of the following two well-known facts about quaternion algebras. (The second property is often referred to as the "common slot property" for quaternion algebras.)

PROPOSITION 1.1. *Let $a, b, c, d \in \dot{F}$. Then*

(1) $(a, b) = 1 \in \mathrm{Br}(F) \Leftrightarrow a \in N_b \Leftrightarrow b \in N_a$, *and*

(2) $(a, b) = (c, d) \in \mathrm{Br}(F) \Leftrightarrow bN_a \cap dN_c \cap N_{ac} \neq \emptyset \Leftrightarrow \exists x \in \dot{F}$ *such that* $(a, bx) = (c, dx) = (ac, x) = 1$.

We let C denote the cyclic group of order 4, D the dihedral group of order 8, and Q the quaternion group of order 8. We write $\langle a_1, a_2, \ldots, a_n \rangle$ to denote the (equivalence class of the) quadratic form $a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2$ over F. The following two theorems are so well known as to be considered folklore.

THEOREM 1.2. *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* $\mathrm{Gal}(L/F) \cong C$, *such that $F(\sqrt{a})$ is the (unique) quadratic intermediate field between L and F.*

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

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

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

THEOREM 1.3. *Let $a, b \in \dot{F}$, independent* mod $\dot{F}^2$. *The following are equivalent.*

i) *There exists a Galois extension L/F with* $\mathrm{Gal}(L/F) \cong D, F \subsetneq F(\sqrt{a}, \sqrt{b}) \subsetneq L$, *and with* $\mathrm{Gal}\big(L/F(\sqrt{ab})\big) \cong C$.

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

iii) *The quadratic form $\langle a, b \rangle$ represents 1 over F.*

Notice that since $(a, -a)$ is always split, D is realizable over any field F with at least 4 square classes, provided that $-1 \notin \dot{F}^2$. In addition to these two results, the criteria for the realizability of Q as a Galois group dates back to Witt [Wi:1936]. We have the following conditions.

THEOREM 1.4. *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.*

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

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

https://doi.org/10.4153/CJM-1994-050-2 Published online by Cambridge University Press

iii) $\langle a, b, ab\rangle \simeq \langle 1, 1, 1\rangle$.

These results can be generalized to encompass a much larger class of 2-groups. The following embedding criterion is a special case of a result proved in [Fr:1985]. (This result, in turn, was inspired by work of Serre [Se:1984], in which the realizability of certain Galois groups was related to properties of the trace form of a field extension.)

THEOREM 1.5 (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* $G = \mathrm{Gal}(K/F) \cong (\mathbb{Z}/2\mathbb{Z})^r$. *Consider a (nonsplit) central extension* $\hat{G}$ *of* $\mathbb{Z}/2\mathbb{Z}$ *by* G:

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \hat{G} \longrightarrow G \longrightarrow 1.$$

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* $c_{ij} = 0$ *if* $[\tau_i, \tau_j] = 1$, $i \neq j$, $c_{ij} = 1$ *otherwise, and* $c_{ii} = 0$ *if* $\tau_i^2 = 1, c_{ii} = 1$ *otherwise. There exists a Galois extension* $L/F, L \supseteq K$, *with* $\mathrm{Gal}(L/F) \cong \hat{G}$, *and such that* $\hat{G} \longrightarrow G$ *is the natural surjection of Galois groups, if and only if* $\prod_{i \leq j}(a_i, a_j)^{c_{ij}} = 1 \in \mathrm{Br}(F)$ *(the Brauer group of central simple algebras over F).*

This theorem provides our principal tool for investigating the realizability of these 2-groups. Since the splitting of one product of quaternion algebras frequently can be manipulated to give the splitting of another product of quaternion algebras, it is possible to use this (combined with a good grasp of the presentations of 2-groups of the type described in the theorem) to show realizability of one group forces realizability of another.

The groups which can be realized as (nonsplit) central extensions $\hat{G}$ of $\mathbb{Z}/2\mathbb{Z}$ by $(\mathbb{Z}/2\mathbb{Z})^r$ are precisely central products of the groups D, Q, C, amalgamating the unique central elements of order 2 in each group, and direct products of such groups with elementary abelian 2-groups. 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 which must split in order for the group to be realized. These central products are investigated in some detail in [LSm:1989]. In particular, they include the extra-special 2-groups, which are central products of the two nonabelian groups of order 8, D and Q.

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. Recall that $s(F)$ is the least positive integer n such that -1 is a sum of n squares in F; $s(F) = \infty$ if -1 is not a sum of squares. We use $D_F(q)$, or simply $D(q)$ when F is understood, to denote the set of nonzero elements of F which are represented over F by the quadratic form q. Then let $a, b \in \dot{F}$, independent mod $\dot{F}^2$. We have

(1) If $s(F) = 1$, then $F(\sqrt{a}, \sqrt{b})$ embeds in a Q-extension of $F \Leftrightarrow$ it embeds in a D-extension of F. Thus D is realizable if and only if Q is realizable, and both groups fail to be realized over F if and only if F is "rigid" ([MiSm:1991]), that is, if and only if $D_F(\langle 1, a\rangle) = \dot{F}^2 \cup a\dot{F}^2 \ \forall a \in \dot{F} \setminus \dot{F}^2$.

https://doi.org/10.4153/CJM-1994-050-2 Published online by Cambridge University Press

(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). This is because $(a,-1)(a,a)(-1,-1) = 1\ \forall a \in \dot{F}$.

