COMMUNICATIONS IN ALGEBRA®
Vol. 31, No. 10, pp. 4745–4763, 2003

The 2-Power Degree Subfields of the Splitting Fields of Polynomials with Frobenius Galois Groups

Blair K. Spearman,[1] Kenneth S. Williams,[2,*] and Qiduan Yang[1]

[1]Department of Mathematics and Statistics, Okanagan University College, Kelowna, British Columbia, Canada
[2]School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, Canada

ABSTRACT

Let $f(x)$ be an irreducible polynomial of odd degree $n > 1$ whose Galois group is a Frobenius group. We suppose that the Frobenius complement is a cyclic group of even order h. Let $2^t\ h$. For each $i = 1, 2, \ldots, t$ we show that the splitting field L of $f(x)$ has exactly one subfield K_i with $[K_i : \mathbb{Q}] = 2^i$. These subfields form a tower of normal extensions $\mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_t$ with $[K_i : K_{i-1}] = 2\ (i = 1, 2, \ldots, t)$ and $K_0 = \mathbb{Q}$. Our main result in this paper is an explicit formula for an element α_i in K_{i-1} such that $K_i = \mathbb{Q}(\sqrt{\alpha_i})\ (i = 1, 2, \ldots, t)$. This result is applied to DeMoivre's quintic $x^5 - 5ax^3 + 5a^2x - b$, solvable

*Correspondence: Kenneth S. Williams, School of Mathematics and Statistics, Carleton University, Ottawa, Ontario K1S 5B6, Canada; E-mail: williams@math.carleton.ca.

DOI: 10.1081/AGB-120023130 0092-7872 (Print); 1532-4125 (Online)

quintic trinomials $x^5 + ax + b$, as well as to some numerical polynomials of degrees 5, 9, and 13.

Key Words: Frobenius group; Subfields of splitting field; Galois group.

1. INTRODUCTION

A finite group G is said to be a Frobenius group if there exists a transitive G-set X such that

$$\text{every } g \in G \setminus \{1\} \text{ has at most one fixed point} \tag{1}$$

and

$$\text{there is some } g \in G \setminus \{1\} \text{ that does not have a fixed point.} \tag{2}$$

It can be proved (Rotman, 2002, Proposition 8.161) that a finite group G is a Frobenius group if and only if it contains a proper nontrivial subgroup H such that

$$H \cap gHg^{-1} = \{1\} \quad \text{for all } g \notin H. \tag{3}$$

Such a subgroup H of G is called a Frobenius complement of G. Let

$$N = \{1\} \cup \left(G \setminus \left(\bigcup_{g \in G} gHg^{-1} \right) \right).$$

N is called the Frobenius kernel of G. Frobenius proved using character theory the following result (Rotman, 2002, Theorem 8.164):

Let G be a Frobenius group with complement H and kernel N. Then N is a normal subgroup of G with $N \cap H = \{1\}$ and $G = NH$. (4)

Furthermore, we have (Robinson, 1982, Ex. 8.5.6)

$$h \mid n - 1, \quad \text{where } h = |H| \text{ and } n = |N|. \tag{5}$$

By (4), G is the semi-direct product of N and H, written $G = N \rtimes H$. Note that there is a natural G-action on N: for σ in G, $\phi_\sigma(v) = \sigma v \sigma^{-1}$, $\nu \in N$. We state the following result without proof.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

The semi-direct product $G = N \rtimes H$ is a Frobenius group with kernel N and complement H if and only if the action of $H \setminus \{1\}$ on $N \setminus \{1\}$ is fixed-point free, that is, if $\sigma \in H$, $\upsilon \in N \setminus \{1\}$ and $\sigma\upsilon\sigma^{-1} = \upsilon$ imply $\sigma = 1$.

(6)

In this paper, we consider irreducible polynomials $f(x) \in \mathbb{Z}[x]$ with Galois group $G = \mathrm{Gal}(f)$ satisfying the following three conditions:

$G = N \rtimes H$ is a Frobenius group with kernel N and complement H, (7a)

H is a cyclic group with even degree h, hence N is abelian, (7b)

$\deg(f(x))$ is odd, greater than 1, and equal to n, the order of N. (7c)

In (7b) the fact that N is abelian follows from Robinson (1982, Ex. 10.5). We define the positive integer t by

$$2^t \parallel h, \tag{8}$$

and the odd positive integer h_1 by

$$h_1 = h/2^t. \tag{9}$$

We denote the splitting field of $f(x)$ by L so that

$$\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(f) = G = N \rtimes H.$$

For each $j = 1, 2, \ldots, t$ we show that L has exactly one subfield K_j with $[K_j : \mathbb{Q}] = 2^j$. These subfields form a tower of normal extensions $\mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_t$ with $[K_i : K_{i-1}] = 2$ $(i = 1, 2, \ldots, t)$ where $K_0 = \mathbb{Q}$. Our objective in this paper is to give an explicit element $\alpha_i \in K_{i-1}$ such that $K_i = \mathbb{Q}(\sqrt{\alpha_i})$ $(i = 1, 2, \ldots, t)$. This determination is given in Sec. 3 after some preliminary results are proved in Sec. 2. In Sec. 4 we apply our results to certain classes of polynomials.

Remark 1. Let K be a subfield of $\mathbb{C}$. Let $\theta_1, \theta_2, \ldots, \theta_n$ be the roots in $\mathbb{C}$ of $f(x) \in K[x]$. The discriminant of $f(x)$ is defined by

$$D_f = \prod_{\substack{i,j=1 \\ i<j}}^{n} (\theta_i - \theta_j)^2.$$

If the roots of $f(x)$ are distinct, we fix some ordering of the roots and view the Galois group G of $f(x)$ as a subgroup of the symmetric group S_n. Galois theory tells us that the field $K(\sqrt{D_f})$ is always a subfield of the splitting field of $f(x)$, and that G is a subgroup of the alternating group A_n if and only if $\sqrt{D_f} \in K$. Therefore the field extension $K(\sqrt{D_f})/K$ is quadratic if and only if G contains odd permutations on $\{\theta_1, \theta_2, \ldots, \theta_n\}$. In this paper, we shall see that when G is not contained in A_n, the quadratic extension K_1/K is reproducing $K(\sqrt{D_f})/K$. It is worth noting that even when G is not a subgroup of A_n, a quadratic tower over K can still be constructed.

