Galois Groups of Polynomials Arising from Circulant Matrices

M. Filaseta[1*], F. Luca[2*], P. Stănică[3*†], R.G. Underwood[3]

[1] Department of Mathematics, University of South Carolina
Columbia, SC 29208; e-mail: filaseta@math.sc.edu

[2] IMATE, UNAM, Ap. Postal 61-3 (Xangari), CP. 58 089
Morelia, Michoacán, Mexico; e-mail: fluca@matmor.unam.mx

[3] Department of Mathematics, Auburn University Montgomery
Montgomery, AL 36124; e-mail: {pstanica,runderwo}@mail.aum.edu

1 Introduction

Computing the Galois group of the splitting field of a given polynomial with integer coefficients is a classical problem in modern algebra. A theorem of Van der Waerden [Wae] asserts that almost all (monic) polynomials in $\mathbb{Z}[x]$ have associated Galois group S_n, the symmetric group on n letters. Thus, cases where the associated Galois group is different from S_n are rare. Nevertheless, examples of polynomials where the associated Galois group is not S_n are well-known. For example, the Galois group of the splitting field of the polynomial $x^p - 1$, $p \geq 3$ prime, is cyclic of order $p-1$. For the polynomial $x^p - 2$, $p \geq 3$, the Galois group is the subgroup of S_p generated by a cycle of length p and a cycle of length $p-1$. An interest in this paper is to find other collections of polynomials with integer coefficients whose Galois groups are isomorphic to these groups.

Using circulant matrices, we are led in the next section to the polynomials

$$f_{p,m}(x) = 1 + \sum_{i=0}^{(p-1)/2} (-1)^i \frac{p}{p-i} \binom{p-i}{i} m^i x^{p-2i},$$

where $p \geq 5$ is prime and m is a positive integer. We will not be using it explicitly, but we make the observation that

$$f_{p,m}(x) = 2m^{p/2} T_p(x/(2m^{1/2})) + 1,$$

*The first author's research is supported by the National Science Foundation and the National Security Agency and the second author's by Grants SEP-CONACyT 37259E and 37260E. The third author is partially supported by a Research Award from the School of Sciences at his institution.

†Also associated with the Institute of Mathematics of Romanian Academy, Bucharest, Romania

where $T_p(x)$ is a Chebyshev polynomial of the first kind, cf. [Ri, (1.10), (1.96)]. Moreover, $f_{p,m}(x)$ can also be related to Dickson polynomials, cf. [LMT].

We will establish various results about the polynomials $f_{p,m}(x)$. We first show that $f_{p,m}(x) \in \mathbb{Z}[x]$. Moreover, the roots of $f_{p,m}(x)$ are all real and are described as the collection

$$\{-\lambda\zeta_p^{-j} - \overline{\lambda}\zeta_p^j\}$$

for $j = 0, \ldots, p-1$, where λ is a fixed p^{th} root of $\gamma_m = \dfrac{1+\sqrt{1-4m^p}}{2}$, $\overline{\lambda}$ is its conjugate, and ζ_p is a primitive p^{th} root of unity.

We will also determine how $f_{p,m}(x)$ factors over the rationals. For the case $p \geq 5$, we show that $f_{p,1}(x)/(x+1)$ is irreducible over $\mathbb{Q}$. For $p \geq 5$ and $m \geq 2$, we will see that $f_{p,m}(x)$ is irreducible over $\mathbb{Q}$. We will use this information to establish the following theorems.

Theorem A. *Let $p \geq 5$ be prime. Let K be the splitting field of $f_{p,1}(x)$ over $\mathbb{Q}$. Then the Galois group of $K/\mathbb{Q}$ is cyclic of order $p-1$.*

Theorem B. *Let $p \geq 5$ be a prime, and let $m \geq 2$ be an integer. The Galois group of the splitting field $K/\mathbb{Q}$ of $f_{p,m}$ is a subgroup of the symmetric group S_p of order $p(p-1)$ generated by a cycle of length p and a cycle of length $p-1$.*

The above theorems achieve the goal indicated in the leading paragraph of this paper. We note that, furthermore, in the course of proving these theorems, we shall exhibit the generators of these Galois groups explicitly.

In the case that m is negative, the coefficients of the polynomials $f_{p,m}(x)$ are all positive, and it is reasonable to consider the analogous results in this case. There are, however, substantial differences that occur in trying to carry out arguments similar to those given here. For example, in this case, $f_{p,m}(x)$ has exactly one real root. What is of more significance here though is that the proof of Lemma 9 leads to the Diophantine equation $px^2 - 1 = 4y^p$ where p is an odd prime. Instead of working in $\mathbb{Q}(\sqrt{-p})$ as is currently done in Lemma 9, considering $m < 0$ leads to working in the field $\mathbb{Q}(\sqrt{p})$, causing difficulties in our present argument as this field has infinitely many units. We therefore do not address the case that $m < 0$ here.

