ON GENERIC POLYNOMIALS FOR CYCLIC GROUPS

ARNE LEDET

Abstract. Starting from a known case of generic polynomials for dihedral groups, we get a family of generic polynomials for cyclic groups of order divisible by four over suitable base fields.

1. Introduction

If K is a field, and G is a finite group, a generic polynomial is a way giving a 'general' description of Galois extensions over K with Galois group G. More precisely:

Definition. A monic separable polynomial $P(\mathbf{t}, X) \in K(\mathbf{t})[X]$, with $\mathbf{t} = (t_1, \dots, t_n)$ being indeterminates, is *generic* for G over K, if

(a) $\mathrm{Gal}(P(\mathbf{t}, X)/K(\mathbf{t})) \simeq G$; and
(b) for any Galois extension M/L with Galois group G and $L \supseteq K$, M is the splitting field over L of a specialisation $P(a_1, \dots, a_n, X)$ of $P(\mathbf{t}, X)$, with $a_1, \dots, a_n \in L$.

Over an infinite field, the existence of a generic polynomial is equivalent to existence of a generic extension in the sense of [Sa], as proved in [Ke2].

We refer to [JL&Y] for further results and references.

In this paper, we show

Theorem. *Let K be an infinite field of characteristic not dividing $2n$, and assume that $\zeta + 1/\zeta \in K$ for a primitive $4n^{\text{th}}$ root of unity, $n \geq 1$. If*

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

is given by

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

then the polynomial

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

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

is generic over K for the cyclic group C_{4n} of order $4n$.

The element $\zeta + 1/\zeta$ is the algebraic equivalent of $2\cos\frac{2\pi}{4n}$.

Examples. Over a field K of characteristic $\neq 2$, the polynomial

$$X^4 - 4sX^2 + \frac{4s^2}{t^2+1}$$

is generic for C_4. If additionally we assume $\sqrt{2} \in K$, we get a generic polynomial

$$X^8 - 8sX^6 + 20s^2X^4 - 16s^3X^2 + \frac{4s^4}{t^2+1}$$

for C_8 over K.

Remarks. (1) A generic description of C_8-extensions over fields of characteristic $\neq 2$ containing $\sqrt{2}$ was given by Schneps in [Sc]. On the other hand, in [Sa], Saltman proves that there is no generic extension (and hence no generic polynomial) for C_n over $\mathbb{Q}$, if $8 \mid n$.

(2) For a cyclic group of odd order n, and a field K containing $\zeta+1/\zeta$ for a primitive n^{th} root of unity ζ, Miyake constructed a one-parameter generic polynomial in [Mi]. And of course, if n is odd, the cyclic group of order $2n$ is just $C_2 \times C_n$, and can be considered using Miyake's result.

(3) Generic descriptions of cyclic Galois extensions of odd degree in general are given by Saltman in [Sa].

2. Proof of the Theorem

In [Le], it is shown that

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

is generic for the dihedral group D_{4n} of degree $4n$ (and order $8n$), when $\zeta + 1/\zeta \in K$. This is done by considering the two-dimensional representation of D_{4n} given by

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

where $D_{4n} = \langle \sigma, \tau \mid \sigma^{4n} = \tau^2 = 1,\ \tau\sigma = \sigma^{-1}\tau \rangle$, and $C = \frac{1}{2}(\zeta + 1/\zeta)$, $S = \frac{1}{2}i(1/\zeta - \zeta)$ (and $i = \sqrt{-1} = \zeta^n$). The corresponding action of D_{4n} on the rational function field $K(u, v)$, given by

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

and

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

then has a rational fixed field, namely $K(s, w)$, where

$$s = u^2 + v^2, \quad w = 2^{4n} \cdot \prod_{j=0}^{4n-1} \sigma^j u,$$

and $Q(s, w, X)$ is the minimal polynomial for $2u$ over $K(s, w)$.