Definition 1. *Let $\theta_1, \theta_2, \ldots, \theta_n$ be the roots in $\mathbb{C}$ of $f(x) \in K[x]$. The discriminant polynomial of $f(x)$ is defined to be*

$$g(x) = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (x - (\theta_i - \theta_j)). \tag{10}$$

It is clear that $g(x) \in K[x]$ and $\deg g(x) = n(n-1)$.

We now state our main result.

Theorem. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial. Let the roots of $f(x)$ in $\mathbb{C}$ be $\theta_1, \theta_2, \ldots, \theta_n$. Let $L = \mathbb{Q}(\theta_1, \theta_2, \ldots, \theta_n)$ be the splitting field of $f(x)$, and $G = \mathrm{Gal}(f) = \mathrm{Gal}(L/\mathbb{Q})$ be the Galois group of $f(x)$. Assume that $f(x)$ and G satisfy the following four conditions:*

(a) *$G = N \rtimes H$ is a Frobenius group with kernel N and complement H.*
(b) *H is a cyclic group with even degree h.*
(c) $\deg(f(x))$ *is odd, greater than* 1, *and equal to n the order of N.*
(d) *The discriminant polynomial of $f(x)$ is squarefree.*

Define t and h_1 as in (8) *and* (9) *respectively. Then L contains exactly one normal subfield K_j with $[K_j : \mathbb{Q}] = 2^j$ for each $j = 1, 2, \ldots, t$. These subfields satisfy*

$$\mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_t \tag{11}$$

with $K_i/\mathbb{Q}$ a cyclic extension of degree 2^i for $i = 0, 1, \ldots, t$. Further, for $i = 0, 1, \ldots, t-1$,

$$g(x) = \prod_{j=1}^{2^i(n-1)/h} g_{ij}(x), \tag{12}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

where each $g_{ij}(x) \in K_i[x]$ *is monic, irreducible, of degree* $nh/2^i$, *and even. Finally, for any* $j \in \{1, 2, \ldots, 2^i(n-1)/h\}$, *we have*

$$K_{i+1} = \mathbb{Q}(\sqrt{g_{ij}(0)}), \quad \textit{for } i = 0, 1, 2, \ldots, t-2, \tag{13}$$

and

$$K_t = \mathbb{Q}(\sqrt{-g_{t-1j}(0)}). \tag{14}$$

Remark 2. The existence of a quadratic tower of the form (11) follows from Galois theory. Let L^N be the subfield of L fixed by N. Then the Galois group of L^N over $\mathbb{Q}$, $\mathrm{Gal}(L^N/\mathbb{Q})$, is isomorphic to G/N, hence to H, which is cyclic of order $2^t h_1$. $\mathrm{Gal}(L^N/\mathbb{Q})$ has a unique sequence of subgroups (each of which is normal since $\mathrm{Gal}(L^N/\mathbb{Q})$ is abelian)

$$P_t \lhd P_{t-1} \lhd \cdots \lhd P_1 \lhd P_0 = \mathrm{Gal}(L^N/\mathbb{Q}),$$

such that $[P_{i-1} : P_i] = 2$, $i \in \{1, 2, \ldots, t\}$. Correspondingly, $G = \mathrm{Gal}(L^N/\mathbb{Q})$ has a unique sequence of normal subgroups

$$M_t \lhd M_{t-1} \lhd \cdots M_1 \lhd M_0 = G, \tag{15}$$

such that $[M_{i-1} : M_i] = 2$, $i \in \{1, 2, \ldots, t\}$, and $N \subseteq M_i$, $i \in \{0, 1, \ldots, t\}$, by the Correspondence Theorem (Rotman, 2002, Proposition 2.76). A quadratic tower of the form (11) thus exists in which each K_i is the fixed field of M_i for $i \in \{1, 2, \ldots, t\}$. Moreover, we claim that every subfield of L of degree 2^j over $\mathbb{Q}$ must be a field in this tower. Such a subfield, written as L^M, is fixed by a subgroup M of G such that $[G : M] = 2^j$, $j \in \{1, 2, \ldots, t\}$. We notice that $\frac{|MN|}{|M|}$ is a power of 2, as it is a factor of $[G : M]$. On the other hand $\frac{|MN|}{|M|} = \frac{|N|}{|M \cap N|}$ is odd since $|N|$ is odd. Hence $\frac{|MN|}{|M|} = 1$. This shows that $N \subseteq M$. Therefore M must be the subgroup M_j in (15) and it follows that the subfield L^M is the field K_j in (11). This implies the uniqueness of the tower (11). The following diagram illustrates the Galois correspondence between some subgroups of G and some subfields of L.

$$\begin{array}{ccccccccccccc} 1 & \lhd & N & \lhd & M_t & \lhd \cdots \lhd & M_2 & \lhd & M_1 & \lhd & M_0 = G \\ \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ L & \supset & L^N & \supset & K_t & \supset \cdots \supset & K_2 & \supset & K_1 & \supset & K_0 = \mathbb{Q} \end{array}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

