JOURNAL OF NUMBER THEORY 35, 227–246 (1990)

Fields Arithmetically Equivalent to a Radical Extension of the Rationals

ELIOT JACOBSON

Department of Mathematics, Ohio University, Athens, Ohio 45701

AND

WILLIAM YSLAS VÉLEZ

Department of Mathematics, The University of Arizona, Tucson, Arizona 85721

Communicated by P. Roquette

Received June 16, 1989; revised September 4, 1989

1. INTRODUCTION

Suppose a number field K is arithmetically equivalent (defined below) to a radical extension $Q(\sqrt[n]{a})$. What can be said about K? If K is assumed to be a radical extension, then K is classified by the results in [E. Jacobson and W. Y. Vélez, *Arch. Math.* **45** (1985), 12–20]. The purpose of this paper is to obtain a complete classification of such fields K.

First of all, if $8 \nmid n$ then we prove that K and $Q(\sqrt[n]{a})$ are isomorphic (see Theorem 3.1c, Theorem 5.1, and Corollary 5.4). For the general case, write $n = 2^e m$, where $e \geqslant 3$ and m is odd. In Theorem 5.1 we show that K is the compositum $K = LM$, where L and M are arithmetically equivalent to $Q(\sqrt[2^e]{a})$ and $Q(\sqrt[m]{a})$, respectively. Owing to Theorem 5.3, which shows that M and $Q(\sqrt[m]{a})$ are isomorphic, this effectively reduces the problem to the case $n = 2^e$. Theorem 3.1 offers a complete classification of the fields L that arise, and thus all K are classified.

Finally, the exceptional case that occurs in Theorem 3.1b demonstrates that the work in [Jacobson and Vélez, 1985] is not sufficient: a non-radical extension and a radical extension can be arithmetically equivalent.

0022-314X/90 $3.00

2. Generalities and Radical Extensions

We begin by reviewing some definitions and results.

Two number fields K_1, K_2 are *arithmetically equivalent* if their zeta functions coincide. A number field K is *solitary* if the only fields arithmetically equivalent to K are those that are isomorphic to K.

For a finite group G and subgroups H_1, H_2 of G, we say that H_1, H_2 are *Gassmann equivalent* if $|H_1 \cap \mathrm{cl}_G(x)| = |H_2 \cap \mathrm{cl}_G(x)|$ for every conjugacy class $\mathrm{cl}_G(x)$ of G. The following result is included for ease of reference; it indicates the variety of disparate areas connected by the concepts defined above.

Theorem 2.1. *Let K_1, K_2 be algebraic number fields, and Ω any Galois extension of Q containing K_1 and K_2. Denote $G = \mathrm{Gal}(\Omega/Q)$, $H_i = \mathrm{Gal}(\Omega/K_i)$, $i = 1, 2$. Then the following are equivalent.*

(a) *K_1, K_2 are arithmetically equivalent.*

(b) *H_1, H_2 are Gassmann equivalent.*

(c) *The permutation characters $1_{H_1}^G$, $1_{H_2}^G$ are equal. (In particular, $|H_1| = |H_2|$.)*

(d) *For every prime p of $\mathbb{Z}$ which is unramified in K_1K_2, we have $K_1 \otimes_Q Q_p \cong K_2 \otimes_Q Q_p$ as Q_p-algebras.*

Proof. The equivalence of (a), (b), and (d) appears in [4]. The inclusion of condition (c) arises from the elementary formula:

$$1_{H_i}^G(x) = |H_i|^{-1} \cdot |C_G(x)| \cdot |H_i \cap \mathrm{cl}_G(x)|,$$

where $C_G(x)$ is the centralizer of x in G. ∎

Most recently, condition (c) has been studied for large subgroups of simple groups in [1, 2].

In the remainder of this paper we use and abuse the abbreviations g.e. for "Gassmann equivalent" and a.e. for "arithmetically equivalent." The following appears in [4].

Theorem 2.2. *Let K_1, K_2 be a.e. number fields. Then K_1, K_2 have the same Galois closure (notation: $\bar{K}_1 = \bar{K}_2$) and the same normal core. Moreover, if $\mathrm{Gal}(\bar{K}_i/K_i)$ is cyclic, then K_i is a solitary field ($K_1 \cong K_2$).*

For the remainder of this section we set the following notation. For the irreducible binomial $x^n - a$ over Q we denote $\Omega = Q(\sqrt[n]{a}, \zeta_n)$, $G = \mathrm{Gal}(\Omega/Q)$, $H = \mathrm{Gal}(\Omega/Q(\sqrt[n]{a}))$. If K denotes a field a.e. to $Q(\sqrt[n]{a})$, then $K \subset \Omega$ and we set $J = \mathrm{Gal}(\Omega/K)$.

Theorem 2.1 allows us to translate questions about arithmetic equivalence to questions about Gassmann equivalence in group theory. We employ this tactic quite frequently. Thus, it is convenient to give a workable description of G.

Let C_n denote the cyclic additive group of integers modulo n, and C_n^* the multiplicative group of integers prime to n. Define a binary operation on the set $C_n \times C_n^*$ via

$$(\alpha, u) \cdot (\beta, v) = (\alpha + \beta u, uv).$$

Then $C_n \times C_n^*$ is a group with identity $(0, 1)$ and inverses given by the rule $(\alpha, u)^{-1} = (-\alpha u^{-1}, u^{-1})$. This group is frequently called the *holomorph* of C_n.

There is a natural embedding of G above into $C_n \times C_n^*$ arising as follows. Given $\sigma \in G$, we have $\sigma(\sqrt[n]{a}) = \zeta_n^\alpha \cdot \sqrt[n]{a}$ and $\sigma(\zeta_n) = \zeta_n^u$ (where ζ_n denotes a primitive nth root of unity) for some integers α, u. Then $\sigma \mapsto (\alpha, u)$ is a monomorphism. We identify G with its image in $C_n \times C_n^*$ under this monomorphism. We now give the basic group theoretic description of subgroups of G that are Gassmann equivalent to H.

Let $T = \mathrm{Gal}(Q(\zeta_n)/Q(\sqrt[n]{a}) \cap Q(\zeta_n))$ viewed as a subgroup of C_n^*. Then it is easy to see that $H = \{(0, u) : u \in T\}$ and that H is abelian.

LEMMA 2.3. *Let G, H, T be as above and suppose that $J \leqslant G$ is g.e. to H in G. Then $J = \{(w_u(1-u), u) : u \in T\}$ for some integers w_u. Moreover, J is abelian.*

Proof. Fix $(0, u) \in H$ *and let* $(\alpha, v) \in G$. *Then* $(\alpha, v)(0, u)(\alpha, v)^{-1} = (\alpha(1-u), u)$, and hence $\mathrm{cl}_G((0, u)) = \{(\alpha(1-u), u) : \alpha \in C_n\}$. Since clearly $|H \cap \mathrm{cl}_G((0, u))| = 1$, by hypothesis we have that $|J \cap \mathrm{cl}_G((0, u))| = 1$ for each $u \in T$. Since $|H| = |J|$, J is as described. Finally, for $u, v \in T$ we have

$$(w_u(1-u), u) \cdot (w_v(1-v), v) = (w_u(1-u) + u \cdot w_v(1-v), uv)$$
$$(w_v(1-v), v) \cdot (w_u(1-u), u) = (w_v(1-v) + v \cdot w_u(1-u), vu).$$

However, J contains exactly one element whose second component is $uv = vu$, so these two must be equal, thus J is abelian. ∎

We finish this section by quoting some useful results on radical extensions (see [5]).

THEOREM 2.4. *Let $n \geqslant 2$ and suppose that $x^n - a$, $x^n - b$ are irreducible over Q. Then*

(a) $Q(\sqrt[n]{a}) \cap Q(\zeta_n) = Q(\sqrt[2^s]{a})$, *for some* $s \geqslant 0$.

(b) *The quadratic subfields of* $Q(\zeta_{2^e})$ $(e \geqslant 3)$ *are* $Q(\zeta_4)$, $Q(\sqrt{2})$, *and* $Q(\sqrt{-2})$.

(c) $Q(\sqrt[n]{a})$, $Q(\sqrt[n]{b})$ *are a.e. if and only if one of the following holds*:

(i) $a = b^i c^n$ *with* $c \in Q$ *and* $(i, n) = 1$; *or*

(ii) $8 \mid n$ *and* $a = b^i c^n 2^{n/2}$ *with* $c \in Q$ *and* $(i, n) = 1$.

(d) $Q(\sqrt[n]{a})$, $Q(\sqrt[n]{b})$ *are isomorphic if and only if one of the following holds* :

(i) $a = b^i c^n$ *with* $c \in Q$ *and* $(i, n) = 1$; *or*

(ii) $8 \mid n$ *and* $-a$, $-b \in Q^2$, *and* $a = b^i c^n 2^{n/2}$ *with* $c \in Q$ *and* $(i, n) = 1$.

3. The Case $n = 2^e$

Fix an irreducible binomial $x^{2^e} - a$ over Q. This section is devoted to the classification of fields arithmetically equivalent to $Q(\sqrt[2^e]{a})$. As agreed in the previous section, we denote $\Omega = Q(\sqrt[2^e]{a}, \zeta_{2^e})$, $G = \mathrm{Gal}(\Omega/Q)$, $H = \mathrm{Gal}(\Omega/Q(\sqrt[2^e]{a}))$, and $Q(\sqrt[2^e]{a}) \cap Q(\zeta_{2^e}) = Q(\sqrt[2^s]{a})$ for some $s \geqslant 0$. We now state the main theorem of this section.