2 Construction of $f_{p,m}$ and the Galois Group of $f_{p,1}$

Let n be a positive integer and let $\zeta_n = \exp(2\pi i/n)$ denote a primitive n^{th} root of unity. Consider the $n \times n$ *circulant matrix*

$$\operatorname{circ}(a_1, a_2, \ldots, a_n) = \begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_n & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \ldots & a_{n-2} \\ \vdots & & & & \vdots \\ a_2 & a_3 & a_4 & \ldots & a_1 \end{pmatrix}.$$

The determinant of $\mathrm{circ}(a_1, a_2, \ldots, a_n)$ is given by the formula

$$\det(\mathrm{circ}(a_1, a_2, \ldots, a_n)) = \prod_{j=0}^{n-1} \left(a_1 + a_2\zeta_n^j + a_3\zeta_n^{2j} + \cdots + a_n\zeta_n^{j(n-1)}\right). \tag{1}$$

Let n be an integer ≥ 3, and consider the $n \times n$ circulant matrix $A = \mathrm{circ}(a, b, c, 0, \ldots, 0)$. In this case, Ore [O] has computed the expansion of (1). Let $\lfloor x \rfloor$ denote the greatest integer less than or equal to x.

Theorem 1 (Ore)**.** *The determinant of A is*

$$\det(A) = a^n + (-1)^{n+1}b^n + c^n - n \sum_{i=1}^{\lfloor n/2 \rfloor} (-1)^{n+i} \frac{1}{n-i} \binom{n-i}{i} (ac)^i b^{n-2i}.$$

Corollary 2. *If n is odd, then*

$$\det(A) = a^n + c^n + b^n + \sum_{i=1}^{(n-1)/2} (-1)^i \frac{n}{n-i} \binom{n-i}{i} (ac)^i b^{n-2i}.$$

Take $n = p \geq 5$ prime. We consider a and c satisfying $a^p + c^p = 1$ with $m = ac$ a positive integer. It follows that a^p and c^p are the roots of the quadratic $g(x) = x^2 - x + m^p$ and, hence, we can take $a^p = (1 + \sqrt{1 - 4m^p})/2$ and $c^p = (1 - \sqrt{1 - 4m^p})/2$. We define $f_{p,m}(x)$ to be the determinant of the $p \times p$ circulant matrix $\mathrm{circ}(a, x, c, 0, 0, \ldots, 0)$. Thus, by Corollary 2,

$$f_{p,m}(x) = x^p - \frac{p}{p-1}\binom{p-1}{1} m\, x^{p-2} + \cdots + (-1)^{(p-1)/2} p\, m^{(p-1)/2}\, x + 1.$$

One can see that $f_{p,m} \in \mathbb{Z}[x]$ through the identity

$$\frac{n}{n-i}\binom{n-i}{i} = \binom{n-i}{i} + \binom{n-i-1}{i-1}.$$

Next, we explicitly describe the zeros of $f_{p,m}$.

Lemma 3. *Set $\gamma_m = (1 + \sqrt{1 - 4m^p})/2$, and let λ be a p^{th} root of γ_m. The roots of $f_{p,m}$ are precisely the p numbers of the form $-\lambda\zeta_p^{-j} - \overline{\lambda}\zeta_p^j$ for $j = 0, \ldots, p-1$.*

Proof. Observe that

$$\lambda^p + \overline{\lambda}^p = 1 \qquad \text{and} \qquad \lambda\overline{\lambda} = |\lambda|^2 = |\gamma_m|^{2/p} = m.$$

Thus, $f_{p,m}$ is the determinant of the $p \times p$ circulant matrix $\mathrm{circ}(\lambda, x, \overline{\lambda}, 0, 0, \ldots, 0)$. Using formula (1), $f_{p,m}(x)$ factors as

$$f_{p,m}(x) = \prod_{j=0}^{p-1} (\lambda + x\zeta_p^j + \overline{\lambda}\zeta_p^{2j}).$$

Thus, the roots of $f_{p,m}$ are $-\lambda\zeta_p^{-j} - \overline{\lambda}\zeta_p^j$, $j = 0, \ldots, p-1$. □

One immediate consequence of Lemma 3 is that it provides some information about the location of the zeros of $f_{p,m}$. For example, $-\lambda\zeta_p^{-j}$ and $-\overline{\lambda}\zeta_p^{j}$ are conjugates each having, by the proof above, absolute value $\sqrt{m}$; hence, each root $-\lambda\zeta_p^{-j} - \overline{\lambda}\zeta_p^{j}$ of $f_{p,m}$ is a real number in the interval $[-2\sqrt{m}, 2\sqrt{m}]$. Furthermore, since the numbers $-\lambda\zeta_p^{-j}$ for $0 \leq j \leq p-1$ are equally spaced along the circle of radius $\sqrt{m}$ centered at the origin in the complex plane, we can deduce that for fixed $m \geq 1$, the roots of the collection of polynomials $\{f_{p,m}(x)\}_{p\geq 5}$ are dense in the interval $[-2\sqrt{m}, 2\sqrt{m}]$.

