PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 108, Number 3, March 1990

A NOTE ON THE QUATERNION GROUP AS GALOIS GROUP

ROGER WARE

(Communicated by Louis J. Ratliff, Jr.)

ABSTRACT. The occurrence of the quaternion group as a Galois group over certain fields is investigated. A theorem of Witt on quaternionic Galois extensions plays a key role.

In [9, §6] Witt proved a theorem characterizing quaternionic Galois extensions. Namely, he showed that if F is a field of characteristic not 2 then an extension $L = F(\sqrt{a}, \sqrt{b})$, $a, b \in F$, of degree 4 over F can be embedded in a Galois extension K of F with $\mathrm{Gal}(K/F) \cong H_8$ (the quaternion group of order 8) if and only if the quadratic form $ax^2 + by^2 + abz^2$ is isomorphic to $x^2 + y^2 + z^2$. In addition he showed how to explicitly construct the Galois extension from the isometry. An immediate and interesting consequence of this is the fact that H_8 cannot be a Galois group over any Pythagorean field.

In this note Witt's theorem is used to obtain additional results about the existence of H_8 as a Galois group over certain fields. If F is a field (of characteristic not 2) with at most one (total) ordering such that H_8 does not occur as a Galois group over F then the structure of the pro-2-Galois groups $G_F(2) = \mathrm{Gal}(F(2)/F)$, $G_{\mathrm{py}} = \mathrm{Gal}(F_{\mathrm{py}}/F)$ (where $F(2)$ and F_{py} are the quadratic and pythagorean closures of F) are completely determined. Moreover it is shown that for any field F of characteristic not two, H_8 occurs as a Galois group over F iff H_8 is a homomorphic image of G_{py} iff the dihedral group D_8 of order 8 is a homomorphic image of G_{py}.

In what follows all fields have characteristic different from 2. If $a_1, \ldots, a_n \in \dot{F} = F \setminus \{0\}$ then $q = \langle a_1, \ldots, a_n \rangle$ denotes the quadratic form with orthogonal basis $e_1, \ldots, e_n$ and $q(e_i) = a_i$. The value set of q is $D(q) = \{a \in \dot{F} | q(x) = a$ for some $x\}$. Any unexplained notations and terminology about quadratic forms can be found in [4].

Lemma 1. *For a field F with $-1 \notin F^2$ and $|\dot{F}/\dot{F}^2| > 2$ the following are equivalent*:

(1) *The level (stufe), $s(F)$, of F is two.*

Received by the editors March 24, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11E81, 12F10; Secondary, 12D15.
Supported in part by NSA research grant No. MDA 904-88-H-2018.

(2) *Every quadratic extension of F can be embedded in a quaternionic Galois extension.*

(3) *$F(\sqrt{-1})$ is contained in a quaternionic Galois extension.*

Proof. (1) $\Rightarrow$ (2). Let $a \in F$, $a \notin F^2 \cup -F^2$. By (1), $\langle 1,1,1\rangle \cong \langle -1, -1, 1\rangle \cong \langle -1, a, -a\rangle$. Hence by Witt's theorem [9, §6], $F(\sqrt{-1}, \sqrt{a})$ is contained in a quaternionic extension.

(3) $\rightarrow$ (1). By Witt's theorem, there exists $a \in \dot{F}$ such that $\langle 1,1,1\rangle \cong \langle -1, a, -a\rangle$. Hence $\langle 1,1,1\rangle$ is isotropic and $s(F) = 2$ (as $-1 \notin F^2$).

An element a in $\dot{F}$ is *rigid* if $a \notin \dot{F}^2 \cup -\dot{F}^2$ and $D(\langle 1, a\rangle) = \dot{F}^2 \cup a\dot{F}^2$.

Lemma 2. *For $a \in D(\langle 1,1\rangle)$, $a \notin F^2$, the following are equivalent*:

(1) *a is not rigid*

(2) *$F(\sqrt{a})$ can be embedded in a quaternionic Galois extension.*

Proof. (1) $\Rightarrow$ (2). As a is not rigid, there exists $b \notin F^2 \cup aF^2$ such that $\langle 1, a\rangle \cong \langle b, ab\rangle$. Hence $\langle 1,1,1\rangle \cong \langle 1, a, a\rangle \cong \langle b, ab, a\rangle$ and [9, §6] applies.