Theorem 3.1. *Let* $x^{2^e} - a$ *be irreducible over* Q *and write* $Q(\sqrt[2^e]{a}) \cap Q(\zeta_{2^e}) = Q(\sqrt[2^s]{a})$. *Let* K *be a number field arithmetically equivalent to* $Q(\sqrt[2^e]{a})$.

(a) *If* $e \geqslant 3$ *and* $s = 0$, *then* K *is isomorphic to either* $Q(\sqrt[2^e]{a})$ *or* $Q(\sqrt[2^e]{a} \cdot \sqrt{2})$.

(b) *If* $e \geqslant 4$, $s = 1$, *and* $Q(\sqrt[2^s]{a}) = Q(\sqrt{2})$, *then* K *is isomorphic to either* $Q(\sqrt[2^e]{a})$ *or* $Q(\sqrt[2^e]{a} \cdot \sqrt{2 + \sqrt{2}})$. *Furthermore,* $Q(\sqrt[2^e]{a} \cdot \sqrt{2 + \sqrt{2}})$ *is not a radical extension.*

(c) *In all other cases,* $Q(\sqrt[2^e]{a})$ *is a solitary field.*

The proof is completed in a sequence of cases. First observe that if H is cyclic then by Theorem 2.2, $Q(\sqrt[2^e]{a})$ is a solitary field. If $s \geqslant 2$, then $\zeta_4 \in Q(\sqrt[2^e]{a})$, so $\zeta_4 \in Q(\sqrt[2^s]{a})$. However, $Q(\zeta_{2^e})/Q(\zeta_4)$ is cyclic, thus H is cyclic. Also, H is cyclic if $e \leqslant 2$, or if $e = 3$ and $s = 1$. Thus in the following we may assume that

$$e \geqslant 3,\ s \leqslant 1, \text{ and if } e = 3 \text{ then } s = 0.$$

Case 1. $e \geqslant 3$ and $s = 0$. In this case, $G \mapsto C_{2^e} \times C_{2^e}^*$ is an isomorphism. Now for $e \geqslant 3$ it is well known that $C_{2^e}^*$ is generated by the residues -1, $5 \pmod{2^e}$. It follows that H is generated by the pairs $(0, -1)$, $(0, 5)$.

LEMMA 3.2. *In the situation of Case* 1, *if* $J \leqslant G$ *is g.e. to* H, *then* J *has generators* $(\alpha, 5)$, $(\beta, -1)$, *where* $\alpha \equiv 0 \pmod 4$, $\beta \equiv 0 \pmod 2$, *and* $2\alpha \equiv -4\beta \pmod{2^e}$.

Proof. As -1, 5 generate $C^*_{2^e}$, the definition of multiplication in G together with Lemma 2.3 shows that J has as generators elements $(w_5(1-5), 5) = (-4w_5, 5) = (\alpha, 5)$, and $(w_{-1}(1-(-1)), -1) = (2w_{-1}, -1) = (\beta, -1)$. So all assertions are clear except the final congruence. But J is abelian by Lemma 2.3, so that

$$(\alpha, 5)(\beta, -1)(\alpha, 5)^{-1} = (\beta, -1).$$

After some computation this yields $(2\alpha + 5\beta, -1) = (\beta, -1)$, so that $2\alpha + 5\beta \equiv \beta \pmod{2^e}$ as needed. ∎

LEMMA 3.3. *In the situation of Case* 1, *there are at most* 2^e *subgroups* $J \leqslant G$ *that are g.e. to* H.

Proof. Any such J has a generating set as described in Lemma 3.2, so it suffices to count generating sets. However, if $(\alpha, 5)$, $(\beta - 1)$ satisfy $\alpha \equiv 0 \pmod 4$, $\beta \equiv 0 \pmod 2$, and $2\alpha \equiv -4\beta \pmod{2^e}$, then clearly there are 2^{e-1} choices for β, and for each β there are exactly two choices for α. ∎

LEMMA 3.4. *In the situation of Case* 1, *if* $J \leqslant G$ *is g.e. to* H *then* $|N_G(J)| = 2^e$. *In particular,* J *has* 2^{e-1} *distinct conjugates in* G.

Proof. Say J has the generating set $\{(\alpha, 5), (\beta, -1)\}$ and let $(\eta, z) \in G$. Then (η, z) normalizes J iff it normalizes the generating set. Straightforward computation now gives that

$$(\eta, z) \in N_G(J) \quad \text{iff} \quad \begin{cases} -4\eta \equiv \alpha(1-z) & \pmod{2^e} \text{ and} \\ 2\eta \equiv \beta(1-z) & \pmod{2^e}. \end{cases}$$

Since $\beta \equiv 0 \pmod 2$, the second congruence has exactly 2 solutions: $\eta \equiv (\beta/2)(1-z), (\beta/2)(1-z) + 2^{e-1} \pmod{2^e}$, for any choice of z. Thus the second congruence has exactly $2 \cdot 2^{e-1} = 2^e$ solutions (η, z).

As z is odd, observe that for any solution (η, z) to the second congruence we have

$$-4\eta \equiv -2\beta(1-z) \equiv -4\beta \frac{(1-z)}{2} \equiv 2\alpha \frac{(1-z)}{2} \equiv \alpha(1-z) \qquad \pmod{2^e},$$

so (η, z) is also a solution to the first congruence. Thus the system of congruences has exactly 2^e solutions, hence $|N_G(J)| = 2^e$. Then $[G : N_G(J)] = 2^{e-1}$, and the last assertion follows. ∎

Conclusion of Case 1. Let $J \leqslant G$ be generated by $\{(2^{e-1}, 5), (0, -1)\}$. Then J has fixed field $Q(\sqrt[2^e]{a} \cdot \sqrt{2})$, which is a.e. but not isomorphic to $Q(\sqrt[2^e]{a})$, by Theorem 2.4 (since if $-a \in Q^2$ then $\zeta_4 \in Q(\sqrt[2^e]{a})$ so $s \geqslant 1$). Thus J is g.e. to H, but not conjugate H. By Lemmas 3.3 and 3.4, there are exactly 2 conjugacy classes of subgroups of G that are g.e. to H, represented by H and J. By Galois theory, there are 2 isomorphism classes of fields that are a.e. to $Q(\sqrt[2^e]{a})$, represented by $Q(\sqrt[2^e]{a})$ and $Q(\sqrt[2^e]{a} \cdot \sqrt{2})$. It follows incidentally, by counting, that any generating set, as in Lemma 3.2, generates a subgroup of G that is g.e. to H.

Note that if $s = 1$, then Theorem 2.4b applies. In this way, there are three cases when $s = 1$, $e \geqslant 4$.

Case 2. $e \geqslant 4$, $s = 1$, and $Q(\sqrt[2^s]{a}) = Q(\sqrt{2})$. In this case the image of G in $C_{2^e} \times C_{2^e}^*$ has index 2. We must compute this image exactly. By the equality $Q(\sqrt{a}) = Q(\sqrt{2})$ we have $a = 2c^2$ for some $c \in Q$. Hence $\sqrt{2} = (1/c)\sqrt{a} = \zeta_8 + \zeta_8^{-1}$. Let $\sigma \in G$ correspond to $(\alpha, u) \in C_{2^e} \times C_{2^e}^*$. We compute $\sigma(\sqrt{2})$ in two ways:

$$\sigma(\sqrt{2}) = \frac{1}{c}\sigma(\sqrt{a}) = \frac{1}{c}\sqrt{a}\,(-1)^\alpha = \sqrt{2} \cdot (-1)^\alpha$$

$$\sigma(\sqrt{2}) = \sigma(\zeta_8 + \zeta_8^{-1}) = \zeta_8^u + \zeta_8^{-u}.$$

Hence $\zeta_8^u + \zeta_8^{-u} = \sqrt{2} \cdot (-1)^\alpha$ and we have

$$(*)\begin{cases} \alpha \equiv 0 \pmod 2 \Leftrightarrow u \equiv 1, 7 \pmod 8 \\ \alpha \equiv 1 \pmod 2 \Leftrightarrow u \equiv 3, 5 \pmod 8, \end{cases}$$

so $G = \{(\alpha, u) \in C_{2^e} \times C_{2^e}^* : (\alpha, u) \text{ satisfies } (*)\}$. (Note that the given subgroup of $C_{2^e} \times C_{2^e}^*$ has index 2, hence must be all of G by counting.) With this description of G, we now have

$$H = \{(0, u) : u \equiv 1, 7 \pmod 8\}.$$

Our analysis is analogous to Case 1, and we just sketch the details.

If $J \leqslant G$ is g.e. to H then $J = \{(w_u(1-u), u) : u \equiv 1, 7 \pmod 8\}$ for some integers w_u. As $C_{2^e}^*$ is generated by -1, 5, it is easy to see that H is generated by $(0, -1)$ and $(0, 5^2) = (0, 25)$. Thus, J has generators $(\alpha, 25)$, $(\beta, -1)$ which in this case must satisfy the congruences $\beta \equiv 0 \pmod 2$, $\alpha \equiv 0 \pmod 8$, and $2\alpha \equiv -24\beta \pmod{2^e}$. There are 2^e such pairs $\{(\alpha, 25), (\beta, -1)\}$ satisfying these congruences, hence at most 2^e subgroups of G are g.e. to H.

Now if $J \leqslant G$ is g.e. to H and is generated by $\{(\alpha, 25), (\beta, -1)\}$ then $(\eta, z) \in G$ normalizes J

$$\text{iff} \begin{cases} -24\eta \equiv \alpha(1-z) \pmod{2^e} \text{ and} \\ \quad 2\eta \equiv \beta(1-z) \pmod{2^e}. \end{cases}$$

As $z \equiv 1 \pmod 2$ and $\beta \equiv 0 \pmod 2$ it follows that $\eta \equiv 0 \pmod 2$ and hence by $(*)$ that $z \equiv 1, 7 \pmod 8$. With these restrictions the second congruence has 2^{e-2} choices for z, and for each z there are exactly 2 η's such that (η, z) is a solution. As before, a solution to the second congruence is also a solution to the first, hence $|N_G(J)| = 2^{e-1}$. It follows that $[G: N_G(J)] = 2^{e-1}$, so J has 2^{e-1} distinct conjugates.