We now specialize to the case $p \geq 5$, $m = 1$ in the definition of $f_{p,m}$. In this case, $\gamma_1 = (1 + i\sqrt{3})/2$, $i = \sqrt{-1}$. Thus, $\gamma_1 = \zeta_6 = \exp(\pi i/3)$. As p is a prime ≥ 5, we have $p \equiv \pm 1 \pmod 6$ so that $p^2 \equiv 1 \pmod 6$. Setting $\lambda = \zeta_6^p$, we deduce

$$\lambda^p = \left(\zeta_6^p\right)^p = \zeta_6^{p^2} = \zeta_6 = \gamma_1. \tag{2}$$

Thus, by Lemma 3, the zeros of $f_{p,1}$ consist of the collection

$$x_j = -\lambda\zeta_p^{-j} - \overline{\lambda}\zeta_p^{j},$$

for $j = 0, \ldots, p-1$.

By the remark following the proof of Lemma 3, each zero of $f_{p,1}$ is in the interval $[-2, 2]$. In fact, precisely one root of $f_{p,1}$ is -1. Indeed, the following is trivial to prove.

Lemma 4. *Let $p \geq 5$, $\lambda = \zeta_6^p$. Then $x_0 = -\lambda - \overline{\lambda} = -1$.*

A polynomial $f(x) \in \mathbb{Z}[x]$ is called Eisenstein if Eisenstein's criterion applies to a translation of $f(x)$. In particular, Eisenstein polynomials are irreducible over $\mathbb{Q}$.

Lemma 5. *For $p \geq 5$, the polynomial $f_{p,1}(x)/(x+1)$ is Eisenstein.*

Proof. For $p \geq 5$, define $h_p(x) = f_{p,1}(x)/(x+1)$. Observe that

$$\begin{aligned} h_p(x-1) &= f_{p,1}(x-1)/x \\ &= \frac{1}{x}\left((x-1)^p - \frac{p}{p-1}\binom{p-1}{1}(x-1)^{p-2} + \cdots + (-1)^{(p-1)/2}p(x-1) + 1\right). \end{aligned}$$

We deduce that $h_p(x-1)$ is a monic polynomial in $\mathbb{Z}[x]$ with every coefficient except the leading coefficient divisible by p. To complete the proof, we show that p^2 does not divide the constant term of $h_p(x-1)$. Let $\lambda = \zeta_6^p$. Then, by Lemma 3, the roots of $f_{p,1}(x-1)$ are of the form

$$1 - \lambda\zeta_p^{-j} - \overline{\lambda}\zeta_p^{j}$$

for $j = 0, \ldots, p-1$. Now, by Lemma 4, the root corresponding to $j = 0$ is 0 and, therefore, accounts for the factor x in $f_{p,1}(x-1)$. Thus, the constant term in $h_p(x-1)$ is

$$\begin{aligned} \prod_{j=1}^{p-1}\left(1 - \lambda\zeta_p^{-j} - \overline{\lambda}\zeta_p^{j}\right) &= \prod_{j=1}^{p-1}\left(\lambda\zeta_p^{j}\left(\lambda + \zeta_p^{-j}\right)\left(1 - \zeta_p^{-j}\right)\right) \\ &= \lambda^{p-1}\prod_{j=1}^{p-1}\left(\lambda + \zeta_p^{-j}\right)\prod_{j=1}^{p-1}\left(1 - \zeta_p^{-j}\right). \end{aligned}$$

Using $\Phi_m(x)$ to denote the m^{th} cyclotomic polynomial, the last product above is simply $\Phi_p(1) = p$. We also use that $\Phi_{3p}(1) = 1$ (indeed, $\Phi_m(1) = 1$ whenever m is not a prime power). From $\lambda = \zeta_6^p = -\zeta_3^{2p}$, we obtain

$$\lambda + \zeta_p^{-j} = \lambda\Big(1 - \zeta_{3p}^{-3j-2p^2}\Big)$$

and $-3j - 2p^2$ is relatively prime to $3p$ for $1 \le j \le p-1$. As

$$1 = \Phi_{3p}(1) = \prod_{\substack{1\le j\le 3p-1\\ \gcd(j,3p)=1}} \big(1 - \zeta_{3p}^{j}\big),$$

each $\lambda + \zeta_p^{-j}$ for $1 \le j \le p-1$ is λ times a unit in $\mathbb{Z}[\zeta_{3p}]$. Also, λ is a unit in $\mathbb{Z}[\zeta_{3p}]$. It follows that the constant term of $h_p(x-1)$ is a unit in $\mathbb{Z}[\zeta_{3p}]$ times p. Since it is also in $\mathbb{Z}$, we deduce that the constant term is $\pm p$, concluding the proof. □

As noted earlier, Lemma 5 shows that the polynomials considered there are irreducible over $\mathbb{Q}$. There are alternative approaches to establishing the irreducibility of these polynomials. We describe such a method next which also provides us some additional information, in particular about the polynomials' associated Galois groups.

