Indian J. pure appl. Math., **36**(6) : 295-300, June 2005

A NOTE ON DIHEDRAL POLYNOMIALS OF PRIME DEGREE

JOAN-C. LARIO AND MARC MASDEU

Faculttat de Mathematiques Aplicada II, *Universitat Politecnica De Catalunya, Cl. Pau, Gargallo* 5 *E*-08028, *Barcelona*

(*Received* 27 *March* 2004; *after final revision* 1 *April* 2005 *accepted* 2 *June* 2005)

We present an algorithm to determine all roots of a prime degree p polynomial with dihedral Galois group D_{2p} as rational functions of any two of them. This must be seen as an effective version of a more general result of Galois valid for prime degree equations with solvable group.

Key Words: Computational Number Theory; Galois Theory

1. INTRODUCTION

Let k be a field of characteristic zero, and $f \in k[x]$ be an irreducible polynomial of prime degree p. A well-known theorem asserts that f is solvable by radicals if and only if all its roots can be expressed as rational functions over k of any two of them. The original proof of this result was exposed in a memoir of Galois rejected by the French Academy in 1831. We refer to [Sig] for an updated proof in a modern language. In addition, it must be pointed out that the proof is far from being algorithmic; it merely shows the existence of such relations among the roots but not how to produce the rational functions themselves.

The first non-trivial case being for $p = 5$, Spearman and Williams provided an algorithm in [Sp-Wi] to solve the problem from a computational point of view for quintic polynomials with Galois group isomorphic to the dihedral group D_{10} of ten elements. In this short note, our aim is to present an algorithm that solves the problem for the dihedral case D_{2p}, where p is any prime.

A brute-force algorithm consists in factoring the polynomial f over $k(\alpha, \beta)$, where α and β denote any two roots of f. Under the solvability hypothesis for its Galois group, f decomposes as linear factors over $k(\alpha, \beta)$. The existent general algorithms to perform this task are based in a

The authors are partially supported by DGICYT Grant BFM 2003-06768-C02-01.

combination of the Hensel's lift followed by a reconstructing process (for instance, see [Rob]). In the specific setting under consideration, our algorithm avoids this double factorization, simplifying somehow the costs of computation. Indeed, we need instead to factorize f only over $k(\alpha)$ and then make use of the Chebotarev density theorem along with basic properties of the dihedral group.

2. THREE LEMMAS

From now on, we assume that $f \in k[x]$ is monic irreducible of odd prime degree p with Galois group isomorphic to D_{2p}. We fix $\bar{k}$ an algebraic closure of k.

Lemma 2.1 — There exist $(p-1)/2$ pairs of polynomials $(g_i(t), h_i(t))$ in $k[t]$ of degree at most $p-1$ such that

$$(x-\alpha)\prod_{i=1}^{(p-1)/2}(x^2+g_i(\alpha)x+h_i(\alpha))$$

is the factorization of $f(x)$ into irreducible polynomials in $k(\alpha)[x]$, where α is any root of f.

PROOF : Fix α a root of f, and let $L=k(\alpha)$. Since f is irreducible, we have that $[L:k]=p$. Clearly, $x-\alpha$ is a factor of f over $L[x]$. On one hand, no other linear factors can occur in the factorization of f over L; otherwise L would be the splitting field of f in accordance with the above mentioned result of Galois since deg f is prime and D_{2p} is a solvable group. On the other hand, no irreducible factors of degree greater than 2 can occur either; otherwise the splitting field of f over k would have degree $>2p$.

The polynomials $g_i(t)$ and $h_i(t)$ in $k[t]$ can be chosen of degree at most $p-1$ since α has degree p, and do not depend on the root α: for if α' is another root of f, then $k(\alpha)$ and $k(\alpha')$ are k-isomorphic. □

Lemma 2.2 — Let α and β two different roots of f. There is a unique $\sigma \in Gal(f)$ of order 2 such that $\sigma(\alpha)=\beta$.

PROOF : After a suitable ordering of the roots of f as $\{x_0, x_1, ..., x_{p-1}\}$ with indices considered mod p, the Galois group of f is generated by the automorphisms $\tau(x_k)=d_{k+1}$ and $\nu(x_k) = x_{-k}$ for all k. Then, $\alpha=x_i$ and $\beta=x_j$ for some indices i and The elements of order 2

are precisely the conjugates of ν. We have that

$$\tau^n \nu \tau^{-n}(x_i) = \tau^n \nu (x_{i-n}) = \tau^n (x_{n-i}) = x_{2n-1}.$$

Since p is odd, there is a unique solution of the congruence $2n - i \equiv j \pmod{p}$. That gives the unique σ with the desired requirements. □

Since we want to make use of an effective version of the Chebotarev density theorem, hereafter we assume that $k = \mathbb{Q}$.

