On Algebraic Properties of Selfreciprocal Polynomials and of Daubechies Filters of Low Order

Andreas Klappenecker[1]
Universität Karlsruhe, IAKS
Am Fasanengarten 5
D–76 128 Karlsruhe, Germany
klappi@ira.uka.de

Abstract — **We show that the generic selfreciprocal polynomial of degree $2n$ has the Galois group $S_2 \wr S_n$. Consequently, "most" selfreciprocal polynomials of degree $2n$ with coefficients in an algebraic number field have the same Galois group. We use these results to determine algebraic properties of the Daubechies Filters of low order.**

I. Introduction

Filter coefficients of orthonormal wavelets in one dimension [2] have an interesting algebraic structure. An essential tool in our study of wavelet filters is the spectral factorization, cf. [3]. We will see from this construction that the algebraic properties of scaling filters are determined to a large extend by the Galois group of a selfreciprocal polynomial.

Recall that for all $A(x) \in \mathbf{R}[x]$ satisfying $\forall x \in [-1,1] : A(x) \geq 0$ there exists a polynomial $B(x) \in \mathbf{R}[x]$ of the same degree such that $A(\cos\omega) = |B(e^{-i\omega})|^2$ holds for all $\omega \in \mathbf{R}$. Roughly speaking, the polynomial $B(x)$ is obtained from $A(x)$ as follows: factor the selfreciprocal polynomial $A^*(x) := x^{\deg A} A((x+1/x)/2)$ in a splitting field, choose one z_j from each pair of zeros $z_j, 1/z_j$ of $A^*(x)$, and build the polynomial $B(x) = \nu \prod_{j=1}^{\deg A}(x - z_j)$, where ν is a normalization factor; this construction is called *spectral factorization.*

II. Selfreciprocal Polynomials

Many algebra textbooks contain a proof of the fact that the Galois group of the generic polynomial of degree n over a field F is the symmetric group S_n. However, selfreciprocal polynomials of degree $n \geq 4$ can *not* possibly have the symmetric group S_n as Galois group. Our next two theorems explain what kind of Galois groups are "typical" for arbitrary selfreciprocal polynomials.

Theorem 1 *Let F be a field and let $s_1, \ldots, s_n$ be algebraically independent over F. Denote by s the vector $(s_1, \ldots, s_n)$. The monic generic selfreciprocal polynomial of degree $2n$ is given by $f(\mathrm{s}, x) = \sum_{i=0}^{2n} s_i x^n$, where $s_{2n-i} = s_i$ and $s_0 = s_{2n} = 1$. Then the Galois group of $f(\mathrm{s}, x)$ over the coefficient field $F(\mathrm{s}) = F(s_1, \ldots, s_n)$ is isomorphic to the wreath product $S_2 \wr S_n$ of order $n!\,2^n$.*

Applying an effective version of Hilbert's irreducibility theorem (cf. [1, 4]) to the previous theorem allows us to prove the following result:

Theorem 2 *Let F be a number field. Then almost all specializations $\mathrm{s} \mapsto \mathbf{a}$, where $\mathbf{a} = (a_1, \ldots, a_n) \in F^n$, of the generic monic selfreciprocal polynomial $f(\mathrm{s}, x)$ of degree $2n$ lead to selfreciprocal polynomials $f(\mathbf{a}, x) \in F[x]$ with Galois group $S_2 \wr S_n$ over the number field F.*

III. Daubechies Filters

We apply the methods developed so far to Daubechies filters of order $N < 100$. Recall that a Daubechies filter of order N can be constructed by applying the spectral factorization to the following polynomial [2]:

$$A_N(x) = \sum_{k=0}^{N-1} \binom{N-1+k}{k} \left(\frac{1-x}{2}\right)^k .$$

The associated selfreciprocal polynomial is given by $A_N^*(x) = x^{N-1} A_N((x+1/x)/2)$. The Galois groups of these polynomials are determined in our next theorem:

Theorem 3 *The Galois group of the selfreciprocal polynomial $A_N^*(x)$ over the rationals is the wreath product $S_2 \wr S_{N-1}$ for all N with $2 \leq N < 100$, and $N \neq 25$. The selfreciprocal polynomial $A_{25}^*(x)$ has a Galois group isomorphic to the wreath product $S_2 \wr A_{24}$ of S_2 with the alternating group on 24 points.*

Using this theorem and the results in [3], we obtain the following corollary:

Corollary 4 *Let $2 \leq N < 100$. Denote by K_N the number field obtained by adjoining the scaling coefficients of the Daubechies wavelet of order N to the rationals. Then the degree of the field K_N over the rationals is given by $[K_N : \mathbf{Q}] = 2^{N-1}$. The fields K_N are non-normal except for $N = 2$. The Galois closure of K_N is the splitting field of $A_N^*(x)$.*

The scaling coefficients of the Daubechies wavelet of order five and less can be expressed by radicals. As a further consequence of the preceeding result we obtain:

Corollary 5 *The scaling coefficients of the Daubechies wavelet of order $6 \leq N < 100$ can not be expressed by radicals.*

Acknowledgements

I thank my advisor Professor Beth for supporting my work.

References

[1] S. D. Cohen. The distribution of Galois groups and Hilbert's irreducibility theorem. *Proc. London Math. Soc.*, 43(3):227–250, 1981.

[2] I. Daubechies. Orthonormal bases of compactly supported wavelets. *Comm. Pure Appl. Math.*, 41:909–996, 1988.

[3] A. Klappenecker and T. Beth. Galois theory and wavelet transforms. In *Proc. 1995 IEEE Int. Symp. on Information Theory*, page 429. IEEE, 1995. Whistler, BC, Canada.

[4] S. Lang. *Fundamentals of Diophantine Geometry.* Springer Verlag, New York Berlin Heidelberg Tokyo, 1983.

[1] This research was supported by DFG under SFB 414.
[1] This abstract will appear in Proc. of ISIT'97, Ulm, 1997.