Theorem 6. *(Theorem A) Let $p \ge 5$ be prime. Let K be the splitting field of $f_{p,1}(x)$ over $\mathbb{Q}$. Then the Galois group of $K/\mathbb{Q}$ is cyclic of order $p-1$.*

Proof. Take $\lambda = \zeta_6^p$. Then $-\lambda$ is a p^{th} root of ζ_3^2 and, hence, a $(3p)^{\text{th}}$ root of unity. The remaining p^{th} roots of ζ_3^2 can be written in the form $-\lambda\zeta_p^{-j}$ where $1 \le j \le p-1$. For $p \ge 5$, one can check directly that ζ_3^{2p} is the only p^{th} root of ζ_3^2 which is not a primitive $(3p)^{\text{th}}$ root of unity. We deduce from Lemma 3 that the splitting field K of $f_{p,1}$ over $\mathbb{Q}$ is precisely the maximal real subfield of $\mathbb{Q}(\zeta_{3p})$. As $p \ge 5$, the degree of this extension is $\phi(3p)/2 = p-1$. The Galois group of the maximal real subfield of $\mathbb{Q}(\zeta_{3p})$ over $\mathbb{Q}$ is cyclic. This completes the proof (and establishes the irreducibility of the polynomials $f_{p,1}(x)/(x+1)$ for $p \ge 5$). □

It is of some interest to describe a generator for these Galois groups. If λ is a p^{th} root of $\zeta_6 = -\zeta_3^2$, then Lemma 3 and

$$(-\lambda - \overline{\lambda})^2 = \lambda^2 + 2 + \overline{\lambda}^2$$

imply that $\sigma(x) = 2 - x^2$ is an automorphism of K over $\mathbb{Q}$. For $p = 3$, one can check directly that σ generates the Galois group of K over $\mathbb{Q}$. For $p \ge 5$, the automorphism σ may or may not generate the Galois group. In particular, if the order of 2 modulo p is even and $< p-1$, then σ will not be a generator for the Galois group (for example, consider $p = 17$ or $p = 41$). To obtain an automorphism that generates the Galois group for all $p \ge 5$, for each $j \in \{1, 2, \ldots, p-1\}$, we consider an integer $k = k(j)$ satisfying $k \equiv 1 \pmod 3$ and $k \equiv j \pmod p$. The automorphism σ_j of $\mathbb{Q}(\zeta_{3p})$ over $\mathbb{Q}$ defined by $\sigma_j(\zeta_{3p}) = \zeta_{3p}^k$ has the property that $\sigma_j(\zeta_3) = \zeta_3$ and $\sigma_j(\zeta_p) = \zeta_p^j$. In other words, the $p-1$ different σ_j are precisely the automorphisms of $\mathbb{Q}(\zeta_{3p})$ over $\mathbb{Q}(\zeta_3)$. We now consider a primitive root g modulo p and fix $\lambda = -\zeta_3^{2p}$. Define $\sigma_g^{(t)}$ to be the composition of t copies of σ_g. Then

$$\sigma_g^{(t)}\big(-\lambda\zeta_p - \overline{\lambda}\zeta_p^{-1}\big) = -\lambda\zeta_p^{g^t} - \overline{\lambda}\zeta_p^{-g^t}.$$

We deduce from Lemma 3 that the restriction of σ_g to K, the maximal real subfield of $\mathbb{Q}(\zeta_{3p})$, is a generator for the Galois group of K over $\mathbb{Q}$.

The above explicit construction of the generator leads naturally to a further conclusion.

Proposition 7. *The polynomial $f_{3,1}(x)$ and the polynomials $f_{p,1}(x)/(x+1)$, for primes $p \geq 5$, are irreducible over $\mathbb{Q}(\zeta_3)$.*

Proof. One checks the above result directly for $p = 3$. For $p \geq 5$, we use that for $2 \leq j \leq p-1$, the roots of $f_{p,1}(x)/(x+1)$ are images of the root $-\lambda\zeta_p - \overline{\lambda}\zeta_p^{-1}$ under applications of the automorphism σ_g of $\mathbb{Q}(\zeta_{3p})$ over $\mathbb{Q}(\zeta_3)$. Since this automorphism fixes the elements of $\mathbb{Q}(\zeta_3)$, the above result follows. The result for $p \geq 5$ also follows from the proof of Lemma 5 (from the fact that $f_{p,1}(x)/(x+1)$ is Eisenstein with respect to a prime which does not ramify in $\mathbb{Q}(\zeta_3)$). □

3 Galois Groups of $f_{p,m}$ for $m > 1$

For a prime $p \geq 5$ and an integer $m \geq 2$, we establish the irreducibility of $f_{p,m}$ over the rationals and compute the Galois group of the splitting field $K/\mathbb{Q}$ of $f_{p,m}$. Multiplying the relation $\lambda^p + \overline{\lambda}^p = 1$ from the proof of Lemma 3 by λ^p shows that the roots of $f_{p,m}$ are associated with the roots of $p_m(x) = x^{2p} - x^p + m^p$. Our investigations here begin with a closer look at the polynomial $p_m(x)$.