If now J is generated by $\{(2^{e-1}, 25), (0, 1)\}$ then J has fixed field $Q(\sqrt[2^e]{a} \cdot (\zeta_{16} + \zeta_{16}^{-1})) = Q(\sqrt[2^e]{a} \cdot \sqrt{2 + \sqrt{2}})$. If this J is conjugate to H then there exists $(\eta, z) \in G$ such that

$$\begin{cases} (\eta, z)(2^{e-1}, 25)(\eta, z)^{-1} = (0, 25) \text{ and} \\ (\eta, z)(0, -1)(\eta, z)^{-1} = (0, -1). \end{cases}$$

Thus

$$\begin{cases} 24\eta \equiv 2^{e-1}z \pmod{2^e} \text{ and} \\ \quad 2\eta \equiv 0 \pmod{2^e}. \end{cases}$$

But $2\eta \equiv 0 \pmod{2^e}$ gives also $24\eta \equiv 0 \pmod{2^e}$, whereas $z \equiv 1 \pmod 2$ gives $2^{e-1}z \not\equiv 0 \pmod{2^e}$. Hence there can be no solution (η, z). By counting, J and H represent the two conjugacy classes of subgroups of G that are g.e. to H. Hence $Q(\sqrt[2^e]{a})$, $Q(\sqrt[2^e]{a} \cdot \sqrt{2 + \sqrt{2}})$ are the isomorphism classes of fields a.e. to $Q(\sqrt[2^e]{a})$.

If $Q(\sqrt[2^e]{a} \cdot \sqrt{2 + \sqrt{2}})$ were a radical extension, then by Theorem 2.4, $Q(\sqrt[2^e]{a} \cdot \sqrt{2 + \sqrt{2}})$ is isomorphic to either $Q(\sqrt[2^e]{a})$ or $Q(\sqrt[2^e]{a} \cdot \sqrt{2})$. However, $\sqrt{2} \in Q(\sqrt[2^e]{a})$ by assumption, hence these last two fields are equal. Since we just saw that $Q(\sqrt[2^e]{a} \cdot \sqrt{2 + \sqrt{2}})$ is not isomorphic to $Q(\sqrt[2^e]{a})$, it follows that $Q(\sqrt[2^e]{a} \cdot \sqrt{2 + \sqrt{2}})$ is not a radical extension.

Case 3. $e \geqslant 4$, $s = 1$, and $Q(\sqrt[2^s]{a}) = Q(\sqrt{-2})$. In this case G corresponds to the pairs (α, u) in $C_{2^e} \times C_{2^e}^*$ that satisfy

$$\begin{cases} \alpha \equiv 0 \pmod 2 \Leftrightarrow u \equiv 1, 3 \pmod 8 \\ \alpha \equiv 1 \pmod 2 \Leftrightarrow u \equiv 5, 7 \pmod 8 \end{cases}$$

and H corresponds to $\{(0, u): u \equiv 1, 3 \pmod 8\}$. Now -5 has order 2^{e-2} in $C_{2^e}^*$ and $(0, -5) \in H$. As also $|H| = 2^{e-2}$, we have that H is cyclic, generated by $(0, -5)$. Thus by Theorem 2.2, $Q(\sqrt[2^e]{a})$ is a solitary field.

Case 4. $e \geqslant 4$, $s=1$, and $Q(\sqrt{a})=Q(\zeta_4)$. In this case H is cyclic. Indeed, one computes that $G=\{(\alpha, u): 2\alpha \equiv 3+u \pmod 4\}$ and therefore $H=\{(0, u): u \equiv 1 \pmod 4\}$. Hence $H=\langle(0, 5)\rangle$.

These cases finish the proof of Theorem 3.1. ∎

4. A Reduction

In this section we address a special case of the following question. Suppose that K_1, K_2 are arithmetically equivalent number fields and that $K_1=L_1M_1$, where $L_1 \cap M_1=Q$ and $([L_1: Q], [M_1: Q])_{\text{gcd}}=1$. Does K_2 contain subfields L_2, M_2 such that $K_2=L_2M_2$ and $\{L_1, L_2\}$, $\{M_1, M_2\}$ are sets of arithmetically equivalent fields?

We are not able to answer this question entirely, though we give some positive results (see Theorem 4.5). Our interest in this question comes from the case when $n=2^e m$, m odd, $K_1=Q(\sqrt[n]{a})$, $L_1=Q(\sqrt[2^e]{a})$, $M_1=Q(\sqrt[m]{a})$. In this specific case, Theorem 4.5 is sufficient to guarantee the existence of the two fields L_2 and M_2.

In the next four lemmas, G denotes an arbitrary finite group.

Lemma 4.1. *Suppose $H_1, H_2 \leqslant G$ are g.e. in G. If $N \lhd G$ then $H_1 \cap N$ g.e. $H_2 \cap N$ in G.*

Proof. If $x \in G$ then either $\mathrm{cl}_G(x) \subseteq N$ or else $\mathrm{cl}_G(x) \cap N=\varnothing$. Hence in either case, $|H_1 \cap N \cap \mathrm{cl}_G(x)|=|H_2 \cap N \cap \mathrm{cl}_G(x)|$. ∎

Lemma 4.2. *Let $G_1 \leqslant G$ and $H_1, H_2 \leqslant G_1$. If H_1 g.e. H_2 in G_1, then H_1 g.e. H_2 in G.*

Proof. By assumption, $1_{H_1}^{G_1}=1_{H_2}^{G_1}$. By transitivity of induction, $1_{H_1}^G=(1_{H_1}^{G_1})^G=(1_{H_2}^{G_1})^G=1_{H_2}^G$. ∎

Lemma 4.3. *Suppose that $G=G_1 \times G_2$ and that $H_1 \leqslant G$ can be written $H_1=H_{11} \times H_{12}$, where $H_{11} \leqslant G_1$, $H_{12} \leqslant G_2$. Let $H_2 \leqslant G$ and assume that H_1 g.e. H_2 in G. Then there are subgroups $H_{21} \leqslant G_1$, $H_{22} \leqslant G_2$ such that $H_2=H_{21} \times H_{22}$, and furthermore H_{11} g.e. H_{21} and H_{12} g.e. H_{22} in G.*

Proof. Every conjugacy class $\mathrm{cl}_G(y)$ of G has the form $\mathrm{cl}_G(y)=\mathrm{cl}_{G_1}(y_1) \times \mathrm{cl}_{G_2}(y_2)$ (where $y=(y_1, y_2)$). Since H_1 g.e. H_2 it follows from Lemma 4.1 that $H_1 \cap G_i$ g.e. $H_2 \cap G_i$ $(i=1,2)$. Set $H_{21}=H_2 \cap G_1$, $H_{22}=H_2 \cap G_2$. Plainly, $H_{1i}=H_1 \cap G_i$ $(i=1,2)$, and from the above we have $|H_{1i}|=|H_{2i}|$ $(i=1,2)$ and $|H_1|=|H_2|$. Then $|H_2| \geqslant |H_{21}| \cdot |H_{22}|=|H_{11}| \cdot |H_{12}|=|H_1|=|H_2|$, so equality holds, and $H_2=H_{21} \times H_{22}$. ∎

LEMMA 4.4. *Suppose* $G = N_1 N_2$ *(internal direct product) and let* A, $B \leqslant N_1$ *be such that* A *g.e.* B *in* G. *Then* AN_2 *g.e.* BN_2 *in* G.

Proof. Easy exercise. ▮

We can now state the result we are after. We first state the Galois theoretic version, and then translate to group theory to effect the proof. Recall that $\bar{K}$ denotes the Galois closure of K over Q.

THEOREM 4.5. *Suppose* K_1, K_2 *are number fields such that* K_1 *a.e.* K_2. *Assume that there are subfields* L_1, M_1 *of* K_1 *such that* $K_1 = L_1 M_1$ *and* $\bar{L}_1 \cap \bar{M}_1 \subseteq K_1$.
Then

$$(\bar{L}_1 \cdot K_1) \cap \bar{M}_1 = K_1 \cap \bar{M},$$

and

$$(\bar{M}_1 \cdot K_1) \cap \bar{L}_1 = K_1 \cap \bar{L}_1.$$

Furthermore, there exist subfields $\mathfrak{L}_2$, $\mathcal{M}_2$ *of* $\bar{K}_1 = \bar{K}_2$ *such that*

(a) $\mathfrak{L}_2$ *a.e.* $K_1 \bar{L}_1$ *and* $\mathcal{M}_2$ *a.e.* $K_1 \bar{M}_1$;

(b) $\mathfrak{L}_2 \cap \bar{M}_1$, $\mathcal{M}_2 \cap \bar{L}_1$ *are subfields of* K_2;

(c) $\mathfrak{L}_2 \cap \bar{M}_1$ *a.e.* $K_1 \cap \bar{M}_1$, *and* $\mathcal{M}_2 \cap \bar{L}_1$ *a.e.* $K_1 \cap \bar{L}_1$;

(d) $K_2 = \mathfrak{L}_2 \cap M_2 = (\mathfrak{L}_2 \cap \bar{M}_1) \cdot (\mathcal{M}_2 \cap \bar{L}_1)$.

