Scientiae Mathematicae Japonicae, 57, No. 1 (2003), 187-190, :e7, 185-188

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 $\in \mathbb{Z}[x]$. 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 Gal(f) of f(x) over 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

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

to denote that f(x) factors modulo p into r distinct irreducible factors of degrees d_1, \dots, d_r and multiplicities n_1, \dots, n_r respectively. The following procedure [4, Proposition, pp. 883-884] has been given for determining Gal(f).

Let p be a prime $\equiv 1 \pmod{5}$ such that

 $f(x) \equiv (1)(1)(1)(1)(1) \pmod{p}.$

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

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

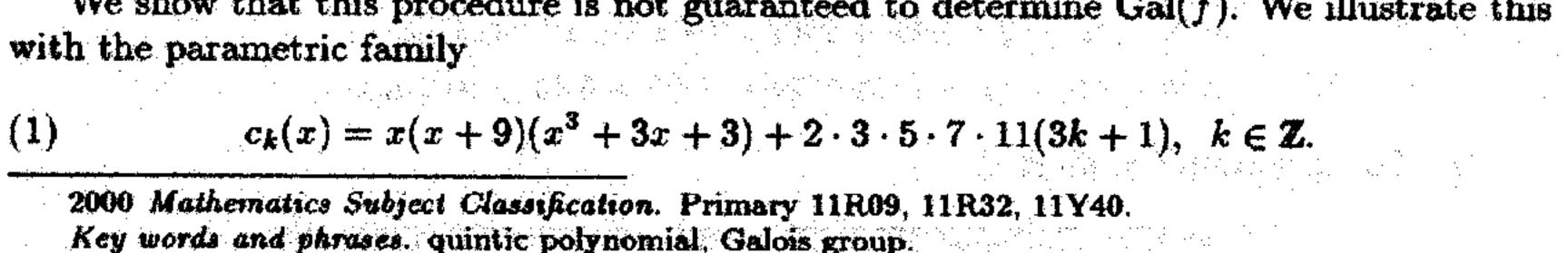
2. If there exists a prime $p_2 < p$ such that $f(x) \equiv (1)(1)(3) \pmod{p_2}$ and case 1 does not hold then $Gal(f) \cong A_5$.

3. If there exists a prime $p_3 < p$ such that $f(x) \equiv (1)(4) \pmod{p_3}$ and cases 2 and 3 do not hold then $Gal(f) \cong F_{20}$.

4. If there exists a prime $p_4 < p$ such that $f(x) \equiv (1)(2)(2) \pmod{p_4}$ and cases 2, 3 and 4 do not hold then $\operatorname{Gal}(f) \cong D_5$.

5. If for every prime q < p either $f(x) \equiv (1)(1)(1)(1)(1) \pmod{q}$ or $f(x) \equiv (5) \pmod{q}$ then $\operatorname{Gal}(f) \cong \mathbb{Z}_5$.

We show that this procedure is not guaranteed to determine Gal(f). We illustrate this



188

(b)

BLAIR K. SPEARMAN AND KENNETH S. WILLIAMS

We prove

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

- $c_{k}(x) \equiv (1)(1)(3) \pmod{2}.$
 - $c_k(x) \equiv (1)^5 \pmod{3}.$
 - $c_k(x) \equiv (1)(1)(3) \pmod{5}.$
- $c_k(x) \equiv (1)(1)(1)(2) \pmod{7}.$
- $c_k(x) \equiv (1)(1)(1)(1)(1) \pmod{11}$.

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

(d) Let $p_1 = 13$, $p_2 = 17$, $p_3 = 19$, ... 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 $c_k(x) \equiv (2)(3) \pmod{p}$ satisfies $p > p_t$.

With p = 11 the procedure gives $Gal(c_k(x)) \cong A_s$ $(k \in \mathbb{Z})$ contradicting $Gal(c_k(x)) \cong S_s$ $(k \in \mathbb{Z})$. 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

Proposition. Let $g(x) \in \mathbb{Z}[x]$. Let p be a prime such that $g(x) \not\equiv ch(x)^2 \pmod{p}, \ c \in \mathbb{Z}, \ h(x) \in \mathbb{Z}[x].$

Then

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

where n denotes the degree of g(x) and $\binom{*}{p}$ 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].

