manuscripta math. 67, 271 - 284 (1990)

manuscripta
mathematica

THE GALOIS GROUP OF A RADICAL EXTENSION OF THE RATIONALS

ELIOT T. JACOBSON AND WILLIAM Y. VÉLEZ

The Galois group of the splitting field of an irreducible binomial $x^{2^e} - a$ over $\mathbf{Q}$ is computed explicitly as a full subgroup of the holomorph of the cyclic group of order 2^e. The general case $x^n - a$ is also effectively computed.

0. Introduction.

The computation of the Galois group for the splitting field over $\mathbf{Q}$ of a polynomial in $\mathbf{Q}[x]$ is a problem most mathematicians see in their first modern algebra course. However, there are very few classes of polynomials for which a universal description of the Galois group is known. Examples include irreducible quadratics, and the cyclotomic polynomials. These two examples in turn are just special cases of computing the Galois group of the splitting field of a binomial $x^n - a$.

It is unexpected that an explicit description of the Galois group of the splitting field of $x^n - a$, where $x^n - a$ is irreducible over $\mathbf{Q}$, does not appear in the literature. In this paper we offer such a description when n is a power of 2. The description for arbitrary n is based on determining the quadratic subfields of $\mathbf{Q}(\zeta_n)$.

The authors thank the referee for his helpful suggestions.

Although the case when n is odd has been known since the time of Galois, it is the exceptional cases that arise when $8|n$ that sparked our interest in this problem. Because arithmetic equivalence amounts to a profound knowledge of the subgroup structure of the Galois groups that arise, these computations give an alternative approach towards answering questions on arithmetic equivalence for radical extensions. Indeed, much of the classification achieved in [4] would not have been possible otherwise.

1. Some properties of radical extensions.

Fixed in this paper is an irreducible binomial $x^n - a$ over $\mathbf{Q}$ with $n \geq 2$. Let ζ_n denote a primitive n^{th}–root of unity, and denote $\Omega = \mathbf{Q}(\sqrt[n]{a}, \zeta_n)$, the splitting field of $x^n - a$. We set $G = Gal(\Omega/\mathbf{Q})$, the Galois group of $x^n - a$. Let $\mathbf{Z}_n$ denote the cyclic group of integers modulo n, and let $\mathbf{Z}_n^*$ be the multiplicative group of integers prime to n. Multiplication in $\mathbf{Z}$ provides a natural isomorphism $\theta\colon \mathbf{Z}_n^* \longrightarrow Aut(\mathbf{Z}_n)$. Let $\mathcal{G}$ denote the semidirect product: $\mathcal{G} = \mathbf{Z}_n \times_\theta \mathbf{Z}_n^*$. In other words, $\mathcal{G}$ is the "holomorph" of $\mathbf{Z}_n$. Thus $\mathcal{G}$ can be described as the set $\mathbf{Z}_n \times \mathbf{Z}_n^*$ with binary operation given by

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

for all $(\alpha, u), (\beta, v) \in \mathcal{G}$. Note that the identity of $\mathcal{G}$ is $(0, 1)$ and that for $(\alpha, u) \in \mathcal{G}$ we have $(\alpha, u)^{-1} = (-\alpha u^{-1}, u^{-1})$. As we shall see, G is naturally embedded in $\mathcal{G}$. We need a preliminary result on radical extensions.

PROPOSITION 1. *([2, Theorem 1 and Proposition 2]). Let $x^n - a$ be irreducible over $\mathbf{Q}$. Then*

(a) $\mathbf{Q}(\sqrt[n]{a}) \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}(\sqrt[2^s]{a})$, *for some* $s \geq 0$. *In particular,* $2^s | \phi(n)$ *(where ϕ is Euler's function).*

(b) *Let* $h = max\{2^q : 2^q | n$ *and* $a = -c^{2^{q-1}}$ *some* $c \in \mathbf{Q}\}$. *Then*

$$2^s = \begin{cases} h, & \text{if } h = 1 \text{ or } h = 2^q, a = -c^{2^{q-1}} \text{ and } \zeta_{2^{q+1}}\sqrt{c} \in \mathbf{Q}(\zeta_n) \\ \dfrac{h}{2}, & \text{otherwise.} \end{cases}$$

In the remainder of this paper, s will always refer to the invariant of Proposition 1; it is fundamental to this work. We can now describe the embedding $G \hookrightarrow \mathcal{G}$.

PROPOSITION 2. *G is naturally isomorphic to a subgroup of* $\mathcal{G}$ *of index* 2^s. *Moreover, the projections of G onto the first and second factor of* $\mathcal{G}$ *are both surjective (i.e., G is a "full" subgroup of* $\mathcal{G}$*).*

PROOF: Any element $\sigma \in G$ is completely determined by its values at $\sqrt[n]{a}$ and ζ_n. If $\sigma(\sqrt[n]{a}) = \sqrt[n]{a} \cdot \zeta_n^{\alpha}$ and $\sigma(\zeta_n) = \zeta_n^u$ for integers α, u with $(u, n)_{gcd} = 1$, then σ corresponds to the pair (α, u). The map $\sigma \longmapsto (\alpha, u)$ is easily seen to be an injective group homomorphism. The index statement follows as $|\mathcal{G}| = n \cdot \phi(n)$ and $|G| = [\Omega : \mathbf{Q}] = n \cdot \phi(n)/2^s$. Finally, by the Isomorphism Extension Theorem, both projections are surjective.