See Fig. 1. To translate this to group theory we need one definition. Given any $H \leqslant G$, we denote by $\mathrm{Core}_G(H) = \mathrm{Core}(H)$ the largest subgroup of H that is normal in G. By Galois theory, it only remains to prove the following theorem.

THEOREM 4.6. *Let* $H_1, H_2 \leqslant G$ *and suppose that* H_1 *g.e.* H_2 *in* G. *Furthermore, assume*

(a) $\mathrm{Core}\, H_1 = \mathrm{Core}\, H_2 = 1$,

(b) *There are subgroups* A_1, B_1 *of* G *such that* $H_1 = A_1 \cap B_1$ *and* $H_1 \subseteq (\mathrm{Core}\, A_1) \cdot (\mathrm{Core}\, B_1)$.
Then

$$(H_1 \cap \mathrm{Core}\, A_1) \cdot \mathrm{Core}\, B_1 = H_1 \cdot \mathrm{Core}\, B_1$$

and

$$(H_1 \cap \mathrm{Core}\, B_1) \cdot \mathrm{Core}\, A_1 = H_1 \cdot \mathrm{Core}\, A_1.$$

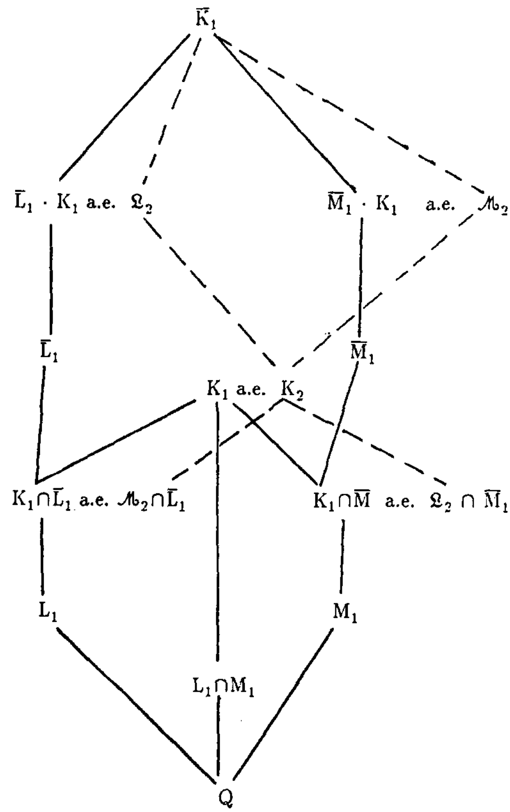

FIGURE 1

Furthermore, there are subgroups $\mathcal{A}_2$, $\mathcal{B}_2$ of G such that

(i) $\mathcal{A}_2$ *g.e.* $H_1 \cap \text{Core } A_1$, $\mathcal{B}_2$ *g.e.* $H_1 \cap \text{Core } B_1$ *in* G;

(ii) $\mathcal{A}_2 \subseteq \text{Core } A_1$, $\mathcal{B}_2 \subseteq \text{Core } B_1$, *and* $H_2 = \mathcal{A}_2 \times \mathcal{B}_2$;

(iii) $\mathcal{A}_2 \cdot \text{Core } B_1$ *g.e.* $H_1 \cdot \text{Core } B_1$, *and* $\mathcal{B}_2 \cdot \text{Core } A_1$ *g.e.* $H_1 \cdot \text{Core } A_1$ *in* G;

(iv) $H_2 = (\mathcal{A}_2 \cdot \text{Core } B_1) \cap (\mathcal{B}_2 \cdot \text{Core } A_1)$.

In this translation, we are letting $\Omega = \bar{K}_1 = \bar{K}_2$, $G = \text{Gal}(\Omega/Q)$, $H_i = \text{Gal}(\Omega/K_i)$, $A_1 = \text{Gal}(\Omega/L_1)$, and $B_1 = \text{Gal}(\Omega/M_1)$. Figure 2 is helpful in following the proof.

Proof. Observe that as $\text{Core } A_1 \cap \text{Core } B_1 \subseteq A_1 \cap B_1 = H_1$, and $\text{Core } H_1 = 1$, we have $\text{Core } A_1 \cap \text{Core } B_1 = 1$. Thus $\text{Core } A_1 \cdot \text{Core } B_1 = \text{Core } A_1 \times \text{Core } B_1$. We claim that

$$H_1 = (H_1 \cap \text{Core } A_1) \times (H_1 \cap \text{Core } B_1).$$

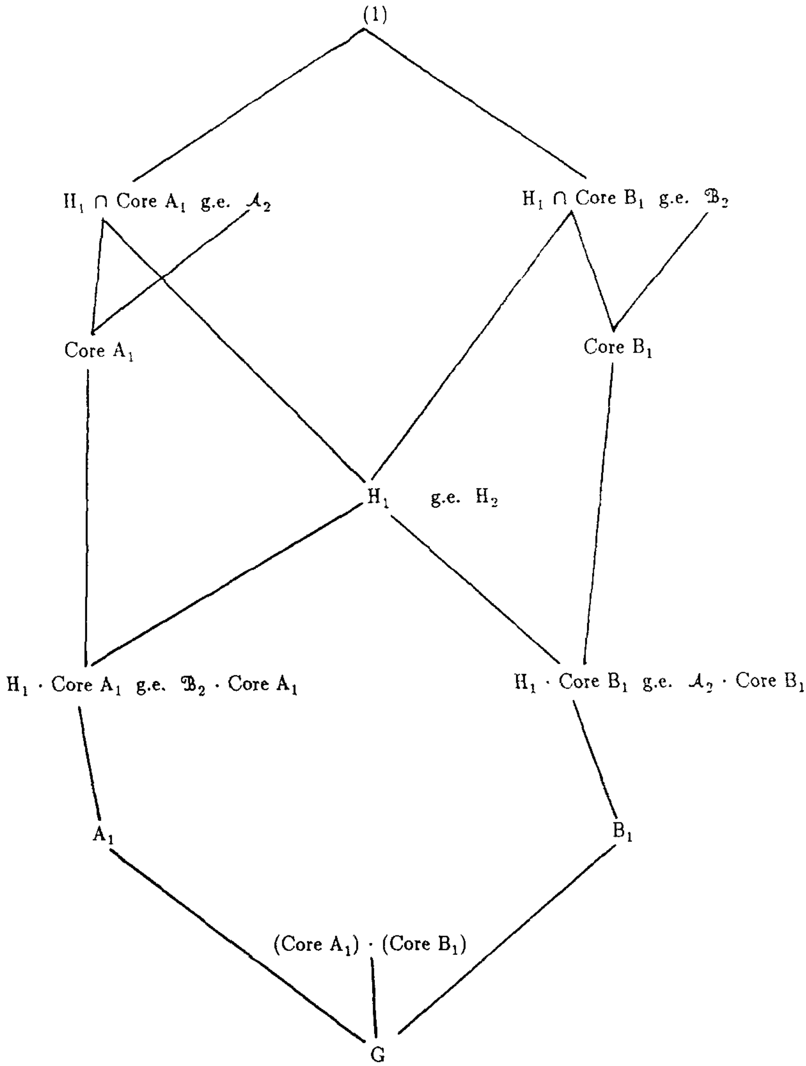

FIGURE 2

Indeed, if $h \in H_1$ then by (b) write $h = ab$ with $a \in \text{Core } A_1$, $b \in \text{Core } B_1$. Then $b = a^{-1}h \in A_1$ so that $b \in A_1 \cap B_1 = H_1$, and thus $b \in H_1 \cap \text{Core } B_1$. Similarly, $a \in H_1 \cap \text{Core } A_1$, establishing the claim.

Now both H_1, $H_2 \subseteq \text{Core } A_1 \cdot \text{Core } B_1$, hence H_1 g.e. H_2 in Core $A_1 \cdot$ Core B_1 (by 2.1(c) and restriction). By Lemma 4.3 we can write $H_2 = \mathcal{A}_2 \times \mathcal{B}_2$, where $\mathcal{A}_2 \subseteq \text{Core } A_1$, $\mathcal{B}_2 \subseteq \text{Core } B_1$, and also $\mathcal{A}_2$ g.e. $H_1 \cap$ Core A_1 and $\mathcal{B}_2$ g.e. $H_1 \cap \text{Core } B_1$ (where this is g.e. in Core $A_1 \cdot$ Core B_1). By Lemma 4.2 the above holds for g.e. in G. This proves (i) and (ii).

For the very first conclusion, let $x \in H_1 \cdot \text{Core } B_1$. Write $x = hb$ ($h \in H_1$, $b \in B_1$). In turn, by the claim write $h = a_1 b_1$ with $a_1 \in H_1 \cap \text{Core } A_1$, $b_1 \in H_1 \cap \text{Core } B_1$. Then $x = hb = a_1(b_1 b) \in (H_1 \cap \text{Core } A_1) \cdot \text{Core } B_1$. As the other containment is clear, we have $(H_1 \cap \text{Core } A_1) \cdot \text{Core } B_1 = H_1 \cdot \text{Core } B_1$. The other statement is proven likewise.

For (iii) we apply Lemma 4.4 in $\text{Core } A_1 \cdot \text{Core } B_1$ to obtain

$$\mathscr{A}_2 \cdot \text{Core } B_1 \text{ g.e. } H_1 \cdot \text{Core } B_1$$

and

$$\mathscr{B}_2 \cdot \text{Core } A_1 \text{ g.e. } H_1 \cdot \text{Core } A_1,$$

where this is g.e. in $\text{Core } A_1 \cdot \text{Core } B_1$. Again by Lemma 4.2 this is g.e. in G also.