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

There are three distinct nonabelian groups of order 16 covered by our version of the embedding criterion. They are DC, the central product of D and C; $D \times \mathbb{Z}/2\mathbb{Z}$; and $Q \times \mathbb{Z}/2\mathbb{Z}$. Since the latter two are realizable if and only if D and Q, respectively, are realizable and the square class group of F is large enough, the group DC is the only one providing new insight. In [MiSm:1991], the following facts concerning the realizability of DC over a field F with $|\dot{F}/\dot{F}^2| \geq 8$ are shown.

(1) DC does not appear as a Galois group over $F \Leftrightarrow F$ is a rigid field (*i.e.* for $a \notin \pm\dot{F}^2, D_F(\langle 1,a\rangle) = \dot{F}^2 \cup a\dot{F}^2$).

(2) If F is a rigid field with at least 4 square classes, then $s(F) = 1 \Leftrightarrow D$ is not a Galois group over $F, s(F) = 2 \Leftrightarrow C$ and D are Galois groups over F, and $s(F) = \infty \Leftrightarrow C$ is not a Galois group over F.

(3) If $s(F) \neq 2$, then also Q cannot be realized as a Galois group over F when F is a rigid field.

2. **Realizability of DD and DQ.** The two extra-special groups of order 32 are DD and DQ, with presentations as given in §1. By the embedding criterion we then have

PROPOSITION 2.1. *Let F be a field,* $\operatorname{char} F \neq 2$.

(1) There exists a Galois extension K/F, with $\operatorname{Gal}(K/F) \cong DD$, *if and only if there exists $a,b,c,d \in \dot{F}$, independent* $\bmod \dot{F}^2$, *such that* $(a,b)(c,d) = 1 \in \operatorname{Br}(F)$.

(2) There exists a Galois extension K/F, with $\operatorname{Gal}(K/F) \cong DQ$, *if and only if there exists $a,b,c,d \in \dot{F}$, independent* $\bmod \dot{F}^2$, *such that* $(a,b)(a,a)(b,b)(c,d) = 1 \in \operatorname{Br}(F)$, *if and only if* $(-a,-b)(-1,-1)(c,d) = 1 \in \operatorname{Br}(F)$.

Necessarily, then, these two groups can be realized only if $|\dot{F}/\dot{F}^2| \geq 16$. We will assume this hereafter. These groups of course have other presentations, but the ones used here turn out to be particularly useful because they involve products of small numbers of quaternion algebras. The relations for the existence of DD cannot be expressed as a product of fewer than two quaternion algebras, and for DQ one requires at least three algebras. It should also be remarked that any quotient of an extra-special 2-group is necessarily elementary abelian. Thus results we obtain on the automatic realizability of other groups, given the realizability of an extra-special group, are indeed nontrivial.

THEOREM 2.2. *DD is realizable as a Galois group over F if and only if the direct product $D \times D$ is also realizable.*

PROOF. One direction is trivial: if $D \times D$ is realizable, then since DD is a quotient of $D \times D$, it must also be realizable. Now suppose DD is a Galois group over F, and let

$a, b, c, d \in \dot{F}$ be independent elements mod $\dot{F}^2$, such that $(a, b)(c, d) = 1 \in \mathrm{Br}(F)$. In order to show $D \times D$ is realizable, we must be able to find two split quaternion algebras, $(r, s) = 1$ and $(t, u) = 1$, with r, s, t, u independent mod $\dot{F}^2$. In that case we have $L_1 \supset F(\sqrt{r}, \sqrt{s}), L_2 \supset F(\sqrt{t}, \sqrt{u})$ with $\mathrm{Gal}(L_i/F) \cong D$, $i = 1, 2$ and $L_1 \cap L_2 = F$, so $L_1 L_2$ is Galois over F with $\mathrm{Gal}(L_1 L_2/F) \cong D \times D$. If $(a, b) = (c, d) = 1$, we are done. If not, the "common slot property" for quaternion algebras (Proposition 1.1 (2)) guarantees the existence of $x \in \dot{F}, x \notin \dot{F}^2$, such that $(a, bx) = (c, dx) = (ac, x) = 1$. We will use this to find two independent split quaternion algebras. By abuse of notation we will identify elements of $\dot{F}$ with their equivalence classes mod $\dot{F}^2$.

