ON GENERIC POLYNOMIALS FOR DIHEDRAL GROUPS

ARNE LEDET

Abstract. We provide an explicit method for constructing generic polynomials for dihedral groups of degree divisible by four over fields containing the appropriate cosines.

1. Introduction

Given a field K and a finite group G, it is natural to ask what a Galois extension over K with Galois group G looks like. One way of formulating an answer is by means of generic polynomials:

Definition. A monic separable polynomial $P(\mathbf{t}, X) \in K(\mathbf{t})[X]$, where $\mathbf{t} = (t_1, \ldots, t_n)$ are indeterminates, is *generic* for G over K, if it satsifies the following conditions:

(a) $\mathrm{Gal}(P(\mathbf{t}, X)/K(\mathbf{t})) \simeq G$; and
(b) whenever M/L is a Galois extension with Galois group G and $L \supseteq K$, there exists $a_1, \ldots, a_n \in L)$ such that M is the splitting field over L of the specialised polynomial $P(a_1, \ldots, a_n, X) \in L[X]$.

The indeterminates $\mathbf{t}$ are the *parameters*.

Thus, if $P(\mathbf{t}, X)$ is generic for G over K, every G-extension of fields containing K 'looks just like' the splitting field of $P(\mathbf{t}, X)$ itself over $K(\mathbf{t})$.

This concept of a generic polynomial was shown by Kemper [Ke2] to be equivalent (over infinite fields) to the concept of a *generic extension*, as introduced by Saltman in [Sa].

For examples and further references, we refer to [JL&Y].

The inspiration for this paper came from [H&M], in which Hashimoto and Miyake describe a one-parameter generic polynomial for the dihedral group D_n of degree n (and order $2n$), provided that n is odd, that $\mathrm{char}\, K \nmid n$, and that K contains the n^{th} cosines, i.e., $\zeta + 1/\zeta \in K$ for a primitive n^{th} root of unity ζ.

1991 *Mathematics Subject Classification.* 12F12, 12E10.

A more general—but considerably less elegant—construction of generic polynomials for odd-degree dihedral groups in characteristic 0 was given in [Le1].

Also, a construction of generic polynomials for dihedral groups of even degree, assuming the appropriate roots of unity to be in the base field, is given by Rikuna in [Ri].

Remark. In this paper, the *dihedral group* of degree n, $n \geq 3$, is the group D_n of symmetries of a regular n-sided polygon. Thus, it has order $2n$, and is generated by elements σ and τ, with relations $\sigma^n = \tau^2 = 1$ and $\tau\sigma = \sigma^{-1}\tau$.

For dihedral groups of even degree, it is not possible to construct a one-parameter generic polynomial, since the *essential dimension* is at least 2, cf. [B&R]. However, assuming the appropriate cosines are in the base field, it is possible to produce a two-parameter polynomial.

We will consider the case where the degree is a multiple of four, showing:

Theorem. *Let K be a field of characteristic not dividing $2n$, and assume that K contains the $4n^{\text{th}}$ cosines, $n \geq 1$. Also, let*

$$q(X) = X^{4n} + \sum_{i=1}^{2n-1} a_i X^{2i} \in \mathbb{Z}[X]$$

be given by

$$q(X + 1/X) = X^{4n} + 1/X^{4n} - 2.$$

Then the polynomial

$$P(s,t,X) = X^{4n} + \sum_{i=1}^{2n-1} a_i s^{2n-i} X^{2i} + t$$

is generic for D_{4n} over K, with parameters s and t.

Remark. It is a well-known 'folklore' result from algebra that $X^m + 1/X^m$ is an integral polynomial in $X + 1/X$ for all natural numbers m. Also, expressing $X^m + 1/X^m$ in terms of $X + 1/X$ is a simple recursive procedure. Thus, finding $q(X)$ for any given n is straightforward.

That $q(X)$ has no terms of odd degree follows directly from the procedure for producing it: If m is even, the expression for $X^m + 1/X^m$ will involve only even powers of $X + 1/X$, and if m id odd, it will involve only odd power of $X + 1/X$.