For the final statement (iv) first observe that if $x \in H_2$ then $x = ab$ ($a \in \mathscr{A}_2$, $b \in \mathscr{B}_2$). So $x = b \cdot (b^{-1}ab) = (a^{-1} \cdot (ab^{-1}a^{-1}))^{-1}$ is in the intersection. Conversely if y is in the intersection, write $y = a_2 b_1 = b_2 a_1$ ($a_1 \in \text{Core } A_1, a_2 \in \mathscr{A}_2$, $b_1 \in \text{Core } B_1, b_2 \in \mathscr{B}_2$). As $\text{Core } A_1 \cap \text{Core } B_1 \subset \text{Core } H_1 = 1$ and $\text{Core } A_1$ and $\text{Core } B_1$ are normal subgroups of G, the elements of $\text{Core } A_1$ and $\text{Core } B_1$ commute. So $1 = a_2 b_1 a_1^{-1} b_2^{-1} = (a_2 a_1^{-1}) \cdot (b_1 b_2^{-1})$ gives $a_2 a_1^{-1} = b_2 b_1^{-1} \in \text{Core } A_1 \cap \text{Core } B_1 = 1$. Thus $a_2 = a_1 \in \mathscr{A}_2$, $b_2 = b_1 \in \mathscr{B}_2$, so $y \in \mathscr{A}_2 \mathscr{B}_2 = H_2$. ∎

We record two other results from Galois theory that are useful in conjunction with Theorem 4.5.

PROPOSITION 4.7. *Let F_1, F_2 be Galois extensions of a field k with $F_1 \cap F_2 = k$. If k_1, k_2 are fields with $k \subseteq k_i \subseteq F_i$ ($i = 1, 2$) then*

(a) $[k_1 k_2 : k] = [k_1 : k][k_2 : k]$, *and*

(b) $(k_1 k_2) \cap F_i = k_i$ ($i = 1, 2$).

Proof. Denote $\Omega = F_1 F_2$, $G = \text{Gal}(\Omega/k)$, $G_i = \text{Gal}(\Omega/F_i)$ ($i = 1, 2$), $H_i = \text{Gal}(\Omega/k_i)$ ($i = 1, 2$). The hypotheses yield $G_1 G_2 = G$, $G_1 \cap G_2 = \{1\}$, and $G_i \lhd G$. Thus $G = G_1 \times G_2$. Since plainly $G_i \leqslant H_i$ ($i = 1, 2$), statement (a) translates to the obvious identity $[G : H_1][G : H_2] = [G : H_1 \cap H_2]$.

For (b) we need only show that $(H_1 \cap H_2) \cdot G_1 = H_1$. Let $y \in H_1$ and write $y = g_1 g_2$ with $g_i \in G_i$. Then $g_2 \in G_2 \subseteq H_2$ and $g_2 = g_1^{-1} y \in H_1$ so $g_2 \in H_1 \cap H_2$. Thus $y \in (H_1 \cap H_2) \cdot G_1$. The other containment is clear. ∎

PROPOSITION 4.8. *Let L_1, L_2, M_1, M_2 be number fields such that L_1 a.e. L_2 and M_1 a.e. M_2. If $[L_i M_i : Q] = [L_i : Q][M_i : Q]$ ($i = 1, 2$), then $L_1 M_1$ a.e. $L_2 M_2$.*

Proof. By Theorem 2.2, $\bar{L}_1 = \bar{L}_2$ and $\bar{M}_1 = \bar{M}_2$, thus $\overline{L_1 M_1} = \overline{L_2 M_2}$. Let

$$\mathscr{S} = \{p : p \in \mathbb{Z} \text{ is a prime, unramified in } \overline{L_1 M_1}\}.$$

Now for any $p \in \mathscr{S}$ (in the following, all tensor products are over Q), Theorem 2.1 gives $L_1 \otimes Q_p \cong L_2 \otimes Q_p$ and $M_1 \otimes Q_p \cong M_2 \otimes Q_p$. The hypothesis on degrees gives $L_i M_i \cong L_i \otimes M_i$ $(i = 1, 2)$. Therefore, $(L_1 M_1) \otimes Q_p \cong Q_p \cong L_1 \otimes M_1 \otimes Q_p \cong L_1 \otimes M_2 \otimes Q_p \cong L_2 \otimes M_2 \otimes Q_p \cong (L_2 M_2) \otimes Q_p$. Thus by Theorem 2.1, $L_1 M_1$ a.e. $L_2 M_2$. ∎

We finish this section with an application of Theorem 4.5 to the study of fields arithmetically equivalent to $Q(\sqrt[n]{a})$.

THEOREM 4.9. *Let $x^n - a$ be irreducible over Q and write $n = 2^e m$ (m odd). Let $L_1 = Q(\sqrt[2^e]{a})$ and $M_1 = Q(\sqrt[m]{a})$. Then $[\bar{L}_1 \cap \bar{M}_1 : Q] \leqslant 2$ and $\bar{L}_1 \cap \bar{M}_1 \subseteq Q(\zeta_m)$. Let K be a number field a.e. to $Q(\sqrt[n]{a})$. Then*

(a) *If $\bar{L}_1 \cap \bar{M}_1 = Q$ then K contains subfields a.e. to L_1 and M_1.*

(b) *If $\bar{L}_1 \cap \bar{M}_1 = Q(\sqrt{c})$ ($c \notin Q^2$) then $K(\sqrt{c})$ contains subfields a.e. to $L_1(\sqrt{c})$ and $M_1(\sqrt{c})$.*

Proof. From Theorem 2.4a we have that $Q(\sqrt[n]{a}) \cap Q(\zeta_n) = Q(\sqrt[2^s]{a})$. Thus $[\Omega : Q] = n \cdot \phi(n)/2^s$ (where ϕ is Euler's totient function). Since $Q(\sqrt[2^s]{a})/Q$ is abelian, we have that $\zeta_{2^s} \in Q(\sqrt[2^e]{a})$ and so $\zeta_{2^s} \in L_1$, which in turn implies that $[\bar{L}_1 : Q] \leqslant 2^e \phi(2^e)/2^{s-1}$. Again from Theorem 2.4a, we have that $[\bar{M}_1 : Q] = m\phi(m)$. Since $\Omega = \bar{L}_1 \bar{M}_1$, it now follows that

$$\begin{aligned} n\phi(n)/2^s = [\Omega : Q] &= [\bar{L}_1 : Q] \cdot [\bar{M}_1 : Q]/[\bar{L}_1 \cap \bar{M}_1 : Q] \\ &\leqslant n\phi(n)/(2^{s-1} \cdot [\bar{L}_1 \cap \bar{M}_1 : Q]), \end{aligned}$$

which yields $[\bar{L}_1 \cap \bar{M}_1 : Q] \leqslant 2$.

Since $\bar{L}_1 \cap \bar{M}_1$ is at most a quadratic extension of Q contained in $Q(\sqrt[m]{a}, \zeta_m)$, where m is odd, it follows that $\bar{L}_1 \cap \bar{M}_1 \subseteq Q(\zeta_m)$. We now prove parts (a) and (b).

For (a), since $\bar{L}_1 \cap \bar{M}_1 = Q$ we can apply Theorem 4.5 (with $K_1 = Q(\sqrt[n]{a})$, $K = K_2$) to obtain fields $\mathfrak{L}_2$, $\mathcal{M}_2$. Now from Proposition 4.7 (with $F_1 = \bar{L}_1$, $F_2 = \bar{M}_1$, $k_1 = L_1$, $k_2 = M_1$) we have

$$K_1 \cap \bar{M}_1 = (k_1 k_2) \cap \bar{M}_1 = M_1,$$

and

$$K_1 \cap \bar{L}_1 = (k_1 k_2) \cap \bar{L}_1 = L_1.$$

Now apply Theorem 4.5b, c to complete the proof.

For part (b) observe that $Q(\sqrt[n]{a}, \sqrt{c})$ a.e. $K(\sqrt{c})$ (apply Proposition 4.8 and Theorem 2.2, if $\sqrt{c} \notin Q(\sqrt[n]{a})$). We want to apply Theorem 4.5 to $K_1 = Q(\sqrt[n]{a}, \sqrt{c})$, $K_2 = K(\sqrt{2})$, and the subfields $\overline{L_1(\sqrt{c})}$, $\overline{M_1(\sqrt{c})}$ of K_1.

First, as $\sqrt{c} \in \bar{L}_1 \cap \bar{M}_1$, we have $\overline{L_1(\sqrt{c})} \cap \overline{M_1(\sqrt{c})} = \bar{L}_1 \cap \bar{M}_1 = Q(\sqrt{c}) \subseteq K_1$. Next, $\overline{L_1(\sqrt{c})} \cdot \overline{M_1(\sqrt{c})} = \overline{L_1 M_1 (\sqrt{c})} = K_1$. Thus to complete the proof of this part we need only compute $K_1 \cap M_1(\sqrt{c})$ and $K_1 \cap L_1(\sqrt{c})$. For this, we once again apply Proposition 4.7b, this time with $k = Q(\sqrt{c})$, $k_1 = \overline{L_1(\sqrt{c})}$, $k_2 = \overline{M_1(\sqrt{c})}$, $F_1 = \bar{k}_1$, $F_2 = \bar{k}_2$. We have $K_1 \cap M_1(\sqrt{c}) = (k_1 k_2) \cap F_2 = k_2 = \overline{M_1(\sqrt{c})}$ and $K_1 \cap L_1(\sqrt{c}) = (k_1 k_2) \cap F_1 = k_1 = \overline{L_1(\sqrt{c})}$. Applying parts (b) and (c) of Theorem 4.5, the proof is done. ∎

5. The General Case

In this section we prove the following theorem, which together with Theorems 3.1 and 5.3 completely solves the problem addressed in this work.