First, if $x = ac$, we have $(a, bac) = (c, dac) = 1$, and a, bac, c, dac are independent mod $\dot{F}^2$, so we are done in this case. If $x \neq ac$ then ac and x are independent mod $\dot{F}^2$. If a, b, c, x are independent, so are a, bx, ac, x, and $(a, bx) = (ac, x) = 1$ realizes $D \times D$. If a, c, d, x are independent, we have $(c, dx) = (ac, x) = 1$ realizing $D \times D$. If both these sets of elements are dependent sets, then necessarily $x = a$ or $x = c$, since we have already excluded $x = 1$ and $x = ac$. In this case, a, bx, c, dx are independent, and $(a, bx) = (c, dx) = 1$ realizes $D \times D$. ∎

Notice that the $D \times D$ extension has a DD-subextension because DD is a quotient of $D \times D$. However, the original DD-extension has $F(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d})$ as its unique maximal multiquadratic subfield, while the DD-extension in $D \times D$ contains this field if and only if x depends on $\{a, b, c, d\}$ mod $\dot{F}^2$.

COROLLARY 2.3. *Realizability of DD as an F-Galois group implies the realizability of D and DC.*

PROOF. Again we remark that these groups are not quotients of DD. However, D is a quotient of $D \times D$, and hence occurs as a Galois group of a subextension of the $D \times D$-extension whose existence is implied by that of the DD-extension. The existence of this extension also implies the existence of two split quaternion algebras $(r, s) = 1$ and $(t, u) = 1$, with r, s, t, u independent mod $\dot{F}^2$. Necessarily, one of the pairs $\{r, s\}$ or $\{t, u\}$, must be independent of $\pm\dot{F}^2$. Say it is $\{r, s\}$. Then $(r, s) = 1 \Rightarrow \langle r, s\rangle$ represents 1, so the form $\langle 1, -s\rangle$ represents r, where $s \notin \pm\dot{F}^2$, and $r \notin \dot{F}^2 \cup -s\dot{F}^2$. This means the field is not rigid, so by [MiSm:1991], DC is a Galois group over F. ∎

THEOREM 2.4. *Let F be a field, $s(F) \leq 2$. Then DD is realizable as an F-Galois group if and only if DQ is realizable.*

PROOF. For $s(F) = 1$, the proof is essentially the same as the proof that Q is realizable if and only if D is. Since $(x, x) = 1\ \forall x \in F$, we have $(a, b)(a, a)(b, b)(c, d) = 1 \Leftrightarrow (a, b)(c, d) = 1$.

For $s(F) = 2$, we have already observed that Q arises as a Galois group provided the square class group is big enough, since $(a, -a)(-1, -1) = 1\ \forall a \in \dot{F}$. Thus if there exist elements $c, d \in \dot{F}$ such that $c, d, -1$ are independent mod squares and $(c, d) = 1$, we have in fact $D \times Q$, and therefore DQ, realizable as a Galois group over F. If DD is an F-Galois group, then we know there exists two independent split quaternion algebras, so

necessarily we have elements $c, d \in \dot{F}$ such that $\{c, d, -1\}$ is independent mod squares and $(c, d) = 1$.

Conversely, assume DQ is realizable, so there exist independent a, b, c, d such that $(-a, -b)(-1, -1)(c, d) = 1$. Since $s(F) = 2$, we have $(-1, -1) = 1$, and so $(-a, -b)(c, d) = 1$. If $-a, -b, c, d$ are independent mod $\dot{F}^2$, we are done. If not, there are two cases to consider: $-a$ or $-b = 1$, or $-a \neq 1 \neq -b$, but $\{c, d, cd\} \cap \{-a, -b, ab\} \neq \emptyset$. Consider the first case, and say $a = -1, b \neq -1$. Then $\{-1, b, c, d\}$ is an independent set mod $\dot{F}^2$, and $1 = (-a, -b)(c, d) = (1, -b)(c, d) = (c, d)$, so $(c, d)(b, -b) = 1$, giving the necessary condition for the realizability of DD. In the second case we may assume without loss of generality that $c = -a$ or $cd = -a$. (Recall that a, b, c, d are independent.) If $c = -a$, then $1 = (-a, -b)(-a, d) = (-a, -bd), -a, -bd, d, -d$ are independent, $(-a, -bd)(d, -d) = 1$ and DD is realizable. If $c = -ad$, then $1 = (-a, -b)(-ad, d) = (-a, -b)(-d, d)(a, d) = (-a, -b)(a, d)$, and $d \neq -1$ because $c \neq a$. In this case $-a, -b, a, d$ are independent, and this implies the realizability of DD. ∎

PROPOSITION 2.5. *Assume $s(F) > 2$ and $|\dot{F}/\dot{F}^2| \geq 16$. If Q is realizable as a Galois group over F, then so are DD, $D \times D$, and DQ.*

PROOF. If Q is realizable and $s(F) > 2$, then Ware [Wa:1990] has shown there exists $a \in \dot{F} \setminus \dot{F}^2, a$ a sum of two squares, such that $(-a, b) = 1$ for some $b \notin \dot{F}^2 \cup a\dot{F}^2$. If $b \in -\dot{F}^2 \cup -a\dot{F}^2$, we would have -1 as a sum of two squares. As this is not the case, a, b, and -1 are independent mod $\dot{F}^2$. Let $c \in \dot{F}$ be such that $a, b, c, -1$ are independent mod $\dot{F}^2$. Then $(-a, b)(c, -c) = 1$ shows that DD and $D \times D$ are realizable. Let $(-a, -b)(-1, -1) = 1$ be a quaternion algebra splitting "realizing" Q. Then $a, b, -1$ must be independent, or else $(-a, -b) = 1$, implying $(-1, -1) = 1$ and thus $s(F) \leq 2$. Choose c independent of $\{a, b, -1\}$. Then $(-a, -b)(-1, -1)(c, -c) = 1$ is a quaternion algebra splitting realizing DQ. ∎

