Ulam Quarterly — Volume 2, Number 3, 1994

Galois Groups for Polynomials Related to Quadratic Map Iterates

(Dedicated to the Memory of Cornelius J. Everett)

W. A. Beyer and J. D. Louck

Theoretical Division

Los Alamos National Laboratory

Los Alamos, NM 87545

Abstract

We develop a theory of Galois groups of polynomials associated with a one parameter family of quadratic maps of the real line into itself arising in function iteration. A contribution to the Galois theory of polynomials is the application of an old algorithm for finding Galois groups, an algorithm seldom used and often dismissed as having no practical value. Let $P_\zeta^{[1]}(x) \equiv \zeta x(2-x)$ and $P_\zeta^{[n+1]}(x) = P_\zeta^{[n]}(P_\zeta^{[1]}(x))$ for $n = 1, 2, \ldots$ with $\zeta = 2$ in the first case and ζ an indeterminate in the second case. We consider the Galois groups of the polynomials $P_\zeta^{[n]}(x) - 1$ of degree 2^n. We show that for $\zeta = 2$ the Galois groups are the cyclic groups C_{2^n} of order 2^n. For ζ indeterminate, we use the algorithm mentioned above to show that the Galois groups of $P_\zeta^{[n]}(x) - 1$ are the wreath products $[S_2]^n$ having order 2^{2^n-1}. S_2 is the permutation group on two objects. We conjecture that these wreath products are the Galois groups for all positive integers $\zeta \neq 2$. We give a set of generators of $[S_2]^n$ as permutations in S_{2^n}. Note that $1 - P_2^{[n]}(x) = T_{2^n}(x-1)$, Chebyshev polynomials of the first kind of degree 2^n. We show that C_{2^n}, as a permutation group of the roots of $T_{2^n}(x-1)$, is a subgroup of $[S_2]^n$ when the roots of $T_{2^n}(x-1)$ are labelled appropriately.

1. Introduction.

In this paper we develop the theory of Galois groups associated with iterates of a one parameter family of quadratic maps of the real line into itself. Galois theory of polynomials usually concerns itself with single polynomials. Here we deal with an infinite family of polynomials arising in function iteration. Our particular family is interesting because each member of the family contains the same parameter that may be taken to be fixed or to be indeterminate.

In recent years function iteration has come to have a number of practical applications. A few of these applications are listed in Beyer, Mauldin and Stein (1986) and May (1976). Function iteration is one of the sources of models for the phenomenon called "chaos". Function iteration has both structural and metric aspects. The structural aspects go under such names as maximal sequences, MSS (Metropolis, Stein, and Stein (1973)) sequences, kneading sequences, and lexical sequences. Metric aspects of function iteration include geometric (Feigenbaum (1979) and Lanford (1982)) and quadratic (Beyer and Stein (1982) and Wang(1987)) convergence in period doubling, and Hausdorff dimension of sets arising in function iteration (Brucks (1989)).

The topic of Galois groups of polynomial iterates should be regarded as part of the structural aspects. In the past the structural aspects of function iteration have provided insights into the metric theory and it is hoped that similar insights may be obtained from Galois group theory. An intersection of the metric and structural theory is found in the problem of bifurcation values in quadratic iteration. This problem has been investigated by Bailey (1993) and is discussed in more detail in Appendix C. See also Silverman (1991, p. 565).

We first review the definition of a Galois group of a polynomial and then review some previous results on the Galois groups of iterated and composite polynomials. We then review quadratic iteration theory and state the origin of our particular polynomial sequence.

The principal contribution of this paper to the Galois theory for polynomials is the application of an old algorithm for finding Galois groups of polynomials. This algorithm is based on one of the oldest algorithms for Galois groups, which is generally dismissed as having no practical value. We apply this algorithm to finding Galois groups of polynomials arising in the iteration problem discussed below.

2. Galois Group of a Polynomial.

In this section we give a definition of the Galois group of a polynomial. This material is taken from Garling (1988). Let R and S be two rings. A one to one mapping ϕ from R to S is called a ring monomorphism if for all r_1 and r_2 in R:

$$\begin{aligned}\phi(r_1 + r_2) &= \phi(r_1) + \phi(r_2),\\ \phi(r_1 r_2) &= \phi(r_1)\phi(r_2),\\ \phi(\mathbf{1_R}) &= \mathbf{1_S},\end{aligned}$$

where $\mathbf{1_R}$ and $\mathbf{1_S}$ are the multiplicative unit elements of R and S respectively. A ring monomorphism of a field onto itself is called an automorphism.

Let K be a field. Let Aut K be the set of all automorphisms of K. Denote by $L : K$ a field extension of the field K; i.e., L is a field containing K as a subfield. Define

$$\Gamma(L : K) = \{\sigma \in \text{Aut } L | \sigma(k) = k, \forall\, k \in K\},$$

which is the set of automorphisms of L that fix K. The set $\Gamma(L:K)$ is a group under composition and is called the Galois group of the extension $L:K$.

Let $f \in K[x]$ (polynomial in the indeterminate x with coefficients in the field K). We say that f splits over the field L if

$$f(x) = \lambda(x-\alpha_1)\ldots(x-\alpha_n)$$

with $\lambda \in K$ and $\alpha_i \in L$. The field extension $L:K$ is the splitting field extension over K for f if f splits over L and there is no proper subfield of L over which f splits. Then $\Gamma(L:K)$ is called the Galois group of f. To summarize: the Galois group of f is the (unique) subgroup of the group of all automorphisms of the splitting field that fix the field K containing the coefficients of f.

3. Finite Wreath Products.

Let G and H be permutation groups:

$$G \subset S_n, \quad H \subset S_m.$$

Let

$$H^{(n)} = \underbrace{H \times H \times \ldots \times H}_{n}$$

denote the n-fold direct product of H with elements

$$h = (h_1, h_2, \ldots, h_n), \quad h_j \in H, \; j = 1, 2, \ldots, n.$$

Consider the direct product set

$$G \times H = \{(g,h) | g \in G, h \in H^{(n)}\},$$

which contains $|G \times H| = |G||H|^n$ elements. Next, we introduce the index sets I, J and K defined by

$$I = \{1, 2, \ldots, m\}, \; J = \{1, 2, \ldots, n\}, \; K = \{1, 2, \ldots, nm\}.$$

We now consider the bijective mapping $\phi : I \times J \rightarrow K$ of the direct product set $I \times J$ onto K by

$$\phi(i,j) = (i-1)n + j = k \in K, \quad i \in I, \quad j \in J.$$

Let $g \in G$ and $h_j \in H$ be given as explicit substitutions on the set J and I, respectively:

$$g : j \rightarrow k_j, \quad j \in J. \tag{1}$$

$$h_j : i \rightarrow h_j^{(i)}, \quad i \in I, \quad j \in J. \tag{2}$$

Define the mapping

$$\Phi : \quad G \times H \rightarrow S_{nm}$$

by the following rule. To each $(g,h) \in G \times H$ associate the permutation $p_k \in S_{nm}$ given by the substitution on the set K as follows: Select $k \in K$ and map k to $p_k \in K$ by the sequence of operations given by

$$k \xrightarrow{\phi^{-1}} (i,j) \xrightarrow{(g,h)} (h_j^{(i)}, k_j) \xrightarrow{\phi} p_k .$$

Thus, we obtain a unique permutation $p \in S_{nm}$ corresponding to (g,h):

$$p : k \rightarrow p_k , \quad k \in K .$$

The set of permutations $\Phi(G \times H) \subset S_{nm}$, is, by definition, the wreath product permutation group $G \wr H$:

$$G \wr H = \Phi(G \times H).$$

Let us also note that, from the results given by Odoni (1985), one can make the direct product set $G \times H$ into a group isomorphic to the permutation group

$$\Phi(G \times H) \subset S_{nm}$$

by defining the product of (g', h') and (g,h) by

$$(g', h'_1, h'_2, \ldots, h'_n) \bullet (g, h_1, h_2, \ldots, h_n) = (g'g, h'_{k_1} h_1, h'_{k_2} h_2, \ldots, h'_{k_n} h_n)$$

for g given by $g : j \rightarrow k_j$. Thus, we can also identify $G \wr H$ with $\{G \times H, \bullet\}$. Moreover, we see from the multiplication rule that the direct product group $H^{(n)}$ is isomorphic to the normal subgroup of $\{G \times H, \bullet\} \cong G \wr H$ given by $\{(e,h) | h \in H^{(n)}\}$, where $e = (1)(2)\ldots(n)$ is the identity in G.

There is a very useful mnemonic for obtaining the mapping $\Phi(g,h)$. We first perform the map $\phi^{-1}(K) = I \times J$ and arrange the elements $(i,j) \in I \times J$ in an $m \times n$ matrix array:

$$X = \begin{bmatrix} (1,1) & (1,2) & \ldots & (1,n) \\ (2,1) & (2,2) & \ldots & (2,n) \\ \vdots & \vdots & \ldots & \vdots \\ (m,1) & (m,2) & \ldots & (m,n) \end{bmatrix}$$

For each $(g,h) \in G \times H$, we effect the permutation g given by (1) on the column indices, followed by effecting the permutation h_j, $\forall j \in J$, given by (2) on the row indices of column j of the new matrix resulting from the operation by g. This gives a new matrix X' whose elements are the same as those of X, but arranged differently in the rows and columns. The elements of the new array X' are now put back into a single row of length nm consisting of the first row of X' followed by the second row, etc. We finally apply the mapping $\phi(I \times J)$ to the elements of this nm-tuple to obtain the relabelling in terms of $1, 2, \ldots, nm$. In this way, the nm-tuple $(1, 2, \ldots, nm)$ is mapped to an nm-tuple $(k_1, k_2, \ldots, k_{nm})$, thus giving the substitution $p \in S_{nm}$ corresponding to (g,h).

We have verified that the above definition of wreath product agrees with that given by Odoni (1985) in the finite case. We give the above definition explicitly because it is stated in a form more in keeping with our method of implementation. One can also consult the definition of wreath product given in Harary and Palmer (1973).

4. Review of Prior Work on Galois Groups of Sets of Polynomials.

Cremona (1989) shows, using a criterion of Odoni (1988) and by use of a computer, that the nth iterate of the polynomial x^2+1 has the wreath product $[S_2]^n$ of the symmetric group S_2 with itself n times as its Galois group for $n \leq 5 \times 10^7$. Stoll (1992) extends this result and shows that for the more general polynomial $x^2 + a$, where a is an integer, that the nth iterate has $[S_2]^n$ as the Galois group for all $n \geq 1$ if either $a > 0$ and $a \equiv 1$ or 2 mod 4 or $a < 0$ and $a \equiv 0$ mod 4.

Odoni (1985) discusses Galois groups of iterates and composites of polynomials. His polynomials are assumed to be monic and generic. The assumption of monicity makes it difficult to apply his results in our case. There seems to be no easy transformation to convert our composite polynomials to composites of monic polynomials. However, Odoni believes most or all of his results hold for nonmonic polynomials. Odoni's polynomials are also assumed to be generic. A polynomial $x^k + s_{k-1}x^{k-1} + \ldots + s_0$ is said to be a generic polynomial of degree k over a field K if $x, s_0, \ldots s_{k-1}$ are independent indeterminates over K. Some discussion of Odoni's results is given in Appendix B.

Grosswald (1978) discusses the Galois groups of Bessel polynomials (also called Krall – Frink polynomials after the inventors of these polynomials). It is shown that if a Bessel polynomial is irreducible, then the Galois group is the symmetric group of degree equal to the degree of the polynomial. It is conjectured that all Bessel polynomials are irreducible.

Bruen, Jensen, and Yui (1986) discuss polynomials with Frobenius groups of prime degree p as Galois groups. They make use of the pth Chebyshev polynomial of the first kind.

Morton and Patel (1992a and 1992b) carry out a program of investigating the Galois groups associated with periodic points Π_n of order n of a polynomial map $\sigma(x)$ in $\kappa[x]$, where κ is an arbitrary field. For example, let $\Sigma_{n,\sigma}$ be the field extension generated over κ by Π_n, that is, the least field containing κ and Π_n. This field is the splitting field of the polynomial $\Phi_{n,\sigma}(x) = \prod_{d|n}(\sigma^{[d]}(x) - x)^{\mu(n/d)}$. Here $\sigma^{[d]}$ denotes the dth iterate of $\sigma(x)$ and μ is the Möbius function. The Galois group $G = \mathrm{Gal}(\Sigma_{n,\sigma}/\kappa)$ is shown to be a subgroup of $S_r \wr \mathbf{Z}/n\mathbf{Z}$, where $r = \deg(\Phi_{n,\sigma})/n$. $\mathbf{Z}$ is the additive group of integers. A method is given for calculating G which reduces the problem to calculating the Galois group to a certain distinguished subfield L of $\Sigma_{n,\sigma}$. Several sufficient conditions are given for G to be $\mathrm{Gal}(L/\kappa) \wr \mathbf{Z}/n\mathbf{Z}$.