Theorem 5.1. *Let $x^n - a$ be irreducible over Q and write $n = 2^e m$, m odd. Let K a.e. $Q(\sqrt[n]{a})$. Then K contains subfields L, M such that L a.e. $Q(\sqrt[2^e]{a})$, M* a.e. *$Q(\sqrt[m]{a})$ and $K = LM$.*

From Theorem 4.9 we see that if $\bar{L}_1 \cap \bar{M}_1 = Q$, then Theorem 5.1 is true. We need some further results dealing with radical extensions of fields, which we collect together in the next result. But first, some notation.

Let F be a field and let $\alpha \neq 0$ be algebraic over F. We let $O_F(\alpha)$ denote the order of the coset αF^* (where $F^* = F \setminus \{0\}$) in the quotient group $F(\alpha)^*/F^*$. The following appears in [5].

Theorem 5.2. *In the setting above*:

(a) *Assume $O_F(\alpha) = m$, and let ω_M denote the number of* mth *roots of unity in F, where* char *$F \nmid m$. Then $F(\alpha)/F$ has abelian Galois group iff there exists $\beta \in F$ with $(\alpha^m)^{\omega_m} = \beta^m$.*

(b) *Assume $O_F(\alpha) = m$ and suppose that $([F(\alpha): F], m) = 1$. Then $\alpha = d\zeta_m$, where $d \in F$.*

(c) *Let $p \in \mathbb{Z}$ be a prime and suppose that $\zeta_{2p} \in F$. If $O_F(\alpha) = p^t$, then $[F(\alpha): F] = p^t$.*

(d) $\zeta_4 \in Q(\sqrt[n]{a})$ *iff* $-a \in Q^2$.

(e) *A finite extension K/F has the "unique subfield property" if for every divisor t of $[K: F]$, there exists a unique subfield of K of degree t*

over F. If $4 \mid n$, *then* $Q(\sqrt[n]{a})/Q$ *has the unique subfield property iff* $\zeta_4 \notin Q(\sqrt[n]{a})$. ∎

The next result is fundamental to the proof of Theorem 5.1.

THEOREM 5.3. *Let m be odd and let* $x^{2m} - a$ *be irreducible over Q. Then* $Q(\sqrt[2m]{a})$ *is a solitary field.*

Proof. Let K be a.e. to $Q(\sqrt[2m]{a})$. Since K and $Q(\sqrt[2m]{a})$ have the same normal core, we have $\sqrt{a} \in K$. Let $\Omega = Q(\zeta_{2m}, \sqrt[2m]{a})$.

Let $\alpha = \sqrt[2m]{a}$ and $t = O_K(\alpha)$. From Lemma 2.3 we have that Ω/K is abelian, so $K(\alpha)/K$ is abelian. If $\omega = \omega_t$ denotes the number of tth roots of unity in K, we have by Theorem 5.2 that there exists $\beta \in K$, such that $(\alpha^t)^{\omega} = \beta^t$.

Now the only roots of unity in $Q(\sqrt[2m]{a})$ (and thus in K) are those contained in $Q(\sqrt[2m]{a}) \cap Q(\zeta_{2m}) = Q(\sqrt[2^s]{a})$ (see Theorem 2.4a), where $2^s \mid 2m$. Thus $s = 0$ or 1, so this intersection is either Q or $Q(\sqrt{a})$. So we have that either $\omega = 6$ if $3 \mid m$ and $a = -3d^2$, $d \in Q$; otherwise $\omega = 2$. We consider these cases.

Case 1. $\omega = 2$. We have that $(\alpha^t)^2 = (\sqrt[2m]{a^t})^2 = \sqrt[m]{a^t} = \beta^t$. Thus $\beta = \zeta_t^i \cdot \sqrt[m]{a}$, so K contains a conjugate of $\sqrt[m]{a}$. But $\sqrt{a} \in K$, so K is isomorphic to $Q(\sqrt[2m]{a})$.

Case 2. $\omega = 6$. (Recall that $\omega = 6$ implies that $3 \mid m$ and $a = -3d^2$, for some $d \in Q$.) We have that $(\alpha^t)^6 = \sqrt[m]{a^{3t}} = \beta^t$, so K contains a conjugate of $\sqrt[m/3]{a}$, and again since $\sqrt{a} \in K$, we have that a conjugate of $\sqrt[2m/3]{a}$ is in K. Thus without loss of generality, we may assume that $Q(\sqrt[2m/3]{a}) \subset K \cap Q(\sqrt[2m]{a})$.

Let $T = \mathrm{Gal}(Q(\zeta_{2m})/Q(\zeta_3)) = \{v : v \equiv 1 \pmod 3\}$ (where $v \leftrightarrow \sigma_v$, and $\sigma_v(\zeta_{2m}) = \zeta_{2m}^v$). Since $\zeta_3 \in Q(\sqrt[2m/3]{a})$ we see that $Q(\sqrt[2m]{a})/Q(\sqrt[2m/3]{a})$ is normal and in fact abelian so $\mathrm{Gal}(\Omega/Q(\sqrt[2m/3]{a})) \cong \mathrm{Gal}(Q(\sqrt[2m]{a})/Q(\sqrt[2m/3]{a})) \oplus T$, where T is identified with $\mathrm{Gal}(\Omega/Q(\sqrt[2m]{a})) = \{(0, v) : v \in T\} = \{(0, v) : v \equiv 1 \pmod 3\}$ (see Section 2 on $C_n \times C_n^*$). In particular, $\mathrm{Gal}(\Omega/Q(\sqrt[2m/3]{a}))$ is abelian.

For notational convenience, denote $L = Q(\sqrt[2m/3]{a})$. By way of contradiction, assume $K \not\cong Q(\sqrt[2m]{a})$. Then since $L \subseteq K$, we must have that $K(\sqrt[2m]{a})$ is a cubic extension of $Q(\sqrt[2m]{a})$ in Ω, and as such, corresponds by Galois theory to a subgroup of index 3 in $\{(0, v) : v \in T\}$. Let this subgroup be $\{(0, v) : v \in T_1\}$, where $[T : T_1] = 3$. Now view T_1 as a subgroup $T = \mathrm{Gal}(Q(\zeta_{2m})/Q(\zeta_3))$. Then the fixed field of T_1 in $Q(\zeta_{2m})$ is a cubic extension of $Q(\zeta_3)$, and from Kummer Theory, this fixed field must have the form $Q(\zeta_3, \sqrt[3]{\gamma})$, where $\gamma \in Q(\zeta_3)$. Thus the fixed field of $\{(0, v) : v \in T_1\}$ is $Q(\sqrt[2m]{a}, \sqrt[3]{\gamma})$, so $K \subset Q(\sqrt[2m]{a}, \sqrt[3]{\gamma})$.

In Fig. 3 we display the lattice of subfields as above, and their corresponding Galois groups. The explicit form of the Galois groups shown can be checked directly. We next give a better description of $J = \mathrm{Gal}(\Omega/K)$.

Since $\mathrm{Gal}(Q(\sqrt[2m]{a}, \sqrt[3]{\gamma})/L) \cong C_3 \oplus C_3$, there are four intermediate fields of degree 3 over L. These are $Q(\sqrt[2m]{a})$, $L(\sqrt[3]{\gamma})$, $Q(\sqrt[2m]{a} \cdot \sqrt[3]{\gamma})$, and $Q(\sqrt[2m]{a} \cdot \sqrt[3]{\gamma^2})$. However, K must be one of these. It is not the first, by assumption. It cannot be the second since $\sqrt[3]{\gamma} \notin K$ (recall that $Q(\zeta_3, \sqrt[3]{\gamma}) \subset Q(\zeta_m)$ and $Q(\sqrt[2m]{a}) \cap Q(\zeta_m) = Q(\zeta_3) = K \cap Q(\zeta_{2m})$). So K must be one of the two latter fields. Now let $T = T_1 \cup hT_1 \cup h^2T_1$ be a coset decomposition, where if $v \in T$ then: $\sigma_v(\sqrt[3]{\gamma}) = \zeta_3^i \sqrt[3]{\gamma}$ iff $v \in h^iT_i$. We can now display J.

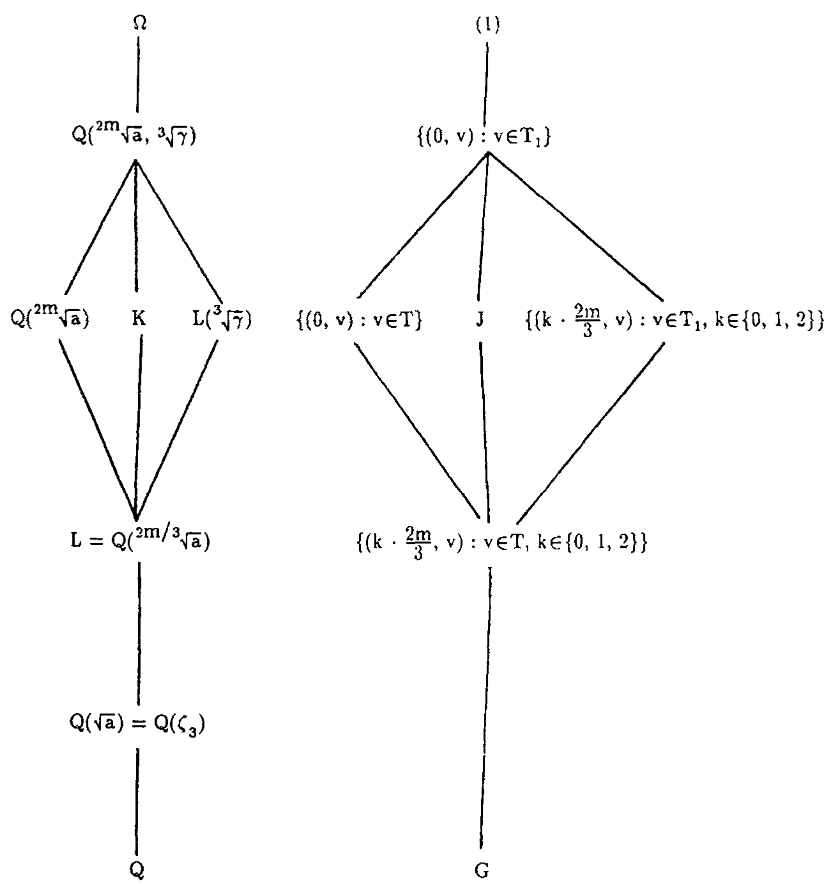

FIGURE 3

If $K=Q(\sqrt[2m]{a}\cdot\sqrt[3]{\gamma})$
then

$$J=\begin{cases}(0, v): & v\in T_1,\\ (2\cdot 2m/3, v): & v\in hT_1,\\ (2m/3, v): & v\in h^2T_1.\end{cases}$$

