ON A PROCEDURE FOR FINDING THE GALOIS GROUP OF A
QUINTIC POLYNOMIAL

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

Received November 27, 2001

Abstract. In [4, Proposition, pp. 883–884] a procedure is given to find the Galois

group of an irreducible quintic polynomial $f(x) \in \mathbb{Z}[x]$. It is shown that this procedure does

not always find the Galois group.

1. Introduction. Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible quintic polynomial. The Galois

group $\text{Gal}(f)$ of $f(x)$ over $\mathbb{Q}$ is isomorphic to one of $S_5$ (the symmetric group of order 120),

$A_5$ (the alternating group of order 60), $F_{20}$ (the Frobenius group of order 20), $D_5$ (the dihedral
group of order 10) or $\mathbb{Z}_5$ (the cyclic group of order 5), see [1, p. 872] or [3, pp.

556–557]. Let $p$ be a prime. We write

$$f(x) \equiv (d_1)^{n_1} \cdots (d_r)^{n_r} \quad (\text{mod } p)$$

to denote that $f(x)$ factors modulo $p$ into $r$ distinct irreducible factors of degrees $d_1, \ldots, d_r$

and multiplicities $n_1, \ldots, n_r$ respectively. The following procedure [4, Proposition, pp.

883–884] has been given for determining $\text{Gal}(f)$.

Let $p$ be a prime $\equiv 1$ (mod 5) such that

$$f(x) \equiv (1)(1)(1)(1)(1) \quad (\text{mod } p).$$

We know that such a prime exists by the Tchebotarev density theorem.

1. If there exists a prime $p_1 < p$ such that $f(x) \equiv (2)(3) \quad (\text{mod } p_1)$ then $\text{Gal}(f) \cong S_5$.

2. If there exists a prime $p_2 < p$ such that $f(x) \equiv (1)(1)(3) \quad (\text{mod } p_2)$ and case 1 does

not hold then $\text{Gal}(f) \cong A_5$.

3. If there exists a prime $p_3 < p$ such that $f(x) \equiv (1)(4) \quad (\text{mod } p_3)$ and cases 2 and 3 do

not hold then $\text{Gal}(f) \cong F_{20}$.

4. If there exists a prime $p_4 < p$ such that $f(x) \equiv (1)(2)(2) \quad (\text{mod } p_4)$ and cases 2, 3 and

4 do not hold then $\text{Gal}(f) \cong D_5$.

5. If for every prime $q < p$ either $f(x) \equiv (1)(1)(1)(1)(1) \quad (\text{mod } q)$ or $f(x) \equiv (5) \quad (\text{mod } q)$

then $\text{Gal}(f) \cong \mathbb{Z}_5$.

We show that this procedure is not guaranteed to determine $\text{Gal}(f)$. We illustrate this

with the parametric family

$$c_k(x) = x(x + 9)(x^3 + 3x + 3) + 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11(3k + 1), \quad k \in \mathbb{Z}. \quad (1)$$

2000 Mathematics Subject Classification. Primary 11R09, 11R32, 11Y40.

Key words and phrases. quintic polynomial, Galois group.
We prove

**Theorem.** (a) \( c_k(x) \) is irreducible for all \( k \in \mathbb{Z} \).

\[
\begin{align*}
c_k(x) &\equiv (1)(3)(\text{mod } 2), \\
c_k(x) &\equiv (1)(3)(\text{mod } 3), \\
c_k(x) &\equiv (1)(3)(\text{mod } 5), \\
c_k(x) &\equiv (1)(1)(2)(\text{mod } 7), \\
c_k(x) &\equiv (1)(1)(1)(1)(\text{mod } 11).
\end{align*}
\]

(c) \( \text{Gal}(c_k(x)) \cong S_5 \) for all \( k \) in \( \mathbb{Z} \).

(d) Let \( p_1 = 13, p_2 = 17, p_3 = 19, \ldots \) be the primes \( > 11 \). For each positive integer \( t \) there exist infinitely many \( k \in \mathbb{Z} \) such that the least prime \( p \) for which \( c_k(x) \equiv (2)(3) \) (mod \( p \)) satisfies \( p > p_t \).

With \( p = 11 \) the procedure gives \( \text{Gal}(c_k(x)) \cong A_5 \) \( (k \in \mathbb{Z}) \) contradicting \( \text{Gal}(c_k(x)) \cong S_5 \) \( (k \in \mathbb{Z}) \). Thus the procedure does not find the correct Galois group for infinitely many quintics. Part (d) of the Theorem shows that however large we choose the prime \( p \) the procedure still fails for infinitely many quintics. In order to prove part (d) of the Theorem we use the following result.

**Proposition.** Let \( g(x) \in \mathbb{Z}[x] \). Let \( p \) be a prime such that

\[
g(x) \not\equiv c h(x)^2 \pmod{p}, \quad c \in \mathbb{Z}, \quad h(x) \in \mathbb{Z}[x].
\]

Then

\[
\sum_{x=0}^{p-1} \left( \frac{g(x)}{p} \right) \leq (n-1)\sqrt{p},
\]

where \( n \) denotes the degree of \( g(x) \) and \( \left( \frac{s}{p} \right) \) is the Legendre symbol modulo \( p \).