Vivaldi and Hatjispyros (1992) give an important discussion of Galois groups associated with periodic points of rational maps.

5. Quadratic Map.

In this section, we give briefly the background of the problem leading to the study of the Galois groups of the equations under consideration in this paper.

The parabolic map $P_\zeta : \mathbb{R} \to \mathbb{R}$ of the real line $\mathbb{R}$ defined by

$$P_\zeta : x \to P_\zeta(x) \equiv \zeta x(2-x), x \in \mathbb{R}, \tag{3}$$

where ζ is an arbitrary parameter in $\mathbb{R}^+$, is a paradigm for illustrating the behavior, called chaotic, of a large class of mathematical functions. The properties of the family of iterated polynomials

$$\{P_\zeta^{[n]}(x) | n = 1, 2, 3, \ldots\}, \tag{4}$$

where

$$P_\zeta^{[n]}(x) \equiv \underbrace{P_\zeta(P_\zeta(\ldots(P_\zeta}_{n}(x))\ldots)), \tag{5}$$

play a rôle in the bifurcation theory of the map (3). This theory has to do with sudden changes in the form of the periods of $P_\zeta(x)$ as ζ is varied. The real roots of the polynomial

$$P_\zeta^{[n]}(x) - x \tag{6}$$

yield all periods of $P_\zeta(x)$ of length r, where r divides n.

In Bivins, Louck, Metropolis and Stein (1991), the critical points of the polynomial $P_\zeta^{[n]}(x)$ play a rôle in the discussion of shift-maximal sequences, also called MSS or lexical sequences. These critical points are determined by the equation

$$\frac{d}{dx} P_\zeta^{[n]}(x) = 0,$$

which may alternatively be written as

$$(2\zeta)^n \prod_{s=0}^{n-1} \left[1 - P_\zeta^{[s]}(x)\right] = 0,$$

where $P_\zeta^{[0]} = x$. This leads to consideration of the roots of

$$P_\zeta^{[n]}(x) - 1, \tag{7}$$

a polynomial of degree 2^n. It is useful to display the first three of these polynomials:

$$\begin{aligned}
&-\zeta x^2 + 2\zeta x - 1, \quad (n = 1)\\
&-\zeta^3 x^4 + 4\zeta^3 x^3 - 2\zeta^2(2\zeta + 1)x^2 + 4\zeta^2 x - 1, \quad (n = 2)\\
&-\zeta^7 x^8 + 8\zeta^7 x^7 - 4\zeta^6(6\zeta + 1)x^6 + 8\zeta^6(4z + 3)x^5\\
&-2\zeta^4(8\zeta^3 + 24\zeta^2 + 2\zeta + 1)x^4 + 8\zeta^4(4\zeta^2 + 2\zeta + 1)x^3\\
&-4\zeta^3(4\zeta^2 + 2\zeta + 1)x^2 + 8\zeta^3 x - 1. \quad (n = 3)
\end{aligned}$$

When $\zeta = 2$, these polynomials become the Chebyshev polynomials of the first kind $T_{2^n}(x-1)$, which are irreducible (Odoni (1992)). Hence, for indeterminate ζ, the polynomials above are irreducible.

As is done in Bivins *et al.* (1991), it is useful to discuss the roots of (7) in terms of the 2^n inverse functions of $P_\zeta^{[n]}$. These 2^n inverse functions may be denoted by $f_\zeta^{[n]}(\sigma; x)$, where σ is an element of the Abelian group Σ_n of order 2^n:

$$\Sigma_n = \underbrace{S_2 \times S_2 \times \ldots \times S_2}_{n},$$

where S_2 is the symmetric group on 2 elements and $\times$ denotes direct product. The group Σ_n can also be realized by

$$\Sigma_n \equiv \{\sigma = (\sigma_1, \sigma_2, \sigma_3, \ldots, \sigma_n) | \text{each } \sigma_i = \pm 1\}, \tag{8}$$

with group multiplication defined by component-wise multiplication.

The inverse functions of $P_\zeta^{[n]}(x)$ are given by

$$f_\zeta^{[n]}(\sigma; x) \equiv$$

$$1+\sigma_1\sqrt{1-\frac{1}{\zeta}\left(1+\sigma_2\sqrt{1-\frac{1}{\zeta}\left(1+\sigma_3\sqrt{1-\ldots-\frac{1}{\zeta}\left(1+\sigma_n\sqrt{1-\frac{x}{\zeta}}\right)\ldots}\right)}\right)}, \tag{9}$$

and satisfy the equation

$$P_\zeta^{[n]}(f_\zeta^{[n]}(\sigma; x)) = x \tag{10}$$

for each of the 2^n quantities $f_\zeta^{[n]}(\sigma; x)$. If a quantity under a radical in (9) is positive, we choose the square root to be positive. Otherwise, we choose the square root (a, b) of a complex number to have $a > 0$ if $a \neq 0$ or $b > 0$ if $a = 0$.

The roots of (7) are thus

$$\{x_\zeta^{[n]}(\sigma) | \sigma \in \Sigma_n\}, \tag{11}$$

where

$$x_\zeta^{[n]}(\sigma) = f_\zeta^{[n]}(\sigma; 1). \tag{12}$$

Let us note, for completeness, the we can define the action of Σ_n on the roots $x_\zeta^{[n]}(\sigma)$ by

$$\sigma(x_\zeta^{[n]}(\sigma')) = x_\zeta^{[n]}(\sigma\sigma'), \tag{13}$$

where $\sigma, \sigma' \in \Sigma_n$. Thus, Σ_n transforms the root set (11) onto itself.

The inverse graph of $P_\zeta^{[n]}$ is the point set:

$$G_\zeta^n \equiv \{(x, f_\zeta^{[n]}(\sigma; x)) | \sigma \in \Sigma_n, x \in \mathrm{IR}, \mathrm{f}_\zeta^{[\mathrm{n}]}(\sigma; \mathrm{x}) \text{ real}\}.$$

This graph is important for the study of the bifurcation properties of the parabolic map. See again Bivins *et al.* (1991).

It is useful to note the recursion property:

$$f_\zeta^{[1]}(\sigma_1; x) = 1 + \sigma_1 \sqrt{1 - \frac{x}{\zeta}},$$

$$f_\zeta^{[n]}(\sigma; x) = 1 + \sigma_1 \sqrt{1 - \frac{1}{\zeta} f_\zeta^{[n-1]}(\sigma'; x)}, \quad n = 2, 3, \ldots, \tag{14}$$

where

$$\sigma = (\sigma_1, \sigma'), \ \sigma' \in \Sigma_{n-1}. \tag{15}$$

¿From (9), (12), and (14) with $x = 1$, we obtain the corresponding relation between the roots of $P_\zeta^{[n]}(x) - 1$ and $P_\zeta^{[n-1]}(x) - 1$:

$$x_\zeta^{[1]}(\sigma) = 1 + \sigma \sqrt{1 - \frac{1}{\zeta}},$$

$$x_\zeta^{[n]}(\sigma_1, \sigma') = 1 + \sigma_1 \sqrt{1 - \frac{1}{\zeta} x_\zeta^{[n-1]}(\sigma')}. \quad n > 1. \tag{16}$$

Because each polynomial $P_\zeta^{[n]}(x) - 1$ has roots given by radicals, it is natural to inquire about the Galois groups of these polynomials, especially because these groups must be solvable. Such a study is useful because one has not only the possibility of obtaining the Galois groups of an infinite family of polynomials of different degrees, but also the different Galois groups of the polynomials depending on the parameter ζ.

6. A Number Theory Lemma.

We need the following lemma for the discussion of the case $\zeta = 2$.

Lemma 1. For $n \geq 2$, the only integers in the set

$$\left\{ \frac{3^k - 1}{2^{n+1}} \Big| k \in A \equiv \{1, 2, \ldots, 2^n\} \right\}$$

are the odd integer

$$a_n = \frac{3^{2^{n-1}} - 1}{2^{n+1}}$$

and the even integer

$$b_n = \frac{3^{2^n} - 1}{2^{n+1}}.$$

Equivalently, for $k \in A$, the only solutions of the congruence relation

$$3^k \equiv 1 \bmod 2^{n+1}$$

are $k = 2^{n-1}$ and $k = 2^n$. Moreover, with $h = 2^{n-1}$, the ordered sets B_s given by

$$B_s = \{3^{sh+1}, 3^{sh+2}, \ldots, 3^{(s+1)h}\}, \quad s = 0, 1, 2, \ldots$$

are all equal mod 2^{n+1} and the integers in the ordered set B_0 are all distinct mod 2^{n+1}.

This lemma follows from the theorem of R. D. Carmichael given in 1910. This theorem is stated and proved in Knuth (1981), pp. 19 and 20.

7. Chebyshev Polynomials.

For $\zeta = 2$, the polynomials $1 - P_2^{[n]}$ are the Chebyshev polynomials of the first kind $T_{2^n}(x - 1)$ (see Oldham and Spanier (1987)). We use this relation in §8 and in §9 below to prove that the Galois group of $1 - P_2^{[n]}(x)$ is the cyclic group C_{2^n}. It is useful to display the formulae and roots for the general polynomials $T_n(x)$:

$$T_n(x) = \cos(n \arccos(x)), \quad -1 \leq x \leq 1$$

$$T_n(x) = \frac{1}{2} \sum_{j=0}^{[n/2]} \frac{n}{n-j} \binom{n-j}{j} (-1)^j (2x)^{n-2j},$$

where $[n/2]$ denotes the integer part of $n/2$.

The Chebyshev polynomials of odd order and of order a power of 2

will be useful to our work. The first few of these are:

$$\begin{aligned}
T_0(x) &= 1,\\
T_1(x) &= x,\\
T_2(x) &= 2x^2 - 1,\\
T_3(x) &= 4x^3 - 3x,\\
T_4(x) &= 8x^4 - 8x^2 + 1,\\
T_5(x) &= 16x^5 - 20x^3 + 5x,\\
T_7(x) &= 64x^7 - 112x^5 + 56x^3 - 7x,\\
T_8(x) &= 256x^8 - 112x^6 + 328x^4 - 64x^2 + 2.
\end{aligned}$$

The roots of $T_n(x)$ are:

$$t_j = \cos\left(\frac{(2j-1)\pi}{2n}\right),\ j = 1, 2, \ldots, n.$$

In this section we prove:

Theorem 1.

$$1 - P_2^{[n]}(x) = T_{2^n}(x-1). \tag{17}$$

Proof. We prove this relation by induction on n, noting first that

$$1 - P_2^{[1]}(x) = 2x^2 - 4x + 1 = 2(x-1)^2 - 1 = T_{2^1}(x-1).$$

Assume that (17) holds with n replaced by $n-1$. We will show that it holds for n. The roots $\alpha_i^{[n-1]}$ of $T_{2^{n-1}}(y)$ are given by

$$\alpha_i^{[n-1]} = \cos(\phi_i^{[n-1]}),\ \phi_i^{[n-1]} = (2i-1)\pi/2^n,\ i = 1, 2, \ldots, 2^{n-1}. \tag{18}$$

By the induction hypothesis, the set of roots

$$\{\alpha_1^{[n-1]}, \alpha_2^{[n-1]}, \ldots, \alpha_{2^{n-1}}^{[n-1]}\}$$

is

$$\{x_2^{[n-1]}(\sigma') - 1 | \sigma' \in \Sigma_{n-1}\};$$

hence,

$$x_2^{[n-1]}(\sigma_i') - 1 = \cos(\phi_i^{[n-1]}),\ \ i = 1, 2, \ldots, 2^{n-1},$$

where σ_i' is the ith σ in Σ_{n-1} in an appropriate ordering of Σ_{n-1}. The set of roots of $1 - P_2^{[n]}(x)$ is

$$\{x_2^{[n]}(\sigma_1, \sigma') | \sigma_1 = \pm 1, \sigma' \in \Sigma_{n-1}\}.$$

By (16), we have

$$\begin{aligned} x_2^{[n]}(\sigma_1,\sigma') - 1 &= \sigma_1\sqrt{1-\frac{1}{2}x_2^{[n-1]}(\sigma_i')} \\ &= \sigma_1\sqrt{\frac{1}{2}-\frac{1}{2}\left[x_2^{[n-1]}(\sigma_i')-1\right]} \\ &= \sigma_1\sqrt{\frac{1}{2}-\frac{1}{2}\cos\left(\phi_i^{[n-1]}\right)} \\ &= \sigma_1\sqrt{\sin^2\left(\phi_i^{[n-1]}/2\right)}. \end{aligned}$$

Hence, the set of roots of $1-P_2^{[n]}(x)$ is

$$\left\{1+\sin\left(\phi_i^{[n-1]}/2\right), 1-\sin\left(\phi_i^{[n-1]}/2\right) \,\middle|\, i=1,2,\ldots,2^{n-1}\right\},$$

which is equal to the set

$$\left\{1+\cos\left(\phi_i^{[n]}/2\right) \,\middle|\, i=1,2,\ldots,2^{n}\right\}.$$

Thus, the roots of $1-P_2^{[n]}(x)$ are the same as those of $T_{2^n}(x-1)$. Since these two polynomials have the same leading term $2^{2^n-1}x^{2^n}$, they are identical. This completes the induction. ■

It is interesting that one has an identity

$$\cos\left(\frac{(2j-1)\pi}{2^{n+1}}\right) = 1 - f_\zeta^{[n]}(\sigma;1),$$

which expresses the cosines on the left in terms of radicals on the right (given in (9)), where one must still determine the identification of index j with σ to make the result fully explicit.