For the remainder of this paper we will view $G \subseteq \mathcal{G}$. We continue this section by stating the results on radical extensions that will be needed.

PROPOSITION 3. *([7, Theorem 2.1]). Let* $x^n - a$, $x^n - b$ *be irreducible over* $\mathbf{Q}$. *Then* $\mathbf{Q}(\sqrt[n]{a}) \cong \mathbf{Q}(\sqrt[n]{b})$ *if and only if either*

(a) $a = b^i c^n$, *where* $(i, n)_{gcd} = 1$ *and* $c \in \mathbf{Q}$; *or*

(b) $8|n$; $-a, -b$ *are squares in* $\mathbf{Q}$, *and* $a = b^i 2^{\frac{n}{2}} c^n$, *where* $(i, n)_{gcd} = 1$ *and* $c \in \mathbf{Q}$.

We say that a field extension E/F has the *unique subfield property* (USP) if for each divisor t of $[E : F]$ there exists exactly one subfield of E of degree t over F.

PROPOSITION 4. *([1, Theorem 2.1] and [3, Theorem 1.8a]). Let F be a field of characteristic 0 and let $x^{2^e} - a$ be irreducible over F. Then*

(a) *$\zeta_4 \in F(\sqrt[2^e]{a})\backslash F$ if and only if $-a = c^2$ for some $c \in F$ (where "$\backslash$" denotes the set-theoretic difference).*

(b) *If $e \geq 2$ then $F(\sqrt[2^e]{a})/F$ has the USP if and only if $\zeta_4 \notin F(\sqrt[2^e]{a})\backslash F$.*

PROPOSITION 5. *([6, Theorem 2.1 and 2.2]). Let F be a field of characteristic 0 and let $x^n - a$ be irreducible over F. Let ω_n be the number of n-th roots of unity in F. Then*

(a) *$F(\sqrt[n]{a})/F$ is an abelian extension if and only if $a^{\omega_n} = b^n$ for some $b \in F$.*

(b) *If $F(\sqrt[n]{a})/F$ is abelian, then $Gal(F(\sqrt[n]{a})/F)$ is either $\mathbf{Z}_n$ or $\mathbf{Z}_2 \oplus \mathbf{Z}_{\frac{n}{2}}$.*

We view the case $s = 0$ as the "general case," the other cases being "exceptional." By virtue of Proposition 1, the general case is solved:

THEOREM A. *If $s = 0$ then $G = \mathcal{G}$. Moreover, $s = 0$ if and only if either*

(a) *n is odd, or*

(b) *n is even , and $\sqrt{a} \notin \mathbf{Q}(\zeta_n)$.*

In particular, a complete computation requires the knowledge of all quadratic subfields of a cyclotomic extension, for which we refer the reader to [8, Exercise 7-4-4].

Thus we assume that n is even and $s \geq 1$. As usual $Gal(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \cong \mathbf{Z}_n^*$, where $u \in \mathbf{Z}_n^*$ corresponds with σ_u given by $\sigma_u(\zeta_n) = \zeta_n^u$. We

also view $Gal(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \cong \{(0,u)\colon u \in \mathbf{Z}_n^*\} \subseteq \mathcal{G}$. Set $H = Gal(\mathbf{Q}(\zeta_n)/\mathbf{Q}(\sqrt[2^s]{a}))$ and view $H \subseteq \mathbf{Z}_n^*$.

Observe that if $s = 1$ then $\mathbf{Q}(\sqrt{a})$ is a quadratic subfield of $\mathbf{Q}(\zeta_n)$, and H is a subgroup of index 2 in $\mathbf{Z}_n^*$. Such subgroups H are easily described. For instance, if $2\|n$ then the quadratic subfields of $\mathbf{Q}(\zeta_n)$ are precisely the fields $\mathbf{Q}(\sqrt{d})$ where d is any square-free divisor of n with $d \equiv 1 (\mathrm{mod}\ 4)$. The corresponding group H_d of index 2 consists precisely of those $u \in \mathbf{Z}_n^*$ for which the Jacobi symbol $\left(\frac{u}{d}\right) = 1$. The next result shows that the computation of H and G are equivalent in this case. In section 3, the groups H that arise when $n = 2^e$ will be listed explicitly.

THEOREM B. *Assume n is even and $s = 1$. Then*

$$G = \{(\alpha, u)\colon \alpha \equiv \begin{cases} 0\ (mod\ 2), & \text{if } u \in H \\ 1\ (mod\ 2), & \text{if } u \notin H \end{cases}\}.$$

PROOF: Certainly, the set described is a subgroup of $\mathcal{G}$ of index 2, so we need only show the containment $\subseteq$. Let $\sigma = (\alpha, u) \in$ G. As $\sqrt{a} \in \mathbf{Q}(\zeta_n)$, write $\sqrt{a} = \sum a_i \cdot \zeta_n^i$ for some $a_i \in \mathbf{Q}$. Observe that

$$\sigma(\sqrt{a}) = \sigma(\sqrt[n]{a})^{\frac{n}{2}} = (\sqrt[n]{a} \cdot \zeta_n^{\alpha})^{\frac{n}{2}} = \sqrt{a} \cdot (-1)^{\alpha}$$

and

$$\sigma(\sqrt{a}) = \sigma(\sum a_i \cdot \zeta_n^i) = \sum a_i \cdot \zeta_n^{ui} = \sigma_u(\sqrt{a}).$$

The equality $\sqrt{a} \cdot (-1)^{\alpha} = \sigma_u(\sqrt{a})$ gives the result.