(2) $\Rightarrow$ (1). By [9, §6] there exists $b \in F \setminus (F^2 \cup aF^2)$ such that $\langle a, b, ab\rangle \cong \langle 1,1,1\rangle \cong \langle a, a, 1\rangle$ and by Witt's cancellation $\langle b, ab\rangle \cong \langle 1, a\rangle$. Hence a is not rigid.

Remark. There exist fields with $s(F) = 2$ such that all elements not in $F^2 \cup -F^2$ are rigid (e.g. $F = \mathbf{F}_3((t_1))\dots((t_n)))$. Of course, for such fields $D(\langle 1,1\rangle) = \dot{F}^2 \cup -\dot{F}^2$ [7, Corollary 1.2].

Let WF denote the Witt ring of anisotropic quadratic forms over F and let $G_F(2) = \mathrm{Gal}(F(2)/F)$, where $F(2)$ is the maximal 2-extension of F. The next theorem improves Theorem 3.5 in [7]:

Theorem 1. *For a field with $|\dot{F}/\dot{F}^2| > 2$ the following are equivalent*:

(1) $WF \cong \mathbf{Z}/2\mathbf{Z}[\dot{F}/\dot{F}^2]$

(2) *$G_F(2)$ has (topological) generators $\{y_i, x\}_{i\in I}$ with relations $y_iy_j = y_jy_i$ and either $xy_ix^{-1} = y_i^{5^m}$ for fixed $m = 2^n (n \geq 0)$ and all $i \in I$ or $xy_i = y_ix$ for all i.*

(3) *The dihedral group D_8 of order 8 does not occur as a Galois group over F.*

(4) *F is not formally real and the quaternion group H_8 does not occur as a Galois group over F.*

Proof. The equivalence of (1) and (3) as well as the implication (3) $\Rightarrow$ (4) is contained in [7, Th. 3.5].

(1) $\Rightarrow$ (2). If all 2-power roots of unity lie in F then by [7, Cor. 3.9(2)] $G_F(2)$ has generators and relations as described with $xy_i = y_ix$ for all $i \in I$. Now assume F does not contain all 2-power roots of unity. By [3, Ths. 2.1, 2.3,

and Lemma 4.1(i)], $G_F(2)$ has the described generators and relations where $n \geq 0$ is the largest integer such that F contains a primitive 2^{n+2}th root of unity.

(2) $\Rightarrow$ (3). As D_8 is a 2-group, D_8 occurs as a Galois group over F iff D_8 is a homomorphic image of $G_F(2)$. However, a pro-2-group with generators and relations described in (2) cannot have D_8 as a homomorphic image.

(4) $\Rightarrow$ (1). Assume (4). From Lemma 2 it follows that any sum of two squares in $F \setminus (F^2 \cup -F^2)$ is rigid and hence a sum of three squares in F can be written as the sum of two squares. Inductively it follows that $\dot{F} = D(\langle 1, 1\rangle)$. Hence by Lemma 2 all elements in $F \setminus (F^2 \cup -F^2)$ are rigid and by Lemma 1, $-1 \in F^2$. Statement (1) now follows from [7, Th. 1.5].

Corollary. *Assume F is not formally real. Then D_8 occurs as a Galois group over F if and only if H_8 occurs over F.*

Remark. If G is a pro-2-group with generators and relations as described in Theorem 1 (2) there is a field F with $G_F(2) \cong G$. This can be seen as follows:

If G is not abelian let $\Gamma = \mathbf{Z}^{(I)}$ (direct sum), let K be a 2-extension of $\mathbf{Q}(e_{n+2})$ maximal with respect to the exclusion of e_{n+3}, where e_k is a primitive 2^kth root of unity, and let $F = K((\Gamma))$ be the generalized henselian power series field. If G is abelian (with basis $\{y_i\}_{i \in I}$) take $F = \mathbf{C}((\Gamma))$. Then (in either case) $G_F(2) \cong G$ by [3, Th. 2.4].

Now let F be formally real, let F_{py} denote the pythagorean closure of F, and let $G_{\mathrm{py}} = \mathrm{Gal}(F_{\mathrm{py}}/F)$ denote the corresponding pro-2-Galois group. In [5], Minač showed that if D_8 is not a homomorphic image of G_{py} then neither is H_8. His argument used an equivalent form of Witt's theorem [2, 7.7 (ii)] (compare [6, Example, 663–664]) and improved Theorem 3.9 in [8] (answering a question raised in [8]). It should be pointed out that there is an oversight in the statement of [8, Theorem 3.9]; namely, the statement should include the assumption that F is formally real (the observation on lines 2–3 of page 104 of [8] is false if F is nonreal of level 2). The next theorem improves Minač's theorem.