Here, we will describe instead the fixed field for the subgroup $C_{4n} = \langle\sigma\rangle$ of D_{4n}: It has the form $K(s, t)$, where

$$t = \frac{(u + iv)^{2n} + (u - iv)^{2n}}{2^{2n} \cdot \prod_{j=0}^{2n-1} \sigma^j u}.$$

Proof. It is clear that $t \in K(u, v)$, and that it is homogeneous of degree 0. The subfield of homogeneous elements of degree 0 is $K(u/v)$, and since t has numerator and denominator of degree $2n$, t generates a subfield of $K(u/v)$ of co-dimension at most $2n$. (t is not a constant, since $v = \sigma^n u$ divides the denominator, but not the numerator.)

Now, C_{4n} acts on $K(u/v)$ in a non-faithful way, with kernel C_2, and t is σ-invariant: Both numerator and denominator changes sign under σ. Consequently, since t is in the fixed field, and the fixed field has co-dimension $2n$, the fixed field is $K(t)$.

By [Ke1, Prop.1.1(a)], $K(u, v)^{C_{4n}}$ is rational over $K(u/v)^{C_{4n}}$, generated by a homogeneous invariant element of minimal degree, with this degree being equal to the order of the kernel of the group action, i.e., 2. We can pick s, and then have $K(u, v)^{C_{4n}} = K(s, t)$. □

By [K&Mt, Thm. 7], the minimal polynomial for $2u$ over $K(s, t)$ is generic for C_{4n} over K. As a polynomial over $K(u, v)$, this is obviously the same as the $Q(s, w, X)$ given above. Thus, the only thing that needs proving is that the constant term is $4s^{2n}/(t^2 + 1)$, i.e., that

$$w = \frac{4s^{2n}}{t^2 + 1}.$$

Proof. The denominator in t is a square root of w. We show that the numerator is a square root of $4s^{2n} - w$. This will prove the claim.

For convenience, we will work over $\mathbb{C}$, where the equation $4s^{2n} - w = [(u + iv)^{2n} + (u - iv)^{2n}]^2$ takes the form

$$(1) \quad 4(u^2 + v^2)^{2n} - \prod_{j=0}^{4n-1} (2\cos\tfrac{2\pi j}{4n} \cdot u + 2\sin\tfrac{2\pi j}{4n} \cdot v) = [(u + iv)^{2n} + (u - iv)^{2n}]^2.$$

Since the left and right hand sides are both homogeneous polynomials in u and v of degree $4n$, we can show them equal by finding $4n+1$ ray classes on which they coincide.

On the ray classes through $(\cos\frac{2\pi k}{4n}, \sin\frac{2\pi k}{4n})$, $0 \leq k < 2n$, it is trivial to see that (1) holds.

In the points $(\cos\frac{2\pi(2\ell+1)}{8n}, \sin\frac{2\pi(2\ell+1)}{4n})$, $0 \leq \ell < 2n$, s evaluates to 1, and the right hand side of (1) evaluates to 0. It is therefore necessary that w evaluates to 4. However, it is easily seen (and shown in [Le]) that the polynomial $r(X)$ with roots $2\cos\frac{2\pi(2j+1)}{8n}$, $0 \leq j < 4n$, is given by $r(X+1/X) = X^{4n} + X^{-4n} + 2$, and so it has constant term $r(0) = r(i+1/i) = 4$. Thus, (1) is satisfied on the ray classes through these points.

Finally, we take the ray class through $(1, i)$. In $(1, i)$, s evaluates to 0, w evaluates to -2^{4n}, and the right hand side in (1) evaluates to 2^{4n}.

This gives us the required $4n+1$ ray classes, and we conclude that (1) holds. □

References

[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.

[Le] A. Ledet, *On generic polynomials for dihedral groups*, preprint, 2006.

[Mi] K. Miyake, *Linear fractional transformations and cyclic polynomials*, Adv. Stud. Contemp. Math. (Pusan) **1** (1999), 137–142.

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

[Sc] L. Schneps, *On cyclic field extensions of degree* 8, Math. Scand. **71** (1992), 24–30.

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

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