PACIFIC JOURNAL OF MATHEMATICS
Vol. 72, No. 2, 1977

PARTIALLY NORMAL RADICAL EXTENSIONS OF THE RATIONALS

DAVID A. GAY, ANDREW MCDANIEL AND WILLIAM YSLAS VÉLEZ

Dedicated to Henry B. Mann on the occasion of his retirement

If K is a field and $\mathrm{char}\, K \nmid n$, then any binomial $x^n - b \in K[x]$ has the property that $K(\alpha)$ is its splitting field for any root α iff a primitive nth root of unity ζ_n is an element of K. Thus, if $\zeta_n \in K$, any irreducible binomial $x^n - b \in K[x]$ is automatically normal. Similar nice results about binomials $x^n - b$ (Kummer theory comes to mind) can be obtained with the assumption $\zeta_n \in K$.

In this paper, without assuming the appropriate roots of unity are in K, one asks: what are the binomials $x^m - a \in K[x]$ having the property that $K(\alpha)$ is its splitting field for some root α? Such binomials are called partially normal. General theorems are obtained in case K is a real field. A complete list of partially normal binomials together with their Galois groups is found in case $K = Q$, the rational numbers.

This is a continuation of work begun in 1926 by Darbi [1] and Bessel-Hagen (see [8], p. 302) who determined all normal binomials over Q. Recently, Mann and Vélez [5] considered binomials having a weaker property than normal but stronger than partially normal, namely, $K(\alpha)$ is the splitting field for *any* root α. They obtained a complete classification of such binomials together with their Galois groups in case the ground field is Q. In a similar direction, but for arbitrary ground field, Schinzel [7] has characterized two types of binomials: (a) those with abelian Galois group and (b) those whose polynomial degree is a power of a prime and which are products of normal factors.

The central role played by partially normal binomials in the general structure theory of pure extensions has been pointed out by Norris and Vélez in [6]. The results of Darbi and Bessel-Hagen, Mann and Vélez have been generalized for real fields by Gay [3].

In §2, we create a general setting by considering partially normal binomials over a typical real algebraic number field. (We have chosen this general setting to begin with in order to give more insight and to sketch how the results of this paper might be generalized to real fields.) In §3, we return to the rational numbers, apply the results of §2, and state a classification theorem. Sections 4 and 5 are devoted to proving this theorem. Finally, in §6, we compute the Galois groups of these binomials.

2. Generalities on partially normal binomial extensions of real fields.

In what follows we let R denote a fixed real algebraic number field. This section will be devoted to consequences of the following.

DEFINITION. The binomial $x^m - a \in R[x]$ is *partially normal over* R if there is a root α of $x^m - a$ such that $R(\alpha)$ is the splitting field of $x^m - a$ over R. Such a root α is called a *generating root.*

Let ζ_n be a primitive nth root of unity. Let $\phi_R(n) = [R(\zeta_n): R]$. Thus ϕ_R is an Euler's ϕ-function relative to the field R. In particular, $\phi_Q(n) = \phi(n)$.

PROPOSITION 2.1. *The binomial $x^m - a \in R[x]$ is partially normal over R iff there exists a root γ of $x^m - a$ such that $R(\zeta_m) \subseteqq R(\gamma)$. Furthermore, if $x^m - a$ is partially normal over R with generating root α, then there is a positive integer s such that $[R(\alpha): R] = s\phi_R(m)$, $R(\alpha^s) = R(\zeta_m)$ and $x^s - \alpha^s$ is the minimal polynomial for α over $R(\zeta_m)$.*

Proof. The first statement of the proposition follows from the fact that if δ is a root of $x^m - a$ then all the roots are $\delta, \zeta_m\delta, \zeta_m^2\delta, \cdots, \zeta_m^{m-1}\delta$.

To prove the second statement, we note that from the first statement $R(\zeta_m) \subseteqq R(\alpha)$. Let $s = [R(\alpha): R(\zeta_m)]$. Then $[R(\alpha): R] = s\phi_R(m)$. Now let $f(x)$ be the minimal polynomial for α over $R(\zeta_m)$. Then $f(x)$ is of degree s and

$$f(x) = \prod_{j=1}^{s} (x - \zeta_m^{i_j}\alpha) .$$

The constant term of $f(x) = \pm\alpha^s \prod_{j=1}^{s} \zeta_m^{i_j}$ and is in $R(\zeta_m)$. Thus $\alpha^s \in R(\zeta_m)$. Since $x^s - \alpha^s$ is a polynomial of degree s over $R(\zeta_m)$ with α as a root, $f(x) = x^s - \alpha^s$. This together with the fact $R(\alpha^s) \subseteqq R(\zeta_m)$ forces $R(\alpha^s) = R(\zeta_m)$.

In what follows, we choose a fixed binomial $x^m - a$, partially normal over R with generating root α and $s = [R(\alpha): R(\zeta_m)]$ as in Proposition 2.1. Let $\beta = \sqrt[m]{|a|}$, the real, positive mth root of $|a|$. Let q be the smallest positive integer such that $\beta^q \in R$. The following results will tell us something about the relationships among β, s and q and their limitations. First, two lemmas.

LEMMA 2.2. *Let γ be algebraic over a field F with $\gamma^r \in F$ and $x^r - \gamma^r$ irreducible over F. Then $\gamma^t \in F$* (t a positive integer) *implies $r \mid t$.*

Proof. If $\gamma^r \in F$ and $x^r - \gamma^r$ irreducible over F, then $[F(\gamma): F] = r$. Thus, if $\gamma^t \in F$, $t \geqq r$. If $r \nmid t$, then write $t = ar + b$ with $0 < b < r$. Hence $\gamma^t = (\gamma^r)^a\gamma^b$ or $\gamma^b \in F$, a contradiction. Thus $r \mid t$.

LEMMA 2.3. *Let K be an abelian extension of the real field R. Suppose $a \in R$ with $a > 0$ and $\sqrt[m]{a} \in K$* ($\sqrt[m]{a}$ is a real mth root). *Then $(\sqrt[m]{a})^2 \in R$.*

Proof. This is a standard result in Galois theory. See [5], Lemma 1.

PROPOSITION 2.4. *We have* (a) *$s \mid m$ and $q \mid m$;* (b) *$\beta^{2s} \in R$;* (c) *if $\beta^s \in R$, then $q \mid s$ and if $\beta^s \notin R$, then $q \mid 2s$.*

Proof. (a) From Proposition 2.1 $x^s - \alpha^s$ is irreducible over $R(\zeta_m)$. But also $\alpha^m = a \in R$. Thus from Lemma 2.2, $s \mid m$. By an argument similar to the proof of Lemma 2.2, q divides any positive integer t such that $\beta^t \in R$. Thus $q \mid m$.

(b) Now $\alpha = \zeta_m^j\zeta_{2m}^{\varepsilon}\beta$ where $\varepsilon = 0$ if $a > 0$ and $\varepsilon = 1$ if $a < 0$. Thus $\alpha^s = \zeta_m^{sj}\zeta_{2m}^{s\varepsilon}\beta^s \in R(\zeta_m)$ by Proposition 2.1. Hence $\beta^s \in R(\zeta_{2m})$. By Lemma 2.3, β^s is either an element of R or is the square root of an element of R. In either case, $\beta^{2s} \in R$.

(c) By (b) and the proof of part (a), $q \mid 2s$. If, in addition, $\beta^s \in R$, then $q \mid s$.

The following result delineates q and s more precisely:

PROPOSITION 2.5. (a) *If $a > 0$ or $a < 0$ and q even, then $\beta^s \in R$ iff $q = s$.*

(b) *If $a < 0$ and q odd, then $\beta^s \in R$ iff $q = s$ or $s = 2q$.*

(c) *$\beta^s \notin R$ iff $q = 2s$.*

Proof. (a) Suppose $\beta^s \in R$ and $a > 0$ or $a < 0$ and q even. Then $\alpha^q = \zeta_m^{qj}\zeta_{2m}^{\varepsilon q}\beta^q \in R(\zeta_m)$. Hence, by Proposition 2.1 and Lemma 2.2, $s \mid q$. By Proposition 2.4 (c), $q \mid s$. Thus $q = s$. The converse is obvious.