8. Properties of Roots of Chebyshev Polynomials.

In this section, we present certain properties of roots of Chebyshev polynomials needed for the subsequent development on Galois groups.

Let α denote any root of $T_n(x)$ and define the polynomials $y_i(\alpha)$ in this root to be the odd-order Chebyshev polynomial

$$y_i(\alpha) = T_{2i-1}(\alpha), \quad i=1,2,\ldots. \tag{19}$$

We refer to this set of polynomials in the root α of $T_n(x)$ as the universal root set of $T_n(x)$. The reason for this terminology is apparent from Theorem 2 below.

We require two well-known properties of Chebyshev polynomials that are easy consequences of trigonometric identities. These are the composition rule and the multiplication rule:

$$T_n(T_m(x)) = T_m(T_n(x)) = T_{nm}(x),$$

and

$$2T_n(x)T_m(x) = T_{n+m}(x) + T_{|n-m|}(x).$$

It follows immediately from these two relations that each polynomial $y_i(\alpha)$ in the universal root set of T_n satisfies the following relations:

$$T_n(y_i(\alpha)) = 0,$$

$$y_{\frac{n}{2}+i}(\alpha) = -y_{\frac{n}{2}-i+1}(\alpha), \quad 1 \le i \le \frac{n}{2}, \quad n \text{ even}, \tag{20}$$

$$y_{\frac{n}{2}+i}(\alpha) = -y_{i-\frac{n}{2}}(\alpha), \quad i > \frac{n}{2}, \quad n \text{ even}, \tag{21}$$

$$y_{\frac{n+1}{2}+i}(\alpha) = -y_{\frac{n+1}{2}-i}(\alpha), \quad 1 \le i \le \frac{n-1}{2}, \quad n \text{ odd}, \tag{22}$$

$$y_{\frac{n+1}{2}+i}(\alpha) = -y_{i-\frac{n-1}{2}}(\alpha), \quad i > \frac{n-1}{2}, \quad n \text{ odd}. \tag{23}$$

For n odd, we note that

$$y_{\frac{n+1}{2}}(\alpha) = 0.$$

For the discussion of the consequences of these relations, it is convenient to define the ordered sets of universal roots of T_n by

$$R_s = \{y_{ns+1}(\alpha), y_{ns+2}(\alpha), \ldots, y_{n(s+1)}(\alpha)\}, \quad s = 0, 1, 2, \ldots,$$
$$\overleftarrow{R_0} = \{y_n(\alpha), y_{n-1}(\alpha), \ldots, y_1(\alpha)\}.$$

Using these relations and definitions, it is straightforward to prove:

Theorem 2. Independently of which root $\alpha \neq 0$ $T_n(x)$ is chosen, the universal root set of $T_n(y)$ is given by

$$\{y_i(\alpha) | i = 1, 2, \ldots\} = R_0 \cup R_1 \cup R_2 \cup \ldots,$$

and it consists of cycles R_s given by

$$R_s = R_0, \quad s \text{ even},$$
$$R_s = \overleftarrow{R_0}, \quad s \text{ odd}.$$

Furthermore, the ordered set or period R_0 itself contains exactly the roots of $T_n(x)$ as given by

$$R_0 = \{y_1(\alpha), \ldots, y_{\frac{n}{2}}(\alpha), -y_{\frac{n}{2}}(\alpha), \ldots, -y_1(\alpha)\}, \quad n \text{ even}, \quad n \ge 2, \tag{24}$$

$$R_0 = \{y_1(\alpha), \ldots, y_{\frac{n-1}{2}}(\alpha), y_{\frac{n+1}{2}}(\alpha), -y_{\frac{n-1}{2}}(\alpha), \ldots, -y_1(\alpha)\}, \quad n \text{ odd}, \quad n \ge 3. \tag{25}$$

Proof. Aside from the application of the (20) - (23), the only additional point needing proof is that the ordered set R_0 contains exactly the roots of $T_n(x)$. The structure of R_0 as given in (24) and (25) is a consequence of (22) and (23), so that if the roots in the respective sets

$$\{y_1(\alpha), y_2(\alpha), \ldots, y_{\frac{n}{2}}(\alpha)\}, \quad n \text{ even}, \ n \geq 2, \tag{26}$$

$$\{y_1(\alpha), y_2(\alpha), \ldots, y_{\frac{n-1}{2}}(\alpha)\}, \quad n \text{ odd}, \ n \geq 3, \tag{27}$$

are distinct, then the proof is complete. Assume that two roots in the set (26) are equal, say the ith and the jth root, where it is no restriction to take $i > j$. Then, we must have

$$P_{i,j}(\alpha) = T_{2i-1}(\alpha) - T_{2j-1}(\alpha) = 0$$

for each root α of $T_n(x)$. Thus, the polynomial $P_{i,j}(x)$ of degree $2i-1$, which is at most $n-1$, has the n distinct roots α as roots, which is impossible. Therefore, the assumption of the equality of two roots in the set (26) is false and all the roots must be distinct. Similarly, one proves that the roots in the set (27) are distinct. ∎

It is a quite remarkable result that the roots of the Chebyshev polynomials are themselves Chebyshev polynomials, as described in Theorem 2. We use this result in the next section with n replaced by 2^n.

9. Automorphism Group of the Roots of $P_2^{[n]}(x) - 1$.

In this section, we prove that the Galois group of $P_2^{[n]}(x) - 1$ is isomorphic to the cyclic group C_{2^n}. However, we will work with the Chebyshev polynomials $T_{2^n}(x)$ because their roots are slightly simpler to express:

$$t_i = \cos\left[\frac{(2i-1)\pi}{2^{n+1}}\right], \quad i = 1, 2, \ldots, 2^n.$$

The field extension of the rational field $\mathbb{Q}$ to the splitting field L of the polynomial $T_{2^n}(x)$ is given by

$$L = \left\{ \sum_{i=0}^{2^n-1} a_i \alpha^i \,\middle|\, a_i \in \mathbb{Q} \right\}, \tag{28}$$

where α is any root of $T_{2^n}(x)$. Because of Theorem 2, the order of the Galois group is 2^n. See Garling (1988), p. 95. The quantities in (28) are clearly closed under addition and closed under multiplication when reduced by use of the identity

$$T_{2^n}(\alpha) = 0. \tag{29}$$

Let α be the largest root of $T_{2^n}(\alpha)$. Define the transformation $\psi : L \to L$ in which an element $a = \sum_{k=0}^{2^n-1} a_k \alpha^k \in L$ undergoes the transformation

$$\psi(a) = \sum_{k=0}^{2^n-1} a_k \left(y_2(\alpha)\right)^k. \tag{30}$$

The transformation ψ is a Galois automorphism because it is a one to one mapping, for $\forall x, y \in L$ it satisfies $\psi(x+y) = \psi(x) + \psi(y)$ and $\psi(xy) = \psi(x)\psi(y)$, and finally it preserves the ground field $\mathbb{Q}$. See Stewart (1989), pp. 39-40. The element $\psi(a)$ can be expressed in terms of the basis of $L : \{1, \alpha, \alpha^2, \ldots, \alpha^{2^n-1}\}$ by expanding $(y_i(\alpha))^k$ in powers of α and reducing to powers less than 2^n by using $T_{2^n}(\alpha) = 0$.

Define the iterated transformations $\psi^{[k]}$ of ψ by

$$\psi^{[k]} = \psi^{[k-1]} \circ \psi^{[1]}, \quad k > 1, \ldots, 2^n$$

with $\psi^{[1]} = \psi$. We show below that $\psi^{[2^n]}$ is the identity.

For the next theorem, it is convenient to partition the positive integers into the following subsets of integers:

$$A_0 = \{1, 2, \ldots, 2^n\},$$
$$A_s = \{2^{n+s-1} + 1, 2^{n+s-1} + 2, \ldots, 2^{n+s}\}, s = 1, 2, \ldots.$$

We are now able to prove:

Theorem 3. The set of automorphisms $\psi^{[i]} : L \to L, \quad i = 1, 2, \ldots, 2^n$ forms a group under composition that is isomorphic to the cyclic group of permutations of the roots generated by

$$y_1(\alpha) = \alpha \to y_{j_1}(\alpha),\ y_2(\alpha) \to y_{j_2}(\alpha), \ldots,\ y_{2^n}(\alpha) \to y_{j_{2^n}}(\alpha), \tag{31}$$

where now α is any root of T_{2^n} and where $j_i \in \{1, 2, \ldots, 2^n\}$ with j_i the integer given by

$$3i - 1 \equiv j_i \bmod 2^n, \text{ for } 3i - 1 \in A_0 \cup A_2 \cup A_4 \cup \ldots,$$
$$3i - 1 \equiv 2^n - j_i + 1 \bmod 2^n, \text{ for } 3i - 1 \in A_1 \cup A_3 \cup \ldots,$$

with $j_i = 0$ identified with 2^n.

Proof. Replace n by 2^n in Theorem 2 so that

$$R_s = \{y_i(\alpha) | i \in A_s\}.$$

Then, by Theorem 2, we have

$$R_s = R_0,\ s \text{ even}, \tag{32}$$

$$R_s = \overleftarrow{R_0},\ s \text{ odd}. \tag{33}$$

Because

$$y_i(y_2(\alpha)) = y_{3i-1}(\alpha), \quad i = 1, 2, \ldots, \tag{34}$$

the integer j_i in the substitution $i \to 3i - 1 \to j_i$ is the subscript of the root

$$y_{3i-1}(\alpha) \in R_0 \cup R_1 \cup R_2 \cup \ldots,$$

after accounting for the cycling of the ordered sets given by (32) and (33). This gives the j_i stated in the theorem.

We next show that the integers $j_k,\ k = 1, 2, \ldots, 2^n$ in (31) are distinct, so that this substitution is indeed a permutation, and we then show that it is a 2^n-cycle. Relation (34) is equivalent to the composition relation

$$y_2^{(k)}(\alpha) = T_3^{(k)}(\alpha) = T_{3^k}(\alpha) = y_{\frac{3^k+1}{2}}(\alpha),\ k = 1, 2, \ldots.$$

To determine the permutation defined by this relation, we must determine the cycle set R_s to which the root $y_{\frac{3^k+1}{2}}(\alpha)$ belongs and then identity it with the corresponding root in R_0. This is solved as follows, using (32) and (33).

Define the integers r_k by

$$\frac{3^k+1}{2} \equiv r_k \bmod 2^n,\ \ n \geq 2. \tag{35}$$

Then

$$y_{\frac{3^k+1}{2}}(\alpha) = y_{r_k}(\alpha),\ \ \text{if } \frac{3^k+1}{2} \in A_0 \cup A_2 \cup A_4 \ldots,$$

$$y_{\frac{3^k+1}{2}}(\alpha) = y_{2^n-r_k+1}(\alpha),\ \ \text{if } \frac{3^k+1}{2} \in A_1 \cup A_3 \cup A_5, \ldots.$$

To show that the integers r_k in (35) are distinct, we rewrite (35) in the equivalent form

$$3^k \equiv 2r_k - 1 \bmod 2^{n+1}.$$

By Lemma 1, the integers in the ordered set

$$\{r_1, r_2, \ldots, r_{2^{n-1}}\} \tag{36}$$

are all distinct, and the integers in the ordered sets

$$\{r_{s2^{n-1}+1}, r_{s2^{n-1}+2}, \ldots, r_{(s+1)2^{n-1}}\},\ s = 0, 1, 2, \ldots$$

are all equal to the integers in the first ordered set $s = 0$.