THEOREM 2.6. *Assume $s(F) > 2$. If DQ is realizable as a Galois group over F, so is DD.*

PROOF. The proof involves using the "common slot" property of quaternion algebras and checking possible dependence relations among the square classes appearing. Assume DQ is realizable, and let $a, b, c, d \in \dot{F}$, independent mod $\dot{F}^2$, such that $(-a, -b)(-1, -1)(c, d) = 1 \in \mathrm{Br}(F)$. First assume $a, b, -1$ are dependent mod $\dot{F}^2$; say $b = -1$ or $a = -b$. Then $(-a, -b) = 1$, so $(-1, -1)(c, d) = 1 \in \mathrm{Br}(F)$, implying the existence of a Q-extension, and thus by the preceding proposition also a DD-extension.

Next assume $a, b, -1$ are independent, but $a, b, c, d, -1$ are dependent mod $\dot{F}^2$. Without loss of generality, we may assume $-1 \in \{c, cd, ac, acd, abc, abcd\}$. If $-1 = c$, we have $-a, -b, -1, -d$ independent, and $(-a, -b)(-1, -d) = 1$. If $-1 = cd$, $(-a, -b)(-1, -1) = 1$, implying realizability of Q, and hence of DD. If $-1 = ac$, we have $(-a, -bd)(-1, -1) = 1$, giving realizability of Q and DD. If $-1 = acd$, we

https://doi.org/10.4153/CJM-1994-050-2 Published online by Cambridge University Press

have $(-a,-b)(-1,-1)(c,-ac) = (-a,-bc)(-1,-1)(c,c) = (-a,-bc)(-1,-c) = 1$, giving the realizability of DD. If $-1 = abc$, we have

$$(a,b)(a,a)(b,b)(-ab,d) = (a,b)(a,a)(b,b)(a,d)(b,d)(d,d) = 1 \in \mathrm{Br}(F).$$

This is precisely the requirement for the group with presentation

$$\langle x,y,z \mid x^2 = y^2 = z^2 = [x,y] = [y,z] = [x,z], x^4 = 1\rangle$$

to be realized as a Galois group over F. But this group is isomorphic to $Q \times \mathbb{Z}/2\mathbb{Z}$ [LSm:1989], so Q is realizable, and therefore so is DD. Finally, let $-1 = abcd$. Then $(-a,-b)(-1,-1)(c,-abc) = (-a,-bc)(-1,-1)(c,bc) = (-ac,-bc)(-1,-c) = 1 \in \mathrm{Br}(F)$, so DD is realizable.

Lastly, assume $a,b,c,d,-1$ are independent mod $\dot{F}^2$, and $(-a,-b)(-1,-1)(c,d) = 1$. We may assume no individual quaternion algebra in this expression is split, or else we are done. Then there exist elements $f,x,y \in \dot{F} \setminus \dot{F}^2$ such that $(-a,-b) = (f,x)$, $(-1,-1) = (f,y), (c,d) = (f,xy)$. If $-f,-y$ are independent mod $\dot{F}^2$, then $(-1,-1)(f,y) = 1$ gives the realizability of Q, and we are done. Otherwise, there are three cases to consider: (i) $f = -1, y \neq \pm 1$, (ii) $y = -1, f \neq \pm 1$, and (iii) $f = y \neq 1$.

First assume $f = -1$. Then $(-a,-b)(-1,x) = 1$ realizes DD unless $x = -a,-b,-1$, ab, a,b, or $-ab$. If $x = -a$, then $(-a,b)(c,-c) = 1$ realizes DD; similarly, if $x = b$, then $(a,-b)(c,-c) = 1$ realizes DD. If $x = -1, (a,b)(-1,-1) = 1 \Rightarrow Q$ is realizable. If $x = ab, (-a,-b)(-1,ab) = (a,b)(-1,-1) = 1 \Rightarrow Q$ is realizable. If $x = a, (-a,-b)(-1,a) = (-a,-b)(-1,-a)(-1,-1) = (-a,b)(-1,-1) = 1 \Rightarrow Q$; an analogous argument holds if $x = b$. Finally, if $x = -ab$, then $1 = (-a,-b)(-1,-ab) = (-a,-b)(-1,-a)(-1,-b) = (a,b)$, so $(a,b)(c,-c) = 1$, realizing DD.

Next consider the case $y = -1$. If $-a,-b,f,x$ are independent, $(-a,-b)(f,x) = 1$ realizes DD. If they are dependent, an analysis as above shows DD is realizable except possibly when $fx \in \{1,-a,-b,ab\}$. If $c,d,f,-x$ are independent, $(c,d)(f,-x) = 1$ realizes DD. If they are dependent, it can again be shown DD is realizable unless $fx \in \{-1,-c,-d,-cd\}$. Since $\{1,-a,-b,ab\} \cap \{-1,-c,-d,-cd\} = \emptyset$, necessarily DD is realizable.