2. SOME PRELIMINARY RESULTS

We recall and reorganize some basic facts about Frobenius groups in Cangelmi 2000 and Robinson (1982) for our purposes. Let $f(x) \in \mathbb{Z}[x]$ satisfy all the assumptions of the Theorem. Let $\{\theta_1, \theta_2, \dots, \theta_n\}$ be the roots of $f(x)$ in $\mathbb{C}$. We may replace $\mathbb{Q}$ by a number field K. For a fixed $i \in \{1, 2, \dots, n\}$, let H_i be the stabilizer of θ_i in G, that is, $H_i = \{\sigma \in G : \sigma(\theta_i) = \theta_i\}$. Then the subfield of the splitting field L fixed by H_i is $K(\theta_i)$. As $f(x)$ is irreducible over K, we have

$$[G : H_i] = [K(\theta_i) : K] = \deg(f(x)) = |N| = [G : H].$$

It follows that $|H_i| = |H|$, hence $N \cap H_i = \{1\}$, $i = 1, 2, \dots, n$, since $|H_i| = h$ and $|N| = n$ are coprime by (5). The natural projection $\sigma \in G \to \sigma N$ restricted to the subgroup H_i must be one-to-one because the kernel of the map is $N \cap H_i = \{1\}$. Therefore $H_i \cong G/N \cong H$ as groups. As G is transitive on the set $\{\theta_1, \theta_2, \dots, \theta_n\}$, for any $j \in \{1, 2, \dots, n\}$ with $j \neq i$ there exists $g \in G$ such that $g(\theta_i) = \theta_j$. Then the group gH_ig^{-1} (a conjugate of H_i) is the stabilizer H_j of the root θ_j. Thus H_i has exactly n conjugates including itself, and each of these fixes exactly one root of $f(x)$. The stabilizer of two distinct roots of $f(x)$ is the trivial subgroup $\{1\}$ of G, since $H_i \cap H_j = \{1\}$ for $i \neq j$. It is clear that (3) is satisfied and G is a Frobenius group with complement H_i for any $i \in \{1, 2, \dots, n\}$. From the orders of N, H_i and G, it is not hard to verify that

$$N = \{1\} \cup \left(G \setminus \left(\bigcup_{g \in G} gHg^{-1} \right) \right).$$

Thus N is the Frobenius kernel with respect to the complement H_i of G. The following is a summary of the above discussion.

Lemma 1. *Let $G = N \rtimes H$ be a Frobenius group serving as the Galois group of an irreducible polynomial $f(x)$ over a number field K, such that $\deg(f(x)) = n = |N|$. Let $\{\theta_1, \theta_2, \dots, \theta_n\}$ be the set of all roots of $f(x)$ in $\mathbb{C}$. Then*

(i) *$G = N \rtimes H_i$, where $H_i = \{\sigma \in G : \sigma(\theta_i) = \theta_i\}$, $i \in \{1, 2, \dots, n\}$.*
(ii) *The set $N \setminus \{1\}$ contains all elements in G that do not have a fixed point in $\{\theta_1, \theta_2, \dots, \theta_n\}$.*
(iii) *If $\sigma \in G$ and $\sigma(\theta_r) = \theta_r$, $\sigma(\theta_s) = \theta_s$ for $r, s \in \{1, 2, \dots, n\}$ with $r \neq s$, then $\sigma = 1$.*

The following result is an easy corollary of Lemma 1.

Proposition 1. *Keep the assumptions in Lemma* 1. *Let i be a fixed integer in* $\{1, 2, \ldots, n\}$. *If H is a cyclic group then there exists* $\alpha \in G$ *such that* $G = N \rtimes \langle\alpha\rangle$ *and* $\alpha(\theta_i) = \theta_i$.

Proof. The subgroup H_i is cyclic since $H_i \cong H$. Let α be a generator of H_i and the statement follows. □

Now we turn to some properties of the Frobenius kernel N.

Proposition 2. *For any* $i \in \{1, 2, \ldots, n\}$, *N is a complete set of left coset representatives of* H_i *in G.*

Proof. Assume that $\nu_1 \in N$, $\nu_2 \in N$ and $\nu_1 H_i = \nu_2 H_i$ so that $\nu_1^{-1}\nu_2 \in H_i$. Hence $\nu_1^{-1}\nu_2 = 1$ since $N \cap H_i = \{1\}$. Thus $\nu_1 = \nu_2$. The proposition now follows from the fact $|N| = [G : H_i]$. □

Proposition 3. *The Frobenius kernel N acts transitively on the set of roots* $\{\theta_1, \theta_2, \ldots, \theta_n\}$ *of* $f(x)$.

Proof. For r, $s \in \{1, 2, \ldots, n\}$, $r \neq s$, there exists $\sigma \in G$, such that $\sigma(\theta_r) = \theta_s$, since G acts transitively on the set $\{\theta_1, \theta_2, \ldots, \theta_n\}$. By Proposition 2, $\sigma \in \nu H_r$ for some $\nu \in N$. Thus $\sigma = \nu\eta$ for some $\eta \in H_r$. Now we have

$$\nu(\theta_r) = \nu\eta(\theta_r) = \sigma(\theta_r) = \theta_s,$$

completing the proof. □

Next we consider the subgroups of G of the form $N \rtimes \langle\alpha^{2^m}\rangle$, $m \in \{0, 1, 2, \ldots, t\}$.

Proposition 4. *For* $m \in \{0, 1, 2, \ldots, t\}$, *we have*

(i) $N \rtimes \langle\alpha^{2^m}\rangle$ *is a subgroup of G containing N.*
(ii) *The index of* $N \rtimes \langle\alpha^{2^m}\rangle$ *in G is* 2^m.
(iii) $N \rtimes \langle\alpha^{2^m}\rangle$ *acts transitively on* $\{\theta_1, \theta_2, \ldots, \theta_n\}$, *the set of roots of* $f(x)$.
(iv) $N \rtimes \langle\alpha^{2^m}\rangle$ *is a Frobenius group with Frobenius kernel N and complement* $\langle\alpha^{2^m}\rangle$.

Proof. (i) is obvious. (ii) follows from the calculations

$$[N \rtimes \langle\alpha\rangle : N \rtimes \langle\alpha^{2^m}\rangle] = \frac{|N||\alpha|}{|N||\alpha^{2^m}|} = \frac{h}{h/2^m} = 2^m.$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

To prove (iii) we notice that, by Proposition 3, N acts transitively on the set $\{\theta_1, \theta_2, \ldots, \theta_n\}$. So does $N \rtimes \langle \alpha^{2^m} \rangle$.