That $q(X)$ has no constant term is clear, since $q(0) = q(i + 1/i) = 0$.

Example. If char $K \neq 2$, the polynomial

$$X^4 - 4sX^2 + t$$

is generic for D_4 over K. This is also easily seen directly.

Example. If char $K \neq 2$ and $\sqrt{2} \in K$, the polynomial

$$X^8 - 8sX^6 + 20s^2X^4 - 16s^3X^2 + t$$

is generic for D_8 over K.

Remark. The dihedral group D_8 has a generic polynomial over any field of characteristic $\neq 2$, cf. [Bl] and [Le2]. In the general case, however, the polynomial is considerably more complicated.

Example. If char $K \neq 2, 3$ and $\sqrt{3} \in K$, the polynomial

$$X^{12} - 12sX^{10} + 54s^2X^8 - 112s^3X^6 + 105s^4X^4 - 36s^5X^2 + t$$

is generic for D_{12} over K.

Example. If char $K \neq 2$ and $\sqrt{2+\sqrt{2}} \in K$, the polynomial

$$X^{16} - 16sX^{14} + 104s^2X^{12} - 352s^3X^{10} + \\ 660s^4X^8 - 672s^5X^6 + 336s^6X^4 - 64s^7X^2 + t$$

is generic for D_{16} over K.

Remark. If n is odd, the dihedral group D_{2n} is isomorphic to $D_n \times C_2$, and can thus be described using the result by Hashimoto and Miyake.

2. The proof

We let K be a field of characteristic not dividing $2n$ containing the $4n^{\text{th}}$ cosines for an $n \geq 1$. For convenience, we let ζ denote a primitive $4n^{\text{th}}$ root of unity, and define

$$C = \tfrac{1}{2}(\zeta + 1/\zeta), \quad S = \tfrac{1}{2}i(1/\zeta - \zeta),$$

where $i = \sqrt{-1} = \zeta^n$.

C and S are then elements in K, and we get a two-dimensional faithful representation of D_{4n} over K by

$$\sigma \mapsto \begin{pmatrix} C & -S \\ S & C \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Correspondingly, we get a linear action of D_{4n} on the rational function field $K(u, v)$ by

$$\sigma \colon u \mapsto Cu + Sv, \quad v \mapsto -Su + Cv$$

and

$$\tau\colon u \mapsto u, \quad v \mapsto -v.$$

The Galois extension $K(u,v)/K(u,v)^{D_{4n}}$ is an example of a *linear Noether extension*, and by a general result (which we will recapitulate below), the fixed field $K(u,v)^{D_{4n}}$ is rational: $K(u,v)^{D_{4n}} = K(s,t)$. Theorem 7 in [K&Mt] then gives us that any polynomial over $K(s,t)$ with splitting field $K(u,v)$ will be generic.

We will find s and t as follows: D_{4n} acts (non-faithfully) on the subfield $K(u/v)$, and by Lüroth's Theorem the fixed field is rational: $K(u/v)^{D_{4n}} = K(w)$. Additionally, by [Ke1, Prop.1.1(a)], the extension $K(u,v)^{D_{4n}}/K(u/v)^{D_{4n}}$ is rational, generated by any homogeneous invariant element of minimal positive degree, with this degree equal to the order of the kernel of D_{4n}'s action on $K(u/v)$.

In this case, the kernel has order 2, and as our invariant homogeneous element we can take $s = u^2 + v^2$.

As w, we pick

$$w = \frac{(u^2+v^2)^{2n}}{\prod_{j=0}^{4n-1} \sigma^j u}:$$

It is clearly homogeneous of degree 0, i.e., in $K(u/v)$, and it is trivial to check that numerator and denominator are D_{4n}-invariant. Moreover, if we write it in terms of u/v, as

$$w = \frac{[(u/v)^2+1]^{2n}}{\prod_{j=0}^{4n-1} \sigma^j u/v},$$

it has numerator and denominator of degree $\leq 4n$, meaning that the extension $K(u/v)/K(w)$ has degree $\leq 4n$. On the other hand, $K(w) \subseteq K(u/v)^{D_{4n}}$, and $K(u/v)/K(u/v)^{D_{4n}}$ has degree $4n$. If follows that $K(u/v)^{D_{4n}} = K(w)$.