We also must show that the integers in the set

$$\{r_k, 2^n - r_k + 1 | k = 1, 2, \ldots, 2^{n-1}\} \tag{37}$$

are distinct. Assume that two integers r_i and r_j are such that

$$r_i + r_j = 2^n + 1. \tag{38}$$

By adding the congruence relations (35) for $k = i$ and $k = j$, we deduce the relation

$$3^i(3^{j-i} + 1) \equiv 0 \bmod 2^{n+1},\ \ i \leq j \in \{1, 2, \ldots, 2^n\},$$

where it is no restriction to take $i \leq j$. Because 2^{n+1} does not divide 3^i, it must divide $3^{j-i}+1$; that is, we must have

$$3^k \equiv -1 \bmod 2^{n+1}, \text{ for some } k \in \{0,1,2,\ldots,2^{n-1}-1\}.$$

But this is impossible, because by squaring this relation, we obtain

$$3^{2k} \equiv 1 \bmod 2^{n+1},$$

and the only integer solution of this relation having k in the prescribed domain is given by Lemma 1 to be $k = 2^{n-2}$, and the number

$$d_n = \frac{3^{2^{n-2}}+1}{2^{n+1}},\ n \geq 2$$

is not an integer. That d_n is not an integer follows from the relation

$$d_n\left(3^{2^{n-2}}-1\right) = a_n,\ n \geq 2,$$

where a_n is the odd integer defined in Lemma 1. Because $3^{2^{n-1}}-1$ is even, d_n cannot be in integer. Thus, relation (38) is false, and the integers in the set (37) are distinct.

To show that the integers in the set (37) define a single cycle of length as given explicitly below, we next show that

$$y_2^{2^n}(\alpha) = \alpha,$$

and that 2^n is the smallest iterate for which one obtains α. The proof is again a consequence of Lemma 1, which asserts that for $k \in \{1,2,\ldots,2^n\}$ and $r_k = 1$ in (35) the only solutions are $k = 2^{n-1}$ and $k = 2^n$. But

$$\frac{3^{2^{n-1}}+1}{2} \in A_1 \cup A_3 \cup \ldots,$$

because the integer a_n (see Lemma 1) is odd and

$$\frac{3^{2^n}+1}{2} \in A_0 \cup A_2 \cup \ldots,$$

because the integer b_n (see Lemma 1) is even. Thus, we have

$$y_{\frac{3^{2^{n-1}}+1}{2}}(\alpha) = y_{2^n}(\alpha),$$

$$y_{\frac{3^{2^n}+1}{2}}(\alpha) = y_1(\alpha).$$

Because the dimension of the field L as a vector space is 2^n and by Theorem 3 a cyclic group of order 2^n is a group of automorphisms of L,

this group is the Galois group in question. See Garling (1988, Theorem 7.1). ∎

Thus, we have

Theorem 4. The Galois group of $T_{2^n}(y)$ and therefore of $P_2^{[n]}(x) - 1$ is isomorphic to the cyclic group $C_{2^n} =< (1, 2, \ldots, 2^n) >$.

We now give an algorithm that calculates the orbit of α under iteration by the automorphism ψ generated by the root transformation: $\alpha \rightarrow y_2(\alpha) \equiv T_1(\alpha)$. This algorithm depends on the composition and multiplication properties of the odd Chebyshev polynomials. The algorithm is carried out using $\pm T_p(\alpha)$ for odd p in place of $y_i(\alpha)$. We denote the quantity $\pm T_p(\alpha)$ by $sf = g$ where s denotes sign ± 1 and f denotes $T_p(\alpha)$.

To start, put $s = +1$, $f = 1$, and $g = sf$. Then for $i : 2$ through 2^n, carry out the following number theory procedure: if $f < 2^n$ then $f \rightarrow 3f$ and $s \rightarrow s$, else $(f \rightarrow |2^{n+1} - 3f|, s \rightarrow -s, g = sf)$. The resulting sequence of positive and negative integers can be regarded as the orbit of α under the iterated automorphisms of ψ.

We obtained the following orbits of α for n = 2,3,4, and 5. The symbol $\pm k$ denotes $\pm T_k(\alpha)$.

n=2: 1, 3, -1, -3, 1.

n=3: 1, 3, -7, 5, -1, -3, 7, -5, 1.

n=4: 1, 3, 9, -5, -15, 13, -7, 11,
-1, -3, -9, 5, 15, -13, 7, -11, 1.

n=5: 1, 3, 9, 27, -17, 13, -25, 11, -31, 29, -23, 5, 15, -19, 7, 21,
-1, -3, -9, -27, 17, -13, 25, -11, 31, -29, 23, -5, -15, 19, -7, -21, 1.

Such calculations were carried out on the computer symbol system DOE-MACSYMA up to $n = 20$ with orbit length $2^{20} \approx 1,000,000$. Each calculation was terminated at -1 because after -1 the orbit repeats, but with the signs changed.

The cyclic group of permutations of the roots $(t_1, t_2, \ldots, t_{2^n})$ corresponding to the group of automorphisms of the field L (with $\alpha = t_1$) that fixes the ground field has as its generator the 2^n-cycle obtained from the above sequences of integers by first mapping the odd integers to integers, using $2i - 1 \rightarrow i$, and then adding 2^n to all nonpositive integers:

$$(1, 3, -1, -3) \rightarrow (1, 2, 0, -1) \rightarrow (1, 2, 4, 3),$$

$$(1, 3, -7, 5, -1, -3, 7, -5) \rightarrow (1, 2, -3, 3, 0, -1, 4, -2) \rightarrow (1, 2, 5, 3, 8, 7, 4, 6).$$

It is useful to express, as above, the permutation of the subscripts of the roots,

$$\begin{pmatrix} 1 & 2 & \ldots & 2^n \\ j_1 & j_2 & \ldots & j_{2^n} \end{pmatrix},$$

given in Theorem 3 as the 2^n-cycle $s = (s_1, s_2, \ldots, s_{2^n})$, which then is also the generator of the cyclic group of the roots $(t_1, t_2, \ldots, t_{2^n})$ and is

isomorphic to the group of automorphisms of the field L. It follows from the results in the proof of Theorem 3 that for $k = 0, 1, 2, \ldots, 2^{n-1}$

$$s_{k+1} = \begin{cases} r_k & \text{if } d_k \text{ is even,} \\ 2^n + 1 - r_k & \text{if } d_k \text{ is odd,} \end{cases}$$

where

$$\frac{3^k + 1}{2} = d_k 2^n + r_k, \quad 1 \leq r_k \leq 2^n - 1.$$

10. Factoring Algorithm for Finding Galois Groups.

A classic theorem for finding Galois groups is reviewed briefly in this section, because we use it subsequently for consideration of the Galois groups of $P_\zeta^{[n]}(x) - 1$.

We consider perhaps the earliest algorithm for finding Galois groups: the clearing irrational algebraic quantities algorithm. (An irrational algebraic quantity is a solution, not in $\mathbb{Q}$, to a polynomial equation with coefficients in $\mathbb{Q}$.) We also call the algorithm the van der Waerden algorithm because of the clear exposition of it in his book, van der Waerden (1970). It is usually dismissed as having little practical importance. We make practical use of this algorithm. It is stated in §8.10 of van der Waerden (1970). To review, let $f(x) \in \Delta[x]$ with Δ a field and f of degree n. Let the zeros of f be α_i, $i = 1, \ldots, n$. Let

$$\theta = \alpha_1 x_1 + \ldots + \alpha_n x_n,$$

where the x_i are indeterminates. Form the product

$$F(z, x) = \prod_{s_x \in S_n} (z - s_x \theta), \tag{39}$$

where S_n is the symmetric group on n symbols and s_x is a permutation of the indeterminates $x_1, x_2, \ldots, x_n$. Factor F into irreducible factors in $\Delta[x, z]$:

$$F(z, x) = F_1(z, x) \ldots F_r(z, x). \tag{40}$$

Each of the factors in (40) can be written as

$$F_j = \prod_{s_x \in A_j} (z - s_x \theta),$$

where $A_1, A_2, \ldots, A_r$ is a partition of S_n. See Garling (1988, p. 156). Label the subscripts of the A_j so that A_1 contains the identity e and thus is a subgroup of S_n. Let G denote the group of permutations that carries F_1 into itself. The other A_j are right cosets of G relative to A_1. (A right coset of the group G relative to A_1 has the form $A_1 g$ with $g \in G$.) This fact about cosets seems not to appear in books on Galois theory.

The theorem of Galois theory (van der Waerden (1970), p. 189) is then:

Theorem 5. G is the Galois group of f: $\Gamma_\Delta(f)$.

A similar result is given by Dehn (1960, chapter 11, p. 143), Dickson (1960, p. 164), and Jacobson (1964, p. 109). Dickson and Jacobson assume that $f(x)$ is monic. Dickson takes the permutation group of F_1 as the definition of the Galois group. The polynomial F_1 is called the resolvent polynomial of $f(x)$, according to Dickson (1930 p. 162).

11. A Basic Theorem on Clearing Radicals.

A basic result for the removal of the radical symbol from the elementary symmetric functions is given by Stein and Zemach (1987, p. 397, Theorem 1). One should also consult Problem 5 on page 104 of Hille (1962). The theorem of Stein and Zemach was partly an outgrowth of work of Beyer and Heller (1987).

We require a significant generalization of the Stein-Zemach theorem. The group Σ_n, introduced in eq. (8) underlies the structure of the generalization, as it also does the Stein-Zemach theorem. We define for each $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n) \in \Sigma_n$, and any set of indeterminates $y = (y_1, y_2, \ldots, y_n)$, the action of σ on y by

$$\sigma y = (\sigma_1 y_1, \sigma_2 y_2, \ldots, \sigma_n y_n).$$

Next, let $Q(y)$ denote an arbitrary polynomial in the y_i over a field that is not even in any y_i. Then, we have:

Theorem 6. The polynomial

$$P(Y, y) = \prod_{\sigma \in \Sigma_n} (Y - Q(\sigma y))$$

is an even function of each y_i; hence, if we choose $y_i = \sqrt{w_i}$, then

$$P\left(Y, \sqrt{w}\right), \quad \sqrt{w} = (\sqrt{w_1}, \sqrt{w_2}, \ldots, \sqrt{w_n})$$

is a polynomial in the indeterminates w_i. Moreover, for the given polynomial Q, the polynomial $P(Y, y)$ of degree 2^n in Y is the polynomial of smallest degree in Y that is even in each y_i, hence clears radicals in the w_i.

Proof. For each

$$\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n) \in \Sigma_n,$$

we define $\sigma^{[i]} \in \Sigma_n$ by

$$\sigma^{[i]} = (\sigma_1, \sigma_2, \ldots, \sigma_{i-1}, -\sigma_i, \sigma_{i+1}, \ldots, \sigma_n), \quad \forall i \in \{1, 2, \ldots, n\}.$$

Because, as σ runs over all elements in Σ_n, so does each $\sigma^{[i]}$, it follows that

$$\prod_{\sigma \in \Sigma_n} (Y - Q(\sigma y)) = \prod_{\sigma^{[i]} \in \Sigma_n} \left(Y - Q(\sigma^{[i]} y)\right), \quad \forall i \in \{1, 2, \ldots, n\}.$$

Thus, $\forall i \in \{1, 2, \ldots, n\}$,

$$P(Y, y_1, y_2, \ldots, y_n) = P(Y, y_1, y_2, \ldots, y_{i-1}, -y_i, y_{i+1}, \ldots, y_n);$$

that is, the polynomial $P(Y,y)$ is invariant under the substitution $y_i \rightarrow -y_i, \quad \forall i \in \{1,2,\ldots,n\}$. Moreover, because the coefficient of Y^{2^n-k} in the expansion of $P(Y,y)$ is $(-1)^k$ times the elementary symmetric function $e_k(\sigma y)$, these elementary symmetric functions themselves are even in each y_i. That the polynomial $P(Y,y)$ is the one of the smallest degree that is even in each y_i follows because Σ_n is the smallest group that reverses the sign of each y_i exactly once. ■

The Stein-Zemach theorem is the special case

$$Q(y) = \sum_{i=1}^{n} y_i$$

of Theorem 6. That Theorem 6 is indeed a generalization of the Stein-Zemach follows from the example

$$Q(y) = ay_1 + by_2 + cy_1y_2,$$

for $n = 2$, where a, b, c are arbitrary constants.

