QUADRATIC MAP ITERATES AND GALOIS GROUPS

W.A. BEYER and J.D. LOUCK
Theoretical Division, Los Alamos National Laboratory
Los Alamos, NM 87545, U.S.A.

In this note we present the results of a theory of Galois groups associated with iterates of a one parameter family of quadratic maps of the real line into itself. The details appear in *Ulam Quarterly*, Beyer and Louck [2]. This journal is a new electronic journal, not yet widely distributed. It was thought useful to announce the results of that paper in the Proceedings of this Conference.

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 [3] and May [9]. 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 [10]) sequences, kneading sequences, and lexical sequences. Metric aspects of function iteration include geometric (Feigenbaum [7] and Lanford [8]) and quadratic (Beyer and Stein [4] and Wang [14]) convergence in period doubling, and Hausdorff dimension of sets arising in function iteration (Brucks [6]).

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 [1]. See also Silverman, p. 565 [12].

The principal contribution of this paper to the Galois theory of polynomials is the application of an old algorithm for finding Galois groups of polynomials, an algorithm generally dismissed as having no practical value. This algorithm is given in van der

Waerden [13]. We apply this algorithm to finding Galois groups of polynomials arising in the iteration problem discussed below.

Let us recall the definition of the Galois group of a polynomial. 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: $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$, $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$, and $\phi(\mathbf{1}_R) = \mathbf{1}_S$, 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 $\Gamma(L : K) = \{\sigma \in \text{Aut } L \mid \sigma(k) = k, \ \forall\, k \in K\}$, 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.

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. The association of the polynomials used here and the quadratic maps are given in Bivins, Louck, Stein, and Metropolis [5].

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 one case and ζ an indeterminate in the other 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.

Some of the results in this work were obtained by different methods by Odoni [11].

References

[1] D.H. Bailey, Algorithm 716: Multiprecision translation and execution of Fortran programs, *ACM Trans. Math. Software* **19** (1993) 288–319.

[2] W.A. Beyer and J.D. Louck, Galois groups for polynomials related to quadratic map iterates, *Ulam Quarterly* **2** (1994) No. 3.

[3] W.A. Beyer, R.D. Mauldin and P.R. Stein, Shift-maximal sequences in function iteration: existence, uniqueness, and multiplicity, *J. Math. Anal. Appl.* **112** (1986), 305–362.
[4] W.A. Beyer and P.R. Stein, Period doubling for trapezoid function iteration: metric theory, *Adv. in Appl. Math.* **3** (1982), 1–17.
[5] R.L. Bivins, J.D. Louck, N. Metropolis and M.L. Stein, Classification of all cycles of the parabolic map, *Phys. D* **51** (1991), 3–27.
[6] K.M. Brucks, Hausdorff dimension and measure of basin boundaries, *Adv. in Math.* **78** (1989), 168–191.
[7] M.J. Feigenbaum, Quantitative universality for a class of nonlinear transformations, *J. Stat. Phys.* **19** (1978), 25–52, **21** (1979), 669–706.
[8] O. Lanford, A computer-assisted proof of the Feigenbaum conjectures, *Bull. Amer. Math. Soc.*, *N.S.* **6** (1982), 427–434.
[9] R.M. May, Simple mathematical models with very complicated dynamics, *Nature* **261** (1976), 459–467.
[10] N. Metropolis, M.C. Stein and P.R. Stein, On finite limit sets for transformations of the unit interval, *J. Combinatorial Theory* **15** (1973), 25–44.
[11] R.W.K. Odoni, Correspondence with the authors, 1992.
[12] R.D. Silverman, A perspective on computational number theory, *Notices Amer. Math. Soc.* **38** (1991), 562–568.
[13] B.L. van der Waerden, *Algebra, Vol. 1*, Translation of the Seventh German Edition, Frederick Ungar Publishing Company, New York, 1970, §8.10.
[14] Li Wang, Corrections for two papers by W.A. Beyer and P.R. Stein, *Adv. in Appl. Math.* **8** (1987), 108–110.