2. Full Subgroups.

In this section we briefly digress to consider full subgroups of semi-direct products. Let $\mathcal{G} = \mathcal{N} \rtimes \mathcal{H}$ be an external semi-direct product (with $\mathcal{N} \times 1$ normal in $\mathcal{G}$, and $\mathcal{H}$ acting on $\mathcal{N}$ on the left). A subgroup $G \subseteq \mathcal{G}$ is said to be a full subgroup if the projections onto $\mathcal{N}$ and $\mathcal{H}$ are

both surjective. The following is a well known characterization of full subgroups. For convenience, $\mathcal{N}$ is written additively (though it need not be abelian) and $\mathcal{H}$ is written multiplicatively.

LEMMA 1. *Let G be a subgroup of $\mathcal{G}$ and let $G_0 = \{(\alpha,1)\colon \alpha \in \mathcal{N}$ and $(\alpha,1) \in G\}$. That is, $G_0 = G \cap (\mathcal{N} \times 1)$.*

(a) *If G is a full subgroup of $\mathcal{G}$ then G_0 is an $\mathcal{H}$-invariant normal subgroup of $\mathcal{N} \times 1$ and there is a surjective crossed homomorphism $\psi\colon \mathcal{H} \longrightarrow (\mathcal{N} \times 1)/G_0$. Furthermore, $|G| = |G_0| \cdot |\mathcal{H}|$.*

(b) *Conversely, if G_0 is an $\mathcal{H}$-invariant normal subgroup of $\mathcal{N} \times 1$ and $\psi\colon \mathcal{H} \longrightarrow (\mathcal{N}\times 1)/G_0$ is a surjective crossed homomorphism, then $G_\psi = \{(\alpha,u)\colon G_0(\alpha,1) = \psi(u)\}$ is a full subgroup of $\mathcal{G}$ of order $|G_0| \cdot |\mathcal{H}|$.*

PROOF: For (a) suppose that G is a full subgroup. Given any $u \in \mathcal{H}$, there exists $\alpha \in \mathcal{N}$ such that $(\alpha,u) \in G$. Define $\psi\colon \mathcal{H} \longrightarrow (\mathcal{N} \times 1)/G_0$ by $\psi(u) = G_0(\alpha,1)$. To see that ψ is well defined, assume that (α_1,u) is also in G. Then $(\alpha_1,u)\cdot(\alpha,u)^{-1} = (\alpha_1,u)\cdot(-u^{-1}\alpha,u^{-1}) = (\alpha_1 - \alpha,1) \in G_0$, so $G_0(\alpha_1,1) = G_0(\alpha,1)$. Thus ψ is well defined, and is obviously surjective. Given $u \in \mathcal{H}$, let $\alpha \in \mathcal{N}$ be such that $(\alpha,u) \in G$. Let $(\alpha_1,1) \in G_0$. Then we have $(\alpha,u)^{-1}(\alpha_1,1)(\alpha,u) = (u^{-1}\alpha_1,1) \in G_0$, so conjugation is independent of choice of α, giving an action (by conjugation) such that G_0 is $\mathcal{H}$-invariant. To show that ψ is a crossed homomorphism, consider $u_1,u_2 \in \mathcal{H}$ with lifts (α_1,u_1), $(\alpha_2,u_2) \in G$. Then $(\alpha_1,u_1)\cdot(\alpha_2,u_2) = (\alpha_1 + u_1\alpha_2, u_1u_2)$, so $\psi(u_1u_2) = G_0(\alpha_1 + u_1\alpha_2,1) = G_0(\alpha_1,1) + u_1G_0(\alpha_2,1) = \psi(u_1) + u_1\psi(u_2)$, with the induced action of $\mathcal{H}$ on $(\mathcal{N} \times 1)/G_0$.

To determine the order of G, observe that if $(\alpha,u) \in G$, then for any $(\alpha_1,1) \in G_0$, $(\alpha_1,1)\cdot(\alpha,u) = (\alpha_1 + \alpha,u) \in G$. Conversely, if (α_1,u), $(\alpha_2,u) \in G$, then $(\alpha_1,u)\cdot(\alpha_2,u)^{-1} = (\alpha_1 - \alpha_2,1) \in G_0$, so every $u \in \mathcal{H}$

lifts to $|G_0|$ elements of G.

The proof of part (b) is even more straightforward, and is omitted.

THEOREM C. *Let G be a full subgroup of $\mathbf{Z}_n \rtimes \mathbf{Z}_n^*$. Then $G \cong Gal(\mathbf{Q}(\sqrt[n]{a}, \zeta_n)/\mathbf{Q})$, for some irreducible binomial $x^n - a$ over $\mathbf{Q}$.*