This character sum estimate is due to Weil [7, p. 207] and is a consequence of his proof of the Riemann hypothesis for algebraic function fields over a finite field [6].

2. **Proof of Theorem.** (a) From (1) we have

\[
c_k(x) = x^5 + 9x^4 + 3x^3 + 30x^2 + 27x + 6930k + 2310
\]

so that \( c_k(x) \) is 3—Eisenstein and thus irreducible.

\[
\begin{align*}
c_k(x) &\equiv x(x+1)(x^3+x+1) \pmod{2}, \\
c_k(x) &\equiv x^5 \pmod{3}, \\
c_k(x) &\equiv x(x+4)(x^3+3x+3) \pmod{5}, \\
c_k(x) &\equiv x(x+2)(x+6)(x^2+x+4) \pmod{7}, \\
c_k(x) &\equiv x(x+2)(x+3)(x+6)(x+9) \pmod{11}.
\end{align*}
\]

(c) The discriminant of \( c_k(x) \) is

\[
d(k) = 720747193753125000k^4 + 148399767947315800k^3
\]
\[+996640539362977500k^2 + 2785738364780554260k + 278489107278162009.\]

As \(d(k) \equiv 5 \pmod{7}\) we deduce that \(d(k)\) is not a perfect square. Hence \(\text{Gal}(c_k(x))\) is not a subgroup of \(A_5\) and so

\[\text{Gal}(c_k(x)) \cong F_{20} \text{ or } S_5.\]

Further, as \(d(k) \not\equiv 0 \pmod{2}\) and

\[c_k(x) \equiv (1)(1)(3) \pmod{2},\]

by [3, Corollary 41, p. 554] \(\text{Gal}(c_k(x))\) contains a 3-cycle. Hence 3 divides the order of \(\text{Gal}(c_k(x))\). But 3 does not divide the order of \(F_{20}\) so \(\text{Gal}(c_k(x)) \cong S_5\).

(d) Let \(p\) be a prime \(> 11\). The number \(N\) of pairs \((k, y)\) of integers modulo \(p\) satisfying the congruence

\[y^2 \equiv d(k) \pmod{p}\]

is

\[N = \sum_{k=0}^{p-1} \left( 1 + \left( \frac{d(k)}{p} \right) \right) = p + \sum_{k=0}^{p-1} \left( \frac{d(k)}{p} \right).\]

Now the coefficient of \(k^4\) in \(d(k)\) is

\[2^4 \cdot 3^8 \cdot 5^6 \cdot 7^4 \cdot 11^4\]

and the discriminant of \(d(k)\) is

\[-2^{20} \cdot 3^{55} \cdot 5^{15} \cdot 7^{12} \cdot 11^{12} \cdot 37^2 \cdot 382103^2 \cdot 8570461^2\]

so that for \(p \neq 37, 382103, 8570461\) we have

\[d(k) \not\equiv c h(k)^2 \pmod{p}\]

for any \(c \in \mathbb{Z}\) and any polynomial \(h(k) \in \mathbb{Z}[x]\). Hence by the Proposition

\[\left| \sum_{k=0}^{p-1} \left( \frac{d(k)}{p} \right) \right| \leq (\deg(d(k)) - 1) \sqrt{p} = 3 \sqrt{p}.\]

Thus for \(p \neq 13, 17, 37, 382103, 8570461\) we have

\[N \geq p - 3 \sqrt{p} \geq 5,\]

so that there exists \(k_p \in \mathbb{Z}\) such that

\[(2) \quad \left( \frac{d(k_p)}{p} \right) = 1.\]

For \(p = 13, 17, 37, 382103, 8570461\) we choose \(k_p = 1, 4, 3, 3, 2\) respectively so that (2) holds in these cases as well.

Let \(t \in \mathbb{N}\). By the Chinese remainder theorem we can choose infinitely many integers \(k\) such that

\[(3) \quad k \equiv k_p \pmod{p_i}, \quad i = 1, \ldots, t.\]
Hence, by (2) and (3), we have

\[
\left( \frac{d(k)}{p_i} \right) = \left( \frac{d(k_{p_i})}{p_i} \right) = 1, \quad i = 1, \ldots, t.
\]

But, by Stickelberger’s theorem [5], [2], we have

\[
\left( \frac{d(k)}{p_i} \right) = (-1)^{5-r_i}, \quad i = 1, \ldots, t,
\]

where \( r_i \) is the number of irreducible factors of \( c_k(x) \) (mod \( p_i \)). Thus, by (4) and (5), we have

\[
r_i \equiv 1 \pmod{2}, \quad i = 1, \ldots, t.
\]

Hence

\[
c_k(x) \not\equiv (2)(3) \pmod{p_i}, \quad i = 1, \ldots, t.
\]

Thus the least prime \( p \) for which

\[
c_k(x) \equiv (2)(3) \pmod{p}
\]

satisfies \( p > p_i \).

References


Department of Mathematics and Statistics
Okanagan University College
Kelowna, British Columbia V1V 1V7
Canada
e-mail: bspearman@okanagan.bc.ca

Centre for Research in Algebra and Number Theory
School of Mathematics and Statistics
Carleton University
Ottawa, Ontario K1S 5B6
Canada
e-mail: williams@math.carleton.ca