Now conditions (1) and (2) in Sec. 1 are satisfied when $\{\theta_1, \theta_2, \ldots, \theta_n\}$ is considered as the $N \rtimes \langle \alpha^{2^m} \rangle$-set. This proves (iv). $\square$

In Remark 2, we observed that $G = \mathrm{Gal}(L/\mathbb{Q})$ has a unique sequence of normal subgroups

$$M_t \lhd M_{t-1} \lhd \cdots \ M_1 \lhd M_0 = G,$$

such that $[M_{i-1} : M_i] = 2$, $i \in \{1, 2, \ldots, t\}$, and $N \subseteq M_i$, $i \in \{0, 1, 2, \ldots, t\}$. Combining this observation and Proposition 4, we obtain

Proposition 5.

(i) $M_m = N \rtimes \langle \alpha^{2^m} \rangle$, $m \in \{0, 1, 2, \ldots, t\}$.
(ii) K_m *is the subfield of* L *fixed by* $M_m = N \rtimes \langle \alpha^{2^m} \rangle$, $m \in \{0, 1, 2, \ldots, t\}$.

Proposition 6. *For* $r, s \in \{1, 2, \ldots, n\}$ *with* $r \neq s$, *there exists* $\tau \in G$ *such that* $\tau(\theta_r) = \theta_s$ *and* $\tau(\theta_s) = \theta_r$.

Proof. For any $i \in \{1, 2, \ldots, n\}$ the subgroup $H_i = \{\sigma \in G : \sigma(\theta_i) = \theta_i\}$ is cyclic of even order. Denote the unique element of order 2 in H_i by τ_i. If $\tau \in G$ is of order 2, then τ lies in H_i for some $i \in \{1, 2, \ldots, n\}$, since $G = (\bigcup_{i=1}^{n} H_i) \cup N$ and $|N|$ is odd. Thus $\tau = \tau_i$ for some i and $\{\tau_1, \tau_2, \ldots, \tau_n\}$ is the complete set of order 2 elements in G. Each τ_i ($i \in \{1, 2, \ldots, n\}$) fixes exactly one root θ_i of $f(x)$, hence τ_i is a product of $(n-1)/2$ transpositions. We point out that no two of these order 2 elements can have a transposition in common. Otherwise, say that the transposition (θ_r, θ_s), for some $r \neq s$, occurs in both τ_i and τ_j, for some $i \neq j$. Then

$$\tau_i\tau_j(\theta_r) = \tau_i(\theta_s) = \theta_r,$$
$$\tau_i\tau_j(\theta_s) = \tau_i(\theta_r) = \theta_s.$$

It follows from Lemma 1(iii) that $\tau_i\tau_j = 1$, hence $\tau_i = \tau_j$, a contradiction. Now assume that $r, s \in \{1, 2, \ldots, n\}$ and $r \neq s$. Then there are $(n-2)$ order 2 elements in G which fix neither θ_r nor θ_s. Let τ_k be such an order 2 element. Then $k \neq r$ and $k \neq s$. τ_k contains a transposition $(\theta_r, \tau_k(\theta_r))$, where $\tau_k(\theta_r) \in \{\theta_1, \theta_2, \ldots, \theta_n\} \setminus \{\theta_r, \theta_k\}$, which is a set of $(n-2)$ elements containing θ_s. Therefore there exists $\tau \in G$, such that $\tau(\theta_r) = \theta_s$ and $\tau(\theta_s) = \theta_r$. $\square$

In the rest of this section we assume the following set of conditions.

Condition Set.

(i) K is a subfield of $\mathbb{C}$ and $\theta_1, \theta_2, \ldots, \theta_n$ are the roots in $\mathbb{C}$ of an irreducible polynomial $f(x) \in K[x]$.
(ii) The discriminant polynomial of $f(x)$

$$g(x) = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} (x - (\theta_i - \theta_j))$$

is squarefree.
(iii) $L = K(\theta_1, \theta_2, \ldots, \theta_n)$ is the splitting field of $f(x)$.
(iv) $G^* = \mathrm{Gal}(L/K)$ is a Frobenius group with Frobenius kernel N and complement H^*, such that H^* is a cyclic group with order $|H^*| = 2^m h_1$, where m is a positive integer and h_1 is an odd positive integer.
(v) The degree of $f(x)$ is odd, greater than 1, and equal to n, the order of N.

Let $\bar{g}(x)$ be an irreducible factor of $g(x)$ over K. We have the following observations.

Proposition 7. *The group $G^* = \mathrm{Gal}(L/K)$ acts transitively on the set of roots of $\bar{g}(x)$. Moreover, G^* acts regularly on the set of roots of $\bar{g}(x)$, that is, the stabilizer of any root of $\bar{g}(x)$ in G^* is the trivial subgroup $\{1\}$.*

Proof. The first statement is clear. A root of $\bar{g}(x)$ is of the form $\theta_r - \theta_s$, for some $r \neq s$, $r, s \in \{1, 2, \ldots, n\}$. If $\sigma \in G^*$ and $\sigma(\theta_r - \theta_s) = \theta_r - \theta_s$, then $\sigma(\theta_r) = \theta_r$ and $\sigma(\theta_s) = \theta_s$, since $g(x)$ is squarefree. Thus $\sigma = 1$ by Lemma 1(iii). □

Corollary. *The degree of $\bar{g}(x)$ is equal to $|G^*|$.*

We note that the discriminant polynomial $g(x)$ is the polynomial $R(-1, f)(x)$ in Cangelmi (2000, p. 852). A more general treatment can be found in Cangelmi (2000, Theorem 3.1).

Proposition 8.