Lemma 8. *Let p be an odd prime and let m be an integer with $m \geq 2$. Then the polynomial $x^{2p} - x^p + m^p$ is irreducible.*

Proof. Let $N = 1-4m^p$ and $\gamma = (1+\sqrt{N})/2$. Thus, $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{N}) = \mathbb{Q}(\sqrt{D})$, where $D < 0$ is a squarefree integer, $D|N$, and N/D is a square. Let λ be a p^{th} root of γ. Thus, λ is a root of $p_m(x)$. We show that $x^p - \gamma$ is irreducible over $\mathbb{Q}(\gamma)$. This will imply $[\mathbb{Q}(\lambda) : \mathbb{Q}(\gamma)] = p$. Since $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 2$, we deduce $[\mathbb{Q}(\lambda) : \mathbb{Q}] = 2p$ and, hence, that $p_m(x)$ is irreducible.

Assume $x^p - \gamma = g(x)h(x)$, where $g(x)$ and $h(x)$ are in $\mathbb{Q}(\gamma)[x]$ with $r = \deg g \in [1, p-1]$. Since the p roots of $x^p - \gamma$ are of the form $\zeta^j\lambda$, where $\zeta = \zeta_p$ and $j \in \{0, 1, \ldots, p-1\}$, we deduce that the constant term of $g(x)$ is of the form $\pm\zeta^k\lambda^r$. Thus, $\zeta^k\lambda^r \in \mathbb{Q}(\gamma)$. Let s and t be integers satisfying $rs + pt = 1$. Since $\gamma = \lambda^p$, we deduce

$$\left(\zeta^k\lambda^r\right)^s\gamma^t = \zeta^{ks}\lambda^{rs+pt} = \zeta^{ks}\lambda \in \mathbb{Q}(\gamma).$$

Setting $\alpha = \zeta^{ks}\lambda$, we see that α is an algebraic integer in $\mathbb{Q}(\sqrt{N})$ and

$$\alpha^p = \frac{1 + \sqrt{1 - 4m^p}}{2} = \frac{1 + \sqrt{N}}{2}. \tag{3}$$

Observe that α is a root of $x^{2p} - x^p + m^p$. Let β be the conjugate of α. Then

$$\beta^p = \frac{1 - \sqrt{N}}{2}.$$

Since $\alpha\beta$ is a real number satisfying $(\alpha\beta)^p = m^p$, we have $\alpha\beta = m$. Next, we determine $\alpha + \beta$. Note that

$$1 = \alpha^p + \beta^p = (\alpha + \beta)\big(\alpha^{p-1} - \alpha^{p-2}\beta + \cdots - \alpha\beta^{p-2} + \beta^{p-1}\big).$$

Each one of the two factors on the right is an algebraic integer expressed as a symmetric function of α and β. Hence, each of these factors must be a rational integer. We deduce that $\alpha + \beta = \pm 1$. We justify that $\alpha + \beta = 1$. Writing $\alpha = (a + b\sqrt{D})/2$, it suffices to show that $a \neq -1$ (i.e., that $\alpha + \beta \neq -1$). Observe that

$$2^{p-1} + 2^{p-1}\sqrt{N} = 2^p\alpha^p = (a + b\sqrt{D})^p = A + B\sqrt{D},$$

where $A \equiv a^p \pmod{p}$. Hence,

$$a^p \equiv 2^{p-1} \equiv 1 \pmod{p}.$$

As p is odd, $a \neq -1$. Thus, $\alpha + \beta = 1$. It follows that α and β are both roots of $x^2 - x + m$.

Writing $\alpha = se^{i\theta}$ with $s > 0$ and $\theta \in [0, 2\pi)$, we have $\beta = se^{-i\theta}$ and $\cos\theta = 1/(2\sqrt{m})$. On the other hand, (3) and $\alpha^p = s^p e^{ip\theta}$ imply $\cos(p\theta) = 1/(2m^{p/2})$. Using that $\cos(p\theta) = T_p(\cos\theta)$, where T_p is the p^{th} Chebyshev polynomial, we get that

$$\cos(p\theta) = 2^{p-1}(\cos\theta)^p - 2^{p-3}p(\cos\theta)^{p-2} + \cdots, \tag{4}$$

where what remains on the right is a sum of smaller odd powers of $\cos\theta$ times p times rational integers (see, for example, (1.10) and (1.96) in [Ri]). Furthermore, the coefficient of each term $(\cos\theta)^j$ on the right is divisible by 2^{j-1} (an immediate consequence of Exercise 1.4.45 in [Ri]). Given that $\cos\theta = 1/(2\sqrt{m})$ and $\cos(p\theta) = 1/(2m^{p/2})$, we see that the expression on the left of (4) equals the first term on the right of (4). Thus, the remaining terms on the right must sum to zero. After factoring out the common factor of $p\cos\theta$ in each term and multiplying through by -1, we deduce $w_1(\cos^2\theta) = 0$ where $w_1(x) \in \mathbb{Z}[x]$ and $\deg w_1(x) = (p-3)/2$. Further, the leading coefficient of $w_1(x)$ is 2^{p-3} and 2^{2j} divides the coefficient of x^j for each j. We deduce that $w_2(x) = w_1(x/4)$ is a monic polynomial with integer coefficients that has $4\cos^2\theta$ as a root. Since rational roots of monic polynomials with integer coefficients are rational integers and since $4\cos^2\theta = 1/m$, we obtain a contradiction to $m \geq 2$. □

Before continuing, we note that one can replace the argument leading to (3) by an application of Capelli's theorem (see [Sc1] and Lemma 28 of [Sc2]). The second part of the argument above (as well as the end of our next proof) is similar to an approach of Lebesgue [Le].