PROOF: Let $G_0 = G \cap (\mathbf{Z}_n \times 1)$. Then there is a surjective crossed homomorphism $\psi: \mathbf{Z}_n^* \longrightarrow (\mathbf{Z}_n \times 1)/G_0 \cong \mathbf{Z}_m$, where $m|n$. So the values $\psi(u)$ can be viewed modulo m, hence ψ induces a crossed homomorphism into the multiplicative group of m^{th} roots of unity, $\psi^*: \mathbf{Z}_n^* \longrightarrow \mathbf{Q}(\zeta_n)^*$ via $\psi^*(u) = \zeta_m^{\psi(u)}$. However, by Hilbert's Theorem 90 [**9**, Theorem 1-5-4] , we have $H_1(\mathbf{Z}_n^*, \mathbf{Q}(\zeta_n)^*) = 1$, so that there exists a $\beta \in \mathbf{Q}(\zeta_n)^*$ such that $\psi^*(u) = \sigma_u(\beta)/\beta$, for all $u \in \mathbf{Z}_n^*$ (where σ_u is defined as on page 4). Thus $\psi^*(u) = \sigma_u(\beta)/\beta = \zeta_m^{\psi(u)}$, so $\sigma_u(\beta) = \zeta_m^{\psi(u)} \cdot \beta$. From this we see that $\sigma_u(\beta^m) = \beta^m$ for all $u \in \mathbf{Z}_n^*$, so $\beta^m = b \in \mathbf{Q}$. Also, since ψ is surjective, $\sigma_u(\beta)$ takes on m distinct values as u varies. Thus $x^m - b$ is irreducible and $\beta = \sqrt[m]{b}$ is contained in an abelian extension of $\mathbf{Q}$. This forces $m = 2^s$ for some $s \geq 0$ (else, if an odd prime $p|m$ then $\mathbf{Q}(\sqrt[p]{b})/\mathbf{Q}$ is abelian, so $\zeta_p \in \mathbf{Q}(\sqrt[p]{b})$, contradicting degrees). Without loss of generality, assume $b \in \mathbf{Z}$.

If $m = 1$ then $G_0 = \mathbf{Z}_n \times 1 \subseteq G$. Now if $(\alpha, u) \in \mathbf{Z}_n \rtimes \mathbf{Z}_n^*$, then since G is full, there exists $\gamma \in \mathbf{Z}_n$ such that $(\gamma, u) \in G$. Since $(\alpha - \gamma, 1) \in G$, this gives $(\alpha - \gamma, 1) \cdot (\gamma, u) = (\alpha, u) \in G$, hence $G = \mathbf{Z}_n \rtimes \mathbf{Z}_n^*$, which we know is the Galois group of a radical extension of $\mathbf{Q}$. Thus we may assume that $m > 1$, and so n is divisible by 2.

Let p be a prime which is relatively prime to nb and let $a = bp^m$. Then $x^n - a$ is irreducible (see [**5**, Theorem 51]), and $\mathbf{Q}(\sqrt[m]{a}) = \mathbf{Q}(\sqrt[m]{b})$. We will show that G is the Galois group of $\mathbf{Q}(\sqrt[n]{a}, \zeta_n)/\mathbf{Q}$. We first show that $\mathbf{Q}(\sqrt[n]{a}) \cap \mathbf{Q}(\zeta_n) = \mathbf{Q}(\sqrt[m]{a})$. We have already shown that $\mathbf{Q}(\sqrt[n]{a}) \cap \mathbf{Q}(\zeta_n) \supseteq \mathbf{Q}(\sqrt[m]{a})$. If this intersection is larger, then it would

contain $\mathbf{Q}(\sqrt[2m]{a})$. However, p is ramified in $\mathbf{Q}(\sqrt[2m]{a})$, yet $(p,n)_{gcd} = 1$, so p is unramified in $\mathbf{Q}(\zeta_n)$, hence the intersection is as indicated. Thus $|Gal(\mathbf{Q}(\sqrt[n]{a},\zeta_n)/\mathbf{Q})| = n\phi(n)/m = |G|$.

Now given $u \in \mathbf{Z}_n^*$, we know that σ_u has n/m distinct extensions to $Gal(\mathbf{Q}(\sqrt[n]{a},\zeta_n)/\mathbf{Q})$. Let τ be one of these extensions. Then $\tau(\sqrt[n]{a}) = \zeta_n^t \cdot \sqrt[n]{a}$, for some $0 \leq t < n$. Raise this equation to the n/m power to obtain $\zeta_m^t \cdot \sqrt[m]{a} = \tau(\sqrt[m]{a}) = \sigma_u(\beta p) = \zeta_m^{\psi(u)} \cdot \beta p = \zeta_m^{\psi(u)} \sqrt[m]{a}$. Thus $t \equiv \psi(u) \pmod m$. So the extensions of σ_u to $Gal(\mathbf{Q}(\sqrt[n]{a},\zeta_n)/\mathbf{Q})$ are $\{\sigma_{u,\alpha} : \alpha \in \mathbf{Z}_n, \alpha \equiv \psi(u) \pmod m\}$, where $\sigma_{u,\alpha}(\sqrt[n]{a}) = \zeta_n^\alpha \cdot \sqrt[n]{a}$. Therefore $Gal(\mathbf{Q}(\sqrt[n]{a},\zeta_n)/\mathbf{Q}) = \{\sigma_{u,\alpha} : u \in \mathbf{Z}_n^*\ ,\ \alpha \in \mathbf{Z}_n,\ \alpha \equiv \psi(u) \pmod m\}$. Observe that $\sigma_{u,\alpha} \circ \sigma_{v,\gamma}(\sqrt[n]{a}) = \sigma_{u,\alpha}(\zeta_n^\gamma \cdot \sqrt[n]{a}) = \zeta_n^{u\gamma+\alpha} \cdot \sqrt[n]{a}$, hence $\sigma_{u,\alpha} \circ \sigma_{v,\gamma} = \sigma_{uv,u\gamma+\alpha}$. The mapping $G \longmapsto Gal(\mathbf{Q}(\sqrt[n]{a},\zeta_n)/\mathbf{Q})$, given by $(\alpha,u) \longmapsto \sigma_{u,\alpha}$ is an isomorphism, by part (b) of the lemma.