Theorem 2 (cf. [5, Th. 2], [8, Th. 3.9]). *For a formally real field the following are equivalent*:

(1) *If $t \in F \setminus F^2$ is a sum of squares then t is rigid.*
(2) *D_8 is not a homomorphic image of G_{py}.*
(3) *H_8 does not occur as a Galois group over F.*
(4) *H_8 is not a homomorphic image of G_{py}.*

Proof The equivalence of (1) and (2) is contained in [8, Th. 3.9] while the equivalence of (1) and (3) follows from Lemma 2. It remains to prove (4) $\Rightarrow$ (3):

Assume there exists a Galois extension K/F such that $\mathrm{Gal}(K/F) \cong H_8$. Then there exist a, b in F, independent mod squares, such that $F(\sqrt{a}, \sqrt{b}) \subseteq K$. By [9, §6] $\langle a, b, ab\rangle \cong \langle 1, 1, 1\rangle$. Hence $F(\sqrt{a}, \sqrt{b}) \subseteq F_{\mathrm{py}}$ so there is an epimorphism $f\colon G_{\mathrm{py}} \to V = \mathrm{Gal}(F(\sqrt{a},\sqrt{b})/F)$ and a diagram

$$\begin{array}{ccccccccc} & & & & & & G_{\mathrm{py}} & & \\ & & & & & & \downarrow & & \\ 1 & \to & \mathbf{Z}/2\mathbf{Z} & \to & H_8 & \xrightarrow{h} & V & \to & 1 \end{array}$$

with exact row. Let $e \in H^2(V,\mathbf{Z}/2\mathbf{Z})$ correspond to the above row. It is well known that there is a surjective homomorphism $\overline{f}\colon G_{\mathrm{py}} \to H_8$ such that $h \circ \overline{f} = f$ if and only if $f^*(e) = 0$ where $f^*\colon H^2(V,\mathbf{Z}/2\mathbf{Z}) \to H^2(G_{\mathrm{py}},\mathbf{Z}/2\mathbf{Z})$ is induced by f (cf., [2, §7], [6, §3]).

Let G_F be the absolute Galois group of F, let $s\colon G_F \to G_{\mathrm{py}}$ be the natural surjection, and let $g = f \circ s$. Then if $\overline{g}\colon G_F \to \mathrm{Gal}(K/F) \cong H_8$ is the natural map, we have $g = h \circ \overline{g}$. Hence $g^*(e) = 0$ in $H^2(G_F,\mathbf{Z}/2\mathbf{Z})$. By [8, Cor. 2.2], $H^2(G_{\mathrm{py}},\mathbf{Z}/2\mathbf{Z}) \to Br(F_{\mathrm{py}}/F) \subseteq Br(F)$ is injective, whence $s^*\colon H^2(G_{\mathrm{py}},\mathbf{Z}/2\mathbf{Z}) \to H^2(G_F,\mathbf{Z}/2\mathbf{Z}) \cong Br_2(F)$ is injective. As $g^* = s^* \circ f^*$ we conclude that $f^*(e) = 0$. Hence H_8 is a homomorphic image of G_{py}, completing the proof of Theorem 2.

An extension K/F is called *totally positive* if every ordering (if any) on F extends to an ordering on K.

Corollary. *For a field F the following are equivalent*:

(1) *H_8 occurs as a Galois group over F.*
(2) *There is a totally positive Galois extension K/F such that* $\mathrm{Gal}(K/F) \cong H_8$.
(3) *There is a totally positive Galois extension L/F such that* $\mathrm{Gal}(L/F) \cong D_8$.

Proof. It is well known that a 2-extension K/F is totally positive iff $K \subseteq F_{\mathrm{py}}$.