(b) If $\beta^s \in R$, $a < 0$ and q odd, then $\alpha^{2q} = \zeta_m^{2qj}\zeta_m^{q}\beta^{2q} \in R(\zeta_m)$. Thus by Proposition 2.1 and Lemma 2.2, $s \mid 2q$. But by Proposition 2.4 (c), $q \mid s$. Thus $s = q$ or $s = 2q$. Again the converse is obvious.

(c) Suppose $\beta^s \notin R$. Thus by Proposition 2.4 (c), $q \mid 2s$. Furthermore, q must be even. Thus $\alpha^q \in R(\zeta_m)$. Again by Lemma 2.2, $s \mid q$.

Thus $s = q$ or $2s = q$. The former cannot happen since $\beta^s \notin R$. Thus $2s = q$. The converse is easy.

The following result will enable us to narrow the possibilities for s considerably.

PROPOSITION 2.6. *In all cases $\phi_R(m) \leqq 2\phi_R(m/s)$. In particular, if $a > 0$ and $\beta^s \in R$, then $\phi_R(m) = \phi_R(m/s)$; if $a < 0$, and $\beta^s \in R$, then $\phi_R(m) = \phi_R(2m/s)$.*

Proof. We have $\alpha = \zeta_m^j \zeta_{2m}^\varepsilon \beta$. Thus $\alpha^{2s} = \zeta_{m/s}^{2j} \zeta_{m/s}^\varepsilon \beta^{2s} \in R(\zeta_{m/s})$. Consequently, $s\phi_R(m) = [R(\alpha): R] = [R(\alpha): R(\zeta_{m/s})][R(\zeta_{m/s}): R] \leqq 2s\phi_R(m/s)$ or $\phi_R(m) \leqq 2\phi_R(m/s)$.

If $a > 0$ and $\beta^s \in R$, then $\alpha^s = \zeta_{m/s}^j \beta^s \in R(\zeta_{m/s})$. Thus $\phi_R(m) = \phi_R(m/s)$. If $s = 2q$, then by 2.5 $\beta^s \in R$ and $\alpha^s = \zeta_{m/s}^j \zeta_{m/q} \beta^s \in R(\zeta_{m/q})$. Thus $\phi_R(m(= \phi_R(m/q) = \phi_R(2m/s)$. Finally, if $a < 0, \beta^s \in R$ and $q = s$, then $\alpha^s = \zeta_{m/s}^j \zeta_{2m/s} \beta^s \in R(\zeta_{2m/s}) \subseteqq R(\zeta_m)$. Thus $\phi_R(m) = \phi_R(2m/s)$.

3. Partially normal pure extensions of the rationals.

In this section we will apply the results of §2 to the field $R = \boldsymbol{Q}$. Without loss of generality, we consider (as in [4]) only those binomials $x^n - a$ with a an integer. The following lemma will enable us to use Proposition 2.6 directly. We use the notation $p^\alpha \| m$, for prime p, to mean $p^\alpha | m$ but $p^{\alpha+1} \nmid m$.

LEMMA 3.1. *Let d and m be positive integers with $d | m$.*

(a) *If $\phi(m) \leqq 2\phi(m/d)$, then $d = 1, 2, 3, 4$ or 6. In case $d = 6$, then $2 \| m$; if $3 | d$, then $3 \| m$; if $d = 4$, then $4 \| m$.*

(b) *If $\phi(m) = \phi(m/d)$, then $d = 1$ or 2. In case $d = 2$, then $2 \| m$.*

Proof. Part (b) is obvious. To prove part (a), we first make an observation. Suppose one of the following occurs:

$$\begin{array}{ll} \text{either} & p | d \text{ with } p \text{ a prime} > 3\,, \\ \text{or} & 9 | m \text{ and } 3 | d\,, \\ \text{or} & 8 | d\,, \\ \text{or} & 4 \| d \text{ and } 8 | m\,, \\ \text{or} & 6 | d \text{ and } 4 | m\,. \end{array}$$

Then $\phi(m) \geqq 3\phi(m/d)$. Thus, in order that $\phi(m) \leqq 2\phi(m/d)$ be true we must have

(i) $d = 1, 2, 3, 4, 6$ or 12; (ii) if $3 | d$ then $3 \| m$; (iii) if $d = 4$, then $4 \| m$; and (iv) if $d = 6$, then $2 \| m$. The case $d = 12$ is impossible, as is easily checked.

COROLLARY 3.2. *If* $x^m - a$ *is partially normal over* $\boldsymbol{Q}$, *then* $s = 1, 2, 3, 4$, *or* 6.

The following result limits s even more and relates its value to the rationality of β^s.

PROPOSITION 3.3. (a) $\beta^s \in \boldsymbol{Q}$ *and* $a > 0$ *implies* $s = 1, 2$ $(s = q)$.
(b) $\beta^s \in \boldsymbol{Q}$ *and* $a < 0$ *implies* $s = 1, 2$ $(s = q)$ *or* $s = 2, q = 1$.
(c) $\beta^s \notin \boldsymbol{Q}$ *implies* $s = 1, 2$ *or* 3 $(q = 2s)$.

[We shall see later that all these possibilities can actually be realized.]

Proof. (a) By Proposition 2.6 and Lemma 3.1, $s = 1$ or 2. By 2.5, $q = s$.

(b) If $a < 0$ and $\beta^s \in R$, then by 2.6 $\phi(m) = \phi(2m/s)$. If q is even, then $q = s = 2s_1$, by 2.5. Thus by 3.1 (b) $s_1 = 1$ or 2. If $s_1 = 2$, then $2 \| m$. But $s = 4$ implies $4 | m$ (2.4). This is a contradiction. Thus $q = s = 2$. If q is odd, then by 2.5 (b) $q = s$ or $2q = s$. If $q = s$, then $\boldsymbol{Q}(\zeta_m) = \boldsymbol{Q}(\alpha^q) = \boldsymbol{Q}(\zeta^j_{m/q}\zeta_{2m/q}) \subseteq \boldsymbol{Q}(\zeta_{2m/q})$. This can happen for q odd only when $q = 1$. On the other hand, if $s = 2q$, then $\phi(m) = \phi(m/q)$ so that, by 3.1 (b), $q = 1$ $(s = 2)$ or $q = 2$ $(s = 4)$. If $q = 2$, then $2 \| m$. But again $s = 4$ implies $4 | m$, a contradiction. Thus $q = 1, s = 2$. This completes the proof of (b).

(c) If $\beta^s \notin \boldsymbol{Q}$, then we know $\phi(m) \leqq 2\phi(m/s)$ (2.6) and $q = 2s$ (2.5 (c)). From the first statement we know $s = 1, 2, 3, 4$ or 6 (3.1). But if $s = 4$, then $q = 8$. Since $q|$m, this contradicts 3.1. Similarly, if $s = 6$, then $q = 12$ and $12 | m$ contradicting 3.1. Thus $s = 4$ and $s = 6$ are impossible. We conclude that $s = 1, 2, 3$ with $q = 2s$.

COROLLARY 3.4. *If* $x^m - a$ *is partially normal over* $\boldsymbol{Q}$, *then there is a positive integer* b *such that either* $a = \pm b^m$, $a = \pm b^{m/2}$, $a = \pm b^{m/4}$, *or* $a = \pm b^{m/6}$.

Corollary 3.4 marks out the possibilities for partially normal binomials over $\boldsymbol{Q}$ quite clearly. The following theorem (our main result) gives necessary and sufficient conditions for when one of these admissible binomials is actually partially normal.