All in all, we therefore have that

$$K(u,v)^{D_{4n}} = K(s,w),$$

and with

$$t = 2^{4n} \prod_{j=0}^{4n-1} \sigma^j u = 2^{4n} \frac{s^{2n}}{w},$$

we also have

$$K(u,v)^{D_{4n}} = K(s,t).$$

As our generic polynomial, we take the minimal polynomial for $2u$ over $K(s,t)$:

$$P(s,t,X) = \prod_{j=0}^{4n-1} (X - 2\sigma^j u).$$

It is clear that this polynomial has some of the properties from the Theorem: It is monic of degree $4n$, the constant term is t, and it is a polynomial having no terms of odd degree. This last part follows from $\sigma^{2n}u = -u$.

To complete the proof, we now need to prove:

Lemma. *For $1 \leq k < 2n$, we have*

$$e_{2k}(\{-2\sigma^j u\}_{j=0}^{4n-1}) = a_{2n-k}s^k, \tag{1}$$

where a_{2n-k} is the degree-$(4n-2k)$ coefficient in $q(X)$, and e_{2k} denotes the elementary symmetric symbol of degree $2k$.

Proof. For simplicity, we will simply conduct all computations over $\mathbb{R}$. This is permissible, since the algebraic behaviour of C and S matches that of $\cos\frac{2\pi}{4n}$ and $\sin\frac{2\pi}{4n}$, and since the results here will give integer coefficients.

First of all, we prove that

$$q(X) = \prod_{j=0}^{4n-1}(X - 2\cos\tfrac{2\pi j}{4n}) :$$

Let $q_2(X)$ be the polynomial on the right-hand side. Then

$$\begin{aligned} q_2(X+1/X) &= \prod_{j=0}^{4n-1}(X + 1/X - 2\cos\tfrac{2\pi j}{4n}) \\ &= X^{-4n}\prod_{j=0}^{4n-1}(X^2 - 2\cos\tfrac{2\pi j}{4n}X + 1) \\ &= X^{-4n}\prod_{j=0}^{4n-1}[(X - e^{2\pi ij/4n})(X - e^{-2\pi ij/4n})] \\ &= X^{-4n}\prod_{j=0}^{4n-1}(X - e^{2\pi ij/4n})^2 \\ &= X^{-4n}(X^{4n}-1)^2 = X^{4n} + X^{-4n} - 2 \\ &= q(X+1/X). \end{aligned}$$

This proves $q(X) = q_2(X)$.

Now, both the left and right hand sides of (1) are homogeneous polynomials in u and v of degree $2k$. To show that they are equal, it is therefore enough to show that they coincide on more than $2k$ ray classes.

Note that over $\mathbb{R}$, (1) takes the form

$$(2)\quad e_{2k}(\{-2(\cos\tfrac{2\pi j}{4n}u+\sin\tfrac{2\pi j}{4n}v)\}_{j=0}^{4n-1}) = e_{2k}(\{-2\cos\tfrac{2\pi j}{4n}\}_{j=0}^{4n-1})(u^2+v^2)^k.$$

First, consider the ray classes through $(\cos\frac{2\pi\ell}{4n},\sin\frac{2\pi\ell}{4n})$, $0\leq\ell<2n$: Here, (2) becomes

$$e_{2k}(\{-2\cos\tfrac{2\pi(j-\ell)}{4n}\}_{j=0}^{4n-1}) = e_{2k}(\{-2\cos\tfrac{2\pi j}{4n}\}_{j=0}^{4n-1}),$$

which is trivially true. This provides us with $2n$ ray classes.