(i) *If $\theta_r - \theta_s$ is a root of $\bar{g}(x)$, for some $r, s \in \{1, 2, \ldots, n\}$ with $r \neq s$, so is $\theta_s - \theta_r$.*
(ii) *$\bar{g}(x) = h(x^2)$ for some $h(x) \in K[x]$.*

Proof. By Proposition 6, there exists $\tau \in G^*$, such that $\tau(\theta_r) = \theta_s$ and $\tau(\theta_s) = \theta_r$. Thus $\tau(\theta_r - \theta_s) = \theta_s - \theta_r$ is a root of $\bar{g}(x)$ if $\theta_r - \theta_s$ is a root of $\bar{g}(x)$. Over L, whenever $x - (\theta_r - \theta_s)$ is a linear factor of $\bar{g}(x)$, so is $x - (\theta_s - \theta_r)$. Therefore $\bar{g}(x)$ is a product of quadratic factors of the form $x^2 - (\theta_r - \theta_s)^2$ for some $r, s \in \{1, 2, \ldots, n\}$ with $r \neq s$. This proves (ii). □

We note that $d = |G^*|/2$ is the degree of $h(x)$. Next we label the roots $\xi_1, \ldots, \xi_d, \xi_{d+1}, \ldots, \xi_{2d}$ of $\bar{g}(x)$ in such a way that $\xi_k = -\xi_{k+d}$, $k = 1, 2, \ldots, d$. We observe that

$$\bar{g}(x) = \prod_{k=1}^{d}(x - \xi_k)(x + \xi_k) = \prod_{k=1}^{d}(x^2 - \xi_k^2),$$

$$\bar{g}(0) = (-1)^d \prod_{k=1}^{d} \xi_k^2,$$

$$h(x) = \prod_{k=1}^{d}(x - \xi_k^2),$$

$$D_h = \prod_{1 \le k < l \le d} (\xi_k^2 - \xi_l^2)^2.$$

Then we have

$$\begin{aligned} D_{\bar{g}} &= \prod_{1 \le k < l \le 2d} (\xi_k - \xi_l)^2 \\ &= \left[\prod_{1 \le k < l \le d} (\xi_k - \xi_l)^2\right]^2 \left[\prod_{k=1}^{d} (2\xi_k)^2\right] \left[\prod_{1 \le k < l \le d} (\xi_k + \xi_l)^2\right]^2 \\ &= \left[\prod_{1 \le k < l \le d} (\xi_k^2 - \xi_l^2)^2\right]^2 (2^{2d}) \prod_{k=1}^{d} \xi_k^2 \\ &= 2^{2d} D_h^2 (-1)^d \bar{g}(0). \end{aligned}$$

It follows that

$$\sqrt{D_{\bar{g}}} = \pm 2^d D_h \sqrt{(-1)^d \bar{g}(0)}.$$

Noting that $D_h \in K$ we have proved the following result.

Proposition 9. $K(\sqrt{D_{\bar{g}}}) = K(\sqrt{(-1)^d \bar{g}(0)})$, *where* $d = \frac{1}{2}|G^*| = \frac{1}{2}\deg(\bar{g}(x))$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Proposition 10. *Assume Condition Set holds. If $\bar{g}(x)$ is an irreducible factor of $g(x)$ over K, then the field extension $K(\sqrt{D_{\bar{g}}}) = K(\sqrt{(-1)^d \bar{g}(0)})$ over K has degree 2.*

Proof. It suffices to show that G^*, viewed as a permutation group on the roots of $\bar{g}(x)$, contains an odd permutation. Fix a root ξ of $\bar{g}(x)$. Then the map $\sigma \in G^* \mapsto \sigma\xi$ is a one-to-one correspondence from G^* onto the set of roots of $\bar{g}(x)$, by Proposition 7. Thus we just need an element of G^* acting as an odd permutation when G^* acts on itself by left multiplication. Let ρ be an element of H^* of order 2^m and μ be an element of H^* of order h_1. Then H^* is the direct product of the two cyclic subgroups generated by ρ and μ respectively. We also notice that $G^* = NH^* = H^*N$ since N is a normal subgroup of G^*. Thus each element in G^* can be represented uniquely as $\rho^i\mu^j\nu$ for some $\nu \in N$, $i \in \{0, 1, \ldots, 2^m - 1\}$ and $j \in \{0, 1, \ldots, h_1 - 1\}$. We now claim that left multiplication by ρ, denoted $\rho_L\colon \sigma \in G^* \mapsto \rho\sigma \in G^*$, serves as an odd permutation on the set G^*. For fixed $j \in \{0, 1, \ldots, h_1 - 1\}$ and $\nu \in N$, the action of ρ_L is $\rho^i\mu^j\nu \mapsto \rho^{i+1}\mu^j\nu$ for $i \in \{0, 1, \ldots, 2^m - 2\}$ and $\rho^{2^m-1}\mu^j\nu \mapsto \mu^j\nu$. Therefore the cycle of length 2^m

$$\pi_{j,\nu} = (\mu^j\nu, \rho\mu^j\nu, \rho^2\mu^j\nu, \ldots, \rho^{2^m-1}\mu^j\nu)$$

occurs in the representation of ρ_L as the product of disjoint cycles, and

$$\rho_L = \prod_{\substack{j=0 \\ \nu\in N}}^{h_1-1} \pi_{j,\nu}.$$

As each $\pi_{j,\nu}$ is an odd permutation and $h_1 n$ is an odd integer, ρ_L is an odd permutation on G^*. □

3. PROOF OF THE THEOREM

We verify that for all $i \in \{0, 1, \ldots, t-1\}$, $K_i = K$ satisfies all five conditions in the Condition Set.

$f(x)$ is irreducible over $K_0 = \mathbb{Q}$ by assumption. To show that $f(x)$ is irreducible over K_i, $i \in \{1, 2, \ldots, t-1\}$, it suffices to show that the Galois group $\mathrm{Gal}(L/K_i)$ acts transitively on the set of roots of $f(x)$. But $\mathrm{Gal}(L/K_i)$ is, by Proposition 5, $M_i = N \rtimes \langle\alpha^{2^i}\rangle$, which acts on $\{\theta_1, \ldots, \theta_n\}$ transitively by Proposition 4(iii). Hence (i) of the Condition Set holds.