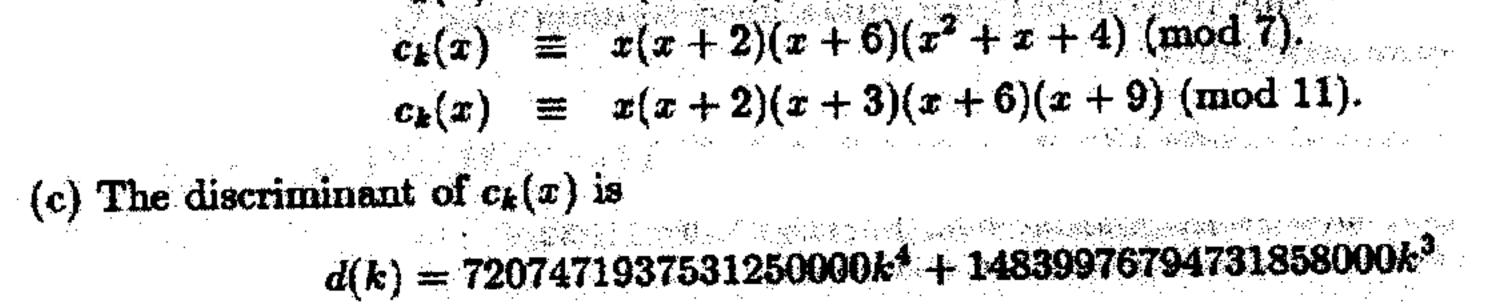
2. Proof of Theorem. (a) From (1) we have

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

so that $c_k(x)$ is 3-Eisenstein and thus irreducible.

(b) $c_k(x) \equiv x(x+1)(x^3+x+1) \pmod{2}.$ $c_k(x) \equiv x^5 \pmod{3}.$

 $c_k(x) \equiv x(x+4)(x^3+3x+3) \pmod{5}.$



GALOIS GROUP OF A QUINTIC

 $+9996640539362977500k^{2} + 2785738364780554260k$

+278489107278162009.

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

 $\operatorname{Gal}(c_k(x)) \cong F_{20} \text{ or } S_5.$

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] $Gal(c_k(x))$ contains a 3-cycle. Hence 3 divides the order of $Gal(c_k(x))$. But 3 does not divide the order of F_{20} so $Gal(c_k(x)) \cong S_5$.

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

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

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

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

18

$$2^4 \cdot 3^8 \cdot 5^9 \cdot 7^4 \cdot 11^4$$

and the discriminant of d(k) is

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

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

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

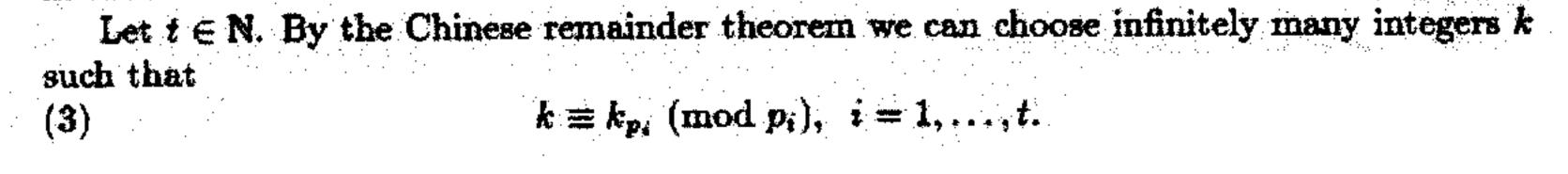
Thus for $p \neq 13, 17, 37, 382103, 8570461$ we have

$$N\geq p-3\sqrt{p}\geq 5,$$

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

(2)
$$\left(\frac{d(k_p)}{p}\right) = 1.$$

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.



Hence, by (2) and (3), we have

190

(4)

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

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

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

where r_i is the number of irreducible factors of $c_k(x) \pmod{p_i}$. Thus, by (4) and (5), we have $r_i \equiv 1 \pmod{2}, i = 1, \dots, t$.

Hence $c_k(x) \not\equiv (2)(3) \pmod{p_i}, i = 1, ..., t.$

Thus the least prime p for which $c_k(x) \equiv (2)(3) \pmod{p}$

satisfies $p > p_t$.

REFERENCES

- G. Butler and J. McKay, The transitive groups of degree up eleven, Comm. Algebra 11 (1983), 863-911.
- [2] L. Carlitz, A theorem of Stickelberger, Math. Scand. 1 (1953), 82-84.
- [3] D. S. Dummit and R. M. Foote, Abstract Algebra, Prentice Hall, New Jersey, 1991.
- [4] S. Kobayashi and H. Nakagawa, Resolution of solvable quintic equation, Math. Japonica 37 (1992), 883-886.
- [5] L. Stickelberger, Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper, Verhandlungen des ersten internationalen Mathematiker-Kongresses in Zürich 1897, Leipzig, 1898, pp. 182–193.
- [6] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, Publ. Inst. Math. Univ. Strasbourg 7 (1945), 1-85.

- [7] A. Weil, On some exponential sums, Proc. Nat. Acad. Sci. (USA) 84 (1948), 204-207.
- 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