If $K=Q(\sqrt[2m]{a}\cdot\sqrt[3]{\gamma^2})$
then

$$J=\begin{cases}(0, v): & v\in T_1,\\ (2m/3, v): & v\in hT_1,\\ (2\cdot 2m/3, v): & v\in h^2T_1.\end{cases}$$

For example, in the first case (with the notation of Section 2), we have that if $v\in h^2T_1$, $(2m/3, v)(\sqrt[2m]{a}\cdot\sqrt[3]{\gamma})=(\zeta_3\cdot\sqrt[2m]{a})\cdot(\zeta_3^2\cdot\sqrt[3]{\gamma})=\sqrt[2m]{a}\cdot\sqrt[3]{\gamma}$.

Now observe if $9\mid m$ and $\gamma=\zeta_3$, then either $K=Q(\sqrt[2m]{a}\cdot\sqrt[3]{\gamma})=Q(\zeta_9\cdot\sqrt[2m]{a})$ or $K=Q(\sqrt[2m]{a}\cdot\sqrt[3]{\gamma^2})=Q(\zeta_9^2\cdot\sqrt[2m]{a})$, and so K is clearly conjugate to $Q(\sqrt[2m]{a})$. Now let $m=3^tm_1$, where $3\nmid m_1$, $t\geqslant 1$.

If $\sqrt[3]{\gamma}\in Q(\zeta_{3^t})$, then since $Q(\zeta_{3^t})/Q(\zeta_3)$ has cyclic Galois group, we would have that $Q(\zeta_3, \sqrt[3]{\gamma})=Q(\zeta_9)$, so then $\gamma=\zeta_3\cdot\beta^3$, thus $Q(\sqrt[2m]{a}\cdot\sqrt[3]{\gamma})=Q(\sqrt[2m]{a}\,\zeta_9\cdot\beta)=Q(\sqrt[2m]{a}\zeta_9)$ since $\zeta_3\in Q(\sqrt[2m]{a}\zeta_9)$, so we are done. Thus in the following we may assume that $\sqrt[3]{\gamma}\notin Q(\zeta_{3^t})$.

Now $\mathrm{Gal}(Q(\zeta_{2m})/Q(\zeta_3))=\{v:v\equiv 1 \pmod{3^t}\}\subseteq C_{2m}^*$. Since $Q(\zeta_3, \sqrt[3]{\gamma})\not\subset Q(\zeta_{3^t})$, there exists $v\equiv 1 \pmod{3^t}$ such that $v\notin T_1$, and so $v\in hT_1$ or $v\in h^2T_1$. So as an element of J (regardless of the two choices for K), this v occurs as either $(2m/3, v)$ or $(2\cdot 2m/3, v)$. It is crucial here to note that 3^{t-1} exactly divides the first component.

Now, $(0, v)\in H$ and $\mathrm{cl}_G(0, v)\subseteq\{(\alpha(1-v), v):\alpha\in C_{2m}\}$, and $3^t\mid\alpha(1-v)$, since v was chosen so that $v\equiv 1 \pmod{3^t}$. Therefore, from the preceeding paragraph, $J\cap\mathrm{cl}_G(0, v)=\varnothing$, while $H\cap\mathrm{cl}_G(0, v)=\{(0, v)\}$. Thus H and J are not Gassmann equivalent, contrary to the assumption that $Q(\sqrt[2m]{a})$ a.e. K. Thus $K\cong Q(\sqrt[2m]{a})$, and $Q(\sqrt[2m]{a})$ is a solitary field. ∎

COROLLARY 5.4. *Assume $n=2^em$, m odd (no restriction on e). If K a.e. $Q(\sqrt[n]{a})$ then a conjugate of $\sqrt[m]{a}$ is in K.*

Proof. This is certainly the case if $\bar{L}_1\cap\bar{M}_1=Q$, so assume $\bar{L}_1\cap\bar{M}_1=Q(\sqrt{c})$ with $c\notin Q^2$. By Theorem 4.9b we have that $K(\sqrt{c})$ contains a subfield a.e. to $Q(\sqrt[m]{a}, \sqrt{c})=Q(\sqrt[2m]{b})$ (for example, with $b=a^2c^m$). But by the previous results $Q(\sqrt[2m]{b})$ is solitary, so $K(\sqrt{c})$

contains a conjugate of $\sqrt[2m]{b}$, hence also a conjugate of $\sqrt[m]{a}$. Thus $\zeta_m^i \sqrt[m]{a} \in K(\sqrt{c})$, for some i.

If $K(\sqrt{c}) = K$, then we are done, so assume $K(\sqrt{c}) \neq K$. Let $O_K(\zeta_m^i \sqrt[m]{a}) = t$, where $t \mid m$. As $[K(\zeta_m^i \cdot \sqrt[m]{a}) : K] \leqslant 2$, it follows from Theorem 5.2b that $\zeta_m^i \cdot \sqrt[m]{a} = \zeta_t \cdot d$ for some $d \in K$. Thus $d = \zeta_t^{-1} \zeta_m^i \sqrt[m]{a} \in K$, so K contains a conjugate of $\sqrt[m]{a}$. ∎

THEOREM 5.5. *If $\zeta_4 \in Q(\sqrt[n]{a})$ then $Q(\sqrt[n]{a})$ is a solitary field.*

Proof. By Theorem 5.3 we can assume $n = 2^e m$, $e \geqslant 2$. From Theorem 5.2d we have that $-a \in Q^2$. Now let K be a.e. to $Q(\sqrt[n]{a})$. If $\bar{L}_1 \cap \bar{M}_1 = Q$ then we are done by Theorems 4.9a, 3.1, and 5.3. So assume $\bar{L}_1 \cap \bar{M}_1 = Q(\sqrt{c})$ with $c \notin Q^2$. By Theorem 4.9b, $K(\sqrt{c})$ contains a subfield a.e. to $Q(\sqrt[2^e]{a}, \sqrt{c})$. However, $-a \in Q^2$, so $\zeta_4 \in Q(\sqrt[2^e]{a}, \sqrt{c})$, and this implies that $\mathrm{Gal}(Q(\sqrt[2^e]{a}, \zeta_{2^e}, \sqrt{c})/Q(\sqrt[2^e]{a}, \sqrt{c}))$ is cyclic. Hence $Q(\sqrt[2^e]{a}, \sqrt{c})$ is a solitary field. Thus it follows that a conjugate of $\sqrt[2^e]{a}$ is contained in $K(\sqrt{c})$, so without loss of generality, we may assume that $\sqrt[2^e]{a} \in K(\sqrt{c})$.

If $\sqrt[2^e]{a} \in K$ then we are done by the previous corollary. So $K(\sqrt[2^e]{a}) = K(\sqrt{c})$ is a quadratic extension of K. However, by Theorem 5.2c (with $p = 2$), we have $[K(\sqrt[2^e]{a}) : K] = O_K(\sqrt[2^e]{a})$ (since $\zeta_4 \in K$), and so $O_K(\sqrt[2^e]{a}) = 2$. Thus $\sqrt[2^{e-1}]{a} \in K$, and since $\sqrt[m]{a} \in K$ by the previous corollary, we have $\sqrt[n/2]{a} \in K$.

It is now easy to see that $\mathrm{Gal}(K(\sqrt{c})/Q(\sqrt[n/2]{a}))$ is $C_2 \oplus C_2$ and that the quadratic extensions of $Q(\sqrt[n/2]{a})$ contained in $K(\sqrt{c})$ are $Q(\sqrt[n]{a})$, $Q(\sqrt[n/2]{a}, \sqrt{c})$, $Q(\sqrt[n]{a} \cdot \sqrt{c})$. K must be one of these. It cannot be the middle field since $\sqrt{c} \notin K$. But now from the fact that $\zeta_4 \in Q(\sqrt[n]{a})$, Theorem 2.4c and d show that the only radical extensions a.e. to $Q(\sqrt[n]{a})$ are those isomorphic to $Q(\sqrt[n]{a})$. Since the other two choices for K are radical extensions, it follows that $Q(\sqrt[n]{a})$ is solitary. ∎

The proof of Theorem 5.1 requires two more technical lemmas.