It is clear that

$$g(x) = \prod_{\substack{i,j=1 \\ i\neq j}}^{n} (x - (\theta_i - \theta_j))$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

is squarefree over K_i, and $L = K(\theta_1, \theta_2, \ldots, \theta_n)$ is the splitting field of $f(x)$. Thus (ii) and (iii) of the Condition Set hold.

The Galois group $\mathrm{Gal}(L/K_i) = M_i = N \rtimes \langle \alpha^{2^i} \rangle$ is a Frobenius group with kernel N and complement $\langle \alpha^{2^i} \rangle$, which is a cyclic group of even order $2^{t-i}h_1$, where $t - i$ is a positive integer and h_1 is an odd positive integer. This verifies (iv) of the Condition Set. Finally, the degree of $f(x)$ is $n = |N|$ by assumption. Thus (v) of the Condition Set is valid.

Recall that the degree of $g(x)$ is $n(n-1)$. According to Proposition 7 and its corollary, each irreducible factor of $g(x)$ over K_i is of degree $|G^*| = 2^{t-i}h_1 n = nh/2^i$. Therefore $g(x)$ has $n(n-1)/|G^*| = 2^i(n-1)/h$ irreducible factors over K_i. Hence over K_i we have

$$g(x) = \prod_{j=1}^{2^i(n-1)/h} g_{ij}(x), \tag{16}$$

where each $g_{ij}(x) \in K_i[x]$ is monic, irreducible, and of degree $|G^*| = 2^{t-i}h_1 n = nh/2^i$. By Proposition 10, the field extension $K_i\left(\sqrt{(-1)^{d_i} g_{ij}(0)}\right)/K_i$ has degree 2, where $d_i = \deg(g_{ij}(x))/2$. It is now clear that for $i \in \{0, 1, \ldots, t-1\}$, the degree of the element $\sqrt{(-1)^{d_i} g_{ij}(0)}$ over the rational field $\mathbb{Q}$ is 2^{i+1}. By the uniqueness of the quadratic tower (11) (Remark 2), we have

$$K_{i+1} = \mathbb{Q}(\sqrt{(-1)^{d_i} g_{ij}(0)}), \quad i \in \{0, 1, \ldots, t-1\}.$$

When $i \in \{0, \ldots, t-2\}$, $d_i = \deg(g_{ij}(x))/2 = 2^{t-1-i}h_1 n$ is even, and it follows that $\sqrt{(-1)^{d_i} g_{ij}(0)} = \sqrt{g_{ij}(0)}$.

When $i = t-1$, $d_{t-1} = \deg(g_{t-1j}(x))/2 = 2^{t-1-(t-1)}h_1 n = h_1 n$ is odd, hence we have $\sqrt{(-1)^{d_{t-1}} g_{t-1j}(0)} = \sqrt{-g_{t-1j}(0)}$.

The proof is now complete since both (13) and (14) are established by (15) and the notes above. □

4. EXAMPLES

Our theorem gives a practical way of determining the normal subfields K_i of degree 2^i of the splitting field of L of f since the polynomial $g(x)$ can be conveniently computed using resultants (see Soicher, 1981) and factored over a number field using for example a package such as

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

MAPLE. If $g(x)$ has repeated factors it is necessary to change the polynomial $f(x)$ by a Tschirnhausen transformation.

Example 1. Let $f(x)=x^5-5ax^3+5a^2x-b\in\mathbb{Z}[x]$ be irreducible. Then $4a^5-b^2\neq 0$, otherwise there exists an integer c such that $a=c^2$, $b=2c^5$, and $f(x)$ has the linear factor $x-2c$. The Galois group G of f is the Frobenius group F_{20}. Here $n=5$, $h=4$, $(n-1)/h=1$ and $t=2$. The polynomial $f(x)$ is known as DeMoivre's quintic. Set

$$g(x)=\frac{\text{Resultant}(f(x+X),f(X))}{x^5}.$$

MAPLE gives $g(x)$ as a polynomial of degree 20 with constant term $g(0)=5^5(4a^5-b^2)^2=g_{01}(0)$. By our theorem the unique quadratic subfield K_1 of L is

$$K_1=\mathbb{Q}(\sqrt{g(0)})=\mathbb{Q}(\sqrt{5}).$$

Next we factor $g(x)$ in $\mathbb{Q}(\sqrt{5})[x]$. MAPLE gives two monic polynomials $g_{11}(x)$ and $g_{12}(x)$ in $\mathbb{Q}(\sqrt{5})[x]$ of degree 10 such that

$$g(x)=g_{11}(x)g_{12}(x).$$

By our theorem these polynomials are irreducible in $\mathbb{Q}(\sqrt{5})[x]$. Evaluating them at $x=0$, MAPLE gives

$$g_{11}(0)=\frac{1000a^5-250b^2}{-25+11\sqrt{5}},\quad g_{12}(0)=\frac{1000a^5-250b^2}{-25-11\sqrt{5}},$$

and our theorem yields the unique quartic subfield K_2 of L as

$$K_2=\mathbb{Q}\left(\sqrt{-\left(\frac{1000a^5-250b^2}{-25+11\sqrt{5}}\right)}\right).$$

Since

$$-\left(\frac{1000a^5-250b^2}{-25+11\sqrt{5}}\right)=\left(\frac{5+5\sqrt{5}}{2}\right)^2(4a^5-b^2)(5+2\sqrt{5}),$$

we have

$$K_2=\mathbb{Q}\left(\sqrt{(4a^5-b^2)(5+2\sqrt{5})}\right)$$

in agreement with Spearman and Williams (1999, Theorem).