THEOREM 3.5. *Let* m *and* b *be positive integers. Then*

(1) $x^m - b^m$ *is partially normal with* $s = q = 1$; $x^m + b^m$ *is partially normal with* $s = 2, q = 1$ (m even) *or* $s = q = 1$ (m odd).

(2) $x^m - b^{m/2}$ *is partially normal with* $s = q = 2 \Leftrightarrow 2 \| m$ *and* $\sqrt{b} \notin \boldsymbol{Q}(\zeta_m)$.

(3) $x^m - b^{m/2}$ *is partially normal with* $s = 1, q = 2 \Leftrightarrow$ *either* $\sqrt{b} \in Q(\zeta_{m/2})$ *and* $\sqrt{b} \notin Q$ or $\sqrt{b} \in Q(\zeta_m), \sqrt{b} \notin Q(\zeta_{m/2})$ *and* $4 \| m$.

(4) $x^m + b^{m/2}$ *is partially normal with* $s = 1, q = 2 \Leftrightarrow \sqrt{b} \in Q(\zeta_{2m})$ *and* $\sqrt{b} \notin Q(\zeta_m)$.

(5) $x^m + b^{m/2}$ *is partially normal with* $s = q = 2 \Leftrightarrow \sqrt{b} \notin Q(\zeta_{2m})$ *or* $\sqrt{b} \in Q(\zeta_m)$ *and* $\sqrt{b} \notin Q$.

(6) $x^m - b^{m/4}$ *is partially normal with* $s = 2, q = 4 \Leftrightarrow \sqrt{b} \in Q(\zeta_m), \sqrt{b} \notin Q(\zeta_{m/2})$ *and* $4 \| m$.

(7) $x^m + b^{m/4}$ *is partially normal with* $s = 2, q = 4 \Leftrightarrow \sqrt{b} \in Q(\zeta_{m/2})$ *and* $\sqrt{b} \notin Q$.

(8) $x^m - b^{m/6}$ *is partially normal with* $s = 3, q = 6 \Leftrightarrow \sqrt{b} \in Q(\zeta_m), \sqrt{b} \notin Q(\zeta_{m/3})$ *and* $2 \| m$.

(9) $x^m + b^{m/6}$ *is partially normal with* $s = 3, q = 6 \Leftrightarrow \sqrt{b} \in Q(\zeta_{2m}), \sqrt{b} \notin Q(\zeta_m)$ *and* $\sqrt{b} \notin Q(\zeta_{2m/3})$.

We will prove this theorem in §5 after stating and proving some useful lemmas.

4. Square roots and generators of cyclotomic extensions.

In this section we will state and prove some results which will be used to prove our main Theorem 3.5. These results are independent of the rest of this paper and are partial responses to the following question: for what positive integers b, m, n is it the case that $Q(\zeta_m\sqrt{b}) = Q(\zeta_n)$? We will use (implicitly) the following known result from Galois theory. (See, for example, [2] p. 240.)

LEMMA 4.1.

(A) *If p is an odd prime, then $\sqrt{p} \in Q(\zeta_p)$ iff $p \equiv 1 \pmod 4$ and $\sqrt{-p} \in Q(\zeta_p)$ iff $p \equiv 3 \pmod 4$; $\sqrt{-1} \in Q(\zeta_4)$; $\sqrt{2} \in Q(\zeta_8)$.*

(B) *Let b be a square free integer. Then, if m is odd, $b | m$ iff $\sqrt{b}$ or $\sqrt{-b} \in Q(\zeta_m) = Q(\zeta_{2m})$ iff $\sqrt{b} \in Q(\zeta_{4m})$ iff $\sqrt{-b} \in Q(\zeta_{4m})$. Further, if $8 | m$, then $\sqrt{b} \in Q(\zeta_m)$ iff $b | m$.*

LEMMA 4.2. *Let m and b be positive integers. Then*

(A) *If m is even, then $\sqrt{b} \in Q(\zeta_{2m})$, $\sqrt{b} \notin Q(\zeta_m)$, and $\sqrt{b} \notin Q(\zeta_{2m/3})$ iff $Q(\zeta_{2m/3}\sqrt{b}) = Q(\zeta_m)$.*

(B) *If m is odd, then $\sqrt{b} \in Q(\zeta_m)$, $\sqrt{b} \notin Q(\zeta_{m/3})$ iff $Q(\zeta_{m/3}\sqrt{b}) = Q(\zeta_m)$.*

Proof. (A) It is sufficient to consider the case where b is square free. Now $\sqrt{b} \in Q(\zeta_{2m})$ and $\sqrt{b} \notin Q(\zeta_{2m/3})$ implies $3 \| m$. Similarly, $\sqrt{b} \in Q(\zeta_{2m})$ and $\sqrt{b} \notin Q(\zeta_m)$ implies $8 \nmid m$. Thus there are two possibilities: (a) $2 \| m$ in which case $b = 3b_1$ with $(b_1, 6) = 1$ and $\sqrt{b_1} \in Q(\zeta_{m/3})$ and (b) $4 \| m$ in which case $b = 6b_1$ with $(b_1, 6) = 1$ and $\sqrt{b_1} \in$

$Q(\zeta_{m/3})$. In both cases $Q(\zeta_{2m/3}\sqrt{b})$ is an extension of $Q(\zeta_{m/3})$. In case (a),

$$\begin{aligned} Q(\zeta_{2m/3}\sqrt{b}) &= Q(\zeta_{m/3}, \zeta_4\zeta_{m/6}\sqrt{3}\sqrt{b_1}) \\ &= Q(\zeta_{m/3}, \zeta_4\sqrt{3}) \\ &= Q(\zeta_{m/3}, \sqrt{-3}) \\ &= Q(\zeta_m); \end{aligned}$$

and, in case (b),

$$\begin{aligned} Q(\zeta_{2m/3}\sqrt{b}) &= Q(\zeta_{m/3}, \zeta_8\zeta_{m/12}\sqrt{2}\sqrt{3}\sqrt{b_1}) \\ &= Q(\zeta_{m/3}, \zeta_8\sqrt{2}\sqrt{3}) \\ &= Q(\zeta_{m/3}, (1+i)\sqrt{3}) \\ &= Q(\zeta_{m/3}, \sqrt{3}) \\ &= Q(\zeta_m) . \end{aligned}$$

Conversely, suppose $Q(\zeta_{2m/3}\sqrt{b}) = Q(\zeta_m)$. Thus $\zeta_{2m/3}\sqrt{b} \in Q(\zeta_{2m})$ and, therefore, $\sqrt{b} \in Q(\zeta_{2m})$. If also $\sqrt{b} \in Q(\zeta_m)$, then also $\zeta_{2m/3} \in Q(\zeta_m)$ contradicting the fact that m is even. Thus $\sqrt{b} \notin Q(\zeta_m)$. Finally, if $\sqrt{b} \in Q(\zeta_{2m/3})$, then $Q(\zeta_m) \subseteqq Q(\zeta_{2m/3})$ which is impossible. Thus also $\sqrt{b} \notin Q(\zeta_{2m/3})$. This completes the proof of (A).

(B) Again we may assume without loss of generality that b is square free. Now $\sqrt{b} \in Q(\zeta_{2m})$ and $\sqrt{b} \notin Q(\zeta_{2m/3})$ implies $3 \| m$, $b = 3b_1$ and $\sqrt{-b_1} \in Q(\zeta_{2m/3}) = Q(\zeta_{m/3})$. Thus, since $Q(\zeta_{2m/3}\sqrt{b})$ is an extension of $Q(\zeta_{m/3})$, we have

$$\begin{aligned} Q(\zeta_{2m/3}\sqrt{b}) &= Q(\zeta_{m/3}, \sqrt{-3}\sqrt{-b_1}) \\ &= Q(\zeta_{m/3}, \sqrt{-3}) \\ &= Q(\zeta_m) . \end{aligned}$$

The proof of the converse is analogous to that of (A).