Lemma 2.3 — Let K be the splitting field of f over k, and let Δ be its discriminant. Assuming the Extended Riemann Hypothesis for the Dedekind zeta function of K, there is a prime ℓ such that

$$\ell \leq (4 \log |\Delta| + 5p + 5)^2 \text{ and } f(x) \equiv \prod_{i=0}^{p-1} (x \in \gamma_i) \pmod{\ell},$$

for some $\gamma_i \in \mathbb{F}_\ell$.

PROOF : This is an immediate consequence of the effective version of the Chebotarev density theorem obtained by Bach and Sorenson in [1]. □

3. THE ALGORITHM

The above lemmas justify the first steps of the following algorithm to determine all roots of a dihedral equation of degree p in terms of any two of them.

Input : $f \in k[x]$ as above, and α, β two different roots of f;

Output : the p roots of f as rational functions of α and β.

1. Factorize $f(x) = (x - \alpha) \prod_{i=1}^{(p-1)/2} P_i(x)$ over $k(\alpha)$.

2. Choose the smallest prime ℓ such that $f(x)$ splits completely mod ℓ.

3. Initialize RootSet := $\{\alpha, \beta\}$, $\beta_{\text{new}} := \alpha$, and ModRoot := β mod ℓ.

4. While # RootSet $< p$, do

Select the (unique) i such that P_i (ModRoot) $\equiv 0 \pmod{\ell}$

$\beta_{\text{new}} := -\text{Coeff}\ (P_i(x), x) - \sigma(\beta_{\text{new}})$;

RootSet := RootSet $\cup$ $\left\{\beta_{\text{new}}, \sigma(\beta_{\text{new}})\right\}$;

ModRoot := $\sigma(\beta_{\text{new}})$ mod f.

5. Return Root Set.

For an efficient implementation of Step 1, we refer to (3). The automorphism σ in Step 4 is the one guaranteed by Lemma 2.2, and the Coeff $(P_i(x), x)$ function returns the linear coefficient of $P_i(x)$. Notice that β_{new} is reassigned to be the root other than $\sigma(\beta_{\text{new}})$ in $P_i(x)$. This new root lies in $k(\alpha, \beta)$, so one gets readily $\sigma(\beta_{\text{new}})$ after switching the occurrences of α and β in β_{new}.

Proposition 3.1 — After $(p-1)/2$ iterations of Step 4, the algorithm terminates.

PROOF : Consider again $\alpha = x_i$ and $\beta = x_j$ as in the proof of Lemma 2.2, and let s_α be the unique element in D_{2p} that fixes α. Then, $\sigma(x_k) = x_{i+j-k}$ and $s_\alpha(x_k) = x_{2i-k}$ for every k.

Step 4 applies alternatively s_α and σ to the initial root β. Starting with $\beta = x_j$, after n iterations we get $\beta_{\text{new}} = x_{n(i-j)+i}$ and $\sigma(\beta_{\text{new}}) = x_{n(j-i)+j}$. Since α and β are different, $(i-j)$ is a generator of the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. It follows that when $n = (p-1)/2$ we will have obtained all roots (the last one fixed by σ). □

4. SOME EXAMPLES

The following polynomials of prime degree and dihedral Galois group have been taken from the database of number fields of given Galois group up to degree 15 elaborated by Klüners and Malle [2]. Class field theory for quadratic imaginary fields with prime class number also provide a wide source of prime degree dihedral polynomials over $\mathbb{Q}$.

Example with $p = 5$ (Spearman-Williams case). Let $f(x)$ be a polynomial of degree 5, and fix two of its roots, say α and β. Let

$$f(x) = (x-\alpha)(x^2 + f_1(\alpha)x + g_1(\alpha))(x^2 + f_2(\alpha)x + g_2(\alpha))$$

be the factorization of f in $k(\alpha)$. Without loss of generality, suppose that the two quadratic polynomials have been labeled such that β is a root of the first one. The first nontrivial root the algorithm will find is $-f_1(\alpha) - \beta$. After applying σ to it, we get the fourth root, $-f_1(\beta) - \alpha$. Finally,

in the last iteration the algorithm finds $-f_2(\alpha)+f_1(\beta)+\alpha$. Note that this last element is fixed for σ.

Example with $p = 7$. Let $f(x) = x^7 - 2x^6 - 7x^5 + 10x^4 + 13x^3 - 10x^2 - x + 1$, and take α and β the roots of f such that are congruent to 17 and 91 mod $\ell = 283$. The other five roots are:

$$16 + 16\alpha - 99\alpha^2 - 38\alpha^3 + 47\alpha^4 + 9\alpha^5 - 6\alpha^6 - \beta;$$

$$16 + 16\beta - 99\beta^2 - 38\beta^3 + 47\beta^4 + 9\beta^5 - 6\beta^6 - \alpha;$$

$$-22 - 5\alpha + 35\alpha^2 + 13\alpha^3 - 16\alpha^4 - 3\alpha^5 + 2\alpha^6$$

$$-16\beta + 99\beta^2 + 38\beta^3 - 47\beta^4 - 9\beta^5 + 6\beta^6;$$

$$-22 - 5\beta + 35\beta^2 + 13\beta^3 - 16\beta^4 - 3\beta^5 + 2\beta^6$$

$$-16\alpha + 99\alpha^2 + 38\alpha^3 - 47\alpha^4 - 9\alpha^5 + 6\alpha^6;$$

$$14 + 5(\alpha+\beta) - 35(\alpha^2+\beta^2) - 13(\alpha^3+\beta^3) + 16(\alpha^4+\beta^4) + 3(\alpha^5+\beta^5) - 2(\alpha^6+\beta^6).$$