Example 2. We choose

$$f(x) = x^5 + ax + b \in \mathbb{Z}[x]$$

to be a solvable, irreducible quintic trinomial with $ab \neq 0$. Let r be the unique rational root of the resolvent sextic of $x^5 + ax + b$ (Spearman and Williams, 1994, p. 988). Set

$$c = \left|\frac{3r - 16a}{4r + 12a}\right|, \quad \varepsilon = \mathrm{sgn}\left(\frac{3r - 16a}{4r + 12a}\right), \quad e = \frac{-5b\varepsilon}{2r + 4a},$$

so that

$$c\,(\geq 0) \in \mathbb{Q}, \quad \varepsilon = \pm 1, \quad e\,(\neq 0) \in \mathbb{Q}.$$

Then (see, for example, Spearman and Williams, 1994, Theorem, p. 987) we have

$$a = \frac{5e^4(3 - 4\varepsilon c)}{c^2 + 1}, \quad b = \frac{-4e^5(11\varepsilon + 2c)}{c^2 + 1}.$$

The Galois group G of f is

$$\begin{cases} D_5, & \text{if } 5(c^2 + 1) \in \mathbb{Q}^2, \\ F_{20}, & \text{if } 5(c^2 + 1) \notin \mathbb{Q}^2, \end{cases}$$

where D_5 is the dihedral group of order 10 and F_{20} is the Frobenius group of order 20 (Spearman and Williams, 1994, p. 990). We note that D_5 is a Frobenius group. We just treat the case when $G = F_{20}$ as the case $G = D_5$ is simpler. Here $n = 5$, $h = 4$, $(n - 1)/h = 1$ and $t = 2$. Set

$$g(x) = \frac{\mathrm{Resultant}(f(x + X), f(X))}{x^5}.$$

MAPLE gives $g(x)$ as a polynomial of degree 20 with constant term

$$g(0) = g_{01}(0) = 2^8 5^5 \frac{(4\varepsilon c^3 - 84c^2 - 37\varepsilon c - 122)^2}{(c^2 + 1)^5}.$$

By the theorem we obtain

$$K_1 = \mathbb{Q}\left(\sqrt{g_{01}(0)}\right) = \mathbb{Q}\left(\sqrt{5(c^2 + 1)}\right),$$

in agreement with Spearman et al. (1995, p. 16).

Next we use MAPLE to factor $g(x)$ over K_1. MAPLE gives $g(x)$ as the product of two monic polynomials $g_{11}(x)$ and $g_{12}(x)$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

in $\mathbb{Q}(\sqrt{5(c^2+1)})[x]$ of degree 10 such that

$$g(x) = g_{11}(x)g_{12}(x).$$

MAPLE gives

$$\begin{aligned} g_{11}(0) &= (\text{square}) \times \left(-25(c^2+1) + (5+10\varepsilon)\sqrt{5(c^2+1)}\right) \\ &= (\text{square}) \times 5(c^2+1)\left(-5 + (1+2\varepsilon)\sqrt{\frac{5}{c^2+1}}\right). \end{aligned}$$

By the theorem we have

$$K_2 = \mathbb{Q}\left(\sqrt{-5 + (1+2\varepsilon)\sqrt{\frac{5}{c^2+1}}}\right)$$

in agreement with Spearman et al. (1995, Theorem, p. 17).

We conclude by giving brief details of four numerical examples.

Example 3.

$$\begin{aligned} f(x) &= x^5 - 70x^3 - 140x^2 + 385x + 28, \\ G &= F_{20},\ n = 5,\ h = 4,\ (n-1)/h = 1,\ t = 2, \\ g_{01}(0) &= 2^{17}\,5^5\,7^4\,43^2, \\ K_1 &= \mathbb{Q}(\sqrt{10}), \\ g_{11}(0) &= 2^8\,5^2\,7^2(-650 + 201\sqrt{10}), \\ g_{12}(0) &= 2^8\,5^2\,7^2(-650 - 201\sqrt{10}), \\ K_2 &= \mathbb{Q}\left(\sqrt{650 + 201\sqrt{10}}\right) \\ &= \mathbb{Q}\left(\sqrt{\left(\frac{17+4\sqrt{10}}{3}\right)^2 (10+\sqrt{10})}\right) \\ &= \mathbb{Q}\left(\sqrt{10+\sqrt{10}}\right). \end{aligned}$$

Example 4.

$$\begin{aligned}
f(x) &= x^9 - 3x^8 + 3x^7 - 15x^6 + 33x^5 - 3x^4 + 24x^3 + 6x^2 - 4,\\
&\quad \text{see (Cangelmi, 2000, p. 856)},\\
G &= (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_4,\\
n &= 9,\ h = 4,\ (n-1)/h = 2,\ t = 2,\\
g_{01}(0) &= 2^8\, 3^6\, 5^7,\\
g_{02}(0) &= 2^4\, 3^6\, 5^{11},\\
K_1 &= \mathbb{Q}(\sqrt{5}),\\
g_{11}(0) &= 2^4\, 3^3\, 5^3 (5 + 2\sqrt{5}),\\
g_{12}(0) &= 2^4\, 3^3\, 5^3 (5 - 2\sqrt{5}),\\
g_{13}(0) &= 2\, 3^3\, 5^5 (5 - \sqrt{5}),\\
g_{14}(0) &= 2\, 3^3\, 5^5 (5 + \sqrt{5}),\\
K_2 &= \mathbb{Q}\left(\sqrt{-(15 + 6\sqrt{5})}\right)\\
&= \mathbb{Q}\left(\sqrt{-\left(\frac{1+\sqrt{5}}{4}\right)^2 (30 + 6\sqrt{5})}\right)\\
&= \mathbb{Q}\left(\sqrt{-(30 + 6\sqrt{5})}\right).
\end{aligned}$$

Example 5.

$$\begin{aligned}
f(x) &= x^9 - 72x^7 + 1464x^5 - 960x^4 - 8928x^3 + 13440x^2\\
&\quad - 2064x - 2560.
\end{aligned}$$