LEMMA 4.3. *Let m and b be positive integers with m even. Then*

(A) *The following statements are equivalent*

(i) $\sqrt{b} \in Q(\zeta_{2m})$ *and* $\sqrt{b} \notin Q(\zeta_m)$

(ii) $Q(\zeta_{2m}\sqrt{b}) = Q(\zeta_m)$

(iii) *either* $2\|m$, *the square free part of b is odd and* $\sqrt{-b} \in Q(\zeta_m)$ *or* $4\|m$, *the square free part of b is even and* $\sqrt{b/2} \in Q(\zeta_m)$.

(B) $2\|m$, $\sqrt{b} \in Q(\zeta_{2m})$ *and* $\sqrt{b} \notin Q(\zeta_m) \Leftrightarrow Q(\zeta_m\sqrt{b}) = Q(\zeta_{2m})$.

Proof. (A) We will show that (i) $\Rightarrow$ (iii) $\Rightarrow$ (ii) $\Rightarrow$ (i). Suppose $\sqrt{b} \in Q(\zeta_{2m})$ and $\sqrt{b} \notin Q(\zeta_m)$. Thus $8 \nmid m$. It follows that, since m is even, either $2\|m$ or $4\|m$. In the first case it also follows that the square free part of b must be odd and that $\sqrt{-b} \in \boldsymbol{Q}(\zeta_m)$. In the second case it also follows that the square free part of b is even and $\sqrt{b/2} \in \boldsymbol{Q}(\zeta_m)$. This shows that (i) implies (iii).

Now assume that (iii) holds. Clearly $\boldsymbol{Q}(\zeta_{2m}\sqrt{b})$ is an extension of $\boldsymbol{Q}(\zeta_m)$. Thus, in case $2 \| m$,

$$\begin{aligned} \boldsymbol{Q}(\zeta_{2m}\sqrt{b}) &= \boldsymbol{Q}(\zeta_m, \zeta_{2m}\sqrt{b}) \\ &= \boldsymbol{Q}(\zeta_m, \zeta_4\zeta_{m/2}\sqrt{b}) \\ &= \boldsymbol{Q}(\zeta_m, \sqrt{-b}) \\ &= \boldsymbol{Q}(\zeta_m) . \end{aligned}$$

In case $4 \| m$,

$$\begin{aligned} \boldsymbol{Q}(\zeta_{2m}\sqrt{b}\,) &= \boldsymbol{Q}\left(\zeta_m, \zeta_8\zeta_{m/4}\sqrt{2}\,\sqrt{\frac{b}{2}}\right) \\ &= \boldsymbol{Q}(\zeta_m, \zeta_8\sqrt{2}\,) \\ &= \boldsymbol{Q}(\zeta_m) . \end{aligned}$$

This shows that (iii) implies (ii).

That (ii) implies (i) is obvious. This completes the proof of part (A) of the lemma.

(B) If $2 \| m, \sqrt{b} \in \boldsymbol{Q}(\zeta_{2m})$ and $\sqrt{b} \notin \boldsymbol{Q}(\zeta_m)$, then $\sqrt{-b} \in \boldsymbol{Q}(\zeta_m)$. Furthermore, $\boldsymbol{Q}(\zeta_m\sqrt{b})$ is an extension of $\boldsymbol{Q}(\zeta_{m/2}) = \boldsymbol{Q}(\zeta_m)$. Thus

$$\begin{aligned} \boldsymbol{Q}(\zeta_m\sqrt{b}) &= \boldsymbol{Q}(\zeta_{m/2}, \zeta_m\sqrt{b}) \\ &= \boldsymbol{Q}(\zeta_{m/2}, \sqrt{b}) \\ &= \boldsymbol{Q}(\zeta_{m/2}, i\sqrt{-b}) \\ &= \boldsymbol{Q}(\zeta_{m/2}, i) \\ &= \boldsymbol{Q}(\zeta_{2m}) . \end{aligned}$$

Conversely, suppose $\boldsymbol{Q}(\zeta_m\sqrt{b}) = \boldsymbol{Q}(\zeta_{2m})$. It follows easily that $\sqrt{b} \in \boldsymbol{Q}(\zeta_{2m})$. If also $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$, then $\boldsymbol{Q}(\zeta_{2m}) \subseteq \boldsymbol{Q}(\zeta_m)$ contradicting the fact that m is even. Thus $\sqrt{b} \in \boldsymbol{Q}(\zeta_{2m})$ and $\sqrt{b} \notin \boldsymbol{Q}(\zeta_m)$. By part (A) of the lemma, either $2 \| m$ or $4 \| m$. We will show that the latter is impossible. Indeed, suppose $4 \| m$ and $\boldsymbol{Q}(\zeta_m\sqrt{b}) = \boldsymbol{Q}(\zeta_{2m})$. On the one hand, $\boldsymbol{Q}(\zeta_{2m})$ is an extension of $\boldsymbol{Q}(\zeta_{m/2})$ of degree 4. On the other hand, $\boldsymbol{Q}(\zeta_m\sqrt{b})$ is an extension of $\boldsymbol{Q}(\zeta_{m/2})$ of degree at most 2. Thus $4 \| m$ cannot happen and part (B) of the lemma follows.

5. Proof of Theorem 3.5.

(1) This is easy.

(2) In this case $\alpha = \zeta_m^j\sqrt{b}$ and thus $\boldsymbol{Q}(\alpha^2) = \boldsymbol{Q}(\zeta_m^{2j}) = \boldsymbol{Q}(\zeta_m)$. Consequently, $2 \| m$ and $\sqrt{b} \notin \boldsymbol{Q}(\zeta_m)$.

Conversely, if $2 \| m$ and $\sqrt{b} \notin \boldsymbol{Q}(\zeta_m)$, then $\boldsymbol{Q}(\zeta_m \sqrt{b})$ is an extension of $\boldsymbol{Q}(\zeta_m)$ of degree exactly 2.

(3) In this case, $\alpha = \zeta_m^j \sqrt{b}$, $s = 1$ and $\boldsymbol{Q}(\alpha) = \boldsymbol{Q}(\zeta_m)$. Thus $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$. If also $\sqrt{b} \notin \boldsymbol{Q}(\zeta_{m/2})$, then by Lemma 4.3 (A), $\boldsymbol{Q}(\zeta_m \sqrt{b}) = \boldsymbol{Q}(\zeta_{m/2})$. Thus $(j, m) = d \neq 1$. Consequently, $\boldsymbol{Q}(\zeta_m) = \boldsymbol{Q}(\zeta_{m/d}\sqrt{b}) = \boldsymbol{Q}(\zeta_{m/d}, \sqrt{b})$ is an extension of degree 2 over $\boldsymbol{Q}(\zeta_{m/d})$. This can happen only when $d = 2$ or 3. If $d = 3$, then by Lemma 4.2 $\boldsymbol{Q}(\zeta_{m/3}\sqrt{b}) = \boldsymbol{Q}(\zeta_{m/2})$ which is a contradiction. On the other hand, if $d = 2$, then $\boldsymbol{Q}(\zeta_{m/2}\sqrt{b}) = \boldsymbol{Q}(\zeta_m)$. This and Lemma 4.3 (B) then implies $4 \| m$.