The concluding case is when $f = y$. Here we have $(-a,-b)(f,x) = 1$ and $(c,d)(f,xf) = 1$. Analyzing as in the preceding case, we see that we can realize DD except perhaps in the case $fx \in \{1,-a,-b,ab\} \cap \{1,c,d,cd\}$. By the independence of $\{-1,a,b,c,d\}$, we see this implies $fx = 1$, so $(c,d) = 1$, and thus $(-a,-b)(-1,-1) = 1$, implying the existence of a Q-extension, and hence also a DD-extension. ∎

The converse to the preceding theorem is not true. There do indeed exist fields which have Galois extensions with group isomorphic to DD, but which do not have extensions with group isomorphic to DQ. The following example, which relies on some results from quadratic form theory, shows the existence of such fields.

EXAMPLE. Let F be a field with Witt ring $W(F) \cong (\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z})[\mathbb{Z}/2\mathbb{Z}]$. (The existence of such a field has been demonstrated by Kula [Ku:1979].) Such a field has 16 square

https://doi.org/10.4153/CJM-1994-050-2 Published online by Cambridge University Press

classes, and we may take $\dot{F}/\dot{F}^2$ to be generated by $-1, a, b, c$, with quaternion algebra relations $(a,b) = 1$, $(a,-1)(a,a) = 1$, $(b,-1)(b,b) = 1$, $(c,-1)(c,c) = 1$. Then the relation $(a,b)(c,-c) = 1$ proves the existence of DD as a Galois group over F. On the other hand, DQ is not realizable as an F-Galois group. Perhaps the "easiest" way to see this is via the so-called W-group of F. This is the Galois group of a certain 2-extension of F, namely the compositum K of all quadratic extensions of F and all quadratic extensions of K which remain Galois over F. Then if DQ is realizable as a Galois group over F, it must in fact be a quotient of the W-group of F. In this case, it is not hard to show ([MiSm:pre]) that the W-group is isomorphic to the group with presentation

$$G = \langle x, y, z, w \mid x^4 = y^4 = z^4 = w^2 = [x,w]x^2 = [y,w]y^2 = [z,w]z^2 = [x,z] = [y,z] = [x,y]^2 = 1 \rangle.$$

If DQ is a quotient of this group, say $DQ \cong G/K$, then the kernel K must be contained in the Frattini (here = commutator) subgroup of G, since DQ also requires a minimum of four generators. Moreover, since the Frattini subgroup of DQ is of order 2 and the commutator subgroup of G is of order 16, the kernel must be one of the 15 subgroups of order 8 in $[G,G]$. An analysis of the various possibilities shows that 11 of these subgroups will give a quotient group with center of order bigger than 2 (and therefore not extra-special), while the remaining 4 give quotients isomorphic to DD. (These correspond to the 4 quaternion splittings $(a,b)(c,-c) = 1$, $(a,b)(ac,-ac) = 1$. $(a,b)(bc,-bc) = 1$, and $(a,b)(abc,-abc) = 1$.)

It is in fact possible to give a complete characterization of all Witt rings of fields which fail to realize DD as a Galois group [Sm:pre]. Since Witt rings of rigid fields are easily seen to fit this description ([Wa:1979]), this observation combined with [MiSm:1991] gives a somewhat roundabout proof that the realizability of DD implies the realizability of DC. Since the W-group can be determined from the Witt ring, the characterization of the realizability of DD in terms of the Witt ring provides a method for constructing examples such as the one above, where DD must occur as a Galois group but DQ need not.

3. **Fields with DD as a Galois group.** In this final section, we give an explicit construction of the Galois extension realizing DD, using the relationship $(a,b)(c,d) = 1$. General formulas for constructing extensions realizing certain types of p-groups as Galois groups, including the group DD, have been given in [Ma:1987]; however, in working with a specific group, as is done here, the description is of course simpler. The construction used here is very similar in nature to the constuction of the Galois extensions realizing DC, given in [MiSm:1991]. We will make heavy use of the facts about splitting of quaternion algebras given in Proposition 1.1.

THEOREM 3.1. *Suppose there exist elements $a, b, c, d \in \dot{F}$, linearly independent* mod $\dot{F}^2$, *such that $(a,b)(c,d) = 1 \in \mathrm{Br}(F)$. Then there is a field L, which is a quadratic extension of $K = F(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d})$, such that L/F is Galois, with* $\mathrm{Gal}(L/F) \cong DD$.

https://doi.org/10.4153/CJM-1994-050-2 Published online by Cambridge University Press