As in the proof of Lemma 8, we set $\gamma = (1 + \sqrt{1 - 4m^p})/2$ and fix λ to be a p^{th} root of γ. By Lemma 8, we have $[\mathbb{Q}(\lambda) : \mathbb{Q}] = 2p$. We consider the cyclotomic polynomial $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$ which is irreducible over $\mathbb{Q}$. We show that it is also irreducible over $\mathbb{Q}(\lambda)$.

Lemma 9. *Let p be a prime ≥ 5, and let m be an integer ≥ 2. Then $\Phi_p(x)$ is irreducible over $\mathbb{Q}(\lambda)$.*

Proof. By way of contradiction, assume $\Phi_p(x)$ is reducible over $\mathbb{Q}(\lambda)$. Then $\mathbb{Q}(\zeta)$, with $\zeta = \zeta_p$, contains a subfield of $\mathbb{Q}(\lambda)$ of degree 2, p or $2p$ over $\mathbb{Q}$. The latter two are not possible since $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. Thus, $\mathbb{Q}(\zeta)$ contains $\mathbb{Q}(\gamma)$ which is the subfield of $\mathbb{Q}(\lambda)$ of degree 2 over $\mathbb{Q}$. Recall that the quadratic subfield in $\mathbb{Q}(\zeta)$ is $\mathbb{Q}\big(\sqrt{(-1)^{(p-1)/2}p}\big)$. Thus, $\mathbb{Q}(\gamma) = \mathbb{Q}\big(\sqrt{(-1)^{(p-1)/2}p}\big)$. Since γ is imaginary, the quadratic field $\mathbb{Q}\big(\sqrt{(-1)^{(p-1)/2}p}\big)$ must contain imaginary numbers. We deduce that $p \equiv 3 \pmod 4$. Since $\mathbb{Q}(\gamma) = \mathbb{Q}(\sqrt{1-4m^p})$, the equality of $\mathbb{Q}(\gamma)$ and $\mathbb{Q}(\sqrt{-p})$ implies that there is a solution to the Diophantine equation

$$px^2 = 4m^p - 1,$$

where $m \geq 2$ is an integer, $p \geq 5$ is a prime $\equiv 3 \pmod 4$, and x is an integer. We conclude the proof by showing that this is impossible.

The Diophantine equation leads to

$$\frac{1 + x\sqrt{-p}}{2} \cdot \frac{1 - x\sqrt{-p}}{2} = m^p.$$

Let $\omega = (1 + x\sqrt{-p})/2$, and let $\overline{\omega}$ be its conjugate. We work in the ring of algebraic integers in $\mathbb{Q}(\sqrt{-p})$. Since $\omega + \overline{\omega} = 1$, the principal ideals (ω) and $(\overline{\omega})$ are coprime. Therefore, each of these ideals is a p^{th} power of some ideal. Let A be an ideal for which $(\omega) = A^p$. The class number h of $\mathbb{Q}(\sqrt{-p})$ is less than p (see, for example, [BS]) and, hence, not divisible by p. Thus, there is an integer p' such that $pp' \equiv 1 \pmod h$. We deduce the fractional ideal equation

$$\big(\omega^{p'}\big) = (\omega)^{p'} = A^{pp'} = A(\beta),$$

for some $\beta \in \mathbb{Q}(\sqrt{-p})$. It follows that $\beta' = \omega^{p'}/\beta$ is an algebraic integer in $\mathbb{Q}(\sqrt{-p})$ and that $A = (\beta')$. Since $(\omega) = (\beta')^p$ and since the only units in the ring of algebraic integers in $\mathbb{Q}(\sqrt{-p})$ are ± 1, we obtain $(1 + x\sqrt{-p})/2 = \alpha^p$, where either $\alpha = \beta'$ or $\alpha = -\beta'$.

Let a and b be integers, necessarily of the same parity, such that $\alpha = (a + b\sqrt{-p})/2$. Comparing real parts of the equation $(1 + x\sqrt{-p})/2 = \alpha^p$, we deduce

$$2^{p-1} = a^p - \binom{p}{2} p a^{p-2} b^2 + \binom{p}{4} p^2 a^{p-4} b^4 - \cdots - \binom{p}{p-1} p^{(p-1)/2} a b^{p-1}. \tag{5}$$

As a and b have the same parity, if a is even, then b is even and the right-hand side of (5) is divisible by 2^p. As the left-hand side is not divisible by 2^p, we deduce that a and b are odd. Since a divides the right-hand side of (5), a divides 2^{p-1} so that $a = \pm 1$. Also, (5) implies $a^p \equiv 2^{p-1} \equiv 1 \pmod p$. Therefore, $a = 1$. Clearly, $b \neq 0$. We complete the proof by showing that with $a = 1$, (5) has no solutions in nonzero integers b.