Conversely, suppose $\sqrt{b} \in \boldsymbol{Q}(\zeta_{m/2})$. Then $\boldsymbol{Q}(\zeta_m \sqrt{b})$ is an extension of $\boldsymbol{Q}(\zeta_{m/2})$ and $\boldsymbol{Q}(\zeta_m \sqrt{b}) = \boldsymbol{Q}(\zeta_{m/2}, \zeta_m \sqrt{b}) = \boldsymbol{Q}(\zeta_{m/2}, \zeta_m) = \boldsymbol{Q}(\zeta_m)$. Thus $\alpha = \zeta_m \sqrt{b}$ generates the splitting field of $x^m - b^{m/2}$ which is therefore p.n. (partially normal) with $s = 1$. On the other hand, suppose $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$, $\sqrt{b} \notin \boldsymbol{Q}(\zeta_{m/2})$ and $4 \| m$. Then by Lemma 4.3 (B), $\boldsymbol{Q}(\zeta_{m/2}\sqrt{b}) = \boldsymbol{Q}(\zeta_m)$ so that $x^m - b^{m/2}$ is p.n. with $s = 1$.

(4) If $\alpha = \zeta_m^j \zeta_{2m} \sqrt{b}$ generates the splitting field of $x^m + b^{m/2}$ with $\boldsymbol{Q}(\alpha) = \boldsymbol{Q}(\zeta_m)$, then clearly $\sqrt{b} \in \boldsymbol{Q}(\zeta_{2m})$ and $\sqrt{b} \notin \boldsymbol{Q}(\zeta_m)$.

Conversely, suppose $\sqrt{b} \in \boldsymbol{Q}(\zeta_{2m})$ and $\sqrt{b} \notin \boldsymbol{Q}(\zeta_m)$. Then by Lemma 4.3 (A), $\boldsymbol{Q}(\zeta_{2m}\sqrt{b}) = \boldsymbol{Q}(\zeta_m)$. Hence $x^m + b^{m/2}$ is p.n. with $s = 1$.

(5) Suppose that $\alpha = \zeta_m^j \zeta_{2m} \sqrt{b}$ generates the splitting field of $x^m + b^{m/2}$ and $\boldsymbol{Q}(\alpha^2) = \boldsymbol{Q}(\zeta_m^{2j}\zeta_m) = \boldsymbol{Q}(\zeta_m)$. Then either $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$ or $\sqrt{b} \notin \boldsymbol{Q}(\zeta_m)$. If the latter, then $\sqrt{b} \notin \boldsymbol{Q}(\zeta_{2m})$ also. For, if $\sqrt{b} \in \boldsymbol{Q}(\zeta_{2m})$ and $\notin \boldsymbol{Q}(\zeta_m)$, then by Lemma 4.3 (A) $\boldsymbol{Q}(\zeta_{2m}\sqrt{b}) = \boldsymbol{Q}(\zeta_m)$. It would then follow that $\boldsymbol{Q}(\alpha) = \boldsymbol{Q}(\zeta_m)$ contradicting the fact that $s = 2$. Thus either $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$ or $\sqrt{b} \notin \boldsymbol{Q}(\zeta_{2m})$.

Conversely, suppose $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$. Then $\boldsymbol{Q}(\zeta_{2m}\sqrt{b}) = \boldsymbol{Q}(\zeta_m, \zeta_{2m}\sqrt{b}) = \boldsymbol{Q}(\zeta_m, \zeta_{2m}) = \boldsymbol{Q}(\zeta_{2m})$. Thus $\alpha = \zeta_{2m}\sqrt{b}$ generates the splitting field of $x^m + b^{m/2}$ so that the latter is p.n. with $s = 2$.

On the other hand suppose that $\sqrt{b} \notin \boldsymbol{Q}(\zeta_{2m})$. Then $\boldsymbol{Q}(\zeta_{2m}\sqrt{b}) = \boldsymbol{Q}(\zeta_m, \zeta_{2m}\sqrt{b})$ is at most a quadratic extension of $\boldsymbol{Q}(\zeta_m)$. If, in fact, $\boldsymbol{Q}(\zeta_{2m}\sqrt{b}) = \boldsymbol{Q}(\zeta_m) \subsetneqq \boldsymbol{Q}(\zeta_{2m})$, then $\sqrt{b} \in \boldsymbol{Q}(\zeta_{2m})$. Thus $\boldsymbol{Q}(\zeta_{2m}\sqrt{b})$ is an extension of degree 2 of $\boldsymbol{Q}(\zeta_m)$. As a result, $x^m + b^{m/2}$ is p.n. with $s = 2$ with splitting field generated by $\zeta_{2m}\sqrt{b}$.

(6) In this case, $\alpha = \zeta_m^j \sqrt[4]{b}$ with $\boldsymbol{Q}(\zeta_m) = \boldsymbol{Q}(\alpha^2) = \boldsymbol{Q}(\zeta_{m/2}^j \sqrt{b})$. Thus $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$. Furthermore, $\sqrt{b} \notin \boldsymbol{Q}(\zeta_{m/2})$ and $4 \| m$ using a slight variation on the argument of Lemma 4.3 (B).

Conversely, suppose $4 \| m$, $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$ and $\sqrt{b} \notin \boldsymbol{Q}(\zeta_{m/2})$. Thus by

Lemma 4.3 (B), $\boldsymbol{Q}(\zeta_{m/2}\sqrt{b}) = \boldsymbol{Q}(\zeta_m)$. Thus $\alpha = \zeta_m\sqrt[4]{b}$ generates the splitting field of $x^m - b^{m/4}$ forcing the latter to be p.n. with $s = 2$.

(7) If $x^m + b^{m/4}$ is p.n. with $s = 2$, then $\alpha = \zeta_m^j\zeta_{2m}\sqrt[4]{b}$ and $\boldsymbol{Q}(\zeta_m) = \boldsymbol{Q}(\alpha^2) = \boldsymbol{Q}(\zeta_{m/2}^j\zeta_m\sqrt{b})$. Thus $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$. We claim also that $\sqrt{b} \in \boldsymbol{Q}(\zeta_{m/2})$. For, if not, then by Lemma 4.3 (A), $\zeta_m\sqrt{b} \in \boldsymbol{Q}(\zeta_{m/2})$. It follows from this that

$$\begin{aligned}\boldsymbol{Q}(\zeta_m) &= \boldsymbol{Q}(\zeta_{m/2}^j\zeta_m\sqrt{b}) \\ &= \boldsymbol{Q}(\zeta_{m/2}, \zeta_m\sqrt{b}) \\ &= \boldsymbol{Q}(\zeta_{m/2})\end{aligned}$$

contradicting the fact that $4|m$.

Conversely, suppose that $\sqrt{b} \in \boldsymbol{Q}(\zeta_{m/2})$. Then $\zeta_{2m}\sqrt[4]{b}$ is a root of $x^2 - \zeta_m\sqrt{b}$ over $\boldsymbol{Q}(\zeta_m)$ and, therefore, $\boldsymbol{Q}(\zeta_m, \zeta_{2m}\sqrt[4]{b})$ is an extension of degree 2 over $\boldsymbol{Q}(\zeta_m)$. Furthermore, $\boldsymbol{Q}(\zeta_m\sqrt{b}) = \boldsymbol{Q}(\zeta_m)$ or $\boldsymbol{Q}(\zeta_{m/2})$. The latter cannot happen by Lemma 4.3 (A). Thus $\zeta_{2m}\sqrt[4]{b}$ generates the splitting field of $x^m + b^{m/4}$ with $s = 2$.

(8) If $\alpha = \zeta_m^j\sqrt[6]{b}$ generates the splitting field of $x^m - b^{m/6}$ with $\boldsymbol{Q}(\alpha^3) = \boldsymbol{Q}(\zeta_m)$, then $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$. Moreover, $\sqrt{b} \notin \boldsymbol{Q}(\zeta_{m/3})$ since otherwise $\boldsymbol{Q}(\alpha^3) = \boldsymbol{Q}(\zeta_{m/3}^j\sqrt{b}) \subseteqq \boldsymbol{Q}(\zeta_{m/3})$. It follows from this that $3\|m$. Furthermore, if $4|m$ then $[\boldsymbol{Q}(\zeta_m): \boldsymbol{Q}(\zeta_{m/6})] = 4$. But $[\boldsymbol{Q}(\alpha^3): \boldsymbol{Q}(\zeta_{m/6})]$ is at most 2. Thus also $2\|m$.