Example with $p = 11$. Let $f(x) = x^{11} - 5x^{10} - 4x^9 + 54x^8 - 53x^7 - 127x^6 + 208x^5 + 69x^4 - 222x^3 + 29x^2 + 56x - 5$, and take α and β the roots of f such that are congruent to 39 and 251 mod $\ell = 397$. The other nine roots are:

$$(-45 + 623\alpha + 795\alpha^2 - 2190\alpha^3 - 670\alpha^4 + 2173\alpha^5 - 111\alpha^6 - 763\alpha^7$$

$$+ 173\alpha^8 + 67\alpha^9 - 18\alpha^{10} - 5\beta)/5;$$

$$(105 - 583\alpha - 831\alpha^2 + 1837\alpha^3 + 776\alpha^4 - 1730\alpha^5 - 31\alpha^6$$

$$+ 589\alpha^7 - 109\alpha^8 - 51\alpha^9 - 623\beta - 795\beta^2 + 2190\beta^3$$

$$+ 670\beta^4 - 2173\beta^5 + 111\beta^6 + 763\beta^7 - 173\beta^8 - 67\beta^9 + 19\beta^{10})/5;$$

$$(-110 = 746\alpha + 862\alpha^2 - 2514\alpha^3 - 637\alpha^4 + 2420\alpha^5 - 188\alpha^6$$

$$- 828\alpha^7 + 198\alpha^8 + 72\alpha^9 - 21\alpha^{10} + 583\beta + 831\beta^2$$

$$- 1837\beta^3 - 776\beta^4 + 1730\beta^5 + 31\beta^6 - 589\beta^7 + 109\beta^8 + 51\beta^9 - 13\beta^{10})/5;$$

$$(90 - 155\alpha - 266\alpha^2 + 497\alpha^3 + 206\alpha^4 - 472\alpha^5 + 13\alpha^6 + 161\alpha^7$$

$$-36\,\alpha^8 - 14\,\alpha^9 + 4\,\alpha^{10} - 746\,\beta - 862\,\beta^2 + 2514\,\beta^3$$

$$+637\,\beta^4 - 2420\,\beta^5 + 188\,\beta^6 + 828\,\beta^7 - 198\,\beta^8 - 72\,\beta^9 + 21\,\beta^{10})/5,$$

their σ-conjugates, and

$$(-55 + 155\,(\alpha+\beta) + 266\,(\alpha^2+\beta^2) - 497\,(\alpha^3+\beta^3) - 206\,(\alpha^4+\beta^4)$$

$$+472\,(\alpha^5+\beta^5) - 13\,(\alpha^6+\beta^6) - 161\,(\alpha^7+\beta^7)$$

$$+36\,(\alpha^8+\beta^8) + 14\,(\alpha^9+\beta^9) - 4\,(\alpha^{10}+\beta^{10}))/5.$$

These and some other examples have been performed using Magma V2.11 on a Pentium 4 at 2.0 GHz. The following table displays the computing times for certain dihedral polynomials of degree $p \leq 23$, comparing the first factorization, the dihedral algorithm, and the double-factorization algorithm. It is noteworthy that the only computing-intensive part of the Dihedral algorithm is the factorization over $k(\alpha)$.

p	First-factorization	Dihedral algorithm	Double-factorization
7	0.058s	0.063s	0.297s
11	0.575s	0.609s	1.969s
13	1.730s	1.810s	5.094s
17	14.442s	14.631s	44.156s
19	22.703s	22.912s	109.210s
23	139.124s	139.854s	1144.747s

REFERENCES

1. E. Bach and J. Sorenson, Explicit bounds for primes in residue classes, *Math. Comp.*, **65** (1996), 1717-35.
2. J. Klüners and G. Malle, *A Database for Number Fields*, in the web page http://www.mathematik.uni-kassel.de/~klueners/minimum/.
3. X. -F. Roblot, Polynomial Factorization Algorithms over Number Fields, *J. Symb. Comput.*, **38** (2004), 1429-43.
4. F. Sigrist, Problem 88-4. *Math. Intelligencer*, **11** (1989), 53-54.
5. B. K. Spearman and K. S. Williams, Dihedral quintic polynomials and a theorem of Galois. *Indian J. Pure Appl. Math.*, **30**(9) (1999), 839-45.