3. The case $n = 2^e$.

Fixed in this section is an irreducible binomial $x^{2^e} - a$ over $\mathbf{Q}$. For small values of e, G is easily computed, thus we assume that $e \geq 3$. In this case it is well known that $\mathbf{Z}_{2^e}^*$ has generators $\{-1,5\}$, where 5 has order 2^{e-2} and generates the subgroup of residues congruent to 1(mod 4). These generators are the basis for our computations in this section.

As usual, let $\mathbf{Q}(\sqrt[2^s]{a}) = \mathbf{Q}(\sqrt[2^e]{a}) \cap \mathbf{Q}(\zeta_{2^e})$, with $s \geq 1$, and let $H = Gal(\mathbf{Q}(\zeta_{2^e})/\mathbf{Q}(\sqrt[2^s]{a}))$, viewed as a subgroup of $\mathbf{Z}_{2^e}^*$.

PROPOSITION 6. *Suppose $x^{2^e} - a$ is irreducible over $\mathbf{Q}$, with $e \geq 3$. Then*

(a) *If $s = 1$ then $\mathbf{Q}(\sqrt{a})$ is one of $\mathbf{Q}(\zeta_4)$, $\mathbf{Q}(\sqrt{2})$ or $\mathbf{Q}(\sqrt{-2})$. Furthermore,*

(i) If $\mathbf{Q}(\sqrt{a}) = \mathbf{Q}(\zeta_4)$ then $H = \langle 5 \rangle = \{u \in \mathbf{Z}_{2^e}^* : u \equiv 1 (mod\ 4)\}$.

(ii) If $\mathbf{Q}(\sqrt{a}) = \mathbf{Q}(\sqrt{2})$ *then* $H = \langle -1, 5^2 \rangle = \{u \in \mathbf{Z}_{2^e}^* : u \equiv 1,7 (mod\ 8)\}$.

(iii) If $\mathbf{Q}(\sqrt{a}) = \mathbf{Q}(\sqrt{-2})$ *then* $H = \langle -5 \rangle = \{u \in \mathbf{Z}_{2^e}^* : u \equiv 1,3 (mod\ 8)\}$.

(b) *If* $s \geq 2$ *then* $\mathbf{Q}(\sqrt[2^s]{a}) = \mathbf{Q}(\zeta_{2^{s+1}})$ *and* $H = \langle 5^{2^{s-1}} \rangle = \{u \in \mathbf{Z}_{2^e}^* : u \equiv 1 (mod\ 2^{s+1})\}$.

PROOF: (a). As $\mathbf{Q}(\sqrt{a}) \subseteq \mathbf{Q}(\zeta_{2^e})$, the first statement follows as $\mathbf{Q}(\zeta_{2^e})$ contains exactly these three quadratic subfields. The rest of (a) follows from the identities $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$ and $\sqrt{-2} = \zeta_8 - \zeta_8^{-1}$, and counting.

(b) For $s \geq 2$, since $\mathbf{Q}(\sqrt[2^s]{a}) \subseteq \mathbf{Q}(\zeta_{2^e})$, the extension $\mathbf{Q}(\sqrt[2^s]{a})/\mathbf{Q}$ is normal and hence $\zeta_{2^s} \in \mathbf{Q}(\sqrt[2^s]{a})$. As $s \geq 2$, $\zeta_4 \in \mathbf{Q}(\sqrt[2^s]{a})$. Then $\mathbf{Q}(\zeta_4) \subseteq \mathbf{Q}(\sqrt[2^s]{a}) \subseteq \mathbf{Q}(\zeta_{2^e})$, and $Gal(\mathbf{Q}(\zeta_{2^e})/\mathbf{Q}(\zeta_4))$ is cyclic. Thus $\mathbf{Q}(\sqrt[2^s]{a})$ must be $\mathbf{Q}(\zeta_{2^{s+1}})$, and the last statement follows.

By virtue of Theorem B and the above proposition, we have finished the case $s = 1$. Likewise, Theorem A handles the case $s = 0$. The next result takes care of the case $s \geq 2$ and completes our description of G when n is a power of 2.

PROPOSITION 7. *Suppose that* $s \geq 2$, *so that* $\mathbf{Q}(\sqrt[2^s]{a}) = \mathbf{Q}(\zeta_{2^{s+1}})$.

(a) *If* $a = -c^{2^s}, c \in \mathbf{Q}$, *then*

$$G \cong \{(\alpha, u) : \alpha \equiv \tfrac{u-1}{2} (mod\ 2^s)\}.$$

(b) *If* $a = -2^{2^{s-1}} \cdot c^{2^s}$, $c \in \mathbf{Q}$, *then*

$$G \cong \{(\alpha, u) : \alpha \equiv \begin{cases} \frac{u-1}{2} (mod\ 2^s), & \text{if } u \equiv 1,7 (mod\ 8) \\ 2^{s-1} + \frac{u-1}{2} (mod\ 2^s), & \text{if } u \equiv 3,5 (mod\ 8) \end{cases}\}.$$

PROOF: The isomorphisms arise because the embedding $G \hookrightarrow \mathcal{G}$ is not canonical, but depends on the choices of the radicals $\sqrt[n]{a}$ and ζ_n. With

these choices fixed, let $\sqrt[2^s]{a} = (\sqrt[2^e]{a})^{2^{e-s}}$, and $\zeta_{2^{s+1}} = (\zeta_{2^e})^{2^{e-s-1}}$ (note $s < e$ in this case, by Proposition 1). Finally, fix $\zeta_{2^s} = (\zeta_{2^{s+1}})^2$.