Conversely, suppose $2\|m$, $3\|m$, $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$ and $\sqrt{b} \notin \boldsymbol{Q}(\zeta_{m/3})$. Then Lemma 4.2 (B) applies and $\boldsymbol{Q}(\zeta_{m/3}\sqrt{b}) = \boldsymbol{Q}(\zeta_m)$. Finally, $\boldsymbol{Q}(\zeta_m\sqrt[6]{b})$ is of degree 3 over $\boldsymbol{Q}(\zeta_m)$. Thus $\zeta_m\sqrt[6]{b}$ generates the splitting field of $x^m - b^{m/6}$ with $s = 3$.

(9) If $\alpha = \zeta_m^j\zeta_{2m}\sqrt[6]{b}$ generates the splitting field of $x^m + b^{m/6}$ with $\boldsymbol{Q}(\alpha^3) = \boldsymbol{Q}(\zeta_m)$, then clearly $\sqrt{b} \notin \boldsymbol{Q}(\zeta_m)$ and $\sqrt{b} \in \boldsymbol{Q}(\zeta_{2m})$. Furthrmore, $\sqrt{b} \notin \boldsymbol{Q}(\zeta_{2m/3})$ for, if otherwise, then

$$\boldsymbol{Q}(\zeta_m) = \boldsymbol{Q}(\alpha^3) = \boldsymbol{Q}(\zeta_{m/3}^j\zeta_{2m/3}\sqrt{b}) \subseteqq \boldsymbol{Q}(\zeta_{2m/3})$$

—clearly a contradiction.

Conversely, suppose $\sqrt{b} \in \boldsymbol{Q}(\zeta_{2m})$, $\sqrt{b} \notin \boldsymbol{Q}(\zeta_m)$ and $\sqrt{b} \notin \boldsymbol{Q}(\zeta_{2m/3})$. Then Lemma 4.2 (A) applies and

$$\boldsymbol{Q}(\zeta_{2m/3}\sqrt{b}) = \boldsymbol{Q}(\zeta_m)\ .$$

Thus $x^m + b^{m/6}$ is p.n. with $\alpha = \zeta_{2m}\sqrt[6]{b}$. Since $\boldsymbol{Q}(\zeta_{2m}\sqrt[6]{b})$ is of degree 3 over $\boldsymbol{Q}(\zeta_m)$, $s = 3$.

This completes the proof of the theorem.

We conclude this section with an example.

Lest one suspect that, if $x^m - b$ is partially normal, its splitting field can always be generated by $\alpha = \zeta_m \sqrt[m]{b}$, consider the polynomial $x^{12} - 3^6$. According to Theorem 3.5 (3), this polynomial is partially normal with s $= 1$, $q = 2$ and generating root $\zeta_{12}^j\sqrt{3}$ for some positive integer j. Thus $\mathbf{Q}(\zeta_{12}^j\sqrt{3}) = \mathbf{Q}(\zeta_{12})$. If $(j, 12) = 2$, then by Lemma 4.3 (B), $\mathbf{Q}(\zeta_{12}^j\sqrt{3}) = \mathbf{Q}(\zeta_{12})$ follows. However, if $(j, 12) = 1$, $\zeta_{12}^j\sqrt{3} = (\pm\zeta_4)(\pm\zeta_3)\sqrt{3} = (\pm 1/2)i(-1 + \sqrt{-3})\sqrt{3} = (\pm 1/2)(\sqrt{-3} + 3)$. Thus $\mathbf{Q}(\zeta_{12}^j\sqrt{3}) = \mathbf{Q}(\zeta_3)$. Consequently, $\zeta_{12}\sqrt{3}$ is not a generating root for $x^{12} - 3^6$ but $\zeta_6\sqrt{3}$ is!

6. Galois groups of partially normal binomials.

In this section we will determine the Galois groups of the binomials listed in Theorem 3.5. We will assume the known facts about the Galois group of $\mathbf{Q}(\zeta_n)$ (see [4], Chapter 8): that $G(\mathbf{Q}(\zeta_{p^n}))$ is cyclic of order $(p - 1)p^{n-1}$ for p an odd prime and that $G(\mathbf{Q}(\zeta_{mn})) = G(\mathbf{Q}(\zeta_m)) \times G(\mathbf{Q}(\zeta_n))$ wherever $(n, m) = 1$. We will also assume the Galois theoretic fact ([4] p. 196) that if A and B are two Galois extensions of C with groups G and H respectively, then the group (over C) of the compositum AB is $G \times H$ iff $A \cap B = C$.

The following theorem determines the groups of the binomials of 3.5 except cases (6) and (7) (which will be treated separately).

THEOREM 6.1. *Let $G(x^m - a)$ denote the group of the partially normal binomial $x^m - a$ over $\mathbf{Q}$. Then the following are the Galois groups numbered according to the scheme of* 3.5:

(1) $G(x^m - b^m) \cong G(x^m - 1)$; $G(x^m + b^m) \cong G(x^{2m} - 1)$.
(2) $G(x^m - b^{m/2}) \cong G(x^{2m} - 1)$.
(3) $G(x^m - b^{m/2}) \cong G(x^m - 1)$.
(4) $G(x^m + b^{m/2}) \cong G(x^m - 1)$.
(5) $G(x^m + b^{m/2}) \cong G(x^{2m} - 1)$.
(8) $G(x^m - b^{m/6}) \cong S_3 \times G(x^m - 1)$.
(9) $G(x^m + b^{m/6}) \cong S_3 \times G(x^{m/3} - 1)$.

Here S_3 denotes the symmetric group on 3 *letters.*

Proof. (1), (3) and (4) are clear.

(2) In this case, $\mathbf{Q}(\alpha) = \mathbf{Q}(\zeta_m\sqrt{b}) = \mathbf{Q}(\zeta_m, \sqrt{b})$. Since $\sqrt{b} \notin \mathbf{Q}(\zeta_m)$, the group of $\mathbf{Q}(\alpha)$ is isomorphic to $\mathbf{Z}_2 \times G(x^m - 1)$ which, since $2 \| m$, is isomorphic to $G(x^{2m} - 1)$.

(5) For this case, either $\sqrt{b} \in \mathbf{Q}(\zeta_m)$ or $\sqrt{b} \notin \mathbf{Q}(\zeta_{2m})$. In the first instance, $\mathbf{Q}(\alpha) = \mathbf{Q}(\zeta_{2m}\sqrt{b}) = \mathbf{Q}(\zeta_m, \zeta_{2m}\sqrt{b}) = \mathbf{Q}(\zeta_m, \zeta_{2m}) = \mathbf{Q}(\zeta_{2m})$. Thus the group is $G(x^{2m} - 1)$. In the second, let $m = 2^k q$, q odd. Then

$\boldsymbol{Q}(\alpha) = \boldsymbol{Q}(\zeta_{2m}\sqrt{b}) = \boldsymbol{Q}(\zeta_q, \zeta_{2^k}, \zeta_{2^{k+1}}\sqrt{b})$. Thus the group of $\boldsymbol{Q}(\alpha)$ is isomorphic to $G(x^q - 1) \times G(\boldsymbol{Q}(\zeta_{2^k}, \zeta_{2^{k+1}}\sqrt{b}))$. The second factor is $G(x^{2^k} + b^{2^{k-1}})$ which for $k \geqq 3$ is isomorphic, by ([4], Theorem 9), to $\boldsymbol{Z}_2 \times \boldsymbol{Z}_{2^{k-1}}$. For $k = 1, 2$ it is easy to check that the same result holds. Hence $G(x^m + b^{m/2}) \cong G(x^{2m} - 1)$ in the second instance also.