12. The Wreath Product Permutation Group $[S_2]^n$.

In this section, we give explicitly a realization of the wreath product group $[S_2]^n$ in terms of permutations in S_{2^n}. This is done by implementing for the case at hand the definition of the wreath product group given §3. In terms of that notation, we have

$$G = [S_2]^{n-1}, \quad H = S_2,$$

so that

$$[S_2]^n = G \wr H = [S_2]^{n-1} \wr S_2, \quad n > 1, \tag{41}$$

with $[S_2]^1 = S_2$.

We assume that we have obtained

$$[S_2]^{n-1} \subset S_{2^{n-1}}$$

as an explicit set of permutations in $S_{2^{n-1}}$. We next introduce the direct product set

$$[S_2]^{n-1} \times (S_2)^{2^{n-1}} = \{(p,s) | p \in [S_2]^{n-1},\ s \in (S_2)^{2^{n-1}}\}, \tag{42}$$

where

$$s = (s_1, s_2, \ldots, s_{2^{n-1}}) \in \underbrace{S_2 \times S_2 \times \ldots \times S_2}_{2^{n-1}}.$$

The number of symbols N_n in the set $[S_2]^n$ is 2^{2^n-1}, a result easily obtained by iterating $N_n = 2^{2^{n-1}} N_{n-1}$ with $N_1 = 2$. So $|[S_2]^n| = 2^{2^n-1}$.

The index mapping ϕ from the set $I \times J$ with $I = \{1,2\}$ and $J = \{1,2,\ldots,2^{n-1}\}$ to the set $\{1,2,\ldots,2^n\}$ is given by

$$\begin{aligned} \phi:\ & (1,j) \rightarrow j,\ j = 1,2,\ldots,2^{n-1}, \\ & (2,j) \rightarrow 2^{n-1} + j,\ j = 1,2,\ldots,2^{n-1}. \end{aligned}$$

The easiest way to obtain the permutations in S_{2^n} corresponding to the elements in the direct product set (42) is to use the mnemonic of §3 and place the integers $1, 2, \ldots, 2^n$ themselves into a $2 \times 2^{n-1}$ matrix array in accordance with the mapping:

$$\phi: \quad I \times J \rightarrow \begin{bmatrix} 1 & 2 & \ldots & 2^{n-1} \\ 2^{n-1}+1 & 2^{n-1}+2 & \ldots & 2^n \end{bmatrix}. \tag{43}$$

An element

$$p: \; j \rightarrow p_j, \quad j = 1, 2, \ldots, 2^{n-1},$$

of $[S_2]^n \subset S_{2^{n-1}}$, permutes the columns of the array (43). It clearly has the unique *extension* p' to the permutation in S_{2^n} given by

$$\begin{aligned} p': \; & j \rightarrow p_j, \quad j = 1, 2, \ldots, 2^{n-1}, \\ & 2^{n-1} + j \rightarrow 2^{n-1} + p_j. \; j = 1, 2, \ldots, 2^{n-1}. \end{aligned}$$

In this way, the group $[S_2]^{n-1} \subset S_{2^{n-1}}$ with permutations $p \in S_{2^{n-1}}$ has the unique extension to its isomorphic version as a subgroup of S_{2^n}. We denote this isomorphic group by the same notation, but write $[S_2]^{n-1} \subset S_{2^n}$ to keep the context clear.

Next, consider

$$s_j \in S_2 = \{(1)(2), (1,2)\}, \tag{44}$$

and

$$s = (s_1, s_2, \ldots, s_j, \ldots, s_{2^{n-1}}) \in (S_2)^{2^{n-1}}. \tag{45}$$

Because the permutation $p \in [S_2]^{n-1} \subset S_{2^{n-1}}$ first permutes the columns in the array (43), and then the S_2 generator (1,2) in (44) interchanges the entries in column j, we see that this S_2 group is isomorphic to the S_2 subgroup of S_{2^n} generated by the transposition $(p_j, 2^{n-1} + p_j)$; that is, the unique extension of S_2 defined by (45) to S_{2^n} is $S_2^{(j)}$ defined by

$$S_2^{(j)} =< (p_j, 2^{n-1} + p_j) > \subset \; S_{2^n}.$$

Because this relation holds for each $j \in J$, we find that it is the transpositions in S_{2^n} defined by

$$T_j = (j, 2^{n-1} + j), \quad j = 1, 2, \ldots, 2^{n-1} \tag{46}$$

that correspond to the permutation $(1, 2) \in S_2$ in the various components of the direct product (42) (the order is unimportant).

We conclude from these results the following:

Theorem 7. The wreath product permutation group $[S_2]^n$ may be defined recursively in terms of the wreath product group $[S_2]^{n-1} \subset S_{2^{n-1}}$ and its unique extension $[S_2]^{n-1} \subset S_{2^n}$ by

$$[S_2]^n =< [S_2]^{n-1}, T_1, T_2, \ldots, T_{2^{n-1}} > .$$

This recursive definition of $[S_2]^n$ gives a unique determination of the elements of this group as permutations in S_{2^n}. The determination goes as follows. We start with $[S_2]^1 =< (1,2) >$ and continue with $n = 2, 3$:

$$[S_2]^2 =< (1,2)(3,4),(1,3),(2,4) >=< (1,2)(3,4),(1,2,3,4) >= D_8,$$
$$[S_2]^3 =< (1,2)(3,4)(5,6)(7,8),(1,2,3,4,5,6,7,8),(1,5),(2,6),(3,7),(4,8) >$$
$$=< (1,2)(3,4)(5,6)(7,8),(1,2,3,4)(5,6,7,8),(1,2,3,4,5,6,7,8) > .$$

These results suggest the following: Define the permutations $L_i \in S_{2^n}$, $i = 1, 2, \ldots, n$, by

$$\begin{aligned} L_1 &= (1,2)(3,4)\ldots(2^n-1, 2^n), \\ L_2 &= (1,2,3,4)(5,6,7,8)\ldots(2^n-3, 2^n-2, 2^n-1, 2^n), \\ &\vdots \\ L_{n-1} &= (1,2,\ldots,2^{n-1})(2^{n-1}+1,\ldots,2^n), \\ L_n &= (1,2,\ldots,2^n). \end{aligned}$$

Thus, L_i is defined by inserting parentheses in the obvious way into the sequence $1, 2, \ldots, 2^n$. Note that L_i above should be called $L_i^{[n]}$, but in all cases below, unless explicitly stated, the superscript on L_i is suppressed.

Theorem 8. The wreath product group $[S_2]^n$ as a subgroup of S_{2^n} is given by

$$[S_2]^n =< L_1, L_2, \ldots, L_n > .$$

Proof. The proof is by induction on n. The theorem holds obviously for $n = 1$. We assume that the theorem holds for n replaced by $n-1$; that is, in terms of generators the wreath product group $[S_2]^{n-1}$ as a subgroup of $S_{2^{n-1}}$ is given by

$$[S_2]^{n-1} =< L_1^{[n-1]}, L_2^{[n-1]}, \ldots, L_{n-1}^{[n-1]} > .$$

There are two steps in moving from $n-1$ to n. The first step, because we are dealing with the wreath product $[S_2]^{n-1} \wr [S_2]^1$, is to extend $L_i^{[n-1]}, i = 1, 2, \ldots, n-1$, to $L_i^{[n]}, i = 1, 2, \ldots, n-1$, using the unique extension described above, and then suppress the superscript. We then adjoin the 2-cycles $(1, 2^{n-1}+1), (2, 2^{n-1}+2), \ldots, (2^{n-1}, 2^n)$ to the generators $L_1, L_2, \ldots, L_{n-1}$ and obtain, with all permutations in S_{2^n}:

$$[S_2]^n =< L_1, L_2, \ldots, L_{n-1}, (1, 2^{n-1}+1), (2, 2^{n-1}+2), \ldots, (2^{n-1}, 2^n) > .$$

We must now prove that

$$[S_2]^n =< L_1, L_2, \ldots, L_n > . \tag{47}$$

The identity

$$L_{n-1}(2^{n-1}, 2^n) = L_n \tag{48}$$

shows that

$$< L_1, L_2, \ldots, L_n > \subset\ [S_2]^n. \tag{49}$$

It follows from (48) that

$$(2^{n-1}, 2^n) = L_{n-1}^{-1} L_n \in < L_1, L_2, \ldots, L_n > .$$

Then, observing that we may write

$$L_n^{-1} = (2^n, 2^n - 1, \ldots, 2, 1),$$

it is easily verified, in turn, for $i = 1, 2, \ldots, 2^{n-1}$, that

$$T_i = L_n T_{i-1} L_n^{-1},$$

where we define

$$T_0 = T_{2^{n-1}}.$$

Therefore,

$$T_i = (L_n)^i T_0 (L_n^{-1})^i.$$

Thus, each 2-cycle T_i belongs to $< L_1, L_2, \ldots, L_n >$, and therefore

$$[S_2]^n \subset < L_1, L_2, \ldots, L_n > . \tag{50}$$

We conclude from (49) and (50) that (47) holds. ∎

13. The Galois Group of $P_\zeta^{[n]}(y) - 1$ is the Wreath Product $[S_2]^n$ for Indeterminate ζ.

The principal result about the Galois group of $P_\zeta^{[n]}(y) - 1$ for indeterminate ζ is stated and proved in Theorem 9 below. (We change the variable x to y because x is used differently below.)

We denote by x the 2^n-tuple

$$x = (x_1, x_2, \ldots, x_{2^{n-1}}, x_{2^{n-1}+1}, \ldots, x_{2^n}),$$

where the x_j, $j = 1, 2, \ldots, 2^n$ denote the 2^n distinct roots of (7) as given by (11). We impose the labelling scheme between the integers j and the roots x_j to be such that

$$x_j + x_{2^{n-1}+j} = 2, \; j = 1, 2, \ldots, 2^{n-1}.$$

Otherwise, we leave arbitrary the explicit identification of the roots x_j with the $x_\zeta^{[n]}(\sigma)$ in (12). For the 2^n-tuple u of indeterminates u_j,

$$u = (u_1, u_2, \ldots, u_{2^{n-1}}, u_{2^{n-1}+1}, \ldots, u_{2^n}), \tag{51}$$

and the 2^n-tuple x of roots x_j, we define the symbol (u, x) by

$$(u, x) = \sum_{i=1}^{2^n} u_i x_i.$$

(We find it convenient to introduce the more explicit notation (u, x) for $\sum_{i=1}^{2^n} u_i x_i$ in place of θ used earlier in §10.)

For each

$$p = \begin{pmatrix} 1 & 2 & \ldots & 2^n \\ i_1 & i_2 & \ldots & i_{2^n} \end{pmatrix} \in S_{2^n},$$

we define the action of p on the 2^n-tuple by

$$p(u_1, u_2, \ldots, u_{2^n}) = (u_{i_1}, u_{i_2}, \ldots, u_{i_{2^n}}).$$

(The permutation p effects substitutions on the subscripts, not on the placement of the letters.) The action of p on the 2^n-tuple of roots x is similarly defined. Thus, one has the following identities:

$$(pu, x) = (u, p^{-1}x) = \sum_{i=1}^{2^n} (pu)_i x_i = \sum_{i=1}^{2^n} u_i (p^{-1}x)_i,$$

$$(pu, px) = (u, x).$$

With these notational preliminaries, we now state and prove a principal result:

Theorem 9. For indeterminate ζ, the Galois group of the polynomial $P_\zeta^{[n]}(x) - 1$ is the wreath product group $[S_2]^n$.