Note that since $\mathbf{Q}(\sqrt[2^s]{a}) = \mathbf{Q}(\zeta_{2^{s+1}}) = \mathbf{Q}(\sqrt[2^s]{-1})$, the cases (a) and (b) above are interpretations of parts (a) and (b) or Proposition 3 in this setting.

(a) Let $a = -c^{2^s}$ with $c \in \mathbf{Q}$. Then c is a root of $x^{2^s} + a = 0$, so that $c = \sqrt[2^s]{a} \cdot \zeta_{2^{s+1}}^z$ for some odd $z \in \mathbf{Z}$.

Now for any $\sigma = (\alpha, u) \in \mathrm{G}$, we have $\sqrt[2^s]{a} \cdot \zeta_{2^{s+1}}^z = c = \sigma(c) = \sigma((\sqrt[2^e]{a})^{2^{e-s}} \cdot (\zeta_{2^e})^{z2^{e-s-1}}) = \sqrt[2^s]{a} \cdot \zeta_{2^s}^{\alpha} \cdot \zeta_{2^{s+1}}^{uz}$, so that $\zeta_{2^{s+1}}^z = \zeta_{2^{s+1}}^{2\alpha} \cdot \zeta_{2^{s+1}}^{uz}$, thus $\alpha \equiv z \cdot \frac{1-u}{2} \pmod{2^s}$ and

$$\mathrm{G} = \{(\alpha, u) : \alpha \equiv z \cdot \tfrac{1-u}{2} (\mathrm{mod}\ 2^s)\}.$$

Let $t \in \mathbf{Z}$ be such that $t \cdot z \equiv -1 (\mathrm{mod}\ 2^s)$. The map $(\alpha, u) \longmapsto (t \cdot \alpha, u)$ is an automorphism of $\mathcal{G}$ that maps G isomorphically onto the required subgroup.

(b) Let $a = -2^{2^{s-1}} \cdot c^{2^s}$, $c \in \mathbf{Q}$. Then $2c$ is a root of $x^{2^s} + a \cdot 2^{2^{s-1}} = 0$, so that $2c = \sqrt[2^s]{a} \cdot \sqrt{2} \cdot \zeta_{2^{s+1}}^z$, for some odd $z \in \mathbf{Z}$. If $u \equiv 1, 7 (\mathrm{mod}\ 8)$ then $\sigma_u(\sqrt{2}) = \sqrt{2}$ and the calculations are the same as above. If $u \equiv 3, 5 (\mathrm{mod}\ 8)$ then $\sigma_u(\sqrt{2}) = -\sqrt{2}$ and we have $\sqrt[2^s]{a} \cdot \sqrt{2} \cdot \zeta_{2^{s+1}}^z = 2c = \sigma(2c) = \sqrt[2^s]{a} \cdot \zeta_{2^s}^{\alpha} \cdot (-\sqrt{2}) \cdot \zeta_{2^{s+1}}^{uz}$. This yields $\alpha \equiv 2^{s-1} + z \cdot \frac{1-u}{2}$ $(\mathrm{mod}\ 2^s)$. The rest of the proof follows as above.

4. General n.

Let $n = 2^e m$, with $m > 1$ odd and $e \geq 1$. Denote $L = \mathbf{Q}(\sqrt[2^e]{a}, \zeta_{2^e})$, and $M = \mathbf{Q}(\sqrt[m]{a}, \zeta_m)$. Then Ω is the compositum of L and M. If $L \cap M = \mathbf{Q}$ then $\mathrm{G} \cong Gal(L/\mathbf{Q}) \oplus Gal(M/\mathbf{Q})$, and both of the Galois groups appearing as summands have been described. However, $L \cap M$ is not necessarily $\mathbf{Q}$, but we do have the following.

PROPOSITION 8. *Let $x^n - a$ be irreducible over $\mathbf{Q}$, and let n, L, M be as above. Then $[L \cap M : \mathbf{Q}] \leq 2$.*

PROOF: Since $\mathbf{Q}(\sqrt[2^s]{a}) = \mathbf{Q}(\sqrt[n]{a}) \cap \mathbf{Q}(\zeta_n)$, we have that $\mathbf{Q}(\sqrt[2^s]{a})/\mathbf{Q}$ is an abelian extension, hence $\zeta_{2^s} \in \mathbf{Q}(\sqrt[2^s]{a}) \subseteq L$. So $\mathbf{Q}(\zeta_{2^s}) \subseteq \mathbf{Q}(\sqrt[2^e]{a}) \cap \mathbf{Q}(\zeta_{2^e})$, which implies that $[L : \mathbf{Q}] \leq 2^e \cdot \phi(2^e)/2^{s-1}$. From this and $[\Omega : \mathbf{Q}] = n \cdot \phi(n)/2^s = [L : \mathbf{Q}][M : \mathbf{Q}]/[L \cap M : \mathbf{Q}]$, we obtain the desired result.