The MAGMA database gives

$$G = T_{15} \ \text{(notation of Butler and McKay, 1983)}, \quad |G| = 72.$$

The group T_{15} has one normal subgroup $N = \mathbb{Z}_3 \times \mathbb{Z}_3$ of order 9 as well as nine conjugate subgroups of order 8, each of which is cyclic. These conjugate subgroups intersect only trivially so G is a Frobenius group and is the semidirect product $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_8$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$$n = 9,\ h = 8,\ (n-1)/h = 1,\ t = 3,$$

$$g_{01}(0) = 2^{67}\,3^{12}\,5^{6}\,7^{2}\,239^{2}\,503^{2},$$

$$K_1 = \mathbb{Q}(\sqrt{2}),$$

$$g_{11}(0) = 2^{33}\,3^{6}\,5^{3}(2 \cdot 29 \cdot 137 \cdot 1193 + 6650041\sqrt{2}),$$

$$K_2 = \mathbb{Q}\left(\sqrt{2 \cdot 5 \cdot 29 \cdot 137 \cdot 1193 + 5 \cdot 6650041\sqrt{2}}\right)$$

$$= \mathbb{Q}\left(\sqrt{10 - 5\sqrt{2}}\right),$$

$$g_{21}(0) = -2^{16}\,3^{2}(5662200 + 3307230\beta - 330870\beta^{2} - 193803\beta^{3}),$$

$$\text{where } \beta = \sqrt{10 - 5\sqrt{2}},$$

$$K_3 = \mathbb{Q}\left(\sqrt{5662200 + 3307230\beta - 330870\beta^{2} - 193803\beta^{3}}\right).$$

Since

$$\left(5662200 + 3307230\beta - 330870\beta^{2} - 193803\beta^{3}\right)\left(30 - 3\beta + \frac{3\beta^{2}}{5}\right)$$
$$= \left(9450 + 5820\beta - 531\beta^{2} - 336\beta^{3}\right)^{2},$$

we have

$$K_3 = \mathbb{Q}\left(\sqrt{30 - 3\beta + \frac{3\beta^{2}}{5}}\right)$$
$$= \mathbb{Q}\left(\sqrt{30 - 3\sqrt{10 + 5\sqrt{2}} + 6\sqrt{10 - 5\sqrt{2}}}\right).$$

Example 6.

$$f(x) = x^{13} - 26x^{10} - 117x^{8} + 143x^{7} - 910x^{6} + 585x^{5}$$
$$- 1794x^{4} + 4472x^{3} - 2951x^{2} + 520x - 131.$$

MAPLE gives the discriminant of $f(x)$ as $2^{8}\,13^{21}\,43^{2}\,2791^{2}\,332699^{2}\,15515891^{2}$ so that the quadratic subfield of L is $\mathbb{Q}(\sqrt{13})$. If α is

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

any root of $f(x)$ MAPLE factors $f(x)$ over $\mathbb{Q}(\alpha, \sqrt{13})$. There are six irreducible quadratics and one linear polynomial in the factorization. Hence

$$[L:\mathbb{Q}] = 2^k\, 13$$

for some $k \in \mathbb{Z}^+$. Therefore $f(x)$ is solvable so $\mathrm{Gal}(f) = F_{13l}$, where $l \mid 12$. It is known that $[L:\mathbb{Q}] = 13l$, where $l \neq 1$ as L has a quadratic subfield and $l \neq 2$ as f does not factor into linear factors over $\mathbb{Q}(\alpha, \sqrt{13})$. Hence $l = 4$ and $\mathrm{Gal}(f) = F_{52}$. We remark that a theorem of Cangelmi (2000, Theorem 3.17, p. 851) provides an alternative way of verifying that $\mathrm{Gal}(f) = F_{52}$.

$$\begin{aligned}
n &= 13,\ h = 4,\ (n-1)/h = 3,\ t = 2,\\
g_{01}(0) &= 13^7\, 15515891^2,\\
g_{02}(0) &= 2^8\, 13^7\, 332699^2,\\
g_{03}(0) &= 13^7\, 43^2\, 2791^2,\\
K_1 &= \mathbb{Q}(\sqrt{13}),\\
g_{11}(0) &= \frac{13^3}{2}(5 \cdot 13^2 \cdot 1822217 + 3^3 \cdot 3793 \cdot 4159\sqrt{13}),\\
K_2 &= \mathbb{Q}\left(\sqrt{-\frac{1}{2}(5 \cdot 13^2 \cdot 1822217 + 3^3 \cdot 3793 \cdot 4159\sqrt{13}}\right)\\
&= \mathbb{Q}\left(\sqrt{-13 - 2\sqrt{13}}\right).
\end{aligned}$$

ACKNOWLEDGMENTS

The authors are grateful to the referee for his/her invaluable suggestions based on his/her thorough reading and understanding of our work. The research of the first two authors was supported by grants from the Natural Sciences and Engineering Research Council of Canada.

REFERENCES

Butler, G., McKay, J. (1983). The transitive groups of degree up to eleven. *Comm. Algebra* 11:863–911.

Cangelmi, L. (2000). Polynomials with Frobenius Galois groups. *Comm. Algebra* 28:845–859.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Robinson, D. J. S. (1982). *A Course in the Theory of Groups*. Graduate Text in Mathematics 80. New York: Springer-Verlag.
Rotman, J. (2002). *Advanced Modern Algebra.* Prentice-Hall.
Soicher, L. (1981). M. Comp. Sci. thesis, Concordia University, Montréal.
Spearman, B. K., Williams, K. S. (1994). Characterization of solvable quintics $x^5 + ax + b$. *Amer. Math. Monthly* 101:986–992.
Spearman, B. K., Williams, K. S. (1999). DeMoivre's quintic and a theorem of Galois. *Far East J. Math. Sci. (FJMS)* 1:137–143.
Spearman, B. K., Spearman, L. Y., Williams, K. S. (1995). The subfields of the splitting field of a solvable quintic trinomial. *J. Math. Sci.* 6:15–18.

Received November 2001
Revised December 2002