Proof. The proof is by induction on n. For $n = 1$, it is easy to show that the Galois group of $P_\zeta^{[1]-1}(x)$ is $S_2 = [S_2]^1$ for indeterminate ζ and also for $\zeta = 2$. We also carried the determination through manually for $n = 2$ using the polynomial $P_\zeta^{[2]}(x) - 1$. The results were that for $\zeta = 2$ the Galois group is C_4 and that for indeterminate ζ the Galois group is $[S_2]^2$ in consequence of the fact that the square root symbol $\sqrt{\ }$ is removed from the eighth degree polynomial

$$\prod_{p \in [S_2]^2} (X - (pu, x)), \tag{52}$$

and $[S_2]^2$ is the smallest group with this radical removal property. In (52), we have indeterminates $u = (u_1, u_2, u_3, u_4)$ and the root labelling given by

$$\begin{gathered} x_1 = 1 + \sqrt{1 - \frac{x_1'}{\zeta}}, \quad x_2 = 1 + \sqrt{1 - \frac{x_2'}{\zeta}}, \\ x_3 = 1 - \sqrt{1 - \frac{x_1'}{\zeta}}, \quad x_4 = 1 - \sqrt{1 - \frac{x_2'}{\zeta}}, \\ x_1' + x_2' = 2, \quad x_1' x_2' = 2/\zeta. \end{gathered} \tag{53}$$

Here x_1, x_2, x_3, x_4 are the roots of $P_\zeta^{[2]}(y) - 1$ and x_1', x_2' are the roots of $P_\zeta^{[1]}(y) - 1$. No other properties of the roots are needed to carry through the indicated calculations. Here C_4 and $[S_2]^2$ are the explicit permutation groups realized by the generators $L_1 = (1,2)(3,4)$ and $L_2 = (1,2,3,4)$:

$$C_4 =< L_2 >, \quad [S_2]^2 =< L_1, L_2 > .$$

Thus, C_4 is a subgroup of $[S_2]^2$, and the factors that clear radicals for $\zeta = 2$ are exactly those from (52) corresponding to this subgroup.

The general induction hypothesis is stated as follows: Consider the polynomial $P_\zeta^{[n-1]}(y) - 1$ and label the roots such that $x_i' + x_{2^{n-2}+i}' = 2, i = 1, 2, \ldots, 2^{n-2} (n \geq 2)$. Effect this root labelling scheme at all levels down to that given by (53). Then, the polynomial in X given by

$$\prod_{p \in [S_2]^{n-1}} (X - (pu', x')) \tag{54}$$

clears radicals by removing the symbols $\sqrt{\ }$ from all expressions when multiplied out. Moreover, $[S_2]^{n-1}$ is the smallest group that removes radicals in this manner. Here $u' = (u_1', u_2', \ldots, u_{2^{n-1}}')$ are indeterminates and

$x' = (x'_1, x'_2, \ldots, x'_{2^{n-1}})$ is a set of roots labelled as described, each of which is a function of the parameter ζ, the value of which is unspecified.

We next use from (16) the fact that the roots x_i $(i = 1, 2, \ldots, 2^n)$ of $P_\zeta^{[n]}(y) - 1$ are related to the roots x'_i $(i = 1, 2, \ldots, 2^{n-1})$ of $P_\zeta^{[n-1]}(y) - 1$ by

$$x_i = 1 + \sqrt{\alpha_i}, \quad x_{2^{n-1}+i} = 1 - \sqrt{\alpha_i}, \quad i = 1, 2, \ldots, 2^{n-1}, \tag{55}$$

where the α_i are defined by

$$\alpha_i = 1 - \frac{x'_i}{\zeta}, \; i = 1, 2, \ldots, 2^{n-1}. \tag{56}$$

Substitution of

$$x'_i = \zeta(1 - \alpha_i) \;\text{ or }\; x' = \zeta(1 - \alpha)$$

into (54) gives

$$\prod_{p \in [S_2]^{n-1}} (X - (pu', x')) = (-\zeta)^{2^{2^{n-1}}-1} \prod_{p \in [S_2]^{n-1}} (X' - (pu', \alpha)), \tag{57}$$

where

$$X' = \sum_{i=1}^{2^{n-1}} u'_i - X/\zeta.$$

In obtaining this expression for X', we have used

$$\sum_{i=1}^{2^{n-1}} (pu')_i = \sum_{i=1}^{2^{n-1}} u'_i, \text{ each } p \in [S_2]^{n-1}.$$

Thus, the induction hypothesis implies that the polynomial (in X' of degree $|[S_2]^{n-1}|$)

$$\prod_{p \in [S_2]^{n-1}} (X' - (pu', \alpha)) \tag{58}$$

clears all radicals when multiplied out, this being true for arbitrary indeterminates u' and $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{2^{n-1}})$, where each α_i is a function of ζ as given by (56).

Consider next the polynomial defined by

$$\prod_{P \in [S_2]^n} (X - (Pu, x)). \tag{59}$$

To show the relation of the polynomials (58) and (59), we use

$$[S_2]^n = [S_2]^{n-1} \wr S_2, \tag{60}$$

and the root relations $x_i + x_{2^{n-1}+i} = 2$, $i = 1, 2, \ldots, 2^{n-1}$. We obtain

$$(u, x) = \sum_{i=1}^{2^n} u_i + \sum_{i=1}^{2^{n-1}} v_i \sqrt{\alpha_i} = A + (v, \sqrt{\alpha}), \tag{61}$$

where

$$v_i = u_i - u_{2^{n-1}+i}, \quad i = 1, 2, \ldots, 2^{n-1},$$
$$A = \sum_{i=1}^{2^n} u_i. \tag{62}$$

Let us next interpret the action of the group $[S_2]^n = [S_2]^{n-1} \wr S_2$ in (59), now accounting for relation (61), using

$$P = (p, s), \quad p \in [S_2]^{n-1}, \quad s \in (S_2)^{2^{n-1}}.$$

For this, we introduce the $2 \times 2^{n-1}$ matrix U, which is written in terms of its columns by

$$U = (U_1, U_2, \ldots, U_{2^{n-1}})$$

where

$$U_i = \begin{pmatrix} v_i \\ v_{2^{n-1}} + i \end{pmatrix}, \quad i = 1, 2, \ldots, 2^{n-1}.$$

A permutation p of the columns of U yields the same permutation of $(v_1, v_2, \ldots, v_{2^{n-1}})$; that is, if

$$pU = (U_{i_1}, U_{i_2}, \ldots, U_{i_{2^{n-1}}}),$$

then

$$pv = (v_{i_1}, v_{i_2}, \ldots, v_{i_{2^{n-1}}}).$$

A permutation s_i of the two elements in a column U_i of U is the same as the operation $\sigma_i v_i$ on component v_i of v. Thus, for $P = (p, s)$, we have

$$(Pu, x) = A + ((p, \sigma)v, \sqrt{\alpha}),$$

where, by definition,

$$(p, \sigma)v = (\sigma_1 v_{p_1}, \sigma_2 v_{p_2}, \ldots, \sigma_{2^{n-1}} v_{p_{2^{n-1}}})$$

and, for $s = (s_1, s_2, \ldots, s_{2^{n-1}})$, we have $\sigma_i = 1$ for $s_i = (1)(2)$ and $\sigma_i = -1$ for $s_i = (1, 2)$. Thus, (59) may be written as

$$\prod_{P \in [S_2]^n} (X - (Pu, x)) = \prod_{\sigma \in \Sigma_{2^{n-1}}} \prod_{p \in [S_2]^{n-1}} (X'' - ((p, \sigma)v, \sqrt{\alpha}))), \tag{63}$$

where

$$X'' = X - \sum_{i=1}^{2^n} u_i.$$

Consider the factor

$$\prod_{p \in [S_2]^{n-1}} \left(X'' - ((p, \sigma)v, \sqrt{\alpha}))\right) = \prod_{p \in [S_2]^{n-1}} \left(X'' - (pv, \sigma\sqrt{\alpha})\right).$$

The right-hand side of this expression is to be compared to (58), which we now rewrite in the form (since X' and u' are indeterminates):

$$\prod_{p\in[S_2]^{n-1}}(X''-(pv,\alpha))=Y-Q(\alpha), \tag{64}$$

where

$$Y=(X'')^N,\ \ N=\left|[S_2]^{n-1}\right|,$$

$$Q(\alpha)=Q(X'',v,\alpha)=\sum_{k=1}^{N}(X'')^{N-k}(-1)^k e_k\left(y(v,\alpha)\right).$$

The e_k in this last result denote the elementary symmetric functions in $y=(y_1,y_2,\ldots,y_n)$, where the $y_i=y_i(v,\alpha)$ denote the quantities in the set

$$\left\{y_p(v,\alpha)=(pv,\alpha)\middle|p\in[S_2]^{n-1}\right\}$$

in any arbitrary order. The important application of the induction hypothesis is that the quantities $Q(\alpha)$ are polynomials in the α_i. Using (64) in (63), we obtain

$$\prod_{p\in[S_2]^n}(X-(pu,x))=\prod_{\sigma\in\Sigma_{2^n}}(Y-Q(\sigma\sqrt{\alpha})).$$

We now apply Theorem 6 to conclude that the polynomial

$$\prod_{p\in[S_2]^n}(X-(pu,x))$$

clears radicals by removal of the symbol $\sqrt{\ }$, and it is the minimal degree polynomial that does so, because $Q(\alpha)$ is not even in any α_i for indeterminate v. This completes the induction and proves that the group $[S_2]^n=G$ is the smallest group that removes the radical symbol $\sqrt{\ }$ from the polynomial

$$\prod_{g\in G}(X-(gu,x)),\ \ G\subset S_{2^n}.$$

We conclude that the wreath product group $[S_2]^n$ is the Galois group of the polynomial in Theorem 9. ■

14. Labelling of Roots and Clearing of Radicals.

The generic theory developed in §13 shows that for indeterminate ζ the Galois group of $P_\zeta^{[n]}(x) - 1$ is the wreath product permutation group

$$[S_2]^n =< L_1, L_2, \ldots, \mathrm{L}_n > .$$

We have also shown in §9 that for $\zeta = 2$, the Galois group of $P_\zeta^{[n]}(x) - 1$ is isomorphic to $C_{2^n} =< L_n >$. We also gave in Theorem 3 an explicit realization of the cyclic group for $\zeta = 2$ as a permutation group acting on the roots $t_i = \cos(2i-1)\pi/2^{n+1}$. In order to compare these $\zeta = 2$ results in §9 with the generic theory, when specialized to $\zeta = 2$, we need to use the same labelling of roots. This is carried out in this section.

The permutation group $[S_2]^n =< L_1, L_2, \ldots, L_n >$ acts on the indices of the roots $x = (x_1, x_2, \ldots, x_{2^n})$ of $P_\zeta^{[n]}(x) - 1$ labelled such that

$$x_i + x_{2^{n-1}+i} = 2, \ i = 1, 2, \ldots, 2^{n-1}, \tag{65}$$

but otherwise the labelling of the roots is arbitrary. This is because the group $[S_2]^n$ removes the symbol $\sqrt{\ }$ from the polynomial

$$\prod_{p \in [S_2]^n} (X - (u, px)) = \prod_{p \in [S_2]^n} (X - (pu, x)), \tag{66}$$

when multiplied out.

The other way, of course, to remove a radical is for the quantity under $\sqrt{\ }$ to be a perfect square: $\sqrt{y^2} = y$. It is the second way in which radicals are cleared for the $\zeta = 2$ theory, where the analyses carried out in §8-9 show that the polynomial

$$\prod_{p \in <s>} (X - (u', px')) = \prod_{p \in <s>} (X - (pu', x')) \tag{67}$$

not only clears radicals, but is also irreducible. In this expression

$$u' = (u'_1, u'_2, \ldots, u'_{2^n})$$

denotes any set of indeterminates. The cyclic group in (67) is realized as the permutation group

$$C'_{2^n} =< s > . \tag{68}$$

where $s = (s_1, s_2, \ldots, s_{2^n})$ is the 2^n-cycle defined in (71) below.

Consider next the form that (66) takes under the relabelling of roots given by $x' = mx$, where $m \in S_{2^n}$ is an arbitrary permutation. Because the indeterminates u' can be relabelled in any way whatsoever in that relation, we can take $u' = mu$ without loss of generality. We obtain

$$\prod_{p \in <s>} (X - (pu', x')) = \prod_{p' \in <s'>} (X - (p'u, x)), \tag{69}$$

where

$$s' = m^{-1}sm.$$

We next consider the detailed relationship between the $\zeta = 2$ results in §7 to §9 and the indeterminate ζ results in §13. The permutation $s = (s_1, s_2, \ldots, s_{2^n})$, which is the generator of the cyclic group C'_{2^n} in (68), is obtained explicitly by the following procedure as described in §9. We determine the integers d_k and r_k in the relation

$$\frac{3^k + 1}{2} = d_k 2^n + r_k, \quad 1 \leq r_k \leq 2^n - 1, \quad k = 0, 1, 2, \ldots. \tag{70}$$

Then, in consequence of Lemma 1, the infinite sequence of integers

$$(r_0, r_1, r_2, \ldots)$$

is periodic in the 2^{n-1} distinct integers $(r_0, r_1, r_2, \ldots, r_{2^{n-1}-1})$.