Next we characterize when $[L \cap M : \mathbf{Q}] = 2$. By virtue of Theorems A and B, we will assume that $s \geq 2$.

PROPOSITION 9. *Let $x^n - a$ be irreducible over $\mathbf{Q}$, and let n, L, M be as above. Assume $s \geq 2$. Then $[L \cap M : \mathbf{Q}] = 2$ if and only if there exists $b \in \mathbf{Q}$ such that $\mathbf{Q}(\sqrt{b})$ is a quadratic subfield of $\mathbf{Q}(\zeta_m)$, and either*

(i) $e = s = 2$, and $a = -(2b)^2 c^4$ for some $c \in \mathbf{Q}$, or

(ii) $e > s \geq 2$, and $a = -b^{2^{s-1}} c^{2^s}$, or $a = -(2b)^{2^{s-1}} c^{2^s}$, for some $c \in \mathbf{Q}$.

PROOF: We first consider the case $e = s = 2$. First assume $b, c \in \mathbf{Q}$ with $a = -(2b)^2 c^4$ and $\sqrt{b} \in \mathbf{Q}(\zeta_m)$. Then $\mathbf{Q}(\sqrt{a}) = \mathbf{Q}(\zeta_4)$ and $\mathbf{Q}(\sqrt[4]{a}) = \mathbf{Q}(\zeta_8 \sqrt{2} \sqrt{b}) = \mathbf{Q}((1 + \zeta_4)\sqrt{b})$. Since $1 + \zeta_4 \in \mathbf{Q}(\sqrt[4]{a})$, we have that $\sqrt{b} \in \mathbf{Q}(\sqrt[4]{a}) = L$ (as $e = s$), and $\sqrt{b} \in M$ by assumption. Thus $L \cap M = \mathbf{Q}(\sqrt{b})$, by Proposition 8.

Conversely, assume $e = s = 2$ and $[L \cap M : \mathbf{Q}] = 2$. Then as $\mathbf{Q}(\sqrt[4]{a})/\mathbf{Q}$ is Galois, $\zeta_4 \in \mathbf{Q}(\sqrt[4]{a})$. Write $L \cap M = \mathbf{Q}(\sqrt{b})$ for some $b \in \mathbf{Q}$. As $[M : \mathbf{Q}(\zeta_m)]$ is odd, $\sqrt{b} \in \mathbf{Q}(\zeta_m)$. Now, in fact, $Gal(\mathbf{Q}(\sqrt[4]{a})/\mathbf{Q}) \cong \mathbf{Z}_2 \oplus \mathbf{Z}_2$ so that $\mathbf{Q}(\sqrt[4]{a}) = \mathbf{Q}(\zeta_4, \sqrt{b_1})$ for some $b_1 \in \mathbf{Q}$. Then $\mathbf{Q}(\sqrt{b}) \subseteq \mathbf{Q}(\zeta_4, \sqrt{b_1})$, so that as $b \neq -1$, we must have $\mathbf{Q}(\sqrt{b}) = \mathbf{Q}(\sqrt{\pm b_1})$. In either case, $\mathbf{Q}(\sqrt[4]{a}) = \mathbf{Q}(\zeta_4, \sqrt{b})$. But it is easy to see that $\mathbf{Q}(\zeta_4, \sqrt{b}) =$

$\mathbf{Q}(\sqrt[4]{-(2b)^2})$, because $\sqrt[4]{-(2b)^2} = (1+\zeta_4)\sqrt{b}$. Hence $\mathbf{Q}(\sqrt[4]{a}) = \mathbf{Q}(\sqrt[4]{-(2b)^2})$. Now apply Proposition 3.

Next we show that if $e = s \geq 3$ then $L \cap M = \mathbf{Q}$. Indeed, if $e = s \geq 3$ then $\mathbf{Q}(\sqrt[2^e]{a})/\mathbf{Q}$ is abelian, and thus $\zeta_8 \in \mathbf{Q}(\sqrt[2^e]{a})$. Then $\mathbf{Q}(\zeta_4)$, $\mathbf{Q}(\sqrt{\pm 2})$ are three distinct quadratic subfields of $\mathbf{Q}(\sqrt[2^e]{a}) = L$ (as $e = s$). By Proposition 5b, these are the only quadratic subfields of L. Since clearly none of these could be in M, we have $L \cap M = \mathbf{Q}$.

Finally, consider the case $e > s \geq 2$. Assume $b, c \in \mathbf{Q}$ with $\sqrt{b} \in \mathbf{Q}(\zeta_m)$ such that *(ii)* holds. If $a = -b^{2^{s-1}} c^{2^s}$ then $\mathbf{Q}(\sqrt[2^s]{a}) = \mathbf{Q}(\zeta_{2^{s+1}}\sqrt{b})$, so $\zeta_{2^{s+1}}\sqrt{b} \in L$. But $e > s$, so $\zeta_{2^{s+1}} \in L$, thus $\sqrt{b} \in L$. As $\sqrt{b} \in M$, we have $L \cap M = \mathbf{Q}(\sqrt{b})$. A similar argument works if $a = -(2b)^{2^{s-1}} c^{2^s}$.