PROOF. Since $(a,b)(c,d) = 1$, there exists $y \in N_c$ such that $bdy \in N_a$ and $dy \in N_{ac}$. Set

$$f_1 = x_1 + y_1\sqrt{c}, \quad f_2 = x_2 + y_2\sqrt{a}, \quad f_3 = x_3 + y_3\sqrt{ac},$$

where $x_i, y_i \in F$, $i \in \{1,2,3\}$, and $N_c(f_1) = y, N_a(f_2) = bdy, N_{ac}(f_3) = dy$. Set $f = f_1f_2f_3$, and $L = K(\sqrt{f})$. Let $\langle \sigma_a, \sigma_b, \sigma_c, \sigma_d \rangle = \mathrm{Gal}(K/F) \cong (\mathbb{Z}/2\mathbb{Z})^4$, where $\sigma_a(\sqrt{a}) = -\sqrt{a}$, but σ_a leaves $\sqrt{b}$, $\sqrt{c}$, and $\sqrt{d}$ fixed, and so forth. To prove the theorem, we must show two things:

(1) $\sigma_a, \sigma_b, \sigma_c, \sigma_d$ extend to automorphisms $\tilde{\sigma}_a, \tilde{\sigma}_b, \tilde{\sigma}_c, \tilde{\sigma}_d$ of L/F, so that L/F is a Galois extension.

(2) Let $\tau \in \mathrm{Gal}(L/F)$ be such that $\tau(\sqrt{f}) = -\sqrt{f}$. Then $DD \cong \mathrm{Gal}(L/F) = \langle \tau, \tilde{\sigma}_a, \tilde{\sigma}_b, \tilde{\sigma}_c, \tilde{\sigma}_d \mid \tau^2 = \tilde{\sigma}_a^2 = \tilde{\sigma}_b^2 = \tilde{\sigma}_c^2 = \tilde{\sigma}_d^2 = 1, \tau = [\tilde{\sigma}_a, \tilde{\sigma}_b] = [\tilde{\sigma}_c, \tilde{\sigma}_d], \tau \text{ central}, [\tilde{\sigma}_a, \tilde{\sigma}_c] = [\tilde{\sigma}_a, \tilde{\sigma}_d] = [\tilde{\sigma}_b, \tilde{\sigma}_c] = [\tilde{\sigma}_b, \tilde{\sigma}_d] = 1 \rangle$

To check (1), define $\tilde{\sigma}(\sqrt{f}) = \sqrt{\sigma(f)}\ \forall \sigma \in \mathrm{Gal}(K/F)$. We calculate this explicitly for the generators $\tilde{\sigma}_a, \tilde{\sigma}_b, \tilde{\sigma}_c, \tilde{\sigma}_d$:

$$\begin{aligned} \tilde{\sigma}_a(f)f &= \sigma_a(f_1)f_1\sigma_a(f_2)(f_2)\sigma_a(f_3)f_3 \\ &= f_1^2 N_a(f_2)N_{ac}(f_3) \\ &= f_1^2 bd^2y^2 = \frac{f^2 bdy^2}{f_2^2 f_3^2} \Rightarrow \sigma_a(f) = \left(\frac{bd^2y^2}{f_2^2 f_3^2}\right)f, \end{aligned}$$

and so

$$\tilde{\sigma}_a(\sqrt{f}) = \sqrt{\sigma_a(f)} = \left(\frac{dy\sqrt{b}}{f_2 f_3}\right)\sqrt{f}.$$

Similarly, one checks that $\tilde{\sigma}_b(\sqrt{f}) = \tilde{\sigma}_d(\sqrt{f}) = \sqrt{f}$, and that $\tilde{\sigma}_c(\sqrt{f}) = (\frac{y\sqrt{d}}{f_1 f_3})\sqrt{f}$.

To check (2), we must see that the relations on $\tau, \tilde{\sigma}_a, \tilde{\sigma}_b, \tilde{\sigma}_c, \tilde{\sigma}_d$ are as given. This is a straightforward calculation; we show $\tilde{\sigma}_a^2 = 1$ as an example.

$$\tilde{\sigma}_a^2(\sqrt{f}) = \tilde{\sigma}_a\left(\frac{dy\sqrt{b}}{f_2 f_3}\sqrt{f}\right) = \left(\frac{dy\sqrt{b}}{\sigma_a(f_2)\sigma_a(f_3)}\right)\left(\frac{dy\sqrt{b}}{f_2 f_3}\right)\sqrt{f} = \left(\frac{d^2y^2b}{bdydy}\right)\sqrt{f} = \sqrt{f}.$$

One checks the remaining relations similarly. Thus $\mathrm{Gal}(L/F) \cong DD$ as desired. ∎

Conversely, given a Galois extension L/F with $\mathrm{Gal}(L/F) \cong DD$,we would like to demonstrate the existence of elements $a, b, c, d \in \dot{F}$, linearly independent mod $\dot{F}^2$, such that $(a,b)(c,d) = 1 \in \mathrm{Br}(F)$. We may assume that the following conditions hold:

(1) $L \supset_{\neq} K = F(\sqrt{a}, \sqrt{b}, \sqrt{c}, \sqrt{d})$, where $\mathrm{Gal}(K/F) = \langle \sigma_a, \sigma_b, \sigma_c, \sigma_d \rangle \cong (\mathbb{Z}/2\mathbb{Z})^4$, and $\sigma_a, \sigma_b, \sigma_c, \sigma_d$ act as in Theorem 3.1.