The entries s_{k+1} in the 2^n-cycle $s = (s_1, s_2, \ldots, s_{2^n})$ are then defined by

$$s_{k+1} = \begin{cases} r_k, & \text{if } d_k \text{ is even;} \\ 2^n + 1 - r_k, & \text{if } d_k \text{ is odd.} \end{cases} \quad k = 0, 1, 2, \ldots, 2^n - 1 \tag{71}$$

In consequence of the periodicity property of the r_k, it also follows that the infinite sequence of integers

$$(s_1, s_2, \ldots) \text{ is periodic in } (s_1, s_2, \ldots, s_{2^n}), \tag{72}$$

where the s_i are distinct and a rearrangement of $1, 2, \ldots, 2^n$. We use this property below in establishing relation (80).

The permutation group C'_{2^n} acts on the roots $x' = (x'_1, x'_2, \ldots, x'_{2^n})$ in (67), which are related to the roots in (65) in the following way: We first have

$$x'_j = 1 + t_j, \quad j = 1, 2, \ldots, 2^n, \tag{73}$$

where

$$t_i = \cos\left[\frac{(2i-1)\pi}{2^{n+1}}\right], \quad i = 1, 2, \ldots, 2^{n-1}, \tag{74}$$

$$t_{2^n - i + 1} = -\cos\left[\frac{(2i-1)\pi}{2^{n+1}}\right], \quad i = 1, 2, \ldots, 2^{n-1}. \tag{75}$$

A set of roots satisfying relation (65) is given by

$$x_i = x'_{2i-1}, \quad x_{2^{n-1}+i} = x'_{2^n - 2i + 2}, \quad i = 1, 2, \ldots, 2^{n-1}, \tag{76}$$

because

$$x'_{2i-1} + x'_{2^n - 2i + 2} = 2.$$

The roots $(x_1, x_2, \ldots, x_{2^n})$ are the real parts, respectively, of the complex points, labelled counterclockwise in order, and separated by equal angles of $\pi/2^{n-1}$ with z_1 at positive angle $\pi/2^{n+1}$:

$$x_j = \mathrm{Re}\ z_j = \mathrm{Re}\ e^{i(4j-1)\pi/2^{n+1}}, \quad j = 1, 2, \ldots, 2^n. \tag{77}$$

(We give below a geometric interpretation of the action of the cycle permutation $s = (s_1, s_2, \ldots, s_{2^n})$ on the roots $t = (t_1, t_2, \ldots, t_{2^n})$ defined in (74) and (75)).

It follows from the relations (76) that the 2^n-cycle $p = (p_1, p_2, \ldots, p_{2^n})$, which acts on the roots x, is obtained from $s = (s_1, s_2, \ldots, s_{2^n})$, which acts on the roots t, by the following rule

$$s_k \to p_k = \begin{cases} \frac{s_k+1}{2}, & \text{if } s_k \text{ is odd}, \\ 2^n + 1 - \frac{s_k}{2}, & \text{if } s_k \text{ is even}, \end{cases} \quad k = 0, 1, 2, \ldots, 2^n - 1.$$

Using this result and (71), we obtain the following relations for the entries in the 2^n-cycle $p = (p_1, p_2, \ldots, p_{2^n})$:

$$p_{k+1} = \begin{cases} \frac{r_k+1}{2}, & d_k \text{ even}, r_k \text{ odd}; \\ 2^{n-1} + \frac{r_k+1}{2}, & d_k \text{ odd}, r_k \text{ odd}; \\ 2^n + 1 - \frac{r_k}{2}, & d_k \text{ even}, r_k \text{ even}; \\ 2^{n-1} + 1 - \frac{r_k}{2}, & d_k \text{ odd}, r_k \text{ even}; \end{cases} \quad k = 0, 1, 2, \ldots, 2^n - 1. \tag{78}$$

This is a complete description of the cycle permutation p, which acts on the roots x, in terms of the divisors d_k and remainders r_k in (70). It is a significant result for this work.

Relations (73) and (76) define a unique permutation $m \in S_{2^n}$ such that $x' = mx$ and, correspondingly $p = m^{-1}sm$, but we do not require m explicitly. Instead, we show below how to utilize (78) directly to show that $p \in [S_2]^n$. This result then implies that there exists a $q \in [S_2]^n$ such that $p = qL_nq^{-1}$, because p and L_n have the same cycle structure. It then follows that $s = (mq)L_n(mq)^{-1}$, and from this that $s' = qL_nq^{-1}$, which appears in (69), so that the group $< s' >$ in (69) is given by

$$< s' > = < L_n > = C_{2^n}.$$

Thus, the proof of Theorem 10 below is a direct consequence of the proof that permutation p defined by (78) is an element of $[S_n]^n$.

Using (78), we now show that p belongs to the wreath product permutation group $[S_2]^n$. For this, we establish a remarkably simple rule for constructing the permutation $P \in [S_2]^{n+1}$ directly from the permutation $p \in [S_2]^n$ defined by (78). (In making this statement, we anticipate that these permutations, in fact, belong to the respective wreath product groups, as proved below.)

We construct the permutation P by exactly the rule (78) now applied to 2^{n+1}. Thus, we define the divisors D_k and remainders R_k by

$$\frac{3^k + 1}{2} = D_k 2^{n+1} + R_k, \quad 1 \le R_k \le 2^{n+1} - 1, \quad k = 0, 1, 2, \ldots. \tag{79}$$

The formula for P_{k+1} in $P = (P_1, P_2, \ldots, P_{2^{n+1}})$ is now obtained simply by replacing n by $n+1$ and all lower case letters by upper case letters in (78), excepting k which is a running index. By using the relations

$$d_k = 2D_k, \quad R_k = r_k, \quad 0 \le k \le 2^n - 1,$$
$$d_k = 2D_k + 1, \quad R_k = 2^n + r_k, \quad 2^n \le k \le 2^{n+1} - 1,$$

we can express the relations for the P_{k+1} in terms of p_{k+1}. This calculation is a bit tedious, but straightforward, and gives the following simple result:

$$P_{k+1} = \begin{cases} p_{k+1}, & \text{if } r_k \text{ and } D_k \text{ have same parity,} \\ p_{k+1} + 2^n, & \text{if } r_k \text{ and } D_k \text{ have opposite parity.} \end{cases} \tag{80}$$

These relations are valid for all $k = 0, 1, 2, \ldots$, when one accounts for the periodicity property (72). This is the key result for proving the following theorem.

Theorem 10 . The cyclic permutation group $< s' >$ in (69) is a subgroup of the wreath product permutation group $[S_2]^n =< L_1, L_2, \ldots, L_n >$ in consequence of $< s' >=< L_n >$.

Proof. We need to prove that $p \in [S_2]^n$. The proof is by induction on n, using relation (80). We assume that

$$p = (p_1, p_2, \ldots, p_{2^n}) \in [S_2]^n,$$

where p is defined by (78), and where we note that for $n = 1$ and $n = 2$ the result is true; that is,

$$(1,2) \in S_2 = [S_2]^1, \quad (1,4,3,2) \in [S_2]^2 =< (1,2)(3,4), (1,2,3,4) > .$$

The unique extension of p to its corresponding element in $[S_2]^{n+1}$ is given by

$$p = (p_1, p_2, \ldots, p_{2^n}) \rightarrow p' = (p_1, p_2, \ldots, p_{2^n}, p_1{+}2^n, p_2{+}2^n, \ldots, p_{2^n}{+}2)^n \in [S_2]^{n+1}.$$

We next prove that P is conjugate to p' by an element in $[S_2]^{n+1}$. Indeed, the element in question is the product of 2-cycles given by

$$T_{k+1} = (p_{k+1}, p_{k+1} + 2^n), \text{ if } r_k \text{ and } D_k \text{ have the same parity.} \tag{81}$$

Thus,

$$T = \prod_k T_{k+1},$$

where the product is over all T_{k+1} defined by condition (81). The permutation T is thus a product of certain of the 2-cycles (for n replaced by $n+1$) defined by (46) in §12, each of which is an element of $[S_2]^{n+1}$. We have the identity

$$P = T^{-1} p' T.$$

The proof of this last relation follows immediately when one recognizes that it is precisely the interchanges of integers given by (81) that converts p' into P. ■

It is useful to observe that the 2^n-cycle s defined by (71), and corresponding to the automorphism of the splitting field L generated by (30) is not a rotation by $\pi/2^{n-1}$ of the unit circle containing the complex root representatives z_j defined in (77). Instead, this permutation corresponds to rotations of these roots onto themselves in groups of 4 that can be described in terms of "colored" roots. In terms of z_j, these 4-tuples of root representatives are given by

$$(z_{3\cdot 2^{n-2}+i+1}, z_{2\cdot 2^{n-2}+i+1}, z_{1\cdot 2^{n-2}+i+1}, z_{i+1},), \quad i = 1, 2, \ldots, 2^{n-2},$$

where for $i = 2^{n-2}$ the first representative satisfies $z_{2^n+1} = z_1$. In terms of complex points w_i with $t_i = \mathrm{Re}\, w_i$, these same 4-tuples of root representatives on the unit circle are given by

$$\begin{gathered}(w_1, w_{2^{n-1}}, w_{2^n}, w_{2^{n-1}+1}),\\ (w_{2i}, w_{2^{n-1}+2i}, w_{2^n-2i+1}, w_{2^{n-1}-2i+1}), \quad i = 1, 2, \ldots, 2^n - 1. \end{gathered} \tag{82}$$

These sets of 4-tuples are to be rotated independently of one another in accordance with the following rules. We describe the situation in terms of the complex points w_i corresponding to the roots t_i. We use the color c_1 to mark the first four points in the first 4-tuple in (82), the color c_2 to mark the second 4-tuple ($i = 1$), the color c_3 to mark the next 4-tuple ($i = 2$), and so on. The color $c_{2^{n-2}}$ will mark the last 4-tuple. We now rotate clockwise and separately these colored 4-tuples by the indicated angles, where $\phi = \pi/2^{n-1}$ denotes the basic angle between adjacent roots:

$$\begin{gathered}\text{color } c_1 \text{ by } (2^n + 1)\phi \equiv \phi\\ \text{color } c_2 \text{ by } (2^n - 3)\phi\\ \vdots\\ \text{color } c_i \text{ by } (2^n - 4i + 5)\phi\\ \vdots\\ \text{color } c_{2^{n-2}} \text{ by } 5\phi\end{gathered}$$

With some work, it may be shown that the resulting permutation of the roots w_i, or equivalently, of the t_i is exactly that given by the cyclic permutation s defined by (71).

It is of use to inquire just how the fourth degree polynomial (69) for $n = 2$ clears radicals for $\zeta = 2$, while for $\zeta \neq 2$, it requires the eighth degree polynomial (66) with $n = 2$ to remove the radical symbol $\sqrt{\ }$. One can do this by the direct procedure of multiplying out (66) with $n = 2$ for general ζ. One encounters a single factor that retains the radical:

$$\sqrt{\zeta^2 - \zeta - 1}. \tag{83}$$

Thus, radicals are not cleared for generic ζ, but remarkably for $\zeta = 2$ the radical (83) is 1. One can show that for no positive integer ζ other than 2 is (83) an integer.

One can carry out this type of detailed analysis forward to, say, $n = 3$. We now have an eighth degree polynomial to consider for C_8, but the full polynomial for $[S_2]^3$ is of degree $2^{2^3-1} = 128$. One encounters again the radical (83) and the additional one:

$$\sqrt{\zeta^6 - 3\zeta^5 + \zeta^4 + 3\zeta^3 - \zeta^2 - \zeta - 1}, \tag{84}$$

which again is 1 for $\zeta = 2$. Calculation shows that for no other ζ, $1 \leq \zeta \leq 500$, is (84) an integer. Determining if there are any positive integer solutions other than $\zeta = 2$, $w = 1$ to the Diophantine equation $\zeta^6 - 3\zeta^5 + \zeta^4 + 3\zeta^3 - \zeta^2 - \zeta - 1 = w^2$ may be a readily solvable problem with some help from the computer.

15. Galois Group Calculations on MAPLE.

Use was made of the symbolic computer program MAPLE to verify that for $n \leq 5$ the groups generated by the generators in §13 have order 2^{2^n-1}. Note that $2^{31} = 2147483648$. MAPLE had no difficulty calculating such a large order.