Next, consider the ray class through $(\cos\frac{2\pi(2\ell+1)}{8n},\sin\frac{2\pi(2\ell+1)}{8n})$, $0\leq\ell<2n$: Here, (2) reduces to

$$e_{2k}(\{-2\cos\tfrac{2\pi(2(j-\ell)-1)}{8n}\}_{j=0}^{4n-1}) = e_{2k}(\{-2\cos\tfrac{2\pi j}{4n}\}_{j=0}^{4n-1}),$$

or

$$e_{2k}(\{-2\cos\tfrac{2\pi(2j-1)}{8n}\}_{j=0}^{4n-1}) = e_{2k}(\{-2\cos\tfrac{2\pi j}{4n}\}_{j=0}^{4n-1}).$$

The claim is then that $q(X)$ and

$$r(X)=\prod_{j=0}^{4n-1}(X-2\cos\tfrac{2\pi(2j-1)}{8n})$$

differ only in their constant term. Since

$$\begin{aligned} r(X+1/X) &= \prod_{j=0}^{4n-1}(X+1/X-2\cos\tfrac{2\pi(2j-1)}{8n}) \\ &= X^{-4n}\prod_{j=0}^{4n-1}(X^2-2\cos\tfrac{2\pi(2j-1)}{8n}X+1) \\ &= X^{-4n}\prod_{j=0}^{4n-1}[(X-e^{2\pi i(2j-1)/8n})(X-e^{-2\pi i(2j-1)/8n})] \\ &= X^{-4n}\prod_{j=0}^{4n-1}(X-e^{2\pi i(2j-1)/4n})^2 \\ &= X^{-4n}(X^{4n}+1)^2 = X^{4n}+X^{-4n}+2, \end{aligned}$$

this is in fact true. Thus, we get another $2n$ ray classes on which (2) holds, and can conclude that the polynomials are equal. □

Remark. As a consequence of these results, we note that

$$K[u,v]^{D_{4n}}=K[s,t]:$$

Clearly, $K[u,v]$ is integral over $K[s,t]$, and $K[s,t]$ is integrally closed. Therefore, $K[u,v]^{D_{4n}}=K(s,t)\cap K[u,v]=K[s,t]$. This is an explicit special case of general results by Shephard–Todd and Chevalley about polynomial invariants for reflection groups, cf. [N&S, Thm. 7.1.4].

References

[Bl] E. V. Black, *Deformations of dihedral* 2*-group extensions of fields*, Trans. Amer. Math. Soc. **351** (1999), 3229–3241.

[B&R] J. Buhler & Z. Reichstein, *On the essential dimension of a finite group*, Compositio Mathematica **106** (1997), 159–179.

[H&M] K. Hashimoto & K. Miyake, *Inverse Galois problem for dihedral groups*, Developments in Mathematics **2**, Kluwer Academic Publishers, 1999, 165–181.

[JL&Y] C. U. Jensen, A. Ledet & N. Yui, *Generic Polynomials: Constructive Aspects of the Inverse Galois Problem*, MSRI Publication Series 45, Cambridge University Press, 2002.

[Ke1] G. Kemper, *A constructive approach to Noether's Problem*, Manuscripta Math. **90** (1996), 343–363.

[Ke2] ———, *Generic polynomials are descent-generic*, Manuscripta Math. **105** (2001), 139–141.

[K&Mt] G. Kemper & E. Mattig, *Generic polynomials with few parameters*, J. Symbolic Computation **30** (2000), 843–857.

[Le1] A. Ledet, *Dihedral extensions in characteristic* 0, C. R. Math. Rep. Canada **21** (1999), 46–52.

[Le2] ———, *Generic polynomials for quasi-dihedral, dihedral and modular extensions of order* 16, Proc. Amer. Math. Soc. **128** (2000), 2213-2222.

[N&S] M. D. Neusel & L. Smith, *Invariant theory of finite groups*, Mathematical Surveys and Monographs **94**, AMS, 2002.

[Ri] Y. Rikuna, *Explicit constructions of generic polynomials for some elementary groups*, 'Galois Theory and Modular Forms' (eds. K. Hashimoto, K. Miyake & H. Nakamura), Developments in Mathematics **11**, Kluwer Academic Publishers, 2004, 173–194.

[Sa] D. J. Saltman, *Generic Galois extensions and problems in field theory*, Adv. Math. **43** (1982), 250–283.

Department of Mathematics and Statistics, Texas Tech University, Lubbock, TX 79409–1042

E-mail address: arne.ledet@ttu.edu