LEMMA 5.6. *Assume that $n = 2^e m$, with $e \geqslant 2$, m odd. If $\zeta_4 \notin Q(\sqrt[n]{a})$ and $\bar{L}_1 \cap \bar{M}_1 = Q(\sqrt{c})$, where $c \notin Q^2$ and $\sqrt{c} \in Q(\zeta_m)$, then $Q(\sqrt[2^e]{a}) \cap Q(\zeta_{2^e}) = Q$ and $[\Omega : Q] = n \cdot \phi(n)/2$ (where $\Omega = Q(\sqrt[n]{a}, \zeta_n)$).*

Proof. As before, let $Q(\zeta_n) \cap Q(\sqrt[n]{a}) = Q(\sqrt[2^s]{a})$. Then $[\Omega : Q] = n\phi(n)/2^s$. Since $Q(\sqrt[2^s]{a})/Q$ is abelian, this implies that $\zeta_{2^s} \in Q(\sqrt[n]{a})$. So by assumption, $s \leqslant 1$. If $s = 0$, this forces $\bar{L}_1 \cap \bar{M}_1 = Q$, contrary to assumption, so $s = 1$. Thus $[\bar{L}_1 \bar{M}_1 : Q] = n \cdot \phi(n)/2 = [\bar{L}_1 : Q] \cdot [\bar{M}_1 : Q]/2 = [\bar{L}_1 : Q]\, m\phi(m)/2$, so $[\bar{L}_1 : Q] = 2^e \phi(2^e)$, hence $Q(\sqrt[2^e]{a}) \cap Q(\zeta_{2^e}) = Q$. ∎

LEMMA 5.7. *Suppose that* $Q(\sqrt[2^e]{a}) \cap Q(\zeta_{2^e}) = Q$.

(a) *If* $e=2$, *then the quadratic subfields of* $\bar{L}_1 = Q(\sqrt[4]{a}, \zeta_4)$ *are* $Q(\sqrt{\pm a})$, $Q(\zeta_4)$.

(b) *If* $e \geqslant 3$, *then the quadratic subfields of* $\bar{L}_1 = Q(\sqrt[2^e]{a}, \zeta_{2^e})$ *are* $Q(\zeta_4)$, $Q(\sqrt{\pm 2})$, $Q(\sqrt{\pm a})$, $Q(\sqrt{\pm 2a})$.

Proof. (a) is trivial, so we shall assume that $e \geqslant 3$. From $Q(\sqrt[2^e]{a}) \cap Q(\zeta_{2^e}) = Q$ we have that $\sqrt{a} \notin Q(\zeta_8)$. Let $Q(\sqrt{d})$ be a quadratic subfield of $\bar{L}_1$. By way of contradiction, suppose that $\sqrt{d} \notin Q(\sqrt{a}, \zeta_8)$. Then $\mathrm{Gal}(Q(\sqrt{a}, \sqrt{d}, \zeta_8)/Q) = C_2 \oplus C_2 \oplus C_2 \oplus C_2$ and so $\mathrm{Gal}(Q(\sqrt{d}, \zeta_8)/Q) = C_2 \oplus C_2 \oplus C_2$.

Since $\zeta_4 \notin Q(\sqrt[2^e]{a})$, the extension $Q(\sqrt[2^e]{a})/Q$ has the unique subfield property by Theorem 5.2e. Since $\sqrt{a} \notin Q(\zeta_8, \sqrt{d})$, this forces $Q(\sqrt[2^e]{a}) \cap Q(\zeta_8, \sqrt{d}) = Q$. Thus $\mathrm{Gal}(Q(\sqrt[2^e]{a}, \zeta_8, \sqrt{d})/Q(\sqrt[2^e]{a})) = C_2 \oplus C_2 \oplus C_2$. This is a contradiction, since $\mathrm{Gal}(Q(\sqrt[2^e]{a}, \zeta_{2^e})/Q(\sqrt[2^e]{a})) = C_{2^{e-2}} \oplus C_2$. Thus $\sqrt{d} \in Q(\sqrt{a}, \zeta_8)$, so $Q(\sqrt{d})$ is one of the listed fields. ∎

Proof of Theorem 5.1. By the results above we may assume that $\zeta_4 \notin Q(\sqrt[n]{a})$, $e \geqslant 2$, and that $\bar{L}_1 \cap \bar{M}_1 = Q(\sqrt{c})$, where $c \notin Q^2$, $\sqrt{c} \in Q(\zeta_m)$.

By Lemmas 5.6 and 5.7, $Q(\sqrt{c})$ must be one of the fields listed in Lemma 5.7. Since $Q(\sqrt{c}) \subseteq Q(\zeta_m)$, and ζ_4, $\sqrt{\pm 2} \notin Q(\zeta_m)$, it cannot be $Q(\zeta_4)$, $Q(\sqrt{\pm 2})$. So there remain four possibilities.

Case 1. $Q(\sqrt{c}) = Q(\sqrt{a})$. Then $Q(\sqrt[n]{a}, \sqrt{c}) = Q(\sqrt[n]{a})$, hence $K(\sqrt{c}) = K$ and $Q(\sqrt[2^e]{a}, \sqrt{c}) = Q(\sqrt[2^e]{a})$. By Theorem 4.9, K contains a subfield a.e. to $Q(\sqrt[2^e]{a})$. Corollary 5.4 completes this case.

Case 2. $Q(\sqrt{c}) = Q(\sqrt{-a})$. Then $Q(\sqrt[2^e]{a}, \sqrt{c}) = Q(\sqrt[2^e]{a}, \zeta_4)$. However, $\mathrm{Gal}(Q(\sqrt[2^e]{a}, \zeta_{2^e})/Q(\sqrt[2^e]{a}, \zeta_4))$ is cyclic, so $Q(\sqrt[2^e]{a}, \sqrt{c})$ is solitary. Thus $K(\sqrt{c})$ contains a conjugate of $\sqrt[2^e]{a}$, so we may as well assume that $\sqrt[2^e]{a} \in K(\sqrt{c})$. But then, $K(\sqrt{c}) = K(\sqrt{-a}) = K(\zeta_4)$. Now let $2^t = O_K(\sqrt[2^e]{a})$. Since $\zeta_4 \notin K$ and $K(\sqrt{c})/K$ is abelian, Theorem 5.2a gives $\beta \in K$ such that $(\sqrt[2^{e-t}]{a})^2 = \beta^{2^t}$ (the only 2^tth roots of unity in K are ± 1). Thus $\beta = \zeta_{2^t}^i \sqrt[2^{e-1}]{a}$, so K contains a conjugate of $\sqrt[2^{e-1}]{a}$. But $\sqrt[m]{a} \in K$, so $\sqrt[n/2]{a} \in K$. Thus $Q(\sqrt[n/2]{a}) \subset K \subset Q(\sqrt[n]{a}, \sqrt{c})$. As in the proof of Theorem 5.5, since $\sqrt{c} \notin K$, K is a radical extension. This case now follows from Theorem 2.4c.

Case 3. $Q(\sqrt{c}) = Q(\sqrt{-2a})$. Then $Q(\sqrt[2^e]{a}, \sqrt{c}) = Q(\sqrt[2^e]{a}, \sqrt{-2})$. Since $e \geqslant 3$ in this case, we have that $\mathrm{Gal}(Q(\sqrt[2^e]{a}, \zeta_{2^e})/Q(\sqrt[2^e]{a}, \sqrt{-2}))$ is cyclic, so $Q(\sqrt[2^e]{a}, \sqrt{-2})$ is solitary. As in the previous case since $\zeta_4 \notin K$, we can conclude that $\sqrt[n/2]{a} \in K$, and the rest of the proof is as in Case 2.

Case 4. $Q(\sqrt{c})=Q(\sqrt{2a})$. Then $Q(\sqrt[2^e]{a}, \sqrt{c})=Q(\sqrt[2^e]{a}, \sqrt{2})$. But this last field is not necessarily solitary, since $\mathrm{Gal}(Q(\sqrt[2^e]{a}, \zeta_{2^e})/Q(\sqrt[2^e]{a}, \sqrt{2}))$ is not cyclic. So we consider an extension of this field.

From Proposition 4.8 we see that $Q(\sqrt[n]{a}, \zeta_8)$ a.e. $K(\zeta_8)$ and so by Theorem 4.5, $K(\zeta_8)$ contains a subfield a.e. to $Q(\sqrt[2^e]{a}, \zeta_8)$. But this field is solitary, so $K(\zeta_8)$ contains a conjugate of $\sqrt[2^e]{a}$, which we may assume is $\sqrt[2^e]{a}$. Then $K \subset K(\sqrt[2^e]{a}) \subset K(\zeta_8)$, and since $\zeta_4 \notin K$ and $\mathrm{Gal}(K(\zeta_8)/K)$ is abelian, we have (by applying Theorem 5.2a) that $\sqrt[2^{e-1}]{a} \in K$, and so $\sqrt[n/2]{a} \in K$. Thus $Q(\sqrt[n/2]{a}) \subset K \subset Q(\sqrt[n]{a}, \zeta_8)$. But the quadratic extensions of $Q(\sqrt[n/2]{a})$ contained in $Q(\sqrt[n]{a}, \zeta_8)$ are $Q(\zeta_4^i \sqrt[n]{a})$, $Q(\sqrt[n]{a} \cdot \sqrt{\pm 2})$, $Q(\sqrt[n/2]{a}, \sqrt{\pm 2})$, and $Q(\sqrt[n/2]{a}, \zeta_4)$. The field K cannot be one of the last three since ζ_4, $\sqrt{\pm 2} \notin K$, so K is one of the first four. But these are all radical extensions, for which the theorem already holds. ∎

References

1. R. M. Guralnick, Subgroups inducing the same permutation representation, *J. Algebra* **81** (1983), 312–319.
2. R. M. Guralnick and D. B. Wales, Subgroups inducing the same permutation representation, II, preprint.
3. E. Jacobson and W. Y. Vélez, On the adèle rings of radical extensions of the rationals, *Arch. Math.* **45** (1985), 12–20.
4. R. Perlis, On the equation $\zeta_K(s)=\zeta_{K'}(s)$, *J. Number Theory* **9** (1977), 342–360.
5. W. Y. Vélez, Several results on radical extensions, *Arch. Math.* **45** (1985), 342–349.