Acknowledgements

We thank Dr. N. Metropolis for his interest in the developments of the material of this paper.

We thank Drs. W. Y. C. Chen, D. J. H. Garling, Susan Landau, John McKay, and Michael Singer for advice in this research.

We wish to acknowledge especially the contributions to this work of Professor R. W. K. Odoni with whom we communicated in 1992 concerning the approaches and problems addressed here. Using more abstract methods than we had planned, he sketched proofs confirming our preliminary results giving C_{2^n} and $[S_2]^n$ as the relevant Galois groups in question. Our methods, using concrete groups and the van der Waerden algorithm, are quite different from Odoni's. We thank him for his interest and communications.

References

Bailey, David H., Algorithm 716: Multiprecision translation and execution of Fortran programs, *ACM Trans. Math. Software*, **19**, 288 - 319, 1993.

Beyer, W. A., R. D. Mauldin, and P. R. Stein, Shift-maximal sequences in function iteration: existence, uniqueness, and multiplicity, *J. Math. Anal. Appl.*, **112**, 305 - 362, 1986.

Beyer, W. A. and L. Heller, A Steiner tree associated with three quarks, *J. Symb. Comput.*, **3**, 283 - 289, 1987.

Beyer, W. A., and P. R. Stein, Period doubling for trapezoid function iteration: metric theory, *Adv. in Appl. Math.*, **3**, 1 - 17, 1982.

Bivins, R. L., J. D. Louck, N. Metropolis, and M. L. Stein, Classification of all cycles of the parabolic map, *Phys. D*, **51**, 3 - 27, 1991.

Brucks, K. M., Hausdorff dimension and measure of basin boundaries, *Adv. in Math.*, **78**, 168 - 191, 1989.

Bruen, Aiden A., Christian U. Jensen, and Noriko Yui, *Polynomials with Frobenius groups of prime degree as galois groups*, C. R. Math. Rep. Acad. Sci. Canada, **7**, 171 - 175, 1985.

Bruen, Aiden A., Christian U. Jensen, and Noriko Yui, *Polynomials with Frobenius groups of prime degree as galois groups II*, J. Number Theory, **24**, 305 - 359, 1986.

Cremona, J. E., On the Galois groups of the iterates of x^2+1, *Mathematika*, **36**, 259 - 261, 1989.

Dehn, E., *Algebraic Equations*, Dover Publications, Inc. reprint, 1960.

Dickson, L. E., *Modern Algebraic Theories*, Benj. H. Sanborn & Co., 1930.

Feigenbaum, M. J., Quantitative universality for a class of nonlinear transformations, *J. Stat. Phys.* **19**, 25 - 52, 1978, **21** 669 - 706, 1979.

Garling, D. J. H., *A Course in Galois Theory*, Cambridge University Press, 1988.

Grosswald, Emil, *Bessel Polynomials*, Springer-Verlag, Lecture Notes in Mathematics, #698, chapter 12, 1978.

Harary, Frank and E. M. Palmer, *Graphical Enumeration*, Academic Press, 1973.

Hille, Einar, *Analytic Function Theory, Volume II*, page 104, Ginn and Company, New York, 1962.

Jacobson, N., *Lectures in Abstract Algebra, Vol III Theory of Fields and Galois Theory*, D. Van Nostrand Co., Inc., 1964.

Knuth, D. E., The Art of Computer Programming, Vol. 2, Second Edition, Addison-Wesley Publishing Company, 1981.

Lanford, Oscar, A computer-assisted proof of the Feigenbaum conjectures, *Bull. Amer. Math. Soc.*, N. S., **6**, pp. 427 - 434, 1982.

May, Robert M., Simple mathematical models with very complicated dynamics, *Nature*, **261**, pp. 459 - 467, 1976.

Metropolis, N., M. C. Stein, and P. R. Stein, On finite limit sets for transformations of the unit interval, *J. Combinatorial Theory*, **15**, 25 - 44, 1973.

Morton, Patrick, Arithmetic properties of quadratic maps, *Acta Arith.* **62**, 343 - 372, 1992.

Morton, Patrick and Pratiksha Patel, The Galois Theory of periodic points of polynomial maps, Submitted to *Math. Comp.*, 1992

Nicolas, J.-L., Correspondence with the authors, 1992.

Odoni, R. W. K., The Galois theory of iterates and composites of polynomials, *Proc. London Math. Soc.*, **51**, 385 - 414, 1985.

Odoni, R. W. K., Realising wreath products of cyclic groups as Galois groups, *Mathematika*, **35**, 101 - 113, 1988.

Odoni, R. W. K., Correspondence with the authors, 1992.

Oldham, Keith B., and Jerome Spanier, *An Atlas of Functions*, Hemisphere Publishing Corporation, 1987.

Silverman, R. D., A perspective on computational number theory, *Notices Amer. Math. Soc.*, **38**, 562-568, 1991.

Stein, P. R. and C. Zemach, On the rationalization of a sum of surds, *Adv. in Appl. Math.*, **8**, 393 - 404, 1987.

Stewart, I, *Galois Theory*, Second Edition, Chapman & Hall, London, 1989.

Stoll, Michael, Galois groups over $\mathbb{Q}$ of some iterated polynomials, *Arch. Math.*, **59**, 1992, 239 - 244, 1992.

van der Waerden, B. L., *Algebra, Volume 1*, Translation of the Seventh German Edition, Frederick Ungar Publishing Company, New York, §8.10, 1970.

Vivaldi, Franco and Spyros Hatjispyros, Galois theory of periodic orbits of rational maps, *Nonlinearity*, **5**, 1992, 961 - 978, 1992.

Wang, Li, Corrections for Two Papers by W. A. Beyer and P. R. Stein, *Adv. in Appl. Math.*, **8**, pp. 108 - 110, 1987.

Appendix A

Galois Groups in the van der Waerden Algorithm.

In this appendix we show that the set A_1 in Garling (1988, p. 156) is the Galois group of the equation under consideration there; i.e. $A_1 = G$. In our notation, this equation is written

$$F(y,u,x) = \prod_{p \in S_n} (y - (pu,x)) = \prod_{i=1}^{r} F_i(y,u,x),$$

where the polynomial F_i is defined by

$$F_i(y,u,x) = \prod_{a_i \in A_i} (y - (a_i u,x)).$$

The sets $A_1, A_2, \ldots, A_r$ are a partition of S_n and A_1 is chosen to contain the identity permutation, but no other properties of the A_i are stated explicitly by Garling. It is then proved by Garling (1988, p. 157) that the group G of all permutations g such that

$$F_1(y,gu,x) = F_1(y,u,x) \tag{85}$$

is the Galois group of the given equation. We show that $A_1 = G$, and, hence, also that the A_i $i = 1,2,\ldots,r$, are cosets Gk_i of G in S_n. First, we observe from (85) that

$$A_1 g = A_1, \ \forall g \in G;$$

that is, $a_1 g \in A_1, \ \forall a_1 \in A_1, \ \forall g \in G$. Because A_1 contains the identity, it contains each $g \in G$; i. e. $A_1 \supset G$. Because Garling shows (1988, p. 157) that G is the Galois group, his polynomial H (top of p.157) may be written

$$H(y,u,x) = \prod_{g \in G} (y - (u,gx)) = \prod_{g \in G} (y - (gu,x)).$$

Garling shows that H is a product of the polynomials F_i defined above containing at least F_1. We conclude from this that $A_1 \subset G$, and therefore, $A_1 = G$, because we have shown above that $A_1 \supset G$. ∎

Appendix B

Odoni's Theorem.

In this appendix we quote a lemma and a theorem from Odoni (1985) that give evidence, but not a proof, that the Galois group of $P_\zeta^{[n]}(x) - 1$ is a subgroup of $[S_2]^n$. The following is Lemma 4.1 of Odoni (1985). It is assumed that K is a field and that $f(X), g(X) \in K[X]$ are monic polynomials of positive degree.

Lemma (Odoni). Let $f(g(x))$ be separable (distinct roots) over K, and let deg $f = k$, deg $g = l$, with $k, l \geq 1$. Then $f(X)$ is also separable over K. Let $\mathcal{F}$ be Gal$f(X)/K$, identified with a subgroup of the permutations of its zeros in the usual way. Then there is an injective homomorphism of Gal$f(g(X))/K$ into $\mathcal{F}[S_l]$.

Theorem (Odoni). Let F be any field of characteristic 0, let $k \geq 2$, and let $\mathcal{F}(X)$ be the generic monic of degree k over F. Then every iterate $\mathcal{F}_n(X)$ is irreducible over K (the extension of F generated by the coefficients of $\mathcal{F}$), and, for every $n \geq 1$, Gal$\mathcal{F}_n(X)/K \doteq [S_k]^n$.

Identity $\mathcal{F}$ with P_ζ. Assume (falsely) that $\mathcal{F}$ is monic. Identify $f(X)$ with $P_\zeta(X) - 1$ and $g(X)$ with $P_\zeta^{[n-1]}$. Assume (again falsely) f and g are monic. It would then follow from the Theorem of Odoni that the Galois group of $P_\zeta^{[n]}(x) - 1$ is $[S_2]^n$.

Let us define the monic polynomial $Q_\zeta^{(n)}(x)$ by

$$Q_\zeta^{(n)}(x) = \left(1 - P_\zeta^{[n]}(x)\right) \Big/ \zeta^{2^n - 1}.$$

Then, it follows from this definition that

$$Q_\zeta^{(n+1)}(x) = Q_\zeta^{(n)}\left(P_\zeta(x)\right) \Big/ \zeta^{2^n};$$

that is,

$$Q_\zeta^{(n+1)}(x) = \zeta^{-2^n} \left(Q_\zeta^{(n)} \circ P_\zeta\right)(x), \tag{86}$$

where P_ζ is the nonmonic quadratic polynomial defined by (2). Because we have proved that the Galois group of $Q_\zeta^{(n)}$ is the wreath product group $[S_2]^n$ for arbitrary n, it follows that the Galois group of (86) is

$$[S_2]^{n+1} = [S_2]^n \wr S_2.$$

Because the Galois group of P_ζ is S_2, we find that the Galois group of the composition of the two functions in (86) is the wreath product of the respective Galois groups. Thus, the conclusion of Odoni's theorem holds for the case at hand despite the fact that the right-hand side of (86) entails the composition of nonmonic polynomials. Odoni (1992) has conjectured that this would be the case for generic ζ. Notice that the result fails to be true for $\zeta = 2$, despite the fact that we can write

$$T_{2^n} = T_{2^{n-1}} \circ T_2.$$

Appendix C.

Calculation of Bifurcation Values

Let $f_r(x) := rx(1-x)$ and let $f_r^{[n]}(x)$ be the nth iterate of $f_r(x)$. The third bifurcation point is the smallest value of r, say r_3, such that with some x the pair:

$$f_r^{[n]}(x) = x \tag{87}$$

$$\frac{df_r^{[n]}(x)}{dx} = 1 \tag{88}$$

of simultaneous equations are satisfied for $n = 3$ and for no smaller n. Nicolas (1992) noted that this problem could be solved by eliminating the variable x between (87) and (88) by using the RESULTANT function in either MACSYMA or MAPLE. (For reasons not clear, Bailey (1993) and Nicolas (1992) used -1 in place of 1 on the right-hand side of (88)).

Table I shows the form of

$$\mathrm{Res}_n(r) \equiv \mathrm{RESULTANT}(f_r^{[n]}(x) - x, \frac{df_r^{[n]}(x)}{dx} - 1, x)$$

for $n = 1, 2, 3$. In each case $\mathrm{Res}_n(r)$ is a power of r times a polynomial $P_k(r)$ of degree k in r with a nonzero constant term. The factor of the bifurcation polynomial $P_k(r)$ that yields the bifurcation value is also given in Table I.

$\underline{n}$	$\underline{\mathrm{Res}_n}$	Factor	BifurcationValue
1	$r\,P_2(r)$	$r-1$	1
2	$r^9 P_8(r)$	$r-3$	3
3	$r^{225} P_{54}(r)$	r^2-2r-5	$3.449...= 1+\sqrt{6}$
4	?	?	?

Table 1. Bifurcation points for the quadratic mapping.

Note that although the third bifurcation value might have been a root of a polynomial of minimal degree 54, it actually is a root of a quadratic polynomial, which is a surprise. What happens for higher values of n? Could Galois theory provide some insight?

e-mail address: beyer@lanl.gov