2000 Mathematics Subject Classification12Y05, 12F10, 12F05

A note on dihedral polynomials of prime degree

Joan-C. Lario and Marc Masdeu

Abstract. 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.

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 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.

Key words and phrases. Computational Number Theory, Galois Theory.
The authors are partially supported by DGICYT Grant BFM 2003-06768-C02-01.

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 $\overline{k}$ 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*

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

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 $\sigma \in \mathrm{Gal}(f)$ of order 2 such that $\sigma(\alpha) = \beta$.*

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

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

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*

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

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 [Bac-Sor]. □

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 $\alpha$, $\beta$ two different roots of $f$;
Output:  the $p$ roots of $f$ as rational functions of $\alpha$ and $\beta$.

1. Factorize $f(x) = (x-\alpha)\prod_{i=1}^{(p-1)/2} P_i(x)$ over $k(\alpha)$.
2. Choose a prime $\ell$ such that $f(x) \equiv \prod_{i=0}^{p-1}(x-\gamma_i) \pmod{\ell}$.
3. Initialize List $:= \{\alpha, \beta\}$ and ModList $:=$ List mod $\ell$.
4. Set $\sigma$ the involution that switches $\alpha$ and $\beta$.
5. While $\#$List $< p$, do
       $P(x) := P_i(x)$ such that $P_i(\mathrm{Last}(\texttt{ModList})) \equiv 0 \pmod{\ell}$;
       $\beta_{\mathrm{new}} := -\,\mathrm{Coeff}(P(x), x) - \mathrm{Last}(\texttt{List})$;
       List $:=$ List $\cup \{\beta_{\mathrm{new}}, \sigma(\beta_{\mathrm{new}})\}$;
       ModList $:=$ ModList $\cup \{\sigma(\beta_{\mathrm{new}}) \mod p\}$.
6. Return List $\setminus$ Last(List).
```

Some comments are in order. The function Last returns the last element of a list, and ModList means the list formed by the mod ℓ reduction of its elements. Notice that the new root β_{new} obtained in Step 5 lies in $k(\alpha, \beta)$, and applying σ to it just represents to switch α and β in β_{new}. Now, we need to ensure that the loop in Step 5 always reaches the end. For it, consider again $\alpha = x_i$ and $\beta = x_j$ as in the proof of lemma 2.2. Then, σ acts as $\sigma(x_k) = x_{i+j-k}$ and $s_\alpha(x_k) = x_{2i-k}$ is the unique element in D_{2p} that fixes α. Step 5 essentially consists in applying s_α and $\sigma \circ s_\alpha$. Starting with x_j, after n iterations we get $x_{n(i-j)+i}$ and $x_{n(j-i)+j}$ as β_{new} and $\sigma(\beta_{\mathrm{new}})$, respectively. Since α and β are different, it follows that when $n = (p-1)/2$ we will have obtained all roots (the last one fixed by σ), and therefore $\#\texttt{List} > p$.

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 [Klu-Mal]. 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 $p = 7$. Let $f(x) = x^7 - 2\,x^6 - 7\,x^5 + 10\,x^4 + 13\,x^3 - 10\,x^2 - x + 1$, 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 $f(x) = x^{11} - 5\,x^{10} - 4\,x^9 + 54\,x^8 - 53\,x^7 - 127\,x^6 + 208\,x^5 + 69\,x^4 - 222\,x^3 + 29\,x^2 + 56\,x - 5$, 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:

$$(-45+623\,\alpha+795\,\alpha^2-2190\,\alpha^3-670\,\alpha^4+2173\,\alpha^5-111\,\alpha^6-763\,\alpha^7+173\,\alpha^8+67\,\alpha^9-19\,\alpha^{10}-5\,\beta)/5\,;$$

$$(105-583\,\alpha-831\,\alpha^2+1837\,\alpha^3+776\,\alpha^4-1730\,\alpha^5-31\,\alpha^6+589\,\alpha^7-109\,\alpha^8-51\,\alpha^9+13\,\alpha^{10}-623\,\beta- \\ 795\,\beta^2+2190\,\beta^3+670\,\beta^4-2173\,\beta^5+111\,\beta^6+763\,\beta^7-173\,\beta^8-67\,\beta^9+19\,\beta^{10})/5\,;$$

$$(-110+746\,\alpha+862\,\alpha^2-2514\,\alpha^3-637\,\alpha^4+2420\,\alpha^5-188\,\alpha^6-828\,\alpha^7+198\,\alpha^8+72\,\alpha^9-21\,\alpha^{10}+ \\ 583\,\beta+831\,\beta^2-1837\,\beta^3-776\,\beta^4+1730\,\beta^5+31\,\beta^6-589\,\beta^7+109\,\beta^8+51\,\beta^9-13\,\beta^{10})/5\,;$$

$$(90-155\,\alpha-266\,\alpha^2+497\,\alpha^3+206\,\alpha^4-472\,\alpha^5+13\,\alpha^6+161\,\alpha^7-36\,\alpha^8-14\,\alpha^9+4\,\alpha^{10}-746\,\beta- \\ 862\,\beta^2+2514\,\beta^3+637\,\beta^4-2420\,\beta^5+188\,\beta^6+828\,\beta^7-198\,\beta^8-72\,\beta^9+21\,\beta^{10})/5\,,$$

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 costs of first factorization, the dihedral algorithm, and the double-factorization. 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	$0.058\,s$	$0.063\,s$	$0.297\,s$
11	$0.575\,s$	$0.609\,s$	$1.969\,s$
13	$1.730\,s$	$1.810\,s$	$5.094\,s$
17	$14.442\,s$	$14.631\,s$	$44.156\,s$
19	$22.703\,s$	$22.912\,s$	$109.210\,s$
23	$139.124\,s$	$139.854\,s$	$1144.747\,s$

References

[Bac-Sor] Bach, E.; Sorenson, J.: “Explicit bounds for primes in residue classes”, Math. Comp. 65 (1996), 1717-1735.

[Klu-Mal] Klüners, J.; Malle, G.: “A Database for Number Fields”, in the web page http://www.mathematik.uni-kassel.de/∼klueners/minimum/.

[Rob] Roblot, X.-F. “Polynomial Factorization Algorithms over Number Fields”, to appear in J. Symbolic Computation.

[Sig] Sigrist, F. “Problem 88-4.” Math. Intelligencer 11 (1989), 53-54.

[Sp-Wi] Spearman, B.K.; Williams, K.S. “Dihedral quintic polynomials and a theorem of Galois.” Indian J. Pure Appl. Math. 30 (1999), no. 9, 839–845.