Assume (5) has a solution with a prime $p \geq 5$, $a = 1$ and b a nonzero integer. The right-hand side of (5) corresponds to the real part of $(2\alpha)^p$, where $\alpha = (a + b\sqrt{-p})/2 = (1 + b\sqrt{-p})/2$. It follows that

$$2^p = (1 + b\sqrt{-p})^p + (1 - b\sqrt{-p})^p.$$

We divide each term in this equation by $(1 + b^2 p)^{p/2}$. With θ satisfying

$$\cos\theta = \frac{1}{\sqrt{1 + b^2 p}} \quad \text{and} \quad \sin\theta = \frac{b\sqrt{p}}{\sqrt{1 + b^2 p}},$$

we deduce

$$\frac{2^p}{(1+b^2p)^{p/2}} = (\cos\theta + i\sin\theta)^p + (\cos\theta - i\sin\theta)^p = e^{ip\theta} + e^{-ip\theta} = 2\cos(p\theta).$$

Thus,

$$\cos(p\theta) = \frac{2^{p-1}}{(1+b^2p)^{p/2}}.$$

With p and θ as above, we appeal to (4) and follow the argument after (4) in the proof of Lemma 8. We deduce that $4\cos^2\theta = 4/(1+b^2p)$ is a rational integer. Since $b \neq 0$ and $p \geq 5$, this is a contradiction. □

Lemma 10. *If $p \geq 5$ is a prime and $m \geq 2$ is an integer, then $f_{p,m}(x)$ is irreducible over $\mathbb{Q}$.*

Proof. By Lemma 8, the polynomial $p_m(x) = x^{2p} - x^p + m^p$ is irreducible. We show now that we have the identity

$$-x^p f_{p,m}\left(-x - \frac{m}{x}\right) = p_m(x). \tag{6}$$

Both polynomials are monic and have the same degree, namely $2p$. Therefore, it suffices to show that the $2p$ roots of p_m are also roots of $-x^p f_{p,m}\left(-x - \frac{m}{x}\right)$. In fact, since both sides of (6) have integer coefficients and the right side is irreducible, it is sufficient to simply show that the two sides have at least one root in common. Take a root $\lambda\zeta^j$ of p_m, where $\zeta = \zeta_p$ and $\lambda = \gamma^{1/p}$ denotes an arbitrary p^{th} root of $\gamma = (1+\sqrt{1-4m^p})/2$. Note that $m\lambda^{-1}\zeta^{-j}$ is the conjugate of $\lambda\zeta^j$. Lemma 3 implies

$$-\lambda^p\zeta^{pj} f_{p,m}(-\lambda\zeta^j - m\lambda^{-1}\zeta^{-j}) = 0.$$

Thus, $\lambda\zeta^j$ is a root of the left-hand side of (6), and (6) follows.

Now, assume that there exist two polynomials f_1 and f_2 in $\mathbb{Q}[x]$ of degrees d_1 and d_2, respectively, such that each $d_j < p$ and

$$f_{p,m}(x) = f_1(x)f_2(x).$$

It follows that

$$x^p f_{p,m}\left(x + \frac{m}{x}\right) = x^p f_1\left(x + \frac{m}{x}\right) f_2\left(x + \frac{m}{x}\right).$$

Since $p = d_1 + d_2$, each

$$x^{d_j} f_j\left(x + \frac{m}{x}\right)$$

is a nonconstant polynomial in $\mathbb{Q}[x]$ dividing $p_m(-x)$ of degree $< 2p$. This contradicts the fact that $p_m(x)$ is irreducible, and the result follows. □

Let γ, λ and ζ be as in the proof of Lemma 10. Since $f_{p,m}$ is irreducible over $\mathbb{Q}$, we have $[\mathbb{Q}(\lambda + \overline{\lambda}) : \mathbb{Q}] = p$. Also, $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = (p-1)/2$. Hence,

$$[\mathbb{Q}(\lambda + \overline{\lambda}, \zeta + \zeta^{-1}) : \mathbb{Q}] = p(p-1)/2. \tag{7}$$

Observe that $-\lambda\zeta - \overline{\lambda}\zeta^{-1}$ satisfies the quadratic polynomial

$$q(x) = x^2 + x(\lambda + \overline{\lambda})(\zeta + \zeta^{-1}) + (\lambda + \overline{\lambda})^2 - 4m + m(\zeta + \zeta^{-1})^2,$$

over $\mathbb{Q}(\lambda + \overline{\lambda}, \zeta + \zeta^{-1})$.