(2) $\mathrm{Gal}(L/F) = \langle \tau, \tilde{\sigma}_a, \tilde{\sigma}_b, \tilde{\sigma}_c, \tilde{\sigma}_d \mid \tau^2 = \tilde{\sigma}_a^2 = \tilde{\sigma}_b^2 = \tilde{\sigma}_c^2 = \tilde{\sigma}_d^2 = 1, \tau = [\tilde{\sigma}_a, \tilde{\sigma}_b] = [\tilde{\sigma}_c, \tilde{\sigma}_d], \tau \text{ central}, [\tilde{\sigma}_a, \tilde{\sigma}_c] = [\tilde{\sigma}_a, \tilde{\sigma}_d] = [\tilde{\sigma}_b, \tilde{\sigma}_c] = [\tilde{\sigma}_b, \tilde{\sigma}_d] = 1 \rangle$, where $\tilde{\sigma}_a|_K = \sigma_a, \tilde{\sigma}_b|_K = \sigma_b, \tilde{\sigma}_c|_K = \sigma_c, \tilde{\sigma}_d|_K = \sigma_d$, and $\tau|_K = 1$.

(3) $\mathrm{Gal}\big(L/F(\sqrt{a}, \sqrt{b})\big) \cong \mathrm{Gal}\big(L/F(\sqrt{c}, \sqrt{d})\big) \cong D$.

(4) $\mathrm{Gal}\big(L/F(\sqrt{a}, \sqrt{b}, \sqrt{cd})\big) \cong \mathrm{Gal}\big(L/F(\sqrt{c}, \sqrt{d}, \sqrt{ab})\big) \cong \mathbb{Z}/4\mathbb{Z}$.

(5) $L = K(\sqrt{f})$ for some $f \in F(\sqrt{a}, \sqrt{c})$, and $\tau(\sqrt{f}) = -\sqrt{f}$.

That we may assume (1) and (2) is clear; (3) and (4) follow from (1) and (2), and (5) follows from the fact that $\mathrm{Gal}\big(L/F(\sqrt{a}, \sqrt{c})\big) \cong (\mathbb{Z}/2\mathbb{Z})^3$. There are seven quadratic extensions of $F(\sqrt{a}, \sqrt{c})$ in L, only three of which lie in K. Choose $f \in F(\sqrt{a}, \sqrt{c})$ such that $F(\sqrt{a}, \sqrt{c}, \sqrt{f}) \subseteq L$, and $\sqrt{f} \notin K$.

THEOREM 3.2. *Let L/F be an extension of F such that (1)–(5) above hold. Then $(a, b)(c, d) = 1 \in \mathrm{Br}(F)$.*

PROOF. We need only find an element $y \in N_c$ such that $bdy \in N_a$ and $dy \in N_a c$. We consider the three elements $k_c = \sigma_c(f)f$, $k_a = \sigma_a(f)f$, and $k_{ac} = \sigma_c\sigma_a(f)f$. Then one can check that in fact k_c, k_a, and k_{ac} are all in $\dot{K}^2$. For example, to see $k_c \in \dot{K}^2$, observe that $\sqrt{k_c} \in L$, so if $\sqrt{k_c} \notin K$, then $L = K(\sqrt{k_c})$, and $\sqrt{k_c} = x + y\sqrt{f}$ for some $x, y \in K$. Thus $k_c = (x + y\sqrt{f})^2 = x^2 + 2xy\sqrt{f} + y^2 \in K$, and necessarily $x = 0$ or $y = 0$. If $y = 0$, then $k_c = x^2 \in \dot{K}^2$ as claimed. If $x = 0$, then $k_c = y^2 f \Rightarrow \sigma_c(f) = y^2 \Rightarrow \tilde{\sigma}_c(\sqrt{f}) = y \in K$, a contradiction. Similarly, one can see that k_a and k_{ac} are in $\dot{K}^2$. Now k_c is fixed by σ_c, so

$$k_c \in F(\sqrt{a}) \cap \dot{K}^2 = \dot{F(\sqrt{a})}\{1, b, c, bc, d, bd, cd, bcd\}.$$

Similarly, we have

$$k_a \in \dot{F(\sqrt{c})}\{1, a, b, ab, d, ad, bd, abd\},$$
$$k_{ac} \in \dot{F(\sqrt{ac})}\{1, b, c, bc, d, bd, cd, bcd\}.$$

Thus we have $k_c = f_c d_a^2, \exists f_c \in F, d_a \in F(\sqrt{a})$; $k_a = f_a d_c^2, \exists f_a \in F, d_c \in F(\sqrt{c})$; and $k_{ac} = f_{ac} d_{ac}^2, \exists f_{ac} \in F, d_{ac} \in F(\sqrt{ac})$. By applying $\tilde{\sigma}_a, \tilde{\sigma}_b, \tilde{\sigma}_c, \tilde{\sigma}_d$ to each of $\sqrt{k_c}, \sqrt{k_a}, \sqrt{k_{ac}}$, we can determine in which of the given eight cosets each of f_c, f_a, f_{ac} lies. We work out the details for f_a.