Conversely, assume $e > s \geq 2$ and $[L \cap M : \mathbf{Q}] = 2$. Since $\mathbf{Q}(\sqrt[2^s]{a})/\mathbf{Q}$ is abelian, Proposition 5a gives $b_1 \in \mathbf{Q}$ with $a^2 = b_1^{2^s}$, hence $a = -b_1^{2^{s-1}}$, since a is not a square. This gives $\sqrt[2^s]{a} = \zeta_{2^{s+1}}\sqrt{b_1}$. If $\sqrt{b_1} \in \mathbf{Q}(\zeta_{2^e})$ then $e > s$ gives $\mathbf{Q}(\sqrt[2^e]{a}) \cap \mathbf{Q}(\zeta_{2^e}) = \mathbf{Q}(\sqrt[2^s]{a})$, which in turn by counting degrees yields $L \cap M = \mathbf{Q}$. So $\sqrt{b_1} \notin \mathbf{Q}(\zeta_{2^e})$. Now write $L \cap M = \mathbf{Q}(\sqrt{b})$ for some $b \in \mathbf{Q}$, with $\sqrt{b} \in \mathbf{Q}(\zeta_m)$. Then $\sqrt{b} \in L$ and $\sqrt{b} \notin \mathbf{Q}(\zeta_{2^e})$ (because no quadratic subfield of $\mathbf{Q}(\zeta_{2^e})$ is in M). Therefore, $\mathbf{Q}(\zeta_{2^e}, \sqrt{b})$, $\mathbf{Q}(\zeta_{2^e}, \sqrt{b_1})$ are quadratic subfields of the extension $\mathbf{Q}(\zeta_{2^e}, \sqrt[2^e]{a})/\mathbf{Q}(\zeta_{2^e})$. But this extension has the USP, by Proposition 4, and hence $\mathbf{Q}(\zeta_{2^e}, \sqrt{b}) = \mathbf{Q}(\zeta_{2^e}, \sqrt{b_1})$. This gives $b_1 = b\gamma^2$ for some $\gamma \in \mathbf{Q}(\zeta_{2^e})$. As $\gamma^2 \in \mathbf{Q}$, this implies that $\gamma^2 = \pm 2$, or ± 1 times a rational square, that is, $b_1 = \pm bc^2$ or $b_1 = \pm 2bc^2$ for some $c \in \mathbf{Q}$, as needed.

We can now determine G in the case $[L \cap M : \mathbf{Q}] = 2$ and $s > 1$. From the statement of the Theorem it will be seen that the calculations are analogous to those of Proposition 7, hence they are omitted.

THEOREM D. *Let $x^n - a$ be irreducible over $\mathbf{Q}$ with $n = 2^e m$, $m \geq 3$ odd, and $e \geq 1$. Assume that $\mathbf{Q}(\sqrt[2^e]{a}, \zeta_{2^e}) \cap \mathbf{Q}(\sqrt[m]{a}, \zeta_m) = \mathbf{Q}(\sqrt{b})$, a quadratic subfield of $\mathbf{Q}(\zeta_m)$. Let $H = Gal(\mathbf{Q}(\zeta_n)/\mathbf{Q}(\sqrt{b}))$.*

(a) *If $a = -b^{2^{s-1}} c^{2^s}$, then $G \cong \{(\alpha, u)$:*

$$\alpha \equiv \left\{ \begin{array}{ll} \frac{u-1}{2} \pmod{2^s}, & \text{if } u \in H \\ \frac{u-1}{2} + 2^{s-1} \pmod{2^s}, & \text{if } u \notin H \end{array} \right\}.$$

(b) *If $a = -(2b)^{2^{s-1}} c^{2^s}$, then $G \cong \{(\alpha, u)$:*

$$\alpha \equiv \left\{ \begin{array}{ll} \frac{u-1}{2} \pmod{2^s}, & \text{if } \left\{ \begin{array}{l} u \in H, u \equiv 1, 7 \pmod 8 \text{ or} \\ u \notin H, u \equiv 3, 5 \pmod 8 \end{array} \right. \\ \frac{u-1}{2} + 2^{s-1} \pmod{2^s}, & \text{if } \left\{ \begin{array}{l} u \in H, u \equiv 3, 5 \pmod 8 \text{ or} \\ u \notin H, u \equiv 1, 7 \pmod 8 \end{array} \right. \end{array} \right\}.$$

References.

[1] Acosta de Orozco, M., Vélez, W.Y., *The lattice of subfields of a radical extension*, J. of Number Theory, 15 (1982), 388-405

[2] Gay, D., Vélez, W.Y., *On the degree of the splitting field of an irreducible binomial*, Pacific J. of Mathematics, 78 (1978), 117-120

[3] Gay, D., Vélez, W.Y., *The torsion group of a radical extension*, Pacific J. of Mathematics, 92 (1981), 317-327

[4] Jacobson, E.T., Vélez, W.Y., *Fields arithmetically equivalent to a radical extension of the rationals*, to appear, J. of Number Theory

[5] Kaplansky, I., *Fields and Rings*, University of Chicago Press, 1969

[6] Vélez, W.Y., *On normal binomials*, Acta Arithmetica, 36 (1980), 113-124

[7] Vélez, W.Y., *Several results on radical extensions*, Arch. Math., 45 (1985), 342-349

[8] Weiss, E., *Algebraic Number Theory*, Chelsea Publishing Company, New York, N.Y., 1976

[9] Weiss, E., *Cohomology of Groups*, Academic Press, 1969

Eliot Jacobson
Department of Mathematics
Ohio University
Athens OH, 45701

William Y. Vélez
Department of Mathematics
University of Arizona
Tucson AZ, 85721

(Received June 13, 1989 ;
in revised form February 16, 1990)