Lemma 11. *The polynomial $q(x)$ is irreducible over $\mathbb{Q}(\lambda+\overline{\lambda}, \zeta+\zeta^{-1})$.*

Proof. By way of contradiction, assume that

$$r = -\lambda\zeta - \overline{\lambda}\zeta^{-1} = \sum_{j=0}^{(p-3)/2} a_j(\zeta+\zeta^{-1})^j,$$

where each $a_j \in \mathbb{Q}(\lambda+\overline{\lambda})$. By Lemma 9, the mapping taking ζ to ζ^{-1} is an automorphism of $\mathbb{Q}(\lambda,\zeta)$ over $\mathbb{Q}(\lambda)$. Under this automorphism, r is mapped to $-\lambda\zeta^{-1} - \overline{\lambda}\zeta \neq -\lambda\zeta - \overline{\lambda}\zeta^{-1}$, while the right-hand side above remains fixed, which is impossible. □

By Lemma 9, $\Phi_p(x)$ is irreducible over $\mathbb{Q}(\lambda)$. Thus, the extension field $\mathbb{Q}(\lambda,\zeta)$ has degree $2p(p-1)$ over $\mathbb{Q}$. Its maximal real subfield must therefore have degree $\leq p(p-1)$.

Lemma 12. *Let p be a prime ≥ 5, and let m be an integer ≥ 2. The splitting field of $f_{p,m}$ is the maximal real subfield of $\mathbb{Q}(\lambda,\zeta)$ and can be written as*

$$K = \mathbb{Q}(\lambda+\overline{\lambda}, \zeta+\zeta^{-1}, \lambda\zeta+\overline{\lambda}\zeta^{-1}).$$

Proof. Observe that K is a real subfield of $\mathbb{Q}(\lambda,\zeta)$ and that all the roots of $f_{p,m}$ are real numbers in $\mathbb{Q}(\lambda,\zeta)$. From (7) and Lemma 11, $[K:\mathbb{Q}] = p(p-1)$. Since K is a real field of degree $p(p-1)$ over $\mathbb{Q}$, it is the maximal real subfield of $\mathbb{Q}(\lambda,\zeta)$, and consequently $f_{p,m}$ splits in K. If L is the splitting field of $f_{p,m}$, it follows that $L \subseteq K$. Note that $\lambda+\overline{\lambda}$, $\lambda\zeta+\overline{\lambda}\zeta^{-1}$ as well as $\lambda\zeta^{-1}+\overline{\lambda}\zeta$ are roots of $f_{p,m}(-x)$ and, hence, in L. To show then that $L = K$ it suffices to show that $\zeta+\zeta^{-1} \in L$, and this follows from

$$\zeta+\zeta^{-1} = \frac{(\lambda\zeta+\overline{\lambda}\zeta^{-1}) + (\lambda\zeta^{-1}+\overline{\lambda}\zeta)}{\lambda+\overline{\lambda}}.$$

This completes the proof. □

We are now ready to establish Theorem B of the introduction.

Theorem 13. *(Theorem B) Let $p \geq 5$ be a prime, and let $m \geq 2$ be an integer. The Galois group of the splitting field $K/\mathbb{Q}$ of $f_{p,m}$ is a subgroup of the symmetric group S_p of order $p(p-1)$ generated by a cycle of length p and a cycle of length $p-1$.*

Proof. As $K \subseteq \mathbb{Q}(\lambda,\zeta)$, an automorphism of K can be described by its actions on λ and ζ. Let g be a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. We show that the Galois group of the splitting field $K/\mathbb{Q}$ of $f_{p,m}$ is the subgroup of the symmetric group S_p generated by the automorphisms σ and τ, where $\sigma(\lambda) = \lambda\zeta$, $\sigma(\zeta) = \zeta$, $\tau(\lambda) = \lambda$, and $\tau(\zeta) = \zeta^g$. One has that σ is an automorphism of K which fixes $\mathbb{Q}$, whose order is p. Moreover, τ is an automorphism of K which fixes $\mathbb{Q}$ of order $p-1$. Since $[K:\mathbb{Q}] = p(p-1)$, we deduce that $\mathrm{Gal}(K/\mathbb{Q})$ is as claimed. □

References

[BS] Z. I. Borevich, I.R. Shafarevich, Number Theory, Academic Press, New York, 1986.

[Le] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation* $x^m = y^2 + 1$, Nouv. Ann. Math., **9**, (1850), 178-181.

[LMT] R. Lidl, G. L. Mullen, G. Turnwald, Dickson polynomials, Pitman Monographs and Surveys in Pure and Applied Mathematics, 65, Longman Scientific & Technical, Harlow; copublished in the United States with John Wiley & Sons, Inc., New York, 1993.

[O] O. Ore, *Some Studies on cyclic determinants*, Duke Math. J., (1951), 343-354.

[Ri] T. J. Rivlin, The Chebyshev Polynomials, John Wiley and Sons, New York, 1974.

[Sc1] A. Schinzel, Selected Topics on Polynomials, Univ. of Michigan Press, Ann Arbor, 1982.

[Sc2] A. Schinzel, *On reducible trinomials*, Dissert. Math., **329**, (1993).

[Wae] B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann., **109**, (1934), 13-16.