Theorem 3. *For a uniquely ordered field F with positive cone P the following are equivalent*:

(1) *$WF \cong \mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}[P/\dot{F}^2]$, the fibre product over $\mathbf{Z}/2\mathbf{Z}$ (= product in the category of Witt rings).*

(2) *$G_F(2) \cong \mathbf{Z}/2\mathbf{Z} * G_{\mathrm{py}}$ (free pro-2-product) and G_{py} has (topological) generators $\{y_i, x\}_{i\in I}$ with relations $y_iy_j = y_jy_i$ and either $xy_ix^{-1} = y_i^{5^m}$ for fixed $m = 2^n$ $(n \geq 0)$ and for all $i \in I$ or $xy_i = y_ix$ for all i.*

(3) *G_{py} has generators and relations as described in* (2).

(4) *H_8 does not occur as a Galois group over F.*

Proof. (1) $\Rightarrow$ (2). By [1], Realization Theorem 4.8 and Remarks 4.9(i) there exist 2-extensions K, L of F such that $WK \cong \mathbf{Z}$, $WL \cong \mathbf{Z}/2\mathbf{Z}[P/\dot{F}^2]$, and the inclusions $F \subseteq K, L$ induce the isomorphisms $WF \xrightarrow{\cong} WK \times WL \cong \mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}[P/\dot{F}^2]$. By [3, Th. 3.4], $G_F(2) \cong G_K(2) * G_L(2) \cong \mathbf{Z}/2\mathbf{Z} * G_L(2)$ and by Theorem 1, $G_L(2)$ has the generators and relations described in (2).

Let I_tF denote the torsion subgroup of the fundamental ideal IF of WF. As $WF \cong \mathbf{Z} \times WL$ the inclusion $F \subseteq L$ induces an isomorphism $I_tF \to IL = I_tL$ whence by [8, Th. 2.10], $G_{\mathrm{py}} \cong G_L(2)$.

(3) $\Rightarrow$ (4). A pro-2-group with generators and relations as described in (2) cannot have H_8 as a homomorphic image. By Theorem 2, H_8 does not occur as a Galois group over F.

(4) $\Rightarrow$ (1). As F is uniquely ordered, P is the set of nonzero sums of squares and $(\dot{F}: P) = 2$. Hence the mapping $\mathbf{Z}[P/\dot{F}^2] \to WF$ via $\sum n_i[t_i] \to \sum n_i\langle t_i\rangle$ is surjective and by Theorem 2 (1), its kernel is additively generated by the elements $2[t] - 2[u]$, t, $u \in P$. On the other hand, $\mathbf{Z}[P/\dot{F}^2] \to \mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}[P/\dot{F}^2]$ via $\sum n_i[t_i] \to (\sum n_i, \sum \overline{n}_i[t_i])$ is surjective and $\sum n_i[t_i]$ lies in the kernel iff all n_i are even and $\sum n_i = 0$. This happens iff $\sum n_i[t_i] = \sum 2([u_j] - [v_j])$, proving (1).

Remark. If G is a pro-2-group with generators and relations described in Theorem 3 (2) then by the remark following Theorem 1 and [8, Th. 4.1] there is a uniquely ordered field F with $G_{\mathrm{py}} \cong G$.

References

1. J. Arason, R. Elman and B. Jacob, *Rigid elements, valuations and realizations of Witt rings*, J. Algebra **110** (1987), 449–467.
2. A. Fröhlich, *Orthogonal representation of Galois groups, Stiefel-Whitney classes and Hasse-Witt invariants*, J. Reine Angew. Math. **360** (1985), 84–123.
3. B. Jacob and R. Ware, *A recursive description of the maximal pro-2-Galois group via Witt rings*, Math. Z. **200** (1989), 379–396.
4. T. Y. Lam, *The algebraic theory of quadratic forms*, Benjamin, Elmsford, New York, 1973.
5. J. Minač, *Quaternion fields inside the Pythagorean closure*, J. Pure Appl. Algebra **57** (1989), 79–82.
6. J.-P. Serre, *L'invariant de Witt de la Forme $Tr(x^2)$*, Comment Math. Helv. **59** (1984), 651–676.
7. R. Ware, *When are Witt rings group rings?* II, Pacific J. Math. **76** (1978), 541–564.
8. ——, *Quadratic forms and pro-2-groups* II: *the Galois group of the Pythagorean closure of a formally real field*, J. Pure Appl. Algebra **30** (1983), 95–107.
9. E. Witt, *Konstruktion von galoisschen Körpen der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f*, J. Reine Angew. Math. **174** (1936), 237–245.

Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802