$$\begin{aligned}
\tilde{\sigma}_a(\sqrt{k_a}) &= \tilde{\sigma}_a^2(\sqrt{f})\tilde{\sigma}_a(\sqrt{f}) = \sqrt{k_a} \\
&= \tilde{\sigma}_a(\sqrt{f_a})\tilde{\sigma}_a(d_c) = \tilde{\sigma}(\sqrt{f_a})d_c, \Rightarrow \tilde{\sigma}_a(\sqrt{f_a}) = \sqrt{f_a}, \Rightarrow f_a \in \{1, b, d, bd\} \\
\tilde{\sigma}_b(\sqrt{k_a}) &= \tilde{\sigma}_b\tilde{\sigma}_a(\sqrt{f})\tilde{\sigma}_b(\sqrt{f}) = -\tilde{\sigma}_a\tilde{\sigma}_b(\sqrt{f})\tilde{\sigma}_b(\sqrt{f}) = -\sqrt{k_a} \\
&= \tilde{\sigma}_b(\sqrt{f_a})\tilde{\sigma}_b(d_c) = \tilde{\sigma}_b(\sqrt{f_a})d_c \Rightarrow \tilde{\sigma}_b(\sqrt{f_a}) = -\sqrt{f_a}, \Rightarrow f_a \in \{b, d\} \\
\tilde{\sigma}_d(\sqrt{k_a}) &= \tilde{\sigma}_d\tilde{\sigma}_a(\sqrt{f})\tilde{\sigma}_d(\sqrt{f}) = \tilde{\sigma}_a\tilde{\sigma}_d(\sqrt{f})\tilde{\sigma}_d(\sqrt{f}) = -\sqrt{k_a} \\
&= \tilde{\sigma}_d(\sqrt{f_a})\tilde{\sigma}_d(d_c) = \tilde{\sigma}_d(\sqrt{f_a})d_c \Rightarrow \tilde{\sigma}_d(\sqrt{f_a}) = \sqrt{f_a}, \Rightarrow f_a = b.
\end{aligned}$$

Similarly, evaluating $\tilde{\sigma}_c, \tilde{\sigma}_b$, and $\tilde{\sigma}_d$ on $\sqrt{k_c}$ and $\sqrt{k_{ac}}$ shows $f_c = d$ and $f_{ac} = bd$. We calulate $\sqrt{f}\tilde{\sigma}_a(\sqrt{f})\tilde{\sigma}_c(\sqrt{f})\tilde{\sigma}_c\tilde{\sigma}_a(\sqrt{f})$ in three different ways.

$$\begin{aligned}
\sqrt{f}\tilde{\sigma}_a(\sqrt{f})\tilde{\sigma}_c(\sqrt{f})\tilde{\sigma}_c\tilde{\sigma}_a(\sqrt{f}) &= \tilde{\sigma}_c(\sqrt{k_a})\sqrt{k_a} = bN_c d_c \\
&= \tilde{\sigma}_a(\sqrt{k_c})\sqrt{k_c} = dN_a d_a \\
&= \tilde{\sigma}_a(\sqrt{k_{ac}})\sqrt{k_{ac}} = bdN_{ac}d_{ac}.
\end{aligned}$$

Now let $y = N_c d_c$. Then $by = dN_a d_a \Rightarrow bdy \in N_a$, and $by = bdN_{ac}d_{ac} \Rightarrow dy \in N_{ac}$. This then shows $(a, b)(c, d) = 1 \in \mathrm{Br}(F)$, as claimed. ∎

https://doi.org/10.4153/CJM-1994-050-2 Published online by Cambridge University Press

REFERENCES

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

[Je:1989a] C. U. Jensen, *On the representations of a group as a Galois group over an arbitrary field,* Théorie des nombres Number Theory, (eds. J.-M. De Koninck and C. Levesque), Walter de Gruyter, 1989, 441–458.

[Je:1989b] ———, *Finite groups as Galois groups over arbitrary fields,* Proc. Int. Malcev Conf. Novosibirsk, 1989.

[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.

[Ku:1979] M. Kula, *Fields with prescribed quadratic form schemes,* Math. Z. **167**(1979), 201–212.

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

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

[Ma:1987] Richard Massy, *Construction de p-extensions Galoisiennes d'un corps de caractéristique différente de p,* J. Algebra **109**(1987), 508–535.

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

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

[Ro:1982] D. J. S. Robinson, *A Course in the Theory of Groups*, Springer-Verlag, New York, 1982.

[Se:1984] J.-P. Serre, *L'invariant de Witt de la Forme* $Tr(x^2)$, Comment. Math. Helv. **59**(1984), 651–676.

[Sm:pre] T. L. Smith, *Witt rings and realizability of small 2-Galois groups,* Proceedings of Symposia in Pure Mathematics, 1992 Summer Research Institute on Quadratic Forms and Division Algebras, (eds. W. Jacob and A. Rosenberg), Amer. Math. Soc., Providence, to appear.

[Wa:1979] R. Ware, *When are Witt rings group rings? II,* Pacific J Math. **76**(1978), 541–564.

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

[Wh:1957] G. Whaples, *Algebraic extensions of arbitrary fields,* Duke Math. J. **24**(1957), 201–204.

[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.

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