(8) Since in this case $2 \| m$, $3 \| m$, and $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$, we have $\boldsymbol{Q}(\alpha) = \boldsymbol{Q}(\zeta_m, \sqrt[6]{b}) = \boldsymbol{Q}(\zeta_m, (\sqrt[3]{b})^{-1}\sqrt{b}) = \boldsymbol{Q}(\zeta_m, \sqrt[3]{b}) = \boldsymbol{Q}(\zeta_{m/3}, \zeta_3, \sqrt[3]{b})$. Thus since $\boldsymbol{Q}(\zeta_{m/3}) \cap \boldsymbol{Q}(\zeta_3, \sqrt[3]{b}) = \boldsymbol{Q}$ and $\boldsymbol{Q}(\zeta_3, \sqrt[3]{b})$ has group S_3, we conclude that $G(x^m - b^{m/6}) \cong S_3 \times G(x^{m/3} - 1)$.

(9) If $x^m + b^{m/6}$ is p.n., then $\alpha = \zeta_{2m}\sqrt[6]{b}$ and therefore $\zeta_m \sqrt[3]{b} \in \boldsymbol{Q}(\alpha)$. Since also $\zeta_m \in \boldsymbol{Q}(\alpha)$, we must have that $\sqrt[3]{b} \in \boldsymbol{Q}(\alpha)$. Consequently, $\boldsymbol{Q}(\zeta_3, \sqrt[3]{b}) \subset \boldsymbol{Q}(\alpha)$. Furthermore, $\boldsymbol{Q}(\zeta_3, \sqrt[3]{b}) \cap \boldsymbol{Q}(\zeta_{m/3}) = \boldsymbol{Q}$ and $[\boldsymbol{Q}(\zeta_3, \sqrt[3]{b}) : \boldsymbol{Q}] \cdot [\boldsymbol{Q}(\zeta_{m/3}) : \boldsymbol{Q}] = 3 \cdot \phi(m)$ since $3 \| m$. Hence $\boldsymbol{Q}(\alpha) = \boldsymbol{Q}(\zeta_{m/3}, \zeta_3, \sqrt[3]{b})$ with Galois group $S_3 \times G(x^{m/3} - 1)$.

The remainder of this section will be devoted to calculating the groups of (6) and (7) of 3.5. To do this we will use the following lemma and its corollaries.

LEMMA 6.2. *Let a and b be relatively prime square free integers. Suppose that A and B are cyclic fields of degrees 2^i and 2^j over $A \cap B = \boldsymbol{Q}$ such that $\sqrt{a} \in A$, $\sqrt{b} \in B$. If $i \leqq j$, then there is a cyclic field C of degree 2^i over $\boldsymbol{Q}$ with $\sqrt{ab} \in C$, $CB = AB$ and $C \cap B = \boldsymbol{Q}$.*

Proof. Let G_A, G_B be the groups of A, B respectively. Then the group of AB is $G_A \times G_B$. If σ, τ generates G_A, G_B respectively, then $\sigma(\sqrt{a}) = -\sqrt{a}$ and $\tau(\sqrt{b}) = -\sqrt{b}$. The subgroup H of $G_A \times G_B$ generated by (σ, τ) is cyclic of order 2^j and fixes $\sqrt{ab}$. Let C be the fixed field of H. Then $\sqrt{ab} \in C$, $G_A \times H = G_A \times G_B$, C has group G_A and the fixed field of G_A is B with group $H \cong G_B$. The lemma follows.

COROLLARY 6.3. *Let $a_1, \cdots, a_n$ be pairwise relatively prime square free integers, K_i a cyclic field of degree 2^{j_i} with $\sqrt{a_i} \in K_i$ $(i = 1, \cdots, n)$ arranged so that $j_1 \leqq j_2 \leqq \cdots \leqq j_n$. Assume that $K_i \cap K_j = \boldsymbol{Q}$ whenever $i \neq j$. Then there exists a cyclic field K_0 of degree 2^{j_1} with $\sqrt{a_1 a_2 \cdots a_n} \in K_0$ and a field K such that $K_0 \cap K = \boldsymbol{Q}$ and $K_0 K = K_1 K_2 \cdots K_n$.*

Proof. Use the lemma and induction on n: successively construct pairs of fields J_i, L_i such that J_i is cyclic of degree 2^{j_1} containing $\sqrt{a_1 a_2 \cdots a_i}$, $J_i \cap L_i = Q$ and $J_i L_i = K_1 K_2 \cdots K_i$. Then $K_0 = J_n$, $K = L_n$ satisfy the conclusion of the corollary.

COROLLARY 6.4. *Let m and b be positive integers such that m is odd and b is square free. Let $b = p_1 p_2 \cdots p_n$ be the prime factorization of b and, for $i = 1, \cdots, n$, let j_i be the positive integer such that $2^{j_i} \| p_i - 1$. By relabelling, if necessary, assume that $j_1 \leqq j_2 \leqq \cdots \leqq j_n$. Then, if $\sqrt{b} \in \boldsymbol{Q}(\zeta_m)$, there exist subfields F_0, F of $\boldsymbol{Q}(\zeta_m)$ such that F_0 is cyclic of degree 2^{j_1}, $\sqrt{b} \in F_0$, $F_0 \cap F = \boldsymbol{Q}$ and $F_0 F = \boldsymbol{Q}(\zeta_m)$.*

Proof. By Lemma 4.1, $b \mid m$. Let d be the largest divisor of m relatively prime to b. Then $G(x^m - 1) = G(x^d - 1) \times G(x^{m/d} - 1)$. Let $G = G(x^{m/d} - 1)$, G_2 its Sylow 2-subgroup, and G_1, the direct product of its Sylow p-subgroups, p an odd prime. Then $G = G_2 \times G_1$. Let J_2, J_1, be the fixed fields of G_1, G_2 respectively. It is easy to see that $\sqrt{b} \in J_2$ and that J_2 is the compositum of pairwise linearly disjoint cyclic fields K_i with $\sqrt{\pm p_i} \in K_i$ and $[K_i : \boldsymbol{Q}] = 2^{j_i} (i = 1, \cdots, n)$. The hypotheses of Corollary 6.3 are thus satisfied so that we can find K_0, $K \subset J_2$ with K_0 cyclic of degree 2^{j_1}, $K_0 \cap K = \boldsymbol{Q}$ and $K_0 K = J_2$.

The corollary follows with $F_0 = K_0$ and $F = K J_1 \boldsymbol{Q}(\zeta_d)$.

We can now compute the group of case (6) of Theorem 3.5.

THEOREM 6.5. *Let $x^m - b^{m/4}$ be a partially normal binomial of type* (6). *Let D_4 denote the dihedral group on four letters. Then there exists a direct cyclic factor H of $G(x^{m/4} - 1)$ of order* 2 *such that $G(x^m - b^{m/4}) \cong D_4 \times (G(x^{m/4} - 1)/H)$.*

Proof. Let $m = 4q$ with q odd. Then

$$\boldsymbol{Q}(\alpha) = \boldsymbol{Q}(\zeta_{4q} \sqrt[4]{b}) = \boldsymbol{Q}(\zeta_q, \zeta_4, \sqrt[4]{b}) .$$

By Theorem 3.5, $\sqrt{b} \in \boldsymbol{Q}(\zeta_{4q})$ but $\sqrt{b} \notin \boldsymbol{Q}(\zeta_q)$. Thus $\sqrt{-b} \in (\zeta_q)$ and $\boldsymbol{Q}(\zeta_q) \cap \boldsymbol{Q}(\zeta_4, \sqrt[4]{b}) = \boldsymbol{Q}(\sqrt{-b})$. By Lemma 4.1 the integer j_1 of Corollary 6.4 must be 1. Hence, by the same corollary, there is a field $F \subset \boldsymbol{Q}(\zeta_q)$ with $\boldsymbol{Q}(\sqrt{-b}) \cdot F = \boldsymbol{Q}(\zeta_q)$ and $\boldsymbol{Q}(\sqrt{-b}) \cap F = \boldsymbol{Q}$. Thus $\boldsymbol{Q}(\alpha) = F \cdot \boldsymbol{Q}(\zeta_4, \sqrt[4]{b})$ and $F \cap \boldsymbol{Q}(\zeta_4, \sqrt[4]{b}) = \boldsymbol{Q}$. The theorem follows.

We now turn to case (7) of Theorem 3.5. Let $p(x) = x^{2^k m} + b^{2^{k-2} m}$ be a fixed partially normal binomial with m odd, b a square free integer and $k \geqq 2$. Thus, by 3.5, $\sqrt{b} \in \boldsymbol{Q}(\zeta_{2^{k-1} m})$ and $\alpha = \zeta_{2^{k+1} m} \sqrt[4]{b}$. It is clear that $\boldsymbol{Q}(\alpha) = \boldsymbol{Q}(\zeta_m, \zeta_{2^{k+1}} \sqrt[4]{b})$.

To compute $G(p(x))$, let $b = 2^{\varepsilon_0} b_1$ where $\varepsilon_0 = 0$ or 1 and b_1 is odd. Let $\delta = 0$ or 1 so that $i^{\delta} \sqrt{b_1} \in \boldsymbol{Q}(\zeta_m)$ (by 4.1). Then by Corollary 6.4

there are fields F_0, $F \subset \boldsymbol{Q}(\zeta_m)$ so that $F_0F = \boldsymbol{Q}(\zeta_m)$, $G(\boldsymbol{Q}(\zeta_m)) = G(F_0) \times G(F)$, F_0 is cyclic of degree 2^{j_1} and $i^\delta\sqrt{b_1} \in F_0$. Thus it is easy to see that $G(p(x)) = G(F_0(\zeta_{2^{k+1}}\sqrt[4]{b})) \times G(F)$. Since $G(F)$ can be computed from 6.4, it is sufficient to determine $G(F_0(\zeta_{2^{k+1}}\sqrt[4]{b}))$.

Let $\beta = \zeta_{2^{k+1}}\sqrt[4]{b}$. We know that $F_0(\beta)$ is an extension of degree 2 over $F_0(\zeta_{2^k})$ so that there is an automorphism σ of $F_0(\beta)$ such that $\sigma(\beta) = -\beta$ with fixed field $F_0(\zeta_{2^k})$. On the other hand, the group of $F_0(\zeta_{2_k})$ is the direct product of cyclic groups of orders 2^{j_1}, 2, 2^{k-2} with respective generators ρ, σ_1, σ_2. Denoting by the same letters extensions of these generators to $F_0(\beta)$, we have that the group G' of $F_0(\beta)$ is generated by σ, ρ, σ_1, σ_2. On $F_0(\zeta_{2^k})$ these generators are defined by

$$\begin{aligned}
&\rho(\zeta_{2^k}) = \zeta_{2^k},\ \rho(\sqrt{b}) = (-1)^{\varepsilon_1}\sqrt{b}\,;\\
&\sigma_2 | F_0 = 1,\ \sigma_2(\zeta_{2^k}) = \zeta_{2^k}^{-1},\ \sigma_2(\sqrt{b}) = \sqrt{b}\,;\\
&\sigma_1 | F_0 = 1,\ \sigma(\zeta_{2^k}) = \zeta_{2^k}^5,\ \sigma_1(\sqrt{b}) = (-1)^{\varepsilon_0}\sqrt{b}
\end{aligned}$$

where ε_0 is as defined above and $\varepsilon_1 = 1$ if b is odd or $\varepsilon_0 = 1$ and $b/2 > 1$ and 0 otherwise. To see how ρ, σ_1, σ_2 may be extended to $F_0(\beta)$, it is sufficient to determine how they act on β:

$$\begin{aligned}
\rho(\beta) &= i^{\varepsilon_1}\beta\ ,\\
\sigma_1(\beta) &= \zeta_{2^k} i^{\varepsilon_0}\beta\ ,\\
\sigma_2(\beta) &= \zeta_{2^k}^{-1}\beta\ .
\end{aligned}$$

From these formulas, it is a straightforward matter to determine relations amongst the generators σ, ρ, σ_1, and σ_2. For one, $\sigma_1^{2^{k-2}} = \sigma$. We summarize the rest in the following.

THEOREM 6.6. *The group $G(x^{2^k m} + b^{2k-1}m)$ is isomorphic to the direct product of an abelian group $G(F)$ with a nonabelian group G' of order 2^{j_1+k} generated by ρ, σ_1, σ_2 and satisfying the following relations*:

$$(*)\qquad \begin{aligned}
&\sigma_2^{2^{k-1}} = \sigma_2^2 = \rho^a = 1 \quad (\text{where } a = \max(2^{j_1}, 4^{\varepsilon_1}))\ ,\\
&\sigma_1\sigma_2 = \sigma_1^{\varepsilon_0 2^{k-2}+1}\sigma_2\ ,\\
&\sigma_2\rho = \rho\sigma_2\sigma_1^{\varepsilon_1 2^{k-2}}\ ,\\
&\sigma_1\rho = \rho\sigma_1\ .
\end{aligned}$$

In particular,

(a) *if $\varepsilon_1 = 0$, then $j_1 = 0$ and $G(F) = G(x^m - 1)$; furthermore G' is isomorphic to a group generated by σ_1, σ_2, satisfying relations $\sigma_1^{2^{k-1}} = \sigma_2^2 = 1$, $\sigma_2\sigma_1 = \sigma_1^{2^{k-2}+1}\sigma_2$;*

(b) *if* $\varepsilon_0 = \varepsilon_1 = 1$ *and* $j_1 \geqq k - 1$, *then* $G(p(x))$ *is isomorphic to* $G(x^m - 1) \times \langle \sigma_1, \sigma_2 \rangle$.

Proof. The relations (*) are easily determined from the discussion preceeding the theorem. Part (a) follows from(*) and the fact that $b = 2$ in this case. Finally, (b) follows from (*) by setting $\tau = \rho\sigma_1$. Then $\sigma_2\tau = \tau\sigma_2$ and τ is an element of order 2^{j_1}. By Corollary 6.4, $\langle \tau, G(F) \rangle \cong G(x^m - 1)$. Furthermore, $\langle \tau \rangle \cap \langle \sigma_1, \sigma_2 \rangle = \{1\}$ and thus $G(p(x)) \cong \langle \sigma_1, \sigma_2 \rangle \times G(x^m - 1)$.

References

1. Giulio Darbi, *Sulla riducibilità delle equazione algebriche*, Annali di Mat. pur. e appl., Ser. 4, **4** (1926), 185-208.
2. Lisl. Gaal, *Classical Galois Theory*, Chelsea, New York, 1973.
3. D. Gay, *On normal radical extensions of real fields*, to appear, Acta Arithmetica, **35** (1978).
4. Serge Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965.
5. Henry B. Mann and William Yslas Vélez, *On normal radical extensions of the rationals*, J. of Lin. and Multilin. Alg., **3** (1975), 73-80.
6. M. J. Norris and W. Y. Vélez, *Structure theorems for radical extensions of fields*, Sandia Laboratories Appl. Math. Report, 1976.
7. A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arithmetica, **32** (1977), 245-274.
8. N. G. Tschebotarev and H. Schwerdtfeger, *Grundzüge der Galoischen Theorie*, Groningen-Djakarta, 1950.

Received December 9, 1976. The first author was supported in part by the Fonds National Suisse and Battelle Institute Grant No: 333-205. The third author was supported in part by a fellowship from the Ford Foundation and by the U.S. Energy and Research Development Administration (ERDA).

University of Arizona,
Tuscon, AZ 85721
and
New College
Sarasota, FL 33580
and
Sandia Laboratories
Albuquerque, NM 87115